



# **Network Camera**

## **User Manual**

UD12038B-A

# Initiatives on the Use of Video Products

## **Thank you for choosing Hikvision products.**

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

## **Please read the following initiatives carefully:**

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

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

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

## **User Manual**

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 Network 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.

**Notice:**

If camera fails to synchronize local time with that of the network, you need to set up camera time manually. Visit the camera and enter system setting interface for time setting.



**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.

	
<b>Warnings</b> Follow these safeguards to prevent serious injury or death.	<b>Cautions</b> Follow these precautions to prevent potential injury or material damage.



**Warnings:**

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



**Cautions:**

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (refer to product specification for working temperature), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, ensure there is good ventilation to the device.
- Keep the camera away from water and any liquids.
- While shipping, pack the camera in its original, or equivalent, packing materials. Or packing the same texture.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

**Notes:**

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

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

body so that the foam ring and the dome cover are attached seamlessly.



## Table of Contents

<b>Chapter 1</b>	<b>System Requirement</b>	<b>11</b>
<b>Chapter 2</b>	<b>Network Connection</b>	<b>12</b>
<b>2.1</b>	<b>Setting the Network Camera over the LAN</b>	<b>12</b>
2.1.1	Wiring over the LAN	12
2.1.2	Activating the Camera	13
2.1.3	(Optional) Setting Security Question	20
<b>2.2</b>	<b>Setting the Network Camera over the WAN</b>	<b>20</b>
2.2.1	Static IP Connection	20
2.2.2	Dynamic IP Connection	21
<b>Chapter 3</b>	<b>Access to the Network Camera</b>	<b>24</b>
<b>3.1</b>	<b>Accessing by Web Browsers</b>	<b>24</b>
<b>3.2</b>	<b>Accessing by Client Software</b>	<b>25</b>
<b>Chapter 4</b>	<b>Live View</b>	<b>27</b>
<b>4.1</b>	<b>Live View Page</b>	<b>27</b>
<b>4.2</b>	<b>Starting Live View</b>	<b>28</b>
<b>4.3</b>	<b>Recording and Capturing Pictures Manually</b>	<b>29</b>
<b>4.4</b>	<b>Operating PTZ Control</b>	<b>29</b>
4.4.1	PTZ Control Panel	29
4.4.2	Setting/Calling a Preset	31
4.4.3	Setting/Calling a Patrol	32
<b>Chapter 5</b>	<b>Network Camera Configuration</b>	<b>33</b>
<b>5.1</b>	<b>Configuring Local Parameters</b>	<b>33</b>
<b>5.2</b>	<b>Configure System Settings</b>	<b>35</b>
5.2.1	Configuring Basic Information	35
5.2.2	Configuring Time Settings	36
5.2.3	Configuring RS232 Settings	38
5.2.4	Configuring RS485 Settings	39
5.2.5	Configuring DST Settings	40
5.2.6	Configuring Image Stitching	41
5.2.7	Open Source Software License	43
<b>5.3</b>	<b>Maintenance</b>	<b>43</b>
5.3.1	Upgrade & Maintenance	43
5.3.2	Log	44
5.3.3	System Service	46
<b>5.4</b>	<b>Security Settings</b>	<b>46</b>

5.4.1	Authentication .....	46
5.4.2	IP Address Filter .....	47
5.4.3	Security Service.....	48
<b>5.5</b>	<b>User Management .....</b>	<b>49</b>
5.5.1	User Management .....	49
5.5.2	Security Question .....	51
5.5.3	Online Users.....	52
<b>Chapter 6</b>	<b><i>Network Settings .....</i></b>	<b>53</b>
<b>6.1</b>	<b>Configuring Basic Settings .....</b>	<b>53</b>
6.1.1	Configuring TCP/IP Settings .....	53
6.1.2	Configuring DDNS Settings.....	55
6.1.3	Configuring PPPoE Settings.....	57
6.1.4	Configuring Port Settings .....	57
6.1.5	Configure NAT (Network Address Translation) Settings.....	59
<b>6.2</b>	<b>Configure Advanced Settings .....</b>	<b>60</b>
6.2.1	Configuring SNMP Settings .....	60
6.2.2	Configuring FTP Settings .....	63
6.2.3	Configuring Email Settings .....	65
6.2.4	HTTPS Settings .....	67
6.2.5	Configuring QoS Settings .....	70
6.2.6	Configuring 802.1X Settings.....	71
6.2.7	Integration Protocol.....	72
<b>Chapter 7</b>	<b><i>Video/Audio Settings .....</i></b>	<b>74</b>
<b>7.1</b>	<b>Configuring Video Settings .....</b>	<b>74</b>
<b>7.2</b>	<b>Configuring Audio Settings .....</b>	<b>77</b>
<b>Chapter 8</b>	<b><i>Image Settings .....</i></b>	<b>79</b>
<b>8.1</b>	<b>Configuring Display Settings .....</b>	<b>79</b>
<b>8.2</b>	<b>Configuring OSD Settings.....</b>	<b>83</b>
<b>8.3</b>	<b>Configuring Picture Overlay .....</b>	<b>85</b>
<b>Chapter 9</b>	<b><i>Event Settings .....</i></b>	<b>86</b>
<b>9.1</b>	<b>Basic Events .....</b>	<b>86</b>
9.1.1	Configuring Alarm Input .....	86
9.1.2	Configuring Alarm Output .....	89
9.1.3	Handling Exception .....	90
<b>Chapter 10</b>	<b><i>Storage Settings.....</i></b>	<b>92</b>
<b>10.1</b>	<b>Configuring Record Schedule .....</b>	<b>92</b>
<b>10.2</b>	<b>Configure Capture Schedule .....</b>	<b>95</b>
<b>10.3</b>	<b>Configuring Net HDD .....</b>	<b>97</b>

<b>Chapter 11</b>	<b>Playback.....</b>	<b>100</b>
<b>Chapter 12</b>	<b>Picture .....</b>	<b>102</b>
<b>Appendix</b>	<b>.....</b>	<b>104</b>
<b>Appendix 1</b>	<b>SADP Software Introduction .....</b>	<b>104</b>
<b>Appendix 2</b>	<b>Port Mapping .....</b>	<b>107</b>

# Chapter 1 System Requirement

## Operating System

Microsoft Windows XP and above version

Mac OS X 10.8 and above version

## CPU

3.0 GHz or higher

## RAM

1G or higher

## Display

1024×768 resolution or higher

## Web Browser

Internet Explorer 8.0 and above version, Mozilla Firefox 30.0-51, Google Chrome 31.0-44 and Apple Safari 8.0 -11.0

### *Note:*

For Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version which are plug-in free, **Picture** and **Playback** functions are hidden.

To use mentioned functions via web browser, change to their lower version, or change to Internet Explorer 8.0 and above version.

## Chapter 2 Network Connection

### **Note:**

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

### **Before you start:**

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

## 2.1 Setting the Network Camera over the LAN

### **Purpose:**

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

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

### 2.1.1 Wiring over the LAN

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

### **Purpose:**

- To test the network camera, you can directly connect the network camera to the

computer with a network cable as shown in Figure 2-1.

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

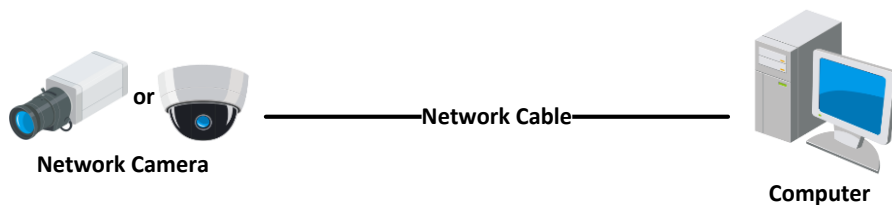


Figure 2-1 Connecting Directly

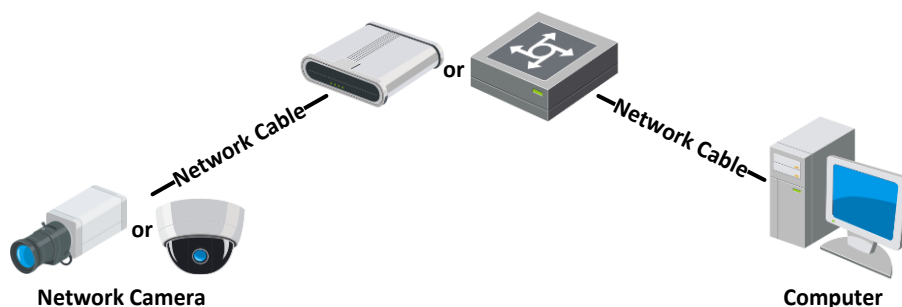


Figure 2-2 Connecting via a Switch or a Router

## 2.1.2 Activating the Camera

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

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

### ❖ Activation via Web Browser

#### *Steps:*

1. Power on the camera, and connect the camera to the network.
2. Input the IP address into the address bar of the web browser, and click **Enter** to enter the activation interface.

#### *Notes:*

- The default IP address of the camera is 192.168.1.64.
- The computer and the camera should belong to the same subnet.
- For the camera enables the DHCP by default, you need to use the SADP software

to search the IP address.

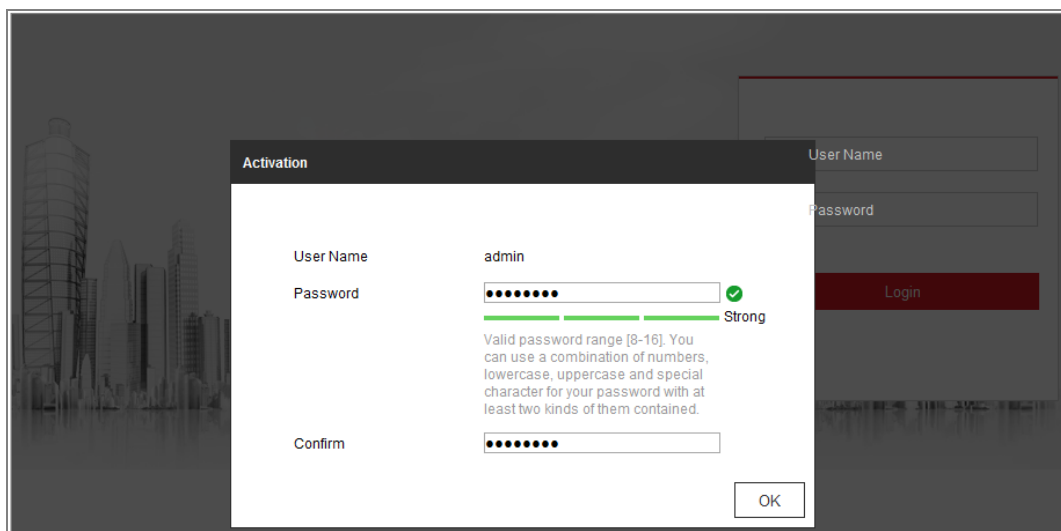


Figure 2-3 Activation via Web Browser

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

A password with user name in it is not allowed.



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

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

#### ❖ **Activation via SADP Software**

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

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

#### **Steps:**

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

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

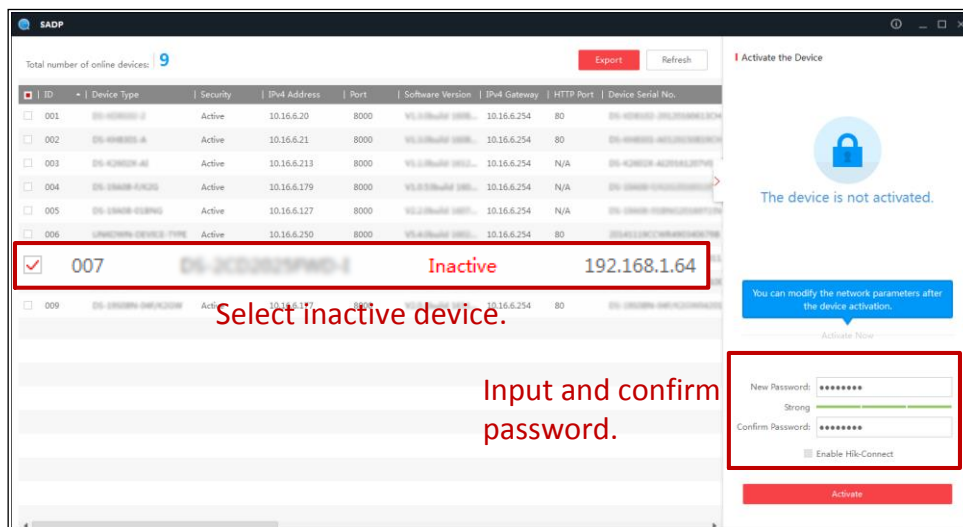



Figure 2-4 SADP Interface

**Note:**

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

3. Create and input the password in the password field, and confirm the password.  
A password with user name in it is not allowed.



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

**Note:**

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

4. Click Activate to start activation.

You can check whether the activation is completed on the popup window. If activation



failed, please make sure that the password meets the requirement and try again.

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

Figure 2-5 Modify the IP Address

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

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

### ❖ Activation via Client Software

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

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

#### **Steps:**

1. Run the client software and the control panel of the software pops up, as shown in

the figure below.

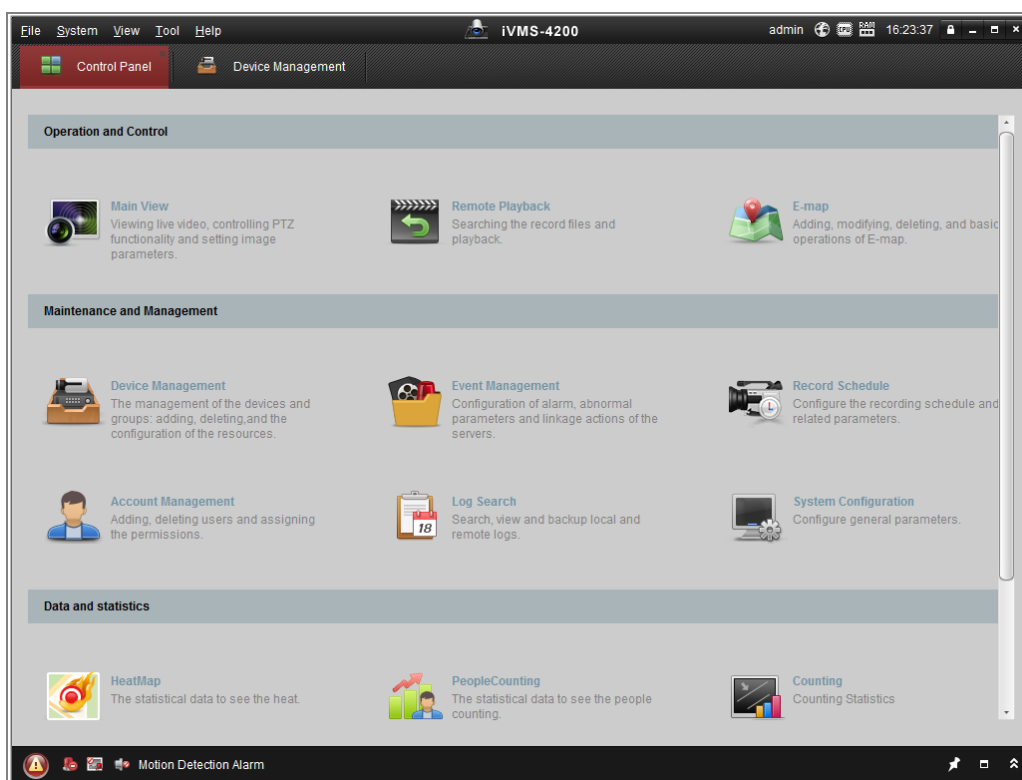


Figure 2-6 Control Panel

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

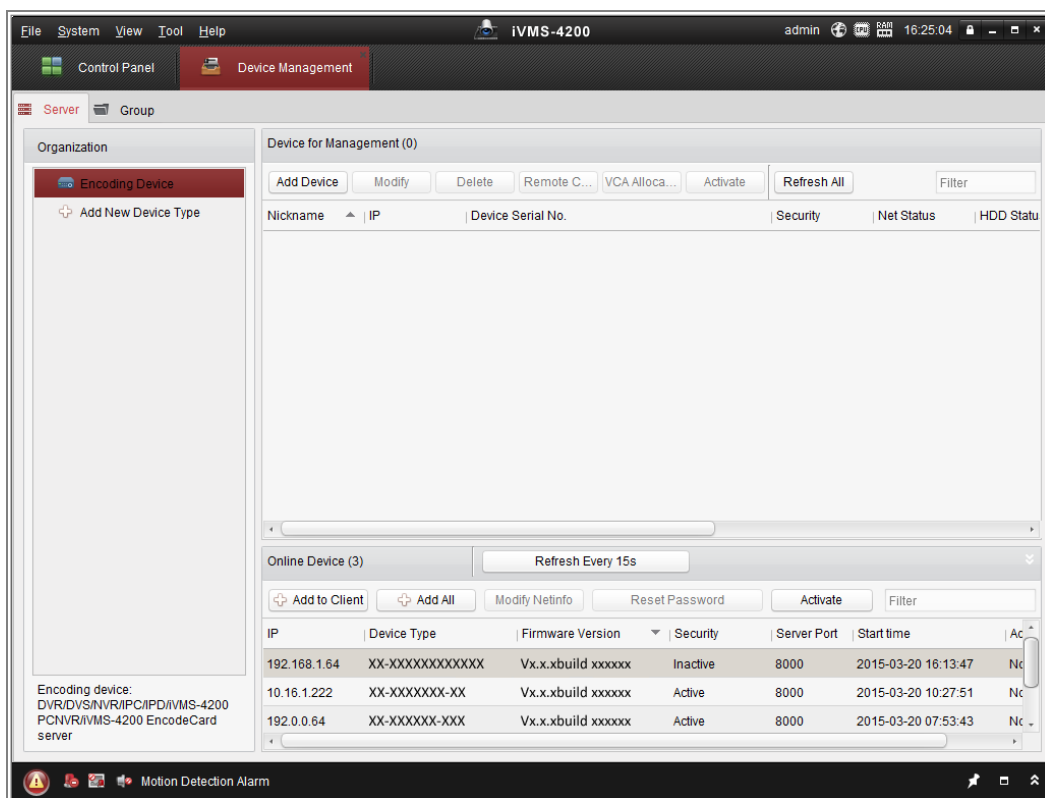


Figure 2-7 Device Management Interface

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

A password with user name in it is not allowed.



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

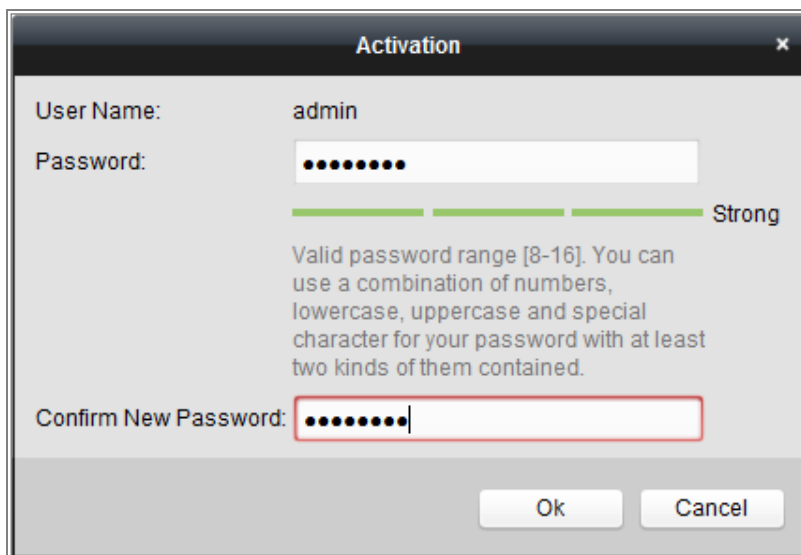


Figure 2-8 Activation Interface (Client Software)

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

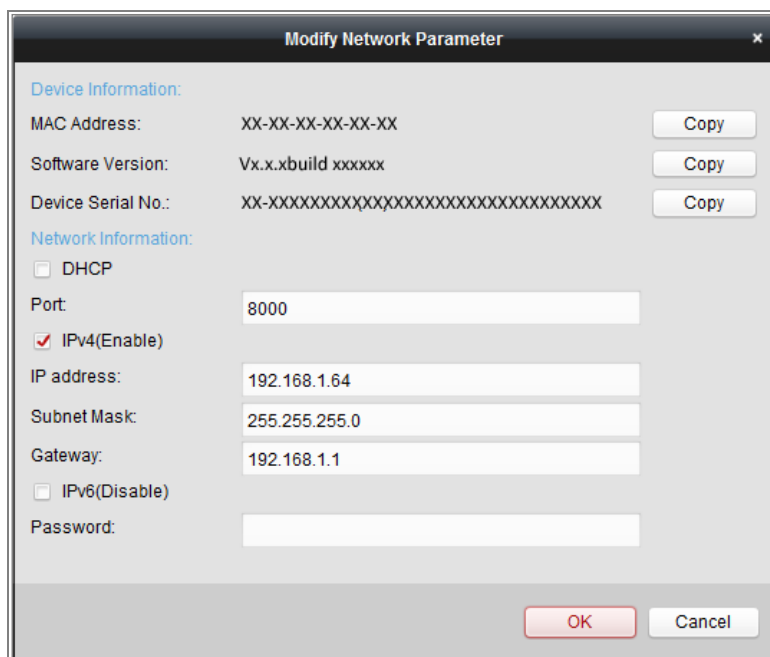


Figure 2-9 Modifying the Network Parameters

8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
9. Input the password to activate your IP address modification.

### 2.1.3 (Optional) Setting Security Question

Security question is used to reset the admin password when admin user forgets the password.

Admin user can follow the pop-up window to complete security question settings during camera activation. Or, admin user can go to **User Management** interface to set up the function.

## 2.2 Setting the Network Camera over the WAN

### *Purpose:*

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

### 2.2.1 Static IP Connection

#### *Before you start:*

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

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

#### *Steps:*

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

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

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

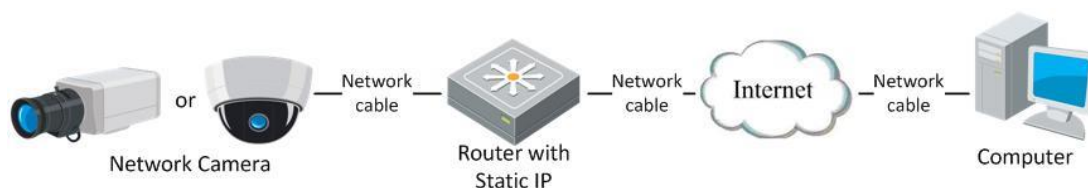


Figure 2-10 Accessing the Camera through Router with Static IP

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

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

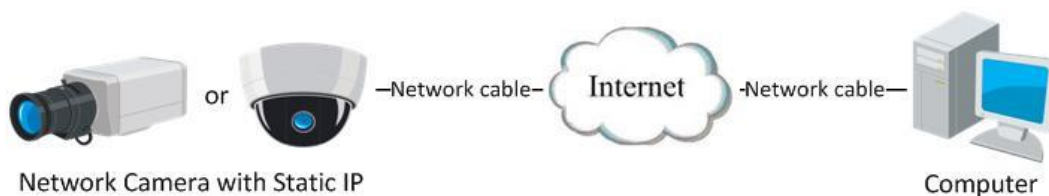


Figure 2-11 Accessing the Camera with Static IP Directly

## 2.2.2 Dynamic IP Connection

### *Before you start:*

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

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

### *Steps:*

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

with port mapping.

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

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

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

**Purpose:**

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to *Section 6.1.3 Configuring PPPoE Settings* for detailed configuration.

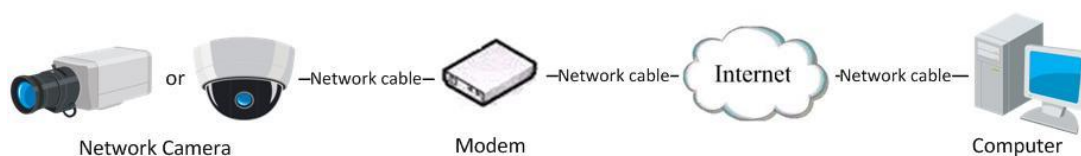


Figure 2-12 Accessing the Camera with Dynamic IP

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

◆ **Normal Domain Name Resolution**

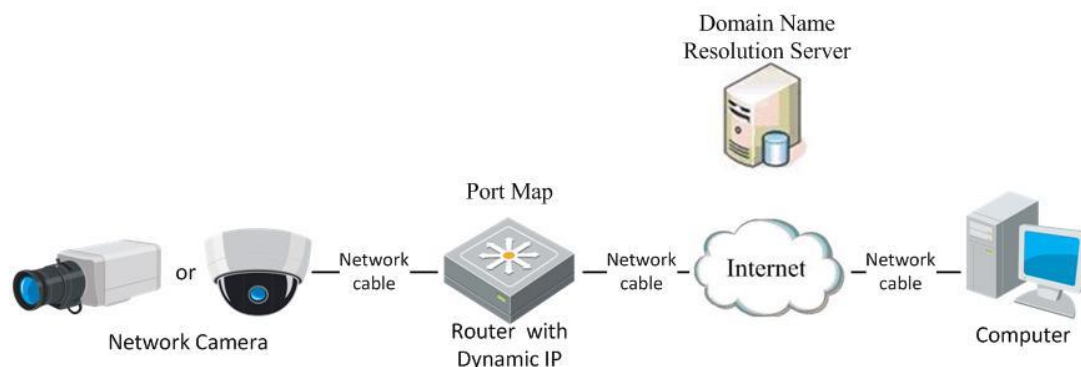


Figure 2-13 Normal Domain Name Resolution

**Steps:**

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to *Section 6.1.2 Configuring DDNS Settings* for detailed configuration.
3. Visit the camera via the applied domain name.



# Chapter 3 Access to the Network Camera

## 3.1 Accessing by Web Browsers

### **Note:**

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

To cancel the notification, install a signed-certificate to the camera. For detailed operation, see *6.2.4 HTTPS Settings*.

### **Steps:**

1. Open the web browser.
2. In the browser address bar, input the IP address of the network camera, and press the **Enter** key to enter the login interface.

### **Note:**

The default IP address is 192.168.1.64. You are recommended to change the IP address to the same subnet with your computer.

3. Input the user name and password and click **Login**.

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

### **Note:**

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



Figure 3-1 Login Interface

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

**Note:**

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

## 3.2 Accessing by Client Software

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

Follow the installation prompts to install the software. The control panel and live view interface of iVMS-4200 client software are shown as below.

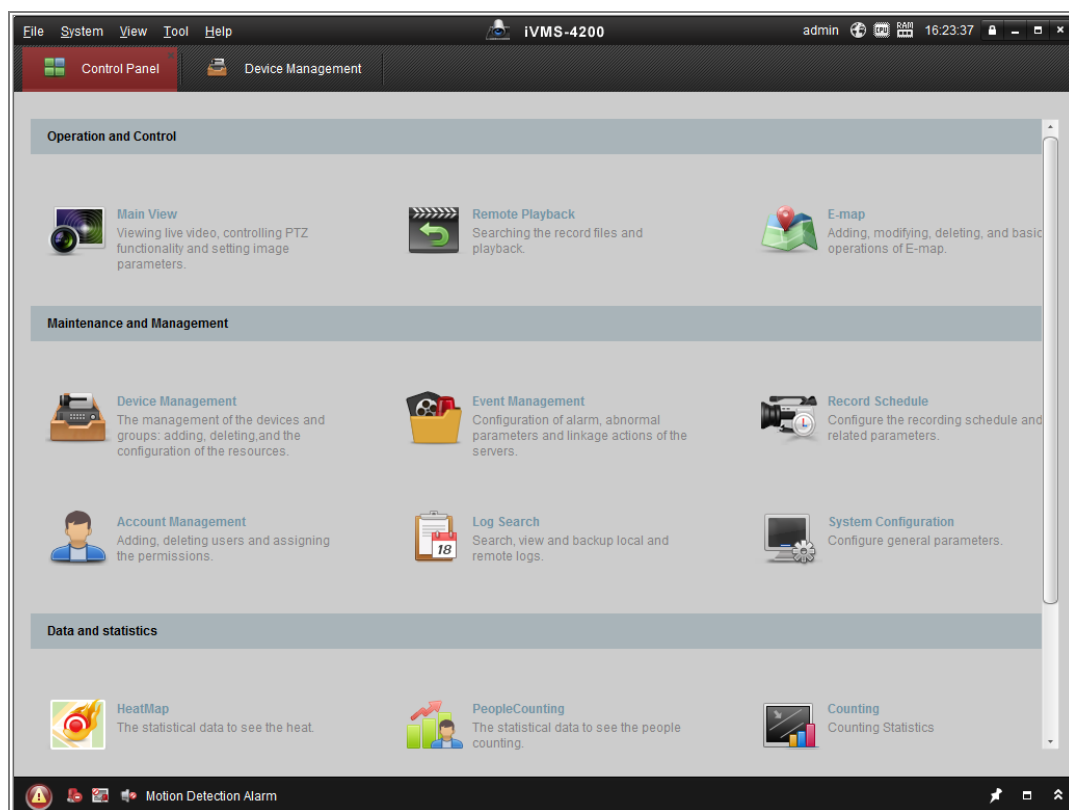


Figure 3-2 iVMS-4200 Control Panel

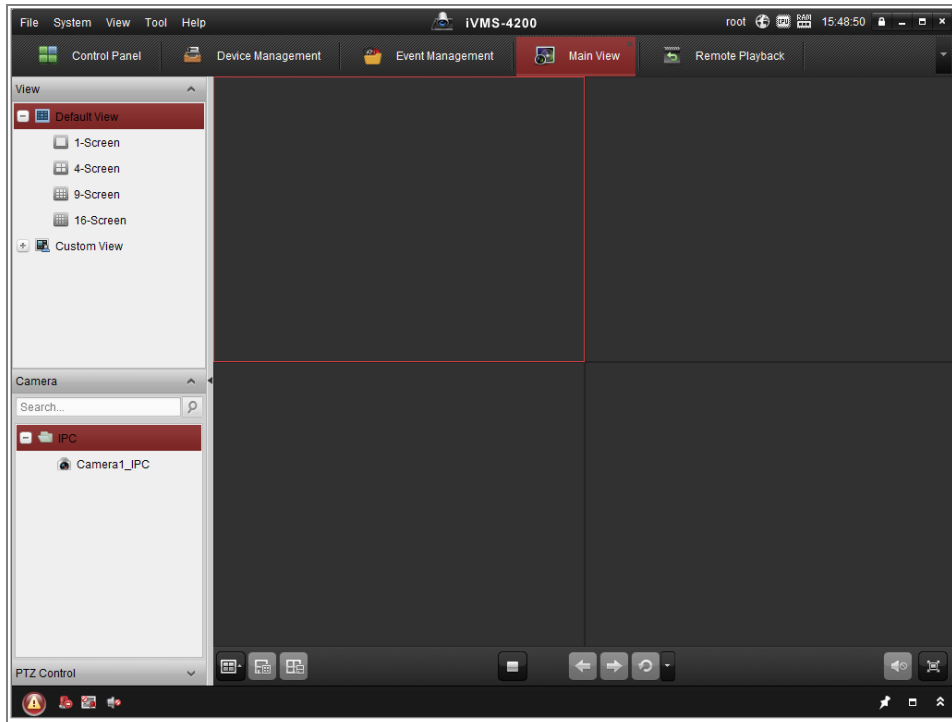


Figure 3-3 iVMS-4200 Main View

# Chapter 4 Live View

## 4.1 Live View Page

### **Purpose:**

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

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

### **Descriptions of the live view page:**

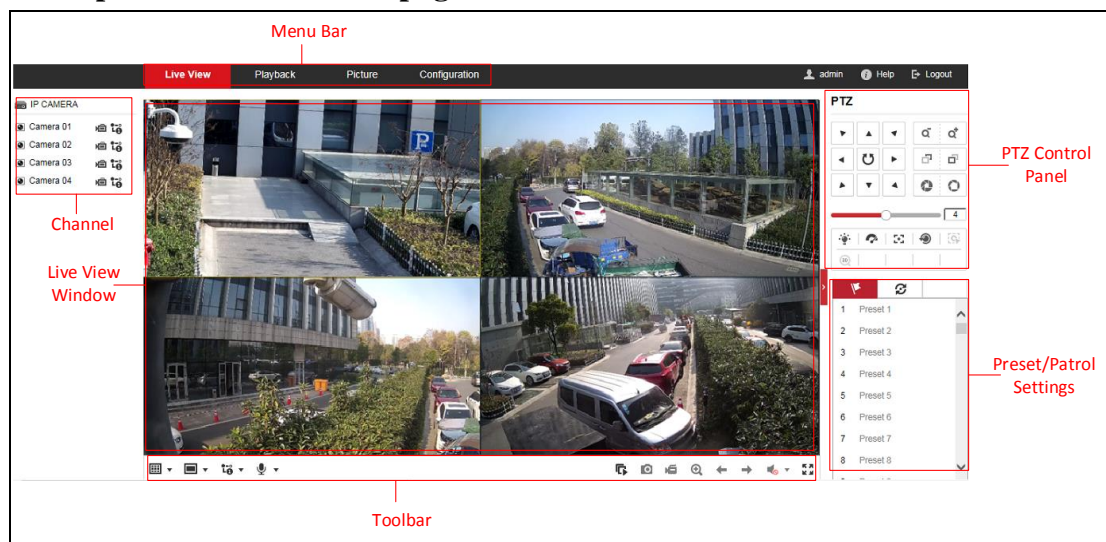


Figure 4-1 Live View Page

### **Menu Bar:**

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

### **Live View Window:**

Display the live video.

### **Toolbar:**

Toolbar allows you to adjust the live view window size, the stream type, and the plug-ins. It also allows you to process the operations on the live view page, e.g., start/stop live view, capture, record, audio on/off, two-way audio, start/stop digital zoom, etc.

For IE (Internet Explorer) users, plug-ins as webcomponents and quick time are selectable. And for Non-IE users, webcomponents, quick time, VLC or MJPEG are selectable if they are supported by the web browser.

**Note:**

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


**PTZ Control:**

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

**Preset/Patrol Settings:**

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

## 4.2 Starting Live View

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

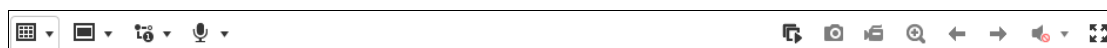






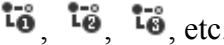









Figure 4-2 Live View Toolbar



Table 4-1 Descriptions of the Toolbar

Icon	Description
	Start/Stop all live view.
	The window size is 4:3.
	The window size is 16:9.
	The original window size or original ratio.
	Self-adaptive window size.
	The window division 1x1, 2x2, or 3x3.
	Live view with the different video streams. Supported video streams vary according to camera models.
	Click to select the third-party plug-in.

Icon	Description
	Manually capture the picture.
	Manually start/stop recording.
	Audio on and adjust volume /Mute.
	Turn on/off microphone.
	Start/stop digital zoom function.
	Previous/next page

**Note:** The icons vary according to the different camera models.

## 4.3 Recording and Capturing Pictures Manually

In the live view interface, click  on the toolbar to capture the live pictures or click  to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration > Local** page. To configure remote scheduled recording, please refer to *Section 6.1*.

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



## 4.4 Operating PTZ Control

### **Purpose:**

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

**Note:** To realize PTZ control, the camera connected to the network must support the PTZ function or have a pan/tilt unit installed to the camera. Please properly set the PTZ parameters on RS485 settings page referring to *Section 5.2.4 RS485 Settings*.

### 4.4.1 PTZ Control Panel

On the live view page, click  next to the right side of the live view window to show the PTZ control panel and click  to hide it.

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



Figure 4-3 PTZ Control Panel

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

**Notes:**

- There are eight direction arrows (▲, ▼, ◀, ▶, ↖, ↗, ↘, ↙) in the control panel. Click the arrows to realize adjustment in the relative positions.
- For the cameras which support lens movements only, the direction buttons are invalid.

Table 4-2 Descriptions of PTZ Control Panel

Icon	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	PTZ speed adjustment
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens
	Adjust speed of pan/tilt movements
	Start Manual Tracking
	Start 3D Zoom

## 4.4.2 Setting/Calling a Preset

### ● Setting a Preset:

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

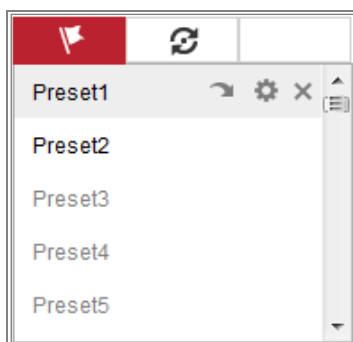





Figure 4-4 Setting a Preset

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

### ● Calling a Preset:

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

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

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

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



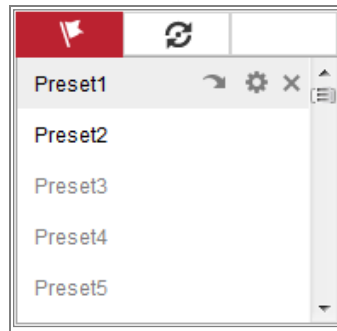




Figure 4-5 Calling a Preset

### 4.4.3 Setting/Calling a Patrol

**Note:**

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

**Steps:**

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

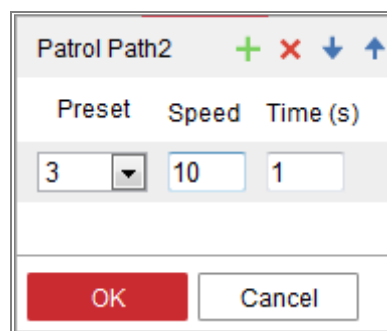





Figure 4-6 Add Patrol Path

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

# Chapter 5 Network Camera Configuration

## 5.1 Configuring Local Parameters

### *Purpose:*

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

### *Steps:*

1. Enter the Local Configuration interface: **Configuration > Local**.

Live View Parameters				
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> MULTICAST	<input type="radio"/> HTTP
Play Performance	<input type="radio"/> Shortest Delay	<input checked="" type="radio"/> Balanced	<input type="radio"/> Fluent	<input type="radio"/> Custom
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Display POS Information	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable		
Auto Start Live View	<input type="radio"/> Yes	<input checked="" type="radio"/> No		
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP		
Record File Settings				
Record File Size	<input type="radio"/> 256M	<input checked="" type="radio"/> 512M	<input type="radio"/> 1G	
Save record files to	<input type="text" value="C:\Users\sunyuanyuan7\Web\Rei"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>	
Save downloaded files to	<input type="text" value="C:\Users\sunyuanyuan7\Web\Do"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>	
Picture and Clip Settings				
Save snapshots in live vi...	<input type="text" value="C:\Users\sunyuanyuan7\Web\Ca"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>	
Save snapshots when pla...	<input type="text" value="C:\Users\sunyuanyuan7\Web\Pla"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>	
Save clips to	<input type="text" value="C:\Users\sunyuanyuan7\Web\Pla"/>	<input type="button" value="Browse"/>	<input type="button" value="Open"/>	

Figure 5-1 Local Configuration Interface

2. Configure the following settings:

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

**TCP:** Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.

**UDP:** Provides real-time audio and video streams.

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

**MULTICAST:** It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Section 7.1.1 Configuring TCP/IP Settings*.

- ◆ **Play Performance:** Set the play performance to Shortest Delay, Balanced or Fluent.
- ◆ **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
- ◆ **Display POS Information:** Enable the function, feature information of the detected target is dynamically displayed near the target in the live image. The feature information of different functions are different. For example, ID and waiting time for Queue Management, height for People Counting, etc.  
**Note:**  
Display POS Information is only available for certain camera models.
- ◆ **Auto Start Live View:** Enable the function to start live view automatically when accessing the camera.
- ◆ **Image Format:** Choose the image format for picture capture.
- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.
- ◆ **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.
- ◆ **Save record files to:** Set the saving path for the manually recorded video files.

- ◆ **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you capture with the web browser.
  - ◆ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.
  - ◆ **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
  - ◆ **Save clips to:** Set the saving path of the clipped video files in playback mode.

**Note:** You can click **Browse** to change the directory for saving the clips and pictures, and click **Open** to open the set folder of clips and picture saving.

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

## 5.2 Configure System Settings

### *Purpose:*

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

### 5.2.1 Configuring Basic Information

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

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

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

### **Online Upgrade**

For some camera models, when memory card is mounted, you can click the **Update** button that appears on the right of **Firmware Version** text field to see if there is a new

version available. If a new version is available, the version number will be displayed in the **New Version** text field below, and you can click the **Upgrade** button to upgrade the firmware for the camera.

Firmware Version	VX.X.X build XXXXXX	Update
New Version	VX.X.X build XXXXXX	Upgrade

Figure 5-2 Online Upgrade

**Note:** When the camera is upgrading, don't power off the camera. During upgrading, the camera may not be accessible. You need to wait 1 or 2 minutes before the upgrade finishes.

## 5.2.2 Configuring Time Settings

### **Purpose:**

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

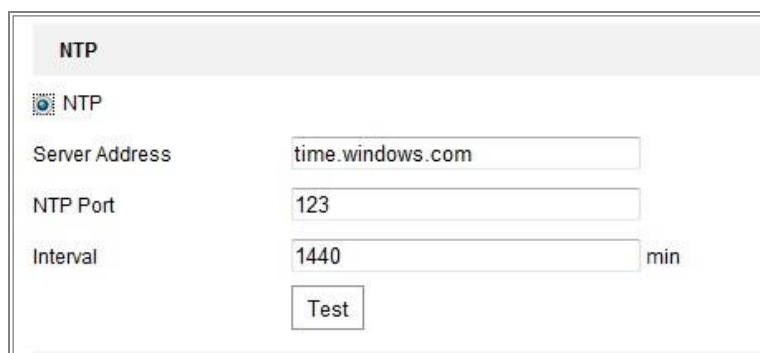
### **Steps:**

1. Enter the Time Settings interface, **Configuration > System > System Settings > Time Settings**.

Basic Information	Time Settings	DST	RS-232	RS-485	Image Stitching	About
Time Zone	(GMT+08:00) Beijing, Urumqi, Singapore, Perth					▼
<b>NTP</b>						
<input type="radio"/> NTP						
Server Address	time.windows.com					
NTP Port	123					
Interval	1440					minute(s)
	Test					
<b>Manual Time Sync.</b>						
<input checked="" type="radio"/> Manual Time Sync.						
Device Time	2018-09-27T15:13:35					
Set Time	2018-09-27T15:13:32					<input type="checkbox"/> Sync. with computer time

Figure 5-3 Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.
  - (1) Click to enable the **NTP** function.
  - (2) Configure the following settings:
    - Server Address:** IP address of NTP server.
    - NTP Port:** Port of NTP server.
    - Interval:** The time interval between the two synchronizing actions with NTP server.
  - (3) (Optional) You can click the **Test** button to test the time synchronization function via NTP server.



NTP	
<input checked="" type="checkbox"/> NTP	
Server Address	<input type="text" value="time.windows.com"/>
NTP Port	<input type="text" value="123"/>
Interval	<input type="text" value="1440"/> min
<input type="button" value="Test"/>	

Figure 5-4 Time Sync by NTP Server

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


- Configure the manual time synchronization.
  - (1) Check the **Manual Time Sync.** item to enable the manual time synchronization function.
  - (2) Click the icon  to select the date, time from the pop-up calendar.
  - (3) (Optional) You can check **Sync. with computer time** item to synchronize the time of the device with that of the local PC.



Figure 5-5 Time Sync Manually

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

### 5.2.3 Configuring RS232 Settings

The RS232 port can be used in two ways:

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

#### **Steps:**

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

Basic Information	Time Settings	<b>RS232</b>	RS485	DST
Baud Rate		115200		
Data Bit		8		
Stop Bit		1		
Parity		None		
Flow Ctrl		None		
Usage		Console		


 Save

Figure 5-6 RS232 Settings

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

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

## 5.2.4 Configuring RS485 Settings

### **Purpose:**

The RS485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

### **Steps:**

1. Enter RS-485 Port Setting interface: **Configuration > System > System Settings > RS485**.



RS485	
Baud Rate	9600
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO-D
PTZ Address	0


 Save

Figure 5-7 RS-485 Settings

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

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

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

### 5.2.5 Configuring DST Settings

**Purpose:**

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

Configure the DST according to your actual demand.

**Steps:**

1. Enter the DST configuration interface.

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

Figure 5-8 DST Settings

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

## 5.2.6 Configuring Image Stitching

### *Purpose:*

You can switch the video output mode for the camera according to your actual demand. There are four video output modes, including Panorama + ePTZ, Panorama, Original and Divided Panorama.

### *Steps:*

1. Enter the Image Stitching configuration interface.

### **Configuration > System > System Settings > Image Stitching**

Figure 5-9 Image Stitching Settings

2. Select the desired video output mode.


**Video Output Mode:** Set the desired output mode as required.

- **Panorama + ePTZ:** One stitched panoramic image (8MP) and multiple channels

ePTZ images. Channel 01 is the 8MP panoramic image, and channel 02 and the subsequent channels are ePTZ images. You can set the number of the channels for the ePTZ image. Ten channels are available. For example, if you set the number of the ePTZ channels to 6, then the live view is seven channels: one 8MP panoramic image and six ePTZ images.

- **Panorama:** One stitched panoramic image (32MP) and the panoramic image output from 1 or 3 encoder track.
- **Original:** Four independent original images (8MP). Take the pendent mounting as an example, when facing the camera lens, the channel order is 01 ~ 04 from right to left.
- **Divided Panorama:** The stitched 32MP panoramic image is divided into four 8MP images.

**Notes:**

- The ePTZ channels support patrol function. You can click  on the live view image to enable or disable the patrol function for ePTZ channels.
  - You can set the image settings for each channel in the original mode.
3. Enter the best stitching distance.

**Best Stitching Distance:** The distance between the lens and the stitching surface you set for the best stitching image quality. The further the distance is, the worse the stitching image quality is.

For example, if you set the best stitching distance to 30 meters, the stitching image of 30 meters far from the lens is the best quality. The stitching image of 20 or 40 meters far from the lens is not good and the image of 10 or 50 meters far from the lens is the worst.

**Notes:**

For the Original mode, Best Stitching Distance are not supported.

4. Click **Save**.

## 5.2.7 Open Source Software License

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



Figure 5-10 Open Source Software Licenses

## 5.3 Maintenance

### 5.3.1 Upgrade & Maintenance

#### *Purpose:*

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

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

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

#### *Notes:*

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

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

This operation requires admin password to proceed.

For the exported file, you also have to create an encryption password. The encryption password is required when you import the file to other cameras.

**Diagnose Information:** click to download log and system information.

- **Import Config. File**

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

**Steps:**

1. Click **Browse** to select the saved configuration file.
2. Click **Import** and input encryption password to start importing configuration file.

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

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

**Steps:**

1. Select firmware or firmware directory to locate the upgrade file.  
Firmware: Locate the exact path of the upgrade file.  
Firmware Directory: Only the directory the upgrade file belongs to is required.
2. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.

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

## 5.3.2 Log

**Purpose:**

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

**Before you start:**

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

**Steps:**

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

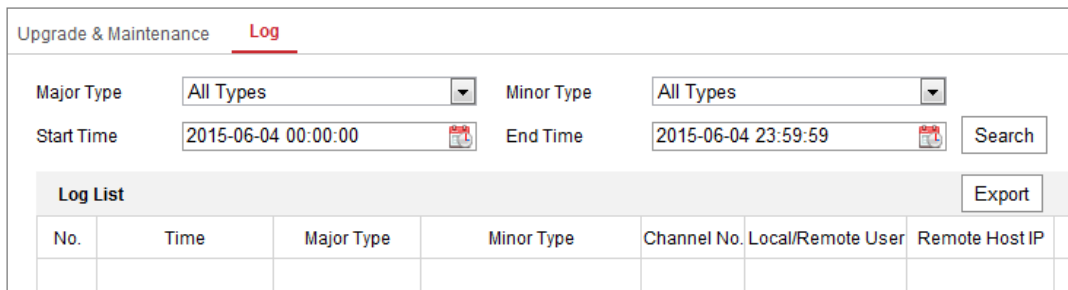


Figure 5-11 Log Searching Interface

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

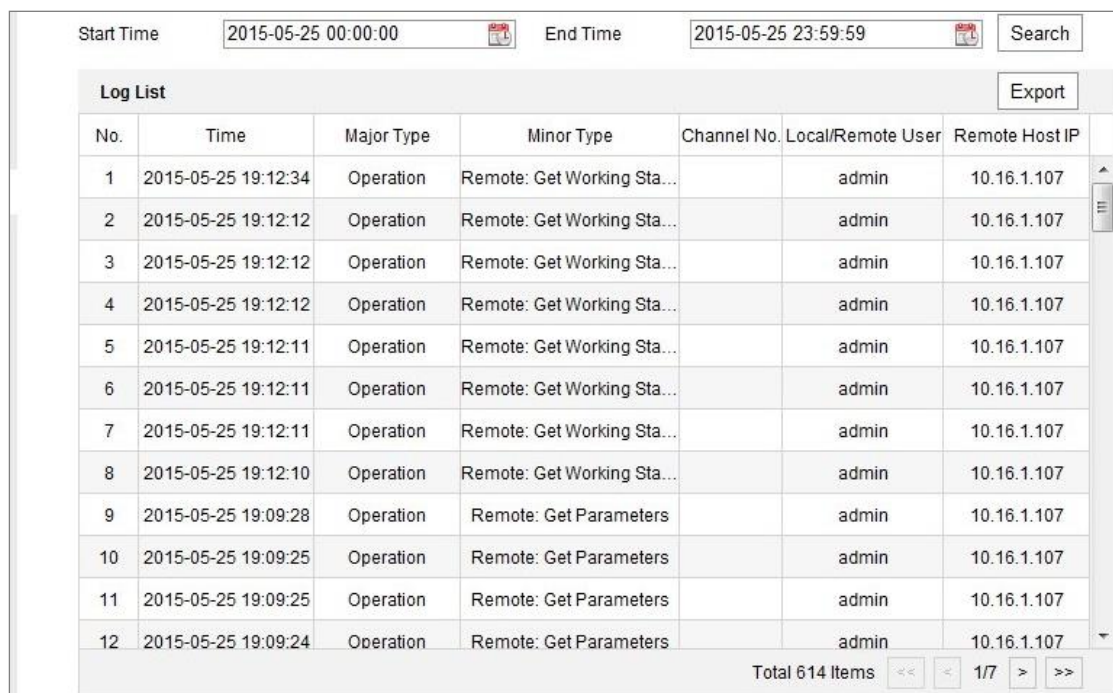



Figure 5-12 Log Searching

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

### 5.3.3 System Service

**Purpose:**

System service settings refer to the hardware service the camera supports. Supported functions vary according to the different cameras. For the cameras support IR Light, ABF (Auto Back Focus), Auto Defog, or Status LED, you can select to enable or disable the corresponding service according to the actual demands.

**ABF:** When ABF function is enabled, you can click  on PTZ control panel to realize auxiliary focus.

**Third Stream:** For some models, third stream is not enabled by default. Check **Enable Third Stream** to enable the function.

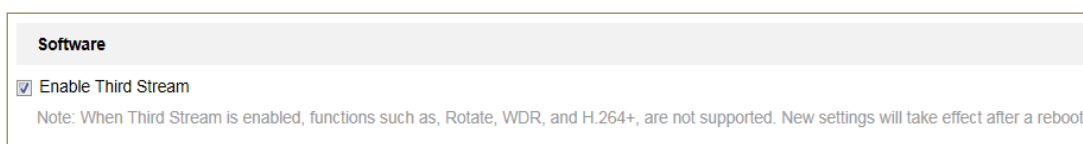


Figure 5-13 Enable Third Stream

## 5.4 Security Settings

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

### 5.4.1 Authentication

**Purpose:**

You can specifically secure the stream data of live view.

**Steps:**

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

Authentication	IP Address Filter	Security Service
RTSP Authentication	digest	
WEB Authentication	digest	

Figure 5-14 Authentication

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

**Caution:**

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

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

### 5.4.2 IP Address Filter

**Purpose:**

This function makes it possible for access control.

**Steps:**

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

Authentication	IP Address Filter	Security Service															
<input checked="" type="checkbox"/> Enable IP Address Filter	Forbidden																
<table border="1"> <thead> <tr> <th colspan="2">IP Address Filter</th> <th>Add</th> <th>Modify</th> <th>Delete</th> </tr> <tr> <th>No.</th> <th>IP</th> <td></td> <td></td> <td></td> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>		IP Address Filter		Add	Modify	Delete	No.	IP									
IP Address Filter		Add	Modify	Delete													
No.	IP																

Figure 5-15 IP Address Filter Interface

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



**Steps:**

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

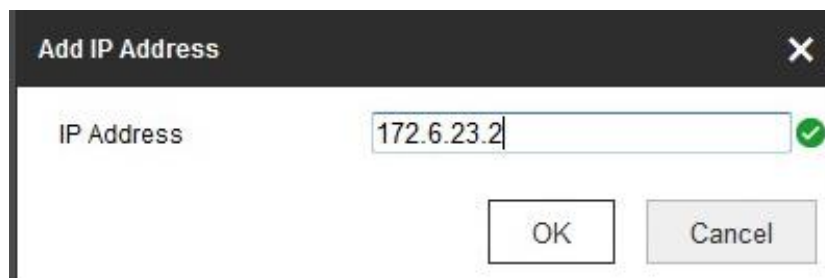


Figure 5-16 Add an IP

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

- Modify an IP Address

**Steps:**

- (1) Left-click an IP address from filter list and click **Modify**.
- (2) Modify the IP address in the text filed.

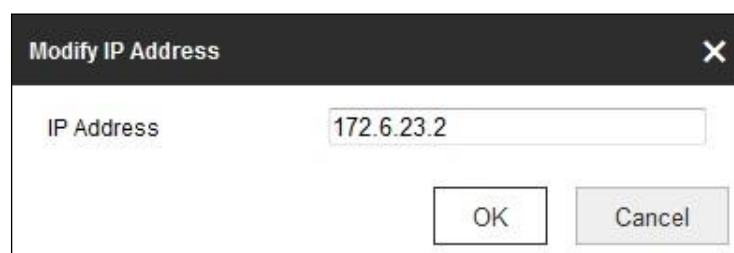


Figure 5-17 Modify an IP

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

- Delete an IP Address or IP Addresses.

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

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

### 5.4.3 Security Service

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

**Steps:**

1. Enter the security service configuration interface: **Configuration > System > Security > Security Service**.

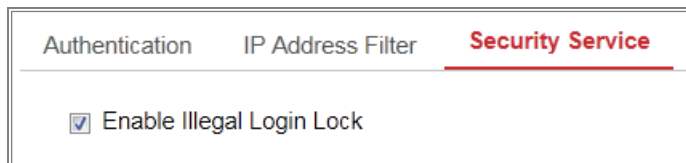


Figure 5-18 Security Service

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

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

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

## 5.5 User Management

### 5.5.1 User Management

- **As Administrator**

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

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

**Note:**

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

User Management		Online Users	
User List		Security Question	Add
		Modify	Delete
No.	User Name	Level	
1	admin	Administrator	
2	test 01	Operator	

Figure 5-19 User Management Interface

- **Adding a User**

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

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

**Steps:**

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

**Notes:**

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



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

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

- **Modifying a User**

**Steps:**

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



**STRONG PASSWORD RECOMMENDED**—We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including at least three of the following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your

password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

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

- **Deleting a User**

**Steps:**

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

- **As Operator or User**

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

## 5.5.2 Security Question

**Purpose:**

Security question is used to reset the admin password when admin user forgets the password.

**Set Security Question:**

You can set the security questions during camera activation. Or you can set the function at user management interface.

Security question setting is not cleared when you restore the camera (not to default).

**Steps:**

1. Enter setting interface:  
**Configuration > System > User Management > User Management**
2. Click **Security Question**.
3. Input correct admin password.
4. Select questions and input answers.
5. Click **OK** to save the settings.

**Reset Admin Password:**

**Before you start:**

The PC used to reset password and the camera should belong to the same IP address

segment of the same LAN.

**Steps:**

1. Enter login interface via web browser.
2. Click **Forget Password**.
3. Answer security question.
4. Create new password.

**Note:**

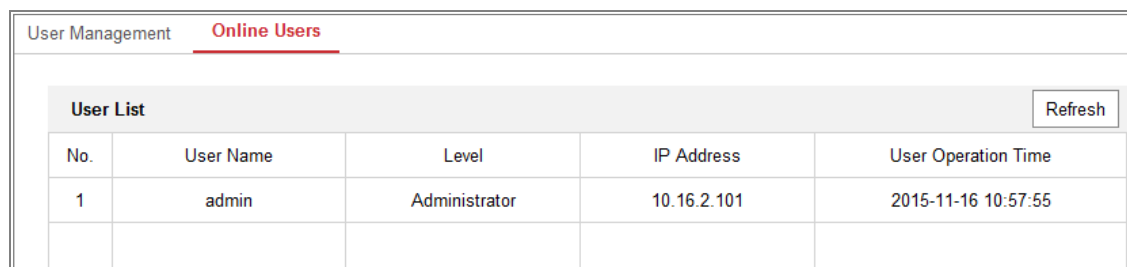
User IP address is locked for 30 minutes after 7 failed attempts of answering security questions.

### 5.5.3 Online Users

**Purpose:**

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

Click **Refresh** to refresh the list.



The screenshot shows a web interface for 'User Management' with a sub-tab for 'Online Users'. Below the tab is a 'User List' table with a 'Refresh' button. The table has five columns: 'No.', 'User Name', 'Level', 'IP Address', and 'User Operation Time'. One row is visible with the following data: No. 1, User Name admin, Level Administrator, IP Address 10.16.2.101, and User Operation Time 2015-11-16 10:57:55.

No.	User Name	Level	IP Address	User Operation Time
1	admin	Administrator	10.16.2.101	2015-11-16 10:57:55

Figure 5-20 View the Online Users

# Chapter 6 Network Settings

## *Purpose:*

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

## 6.1 Configuring Basic Settings

### *Purpose:*

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

### 6.1.1 Configuring TCP/IP Settings

#### *Purpose:*

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

#### *Steps:*

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

The screenshot shows the TCP/IP configuration page. At the top, there are tabs for 'TCP/IP', 'DDNS', 'PPPoE', 'Port', and 'NAT'. The 'TCP/IP' tab is selected. The configuration fields are as follows:

- NIC Type: Auto (dropdown)
- DHCP
- IPv4 Address: 10.11.37.120 (text input) with a 'Test' button
- IPv4 Subnet Mask: 255.255.255.0 (text input)
- IPv4 Default Gateway: 10.11.37.254 (text input)
- IPv6 Mode: Route Advertisement (dropdown) with a 'View Route Advertisement' button
- IPv6 Address: :: (text input)
- IPv6 Subnet Mask: 0 (text input)
- IPv6 Default Gateway: :: (text input)
- Mac Address: c0:56:e3:60:27:5d (text input)
- MTU: 1500 (text input)
- Multicast Address: (text input)
- Enable Multicast Discovery

Below these fields is a 'DNS Server' section with a grey header:

- Preferred DNS Server: 8.8.8.8 (text input)
- Alternate DNS Server: (text input)

At the bottom left, there is a red button with a floppy disk icon and the text 'Save'.

Figure 6-1 TCP/IP Settings

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.
3. (Optional) Check the checkbox of **Enable Multicast Discovery**, and then the online network camera can be automatically detected by client software via private multicast protocol in the LAN.
4. Configure the DNS server. Input the preferred DNS server, and alternate DNS server.
5. Click **Save** to save the above settings.

**Notes:**

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

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

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

## 6.1.2 Configuring DDNS Settings

### *Purpose:*

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

### *Before you start:*

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

### *Steps:*

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

### *Steps:*

- (1)Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
- (2)In the **Domain** text field, enter the domain name obtained from the DynDNS website.
- (3)Enter the **User Name** and **Password** registered on the DynDNS website.
- (4)Click **Save** to save the settings.



Figure 6-2 DynDNS Settings

- NO-IP:

**Steps:**

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

Figure 6-3 NO-IP DNS Settings

- (2) Enter the Server Address as [www.noip.com](http://www.noip.com)
- (3) Enter the Domain name you registered.
- (4) Enter the User Name and Password.
- (5) Click **Save** and then you can view the camera with the domain name.

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

### 6.1.3 Configuring PPPoE Settings

**Steps:**

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

#### PPPoE

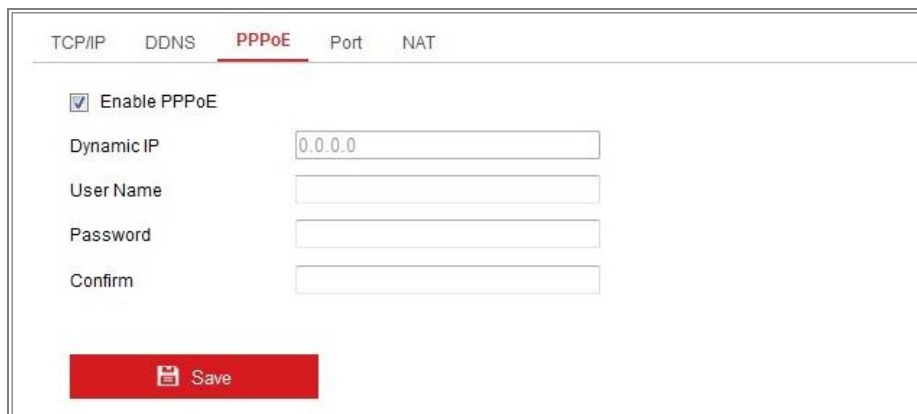


Figure 6-4 PPPoE Settings

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

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



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

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

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

### 6.1.4 Configuring Port Settings

**Purpose:**

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

**Steps:**

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

**Port**

TCP/IP	DDNS	PPPoE	Port	NAT
			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"/>
			WebSocket Port	<input type="text" value="7681"/>
			WebSockets Port	<input type="text" value="7682"/>

Figure 6-5 Port Settings

2. Set the ports of the camera.

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

**RTSP Port:** The default port number is 554 and it can be changed to any port No. ranges from 1 to 65535.

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

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

**Note:**

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

**WebSocket Port:** The default port number is 7681. It can be changed to any port No. ranges from 1 to 65535.

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

**Note:**

WebSocket and WebSockets protocol are used for plug-in free live view. For detailed information, see [错误! 未找到引用源。](#) .

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

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

## 6.1.5 Configure NAT (Network Address Translation) Settings

**Purpose:**

NAT interface allows you to configure the UPnP™ parameters.

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

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

Port Mapping Mode: Auto				
Port Type	External Port	External IP Address	Internal Port	Status
HTTP	80	0.0.0.0	80	Not Valid
RTSP	554	0.0.0.0	554	Not Valid
Server Port	8000	0.0.0.0	8000	Not Valid
WEBSOCKET	7681	0.0.0.0	7681	Not Valid
WEBSOCKETS	7682	0.0.0.0	7682	Not Valid

Figure 6-6 UPnP Settings

**Steps:**

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

**Note:**

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

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

**Note:**

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

If you select Manual, you can customize the value of the external port and complete port mapping settings on router manually.

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

## 6.2 Configure Advanced Settings

**Purpose:**

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

### 6.2.1 Configuring SNMP Settings

**Purpose:**

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

**Before you start:**

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

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



- *For your privacy and to better protect your system against security risks, we*

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

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

**Steps:**

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

**SNMP**   FTP   Email   HTTPS   QoS   802.1x

**SNMP v1/v2**

Enable SNMPv1

Enable SNMP v2c

Read SNMP Community: public

Write SNMP Community: private

Trap Address:

Trap Port: 162

Trap Community: public

**SNMP v3**

Enable SNMPv3

Read UserName:

Security Level: no auth, no priv

Authentication Algorithm:  MD5  SHA

Authentication Password:

Private-key Algorithm:  DES  AES

Private-key password:

Write UserName:

Security Level: no auth, no priv

Authentication Algorithm:  MD5  SHA

Authentication Password:

Private-key Algorithm:  DES  AES

Private-key password:

**SNMP Other Settings**

SNMP Port: 161

**Save**

Figure 6-7 SNMP Settings

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

**Note:** The settings of the SNMP software should be the same as the settings you

configure here.

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

**Notes:**

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

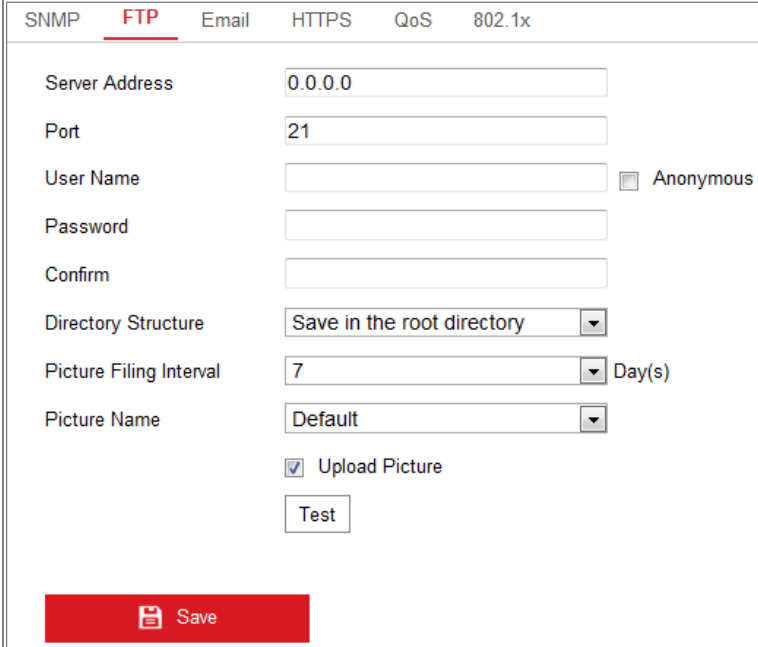
## 6.2.2 Configuring FTP Settings

**Purpose:**

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

**Steps:**

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



SNMP	<b>FTP</b>	Email	HTTPS	QoS	802.1x
Server Address	0.0.0.0				
Port	21				
User Name					<input type="checkbox"/> Anonymous
Password					
Confirm					
Directory Structure	Save in the root directory				
Picture Filing Interval	7				Day(s)
Picture Name	Default				
	<input checked="" type="checkbox"/> Upload Picture				
	Test				
<b>Save</b>					

Figure 6-8 FTP Settings

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



FTP server login.



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

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

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

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

*IP address\_channel number\_capture time\_event type.jpg*

(e.g., *10.11.37.189\_01\_20150917094425492\_FACE\_DETECTION.jpg*).

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

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

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

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

anonymous access to the FTP server.

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

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

### 6.2.3 Configuring Email Settings

**Purpose:**

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

**Before you start:**

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

**Steps:**

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

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

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

3. Configure the following settings:

**Sender:** The name of the email sender.

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

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

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

**Email Encryption:** None, SSL, and TLS are selectable. When you select SSL or TLS and disable STARTTLS, e-mails will be sent after encrypted by SSL or TLS.

The SMTP port should be set as 465 for this encryption method. When you select SSL or TLS and enable STARTTLS, emails will be sent after encrypted by STARTTLS, and the SMTP port should be set as 25.

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

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

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

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



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

The **Receiver** table: Select the receiver to which the email is sent. Up to 3 receivers can be configured.

**Receiver:** The name of the user to be notified.

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

SNMP FTP **Email** HTTPS QoS 802.1x

Sender: test ✓

Sender's Address: test@gmail.com ✓

SMTP Server:

SMTP Port: 25

E-mail Encryption: None

Attached Image

Interval: 2 s

Authentication

User Name:

Password:

Confirm:

Receiver			
No.	Receiver	Receiver's Address	Test
1			<input type="text" value="Test"/>
2			
3			

Figure 6-9 Email Settings

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

## 6.2.4 HTTPS Settings

**Purpose:**

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

**Note:**

- HTTPS is enabled by default for certain camera models.
- If HTTPS is enabled, the camera creates an unsigned certificate automatically. When accessing via HTTPS, the web browser will send a prompt that installing a signed certificate is recommended.

**Steps:**

1. Enter the HTTPS settings interface. **Configuration > Network > Advanced**

**Settings > HTTPS.**

2. Check **Enable** to access the camera via HTTP or HTTPS protocol.



Figure 6-10 HTTPS Configuration Interface

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

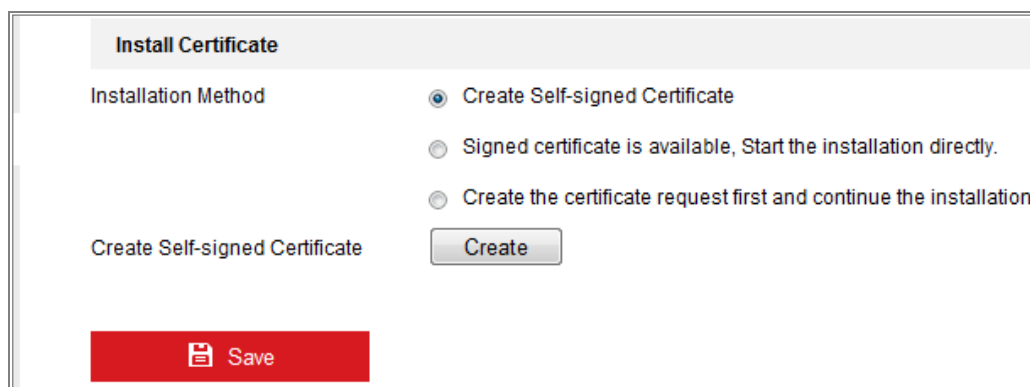


Figure 6-11 Create Self-signed Certificate

- Create the self-signed certificate
  - (1) Select **Create Self-signed Certificate** as the Installation Method.
  - (2) Click **Create** button to enter the creation interface.
  - (3) Enter the country, host name/IP, validity and other information.
  - (4) Click **OK** to save the settings.
 

*Note:* If you already had a certificate installed, the Create Self-signed Certificate is grayed out.
- Create the request and import the authorized certificate
  - (1) Select **Create the certificate request first and continue the installation** as

the Installation Method.

- (2) Click **Create** button to create the certificate request. Fill in the required information in the popup window.
- (3) Click **Download** to download the certificate request and submit it to the trusted certificate authority for signature.
- (4) After receiving the signed valid certificate, you can import the certificate in two ways:
  - a) Select **Signed certificate is available, Start the installation directly**. Click **Browse** and **Install** to import the certificate to the device.

The screenshot shows a dialog box titled "Install Certificate". Under "Installation Method", three radio buttons are present: "Create Self-signed Certificate", "Signed certificate is available, Start the installation directly." (which is selected), and "Create the certificate request first and continue the installation.". Below this, there is a text input field for "Install Signed Certificate" with "Browse" and "Install" buttons to its right. At the bottom left, there is a red "Save" button with a floppy disk icon.

Figure 6-12 Import the Certificate (1)

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

The screenshot shows the same "Install Certificate" dialog box. In this view, the radio button for "Create the certificate request first and continue the installation." is selected. Below the radio buttons, there are three rows of controls: "Create Certificate Request" with a "Create" button and the text "C=CN, H/IP=10.11.11.111"; "Download Certificate Request" with a "Download" button; and "Delete Certificate Request" with a "Delete" button. At the bottom, there is a text input field for "Install Generated Certificate" with "Browse" and "Install" buttons to its right.

Figure 6-13 Import the Certificate (2)

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



Figure 6-14 Installed Certificate

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

## 6.2.5 Configuring QoS Settings

### ***Purpose:***

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

### ***Steps:***

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

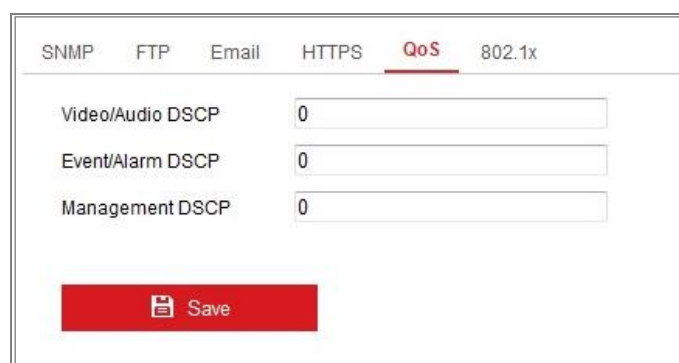


Figure 6-15 QoS Settings

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

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

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

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

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

## 6.2.6 Configuring 802.1X Settings

### **Purpose:**

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

### **Before you start:**

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



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

### **Steps:**

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



The screenshot shows a web interface for configuring 802.1X settings. At the top, there are navigation tabs: SNMP, FTP, Email, HTTPS, QoS, and 802.1x. The 802.1x tab is selected and highlighted in red. Below the tabs, there is a section for 802.1X settings. It starts with a checkbox labeled 'Enable IEEE 802.1X' which is checked. Below this are several configuration options: 'Protocol' is a dropdown menu set to 'EAP-MD5'; 'EAPOL version' is a dropdown menu set to '1'; 'User Name', 'Password', and 'Confirm' are text input fields. At the bottom of the form is a red button with a floppy disk icon and the text 'Save'.

Figure 6-16 802.1X Settings

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

**Note:** The **EAPOL version** must be identical with that of the router or the switch.

4. Enter the user name and password to access the server.
5. Click **Save** to finish the settings.

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

## 6.2.7 Integration Protocol

### **Purpose:**

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

#### ● **CGI**

Check the Enable Hikvision\_CGI checkbox and then select the authentication from the drop-down list.

**Note:** Digest is the recommended authentication method.

#### ● **ONVIF**

### **Steps:**

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

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

**Note:** ONVIF user account is different from the camera user account. You have set ONVIF user account independently.

3. Save the settings.

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

# Chapter 7 Video/Audio Settings

## *Purpose:*

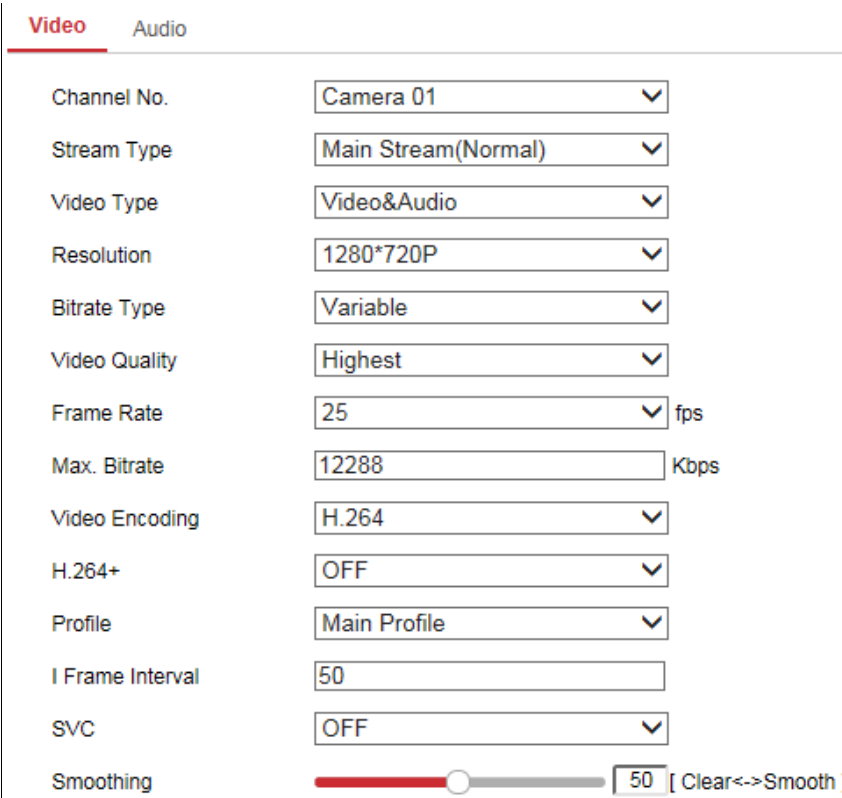
Follow the instructions below to configure the video setting, audio settings, ROI, Display info. on Stream, etc.

## 7.1 Configuring Video Settings

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

## *Steps:*

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



The screenshot displays the 'Video' settings interface. At the top, there are two tabs: 'Video' (selected) and 'Audio'. Below the tabs, a list of settings is shown, each with a label and a control element (dropdown menu, text input, or slider). The settings are: Channel No. (Camera 01), Stream Type (Main Stream(Normal)), Video Type (Video&Audio), Resolution (1280\*720P), Bitrate Type (Variable), Video Quality (Highest), Frame Rate (25 fps), Max. Bitrate (12288 Kbps), Video Encoding (H.264), H.264+ (OFF), Profile (Main Profile), I Frame Interval (50), SVC (OFF), and Smoothing (a slider set to 50 with 'Clear<->Smooth' buttons).

Setting	Value
Channel No.	Camera 01
Stream Type	Main Stream(Normal)
Video Type	Video&Audio
Resolution	1280*720P
Bitrate Type	Variable
Video Quality	Highest
Frame Rate	25 fps
Max. Bitrate	12288 Kbps
Video Encoding	H.264
H.264+	OFF
Profile	Main Profile
I Frame Interval	50
SVC	OFF
Smoothing	50 [ Clear<->Smooth ]

Figure 7-1 Video Settings

2. Select the desired channel number.
3. Select the Stream Type.

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

**Notes:**

- For some models, the **Third Stream** is not enabled by default. Go to **System > Maintenance > System Service > Software** to enable the function is required.
  - The main stream is usually for recording and live view with good bandwidth, and the sub-stream can be used for live view when the bandwidth is limited.
4. You can customize the following parameters for the selected stream type.

**Video Type:**

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

**Resolution:**

Select the resolution of the video output.

**Bitrate Type:**

Select the bitrate type to constant or variable.

**Video Quality:**

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

**Frame Rate:**

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

**Max. Bitrate:**

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

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

**Video Encoding:**

The camera supports multiple video encodings types, such as H.264, H.265, MJPEG, and MPEG4. Supported encoding type for different stream types may differ. H.265 is a new encoding technology. Compared with H.264, it reduces the

transmission bitrate under the same resolution, frame rate and image quality.

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

**H.264+ and H.265+:**

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

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

**Notes:**

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

**Max. Average Bitrate:**

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

**Profile:**

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

**I Frame Interval:**

Set I Frame Interval from 1 to 400.

**SVC:**

Scalable Video Coding is an extension of the H.264/AVC and H.265 standard. Select OFF/ON to disable/enable the SVC function. Select Auto and the device will automatically extract frames from the original video when the network bandwidth is insufficient.

**Smoothing:**

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

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

**Note:**

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

## 7.2 Configuring Audio Settings

**Steps:**

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

Video	Audio
Audio Encoding	G.711alaw
Audio Input	LineIn
Input Volume	50
Environmental Noise Filter	OFF

Figure 7-2 Audio Settings

2. Configure the following settings.

**Note:** Audio settings vary according to different camera models.

**Audio Encoding:** G.722.1, G.711 ulaw, G.711alaw, G.726, MP2L2 and PCM are selectable. For MP2L2, the Sampling Rate and Audio Stream Bitrate are configurable. For PCM, the Sampling Rate can be set.

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

**Input Volume:** 0-100 adjustable.

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

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

- 1.

# Chapter 8 Image Settings

## **Purpose:**

Follow the instructions in this chapter to configure the image parameters, including display settings, OSD settings, and picture overlay.

## 8.1 Configuring Display Settings

### **Purpose:**

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

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

### **Steps:**

1. Enter the Display Settings interface, **Configuration > Image > Display Settings**.



Figure 8-1 Display Settings

2. Set the image parameters of the camera.

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

### ● **Image Adjustment**

**Brightness** describes bright of the image, which ranges from 1 to 100.

**Contrast** describes the contrast of the image, which ranges from 1 to 100.



**Saturation** describes the colorfulness of the image color, which ranges from 1 to 100.

**Sharpness** describes the edge contrast of the image, which ranges from 1 to 100.

- **Exposure Settings**

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

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

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

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

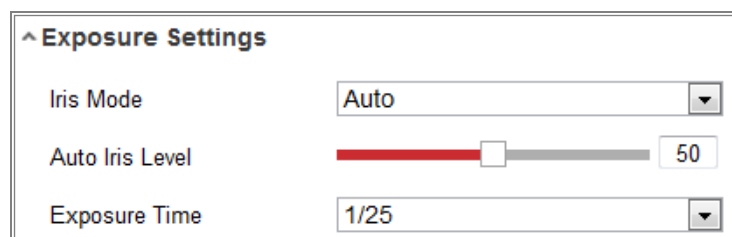


Figure 8-2 Exposure Settings

- **Day/Night Switch**

Select the Day/Night Switch mode according to different surveillance demand.

Day, Night, Auto, Scheduled-Switch, and Triggered by alarm input are selectable for day/night switch.

^ Day/Night Switch	
Day/Night Switch	Auto
Sensitivity	4
Filtering Time	5
Smart Supplement Light	ON
Mode	Manual
Light 1 Distance	50
Light 2 Distance	50
Light 3 Distance	50
Light 4 Distance	50

Figure 8-3 Day/Night Switch

**Day:** the camera stays at day mode.

**Night:** the camera stays at night mode.

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

**Scheduled-Switch:** Set the start time and the end time to define the duration for day/night mode.

**Triggered by alarm input:** The switch is triggered by alarm input. You can set the triggered mode to day or night.

**Smart Supplement Light:** Set the supplement light to ON, and Auto and Manual are selectable for light mode.

Select **Auto**, and the supplement light changes according to the actual luminance. E.g., if the current scene is bright enough, then the supplement light adjusts itself to lower power; and if the scene is not bright enough, the light adjusts itself to higher power.

Select **Manual**, and you can adjust the distance of the supplement light. There are four supplement lights and you can adjust the distance for the each light. If the object is near the camera, the device adjusts the supplement light to lower power, and the light is in higher power if the object is far away.

- **Backlight Settings**

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

**Note:** If BLC mode is set as Custom, you can draw a red rectangle on the live view image as the BLC area.

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

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

- **White Balance**

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



Figure 8-4 White Balance

- **Image Enhancement**

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

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

**EIS (Electrical Image Stabilizer):** EIS reduces the effects of vibration in a

video.

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

- **Video Adjustment**

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

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

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

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

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

**Lens Distortion Correction:** For cameras equipped with motor-driven lens, image may appear distorted to some extent. Turn on this function to correct the distortion.

- **Others**

Some camera models support CVBS, SDI, or HDMI output. Set the local output ON or OFF according to the actual device.

## 8.2 Configuring OSD Settings

***Purpose:***

You can customize the camera name, time/date format, display mode, and OSD size displayed on the live view.



Figure 8-5 OSD Settings

**Steps:**

1. Enter the OSD Settings interface: **Configuration > Image > OSD Settings**.
2. Select the desired channel number from the drop-down list.
3. Check the corresponding checkbox to select the display of camera name, date or week if required.
4. Edit the camera name in the text field of **Camera Name**.
5. Select from the drop-down list to set the time format and date format.
6. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
7. Configure the text overlay settings.
  - (1) Check the checkbox in front of the textbox to enable the on-screen display.
  - (2) Input the characters in the textbox.

**Note:** Up to 8 text overlays are configurable.

8. Adjust the position and alignment of text frames.

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

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

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

## 8.3 Configuring Picture Overlay

### *Purpose:*

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

### *Steps:*

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

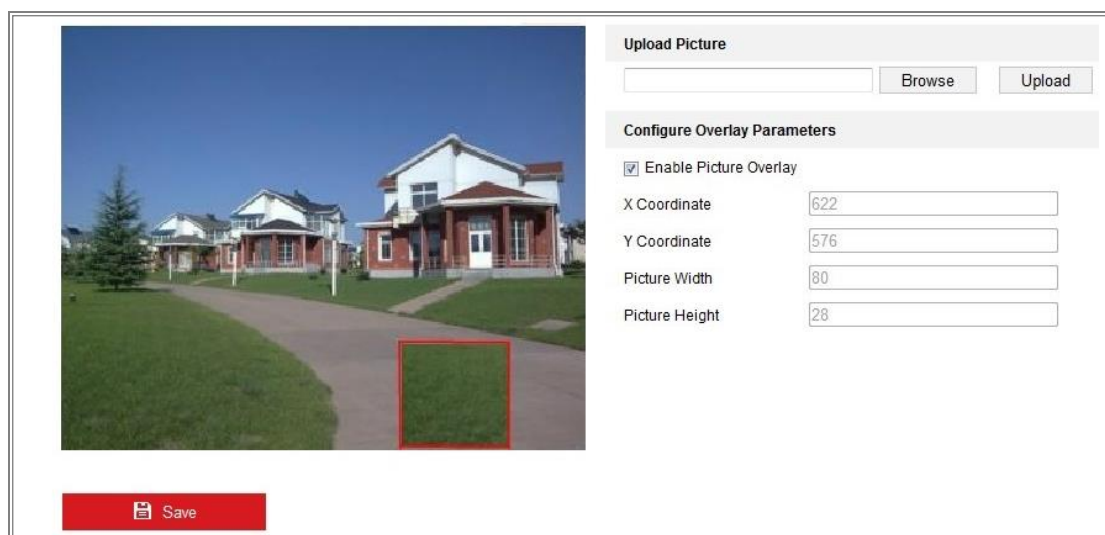


Figure 8-6 Picture Overlay

2. Select the desired channel number from the drop-down list.
3. Click **Browse** to select a picture.
4. Click **Upload** to upload it.
5. Check **Enable Picture Overlay** checkbox to enable the function.
6. Set X Coordinate and Y Coordinate values adjust the picture position on the image. Adjust Picture Width and Picture Height to the desired size.
7. Click **Save** to save settings.

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

## Chapter 9 Event Settings

This section explains how to configure the network camera to respond to alarm events, including basic event and smart event.

### 9.1 Basic Events

You can configure the basic events by following the instructions in this section, including alarm input, alarm output, and exception. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

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

#### 9.1.1 Configuring Alarm Input

**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). Edit the name to set a name for the alarm input (optional).

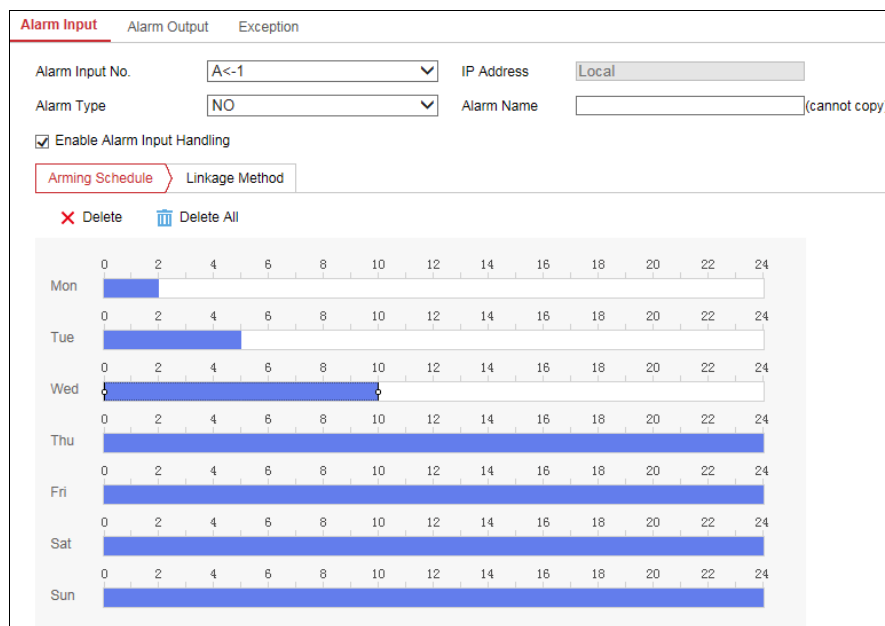


Figure 9-1 Alarm Input Settings

3. Click **Arming Schedule** to set the arming schedule for the alarm input.

**Task 1: Set the Arming Schedule**

**Steps:**

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

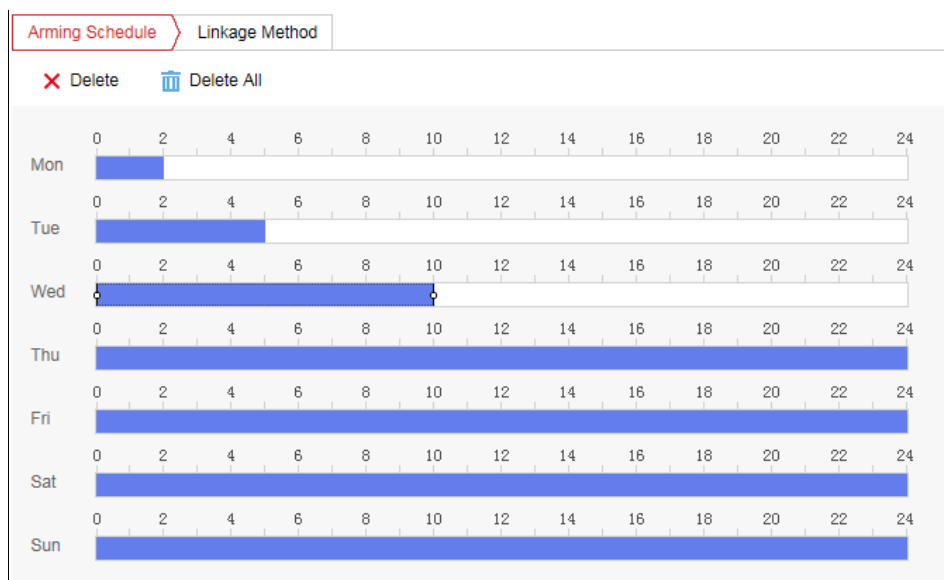


Figure 9-2 Arming Schedule

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

- 3) (Optional) Click Delete to delete the current arming schedule, or click Save to



save the settings.

- 4) Move the mouse to the end of each day, a copy dialogue box pops up, and you can copy the current settings to other days.
- 5) Click **Save** to save the settings.

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

4. Click **Linkage Method** and check the checkbox to select the linkage method for the alarm input.

**Task 2: Set the Linkage Method**

Check the checkbox to select the linkage method. Audible Warning, Send Email, Notify Surveillance Center, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output are selectable. You can specify the linkage method when an event occurs.

Arming Schedule		Linkage Method
<input type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output	<input type="checkbox"/> Trigger Recording
<input type="checkbox"/> Send Email	<input checked="" type="checkbox"/> A->1	<input type="checkbox"/> A1
<input type="checkbox"/> Notify Surveillance Center	<input type="checkbox"/> A->2	<input type="checkbox"/> A2
<input type="checkbox"/> Upload to FTP/Memory Card/...		<input type="checkbox"/> A3
		<input type="checkbox"/> A4
		<input type="checkbox"/> A5
		<input type="checkbox"/> A6
		<input type="checkbox"/> A7
		<input type="checkbox"/> A8
		<input type="checkbox"/> A9

Figure 9-3 Linkage Method

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

- **Audible Warning**

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

- **Notify Surveillance Center**

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

occurs.

- **Send Email**

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

**Note:** To send the Email when an event occurs, please refer to *Section 7.2.3* to complete Email setup in advance.

- **Upload to FTP/Memory Card/NAS**

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

**Notes:**

- Set the FTP address and the remote FTP server first. Refer to *Section 6.2.2 Configuring FTP Settings* for detailed information.
- Go to **Configuration > Storage > Schedule Settings > Capture > Capture Parameters** page, enable the event-triggered snapshot, and set the capture interval and capture number.
- The captured image can also be uploaded to the available SD card or network disk.

- **Trigger Channel**

The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 11.1* for detailed information.

- **Trigger Alarm Output**

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

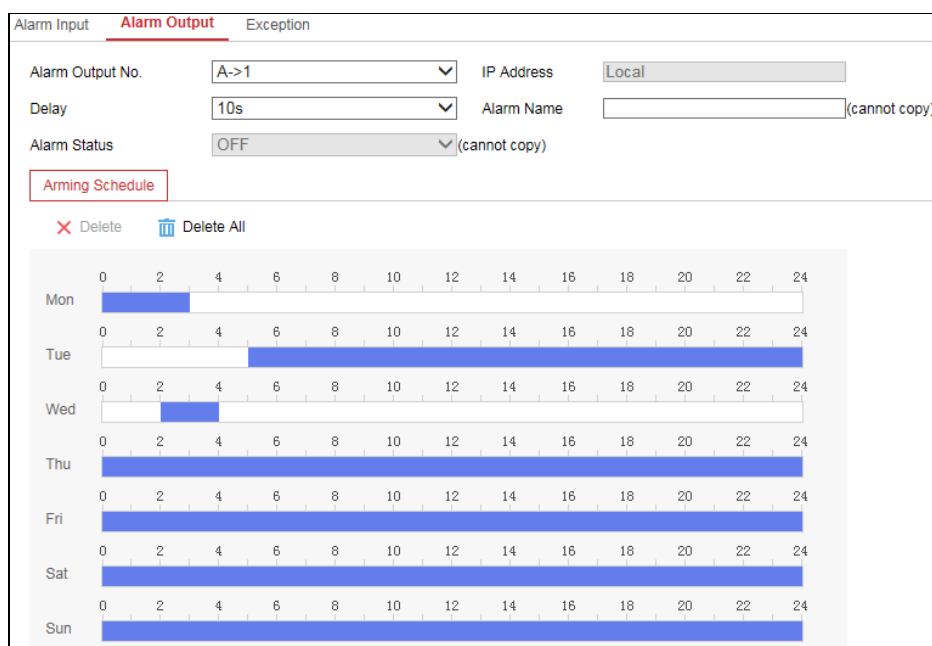
**Note:** To trigger an alarm output when an event occurs, please refer to *Configuring Alarm Output* to set the related parameters.

5. You can copy your settings to other alarm inputs.
6. Click **Save** to save the settings.

## 9.1.2 Configuring Alarm Output

**Steps:**

1. Enter the Alarm Output Settings interface: **Configuration > Event > Basic Event > Alarm Output.**



Alarm Input **Alarm Output** Exception

Alarm Output No.  IP Address

Delay  Alarm Name

Alarm Status  (cannot copy)

**Arming Schedule**

Day	0	2	4	6	8	10	12	14	16	18	20	22	24
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 9-4 Alarm Output Settings

2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Click **Arming Schedule** to enter the Edit Schedule Time interface. The time schedule configuration is the same as the settings of the arming schedule for motion detection Refer to **Task 1: Set the Arming Schedule** in *Section 9.1.1*.
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

### 9.1.3 Handling Exception

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

**Steps:**

1. Enter the Exception Settings interface: **Configuration > Event > Basic Event > Exception**.
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Task 3: Set the Linkage Method for Motion Detection* in Section *错误!未找到引用源。*.

Motion Detection	Video Tampering	Alarm Input	Alarm Output	<b>Exception</b>
Exception Type: Illegal Login				
<input checked="" type="checkbox"/> Normal Linkage	<input type="checkbox"/> Trigger Alarm Output			
<input checked="" type="checkbox"/> Send Email	<input type="checkbox"/> A->1			
<input checked="" type="checkbox"/> Notify Surveillance Center				

Figure 9-5 Exception Settings

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

# Chapter 10 Storage Settings

## *Before you start:*

To configure record settings, please make sure that you have the network storage device or local storage device configured.

## 10.1 Configuring Record Schedule

### *Purpose:*

There are two kinds of recording for the cameras: 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 local storage or in the network disk.

### *Steps:*

1. Enter the Record Schedule Settings interface: **Configuration > Storage > Schedule Settings > Record Schedule.**

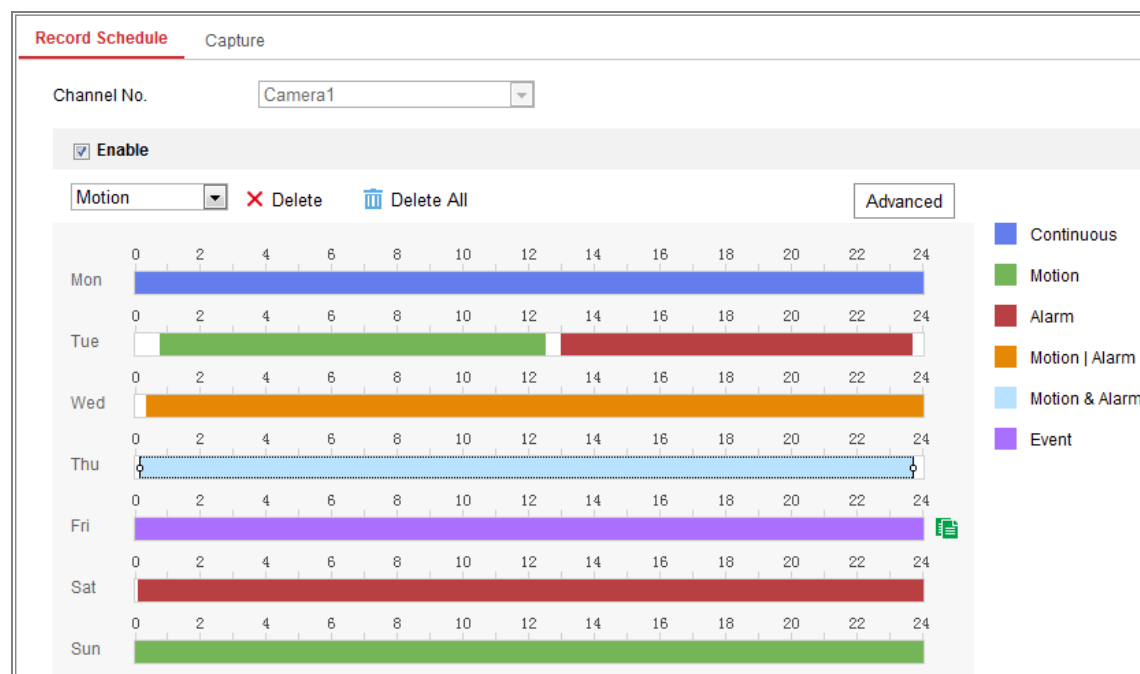


Figure 10-1 Recording Schedule Interface

2. Select the desired channel number.
3. Check the checkbox of **Enable** to enable scheduled recording.

- Click **Advanced** to set the camera record parameters.

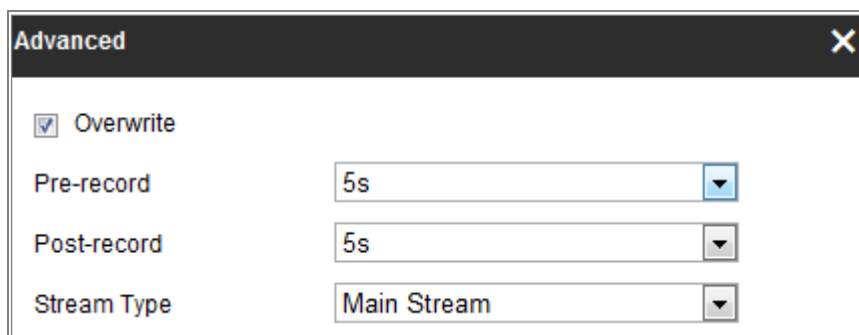


Figure 10-2 Record Parameters

- **Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.  
The Pre-record time can be configured as No Pre-record, 5s, 10s, 15s, 20s, 25s, 30s or not limited.
- **Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.  
The Post-record time can be configured as 5s, 10s, 30s, 1 min, 2 min, 5 min or 10 min.
- **Stream Type:** Select the stream type for recording.

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

- Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, and Event.

- **Continuous**

If you select **Continuous**, the video will be recorded automatically according to the time of the schedule.

- **Record Triggered by Motion Detection**

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

Besides configuring the recording schedule, you have to set the motion detection area and check the checkbox of Trigger Channel in the Linkage

Method of Motion Detection Settings interface. For detailed information, please refer to the *Task 1: Set the Motion Detection Area* in the *Section 错误! 未找到引用源。* .

- **Record Triggered by Alarm**

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

Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method of Alarm Input Settings** interface. For detailed information, please refer to *Section 9.1.1*.

- **Record Triggered by Motion & Alarm**

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

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 错误! 未找到引用源。* .and *Section 9.1.1* for detailed information.

- **Record Triggered by Motion | Alarm**

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

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 错误! 未找到引用源。* .and *Section 9.1.1* for detailed information.

- **Record Triggered by Events**

If you select **Event**, the video will be recorded if any of the events is triggered. Besides configuring the recording schedule, you have to configure the event settings.

6. Select the record type, and click-and-drag the mouse on the time bar to set the record schedule.
7. Click **Save** to save the settings.

## 10.2 Configure 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.

### *Steps:*

1. Enter the Capture Settings interface: **Configuration > Storage > Storage Settings > Capture.**

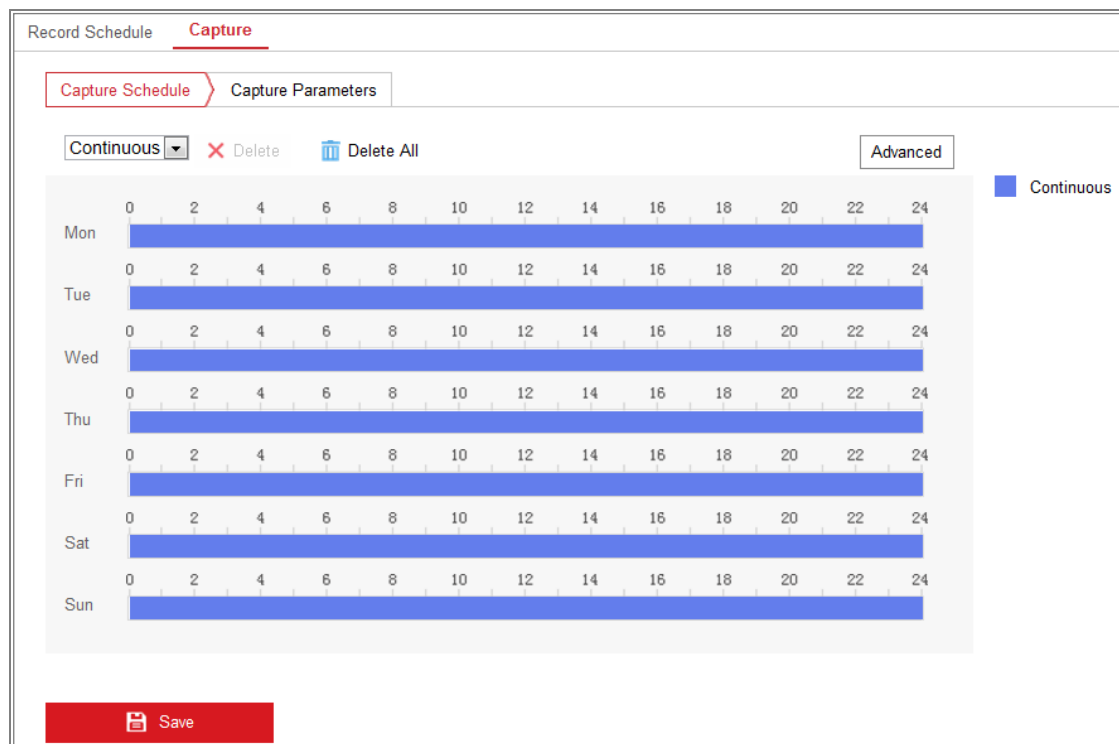


Figure 10-3 Capture Configuration

2. Select the desired channel number.
3. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar. You can copy the record schedule to other days by clicking the green copy icon on the right of each time bar.
4. Click **Advanced** to select stream type.



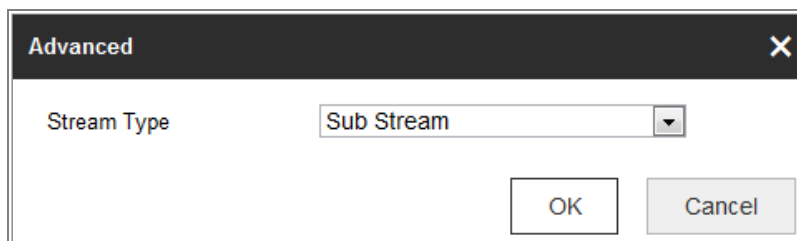


Figure 10-4 Advanced Setting of Capture Schedule

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

The image is a screenshot of a web interface for configuring a network camera. At the top, there are two tabs: "Record Schedule" and "Capture". The "Capture" tab is selected and highlighted in red. Below the tabs, there are two sub-tabs: "Capture Schedule" and "Capture Parameters". The "Capture Parameters" sub-tab is selected and highlighted in red. The main content area is divided into two sections: "Timing" and "Event-Triggered".  
**Timing Section:**  
- A checkbox labeled "Enable Timing Snapshot" is checked.  
- "Format" is set to "JPEG".  
- "Resolution" is set to "704\*576".  
- "Quality" is set to "High".  
- "Interval" is set to "500" milliseconds.  
**Event-Triggered Section:**  
- A checkbox labeled "Enable Event-Triggered Snapshot" is checked.  
- "Format" is set to "JPEG".  
- "Resolution" is set to "704\*576".  
- "Quality" is set to "High".  
- "Interval" is set to "500" milliseconds.  
- "Capture Number" is set to "4".  
At the bottom of the page, there is a red button with a save icon and the text "Save".

Figure 10-5 Set Capture Parameters

7. Set the time interval between two snapshots.
8. Click **Save** to save the settings.

## 10.3 Configuring Net HDD

### *Before you start:*

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

### *Steps:*

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

The screenshot shows the 'Net HDD' management interface. It features a table with columns for HDD No., Server Address, File Path, Type, and Delete. Below the table are input fields for Mounting Type (SMB/CIFS), User Name (cxy1), Password (masked with dots), and a Test button.

HDD No.	Server Address	File Path	Type	Delete
1	10.10.36.61	/cxy_1	NAS	✘
2	10.10.36.252	/dvr/yanjian_1	NAS	✘
3			NAS	✘

Mounting Type:  User Name:  Password:

Figure 10-6 Add Network Disk

- (2) Enter the IP address of the network disk, and enter the file path.
- (3) Select the mounting type. NFS and SMB/CIFS are selectable. And you can set the user name and password to guarantee the security if SMB/CIFS is selected.

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



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

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

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

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

2. Initialize the added network disk.

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

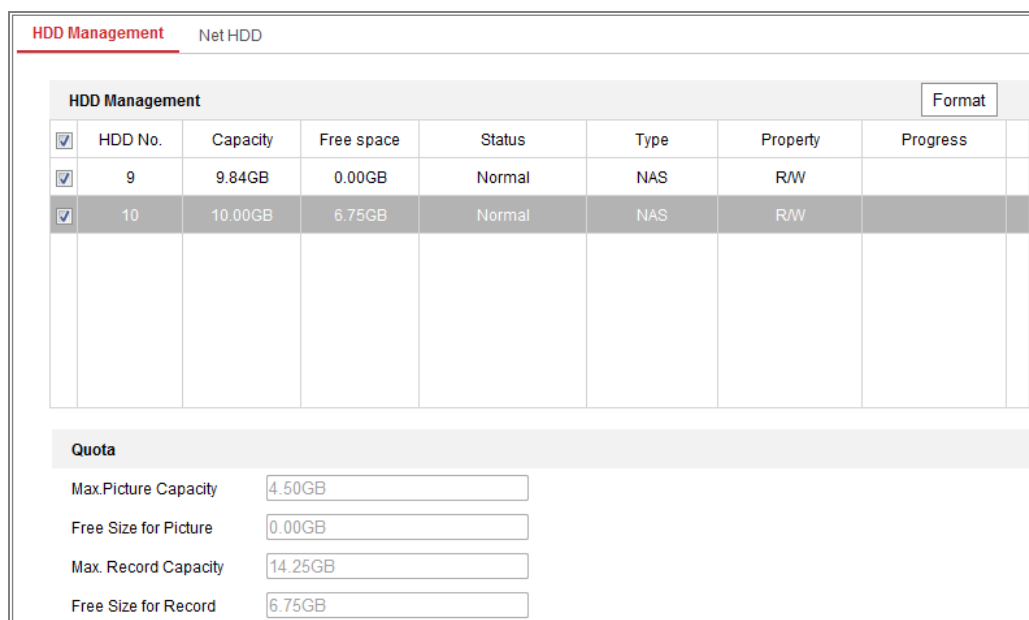


Figure 10-7 Storage Management Interface

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

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

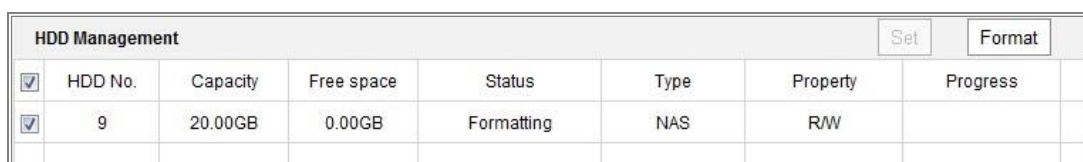


Figure 10-8 View Disk Status

3. Define the quota for record and pictures.

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

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

Quota	
Max. Picture Capacity	<input type="text" value="4.75GB"/>
Free Size for Picture	<input type="text" value="4.75GB"/>
Max. Record Capacity	<input type="text" value="14.50GB"/>
Free Size for Record	<input type="text" value="14.50GB"/>
Percentage of Picture	<input type="text" value="25"/> %
Percentage of Record	<input type="text" value="75"/> %


 Save

Figure 10-9 Quota Settings

**Note:**

Up to 8 NAS disks can be connected to the camera.

# Chapter 11 Playback

## Purpose:

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

## Steps:

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

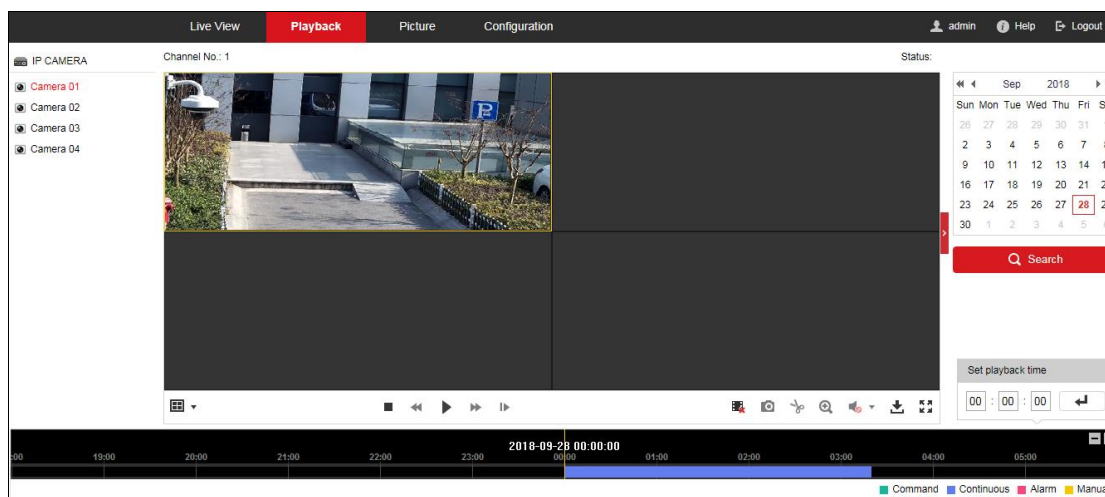


Figure 11-1 Playback Interface

2. Select the desired channel number.
3. Select the date and click **Search**.



Figure 11-2 Search Video

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

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

process.



Figure 11-3 Playback Toolbar

Table 11-1 Description of the buttons

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

**Note:** You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface.

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.

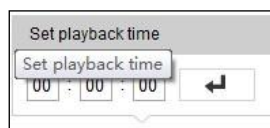


Figure 11-4 Set Playback Time

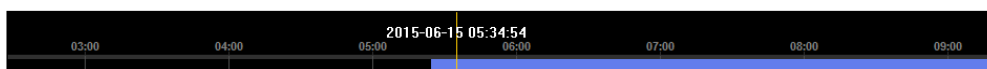


Figure 11-5 Progress Bar

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

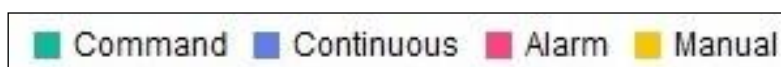


Figure 11-6 Video Types

## Chapter 12 Picture

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

### Notes:

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

The screenshot shows the 'Picture' tab in the interface. On the left, under 'Search Conditions', there are fields for 'Channel No.' (set to 'Camera 01'), 'File Type' (set to 'Continuous'), 'Start Time' (2015-07-02 00:00:00), and 'End Time' (2015-07-10 23:59:59). A red 'Search' button is at the bottom of this section. On the right, the 'File List' table displays 11 search results with columns for No., File Name, Time, File Size, and Progress. At the top right of the table are 'Download' and 'Stop Downloading' buttons.

No.	File Name	Time	File Size	Progress
1	ch01_08000000000068600	2015-07-10 15:35:13	134 KB	
2	ch01_08000000000068700	2015-07-10 15:35:18	134 KB	
3	ch01_08000000000068800	2015-07-10 15:35:24	134 KB	
4	ch01_08000000000068900	2015-07-10 15:35:29	132 KB	
5	ch01_08000000000069000	2015-07-10 15:35:34	132 KB	
6	ch01_08000000000069100	2015-07-10 15:35:39	133 KB	
7	ch01_08000000000069200	2015-07-10 15:35:45	133 KB	
8	ch01_08000000000069300	2015-07-10 15:35:50	131 KB	
9	ch01_08000000000069400	2015-07-10 15:35:55	131 KB	
10	ch01_08000000000069500	2015-07-10 15:36:01	132 KB	
11	ch01_08000000000069600	2015-07-10 15:36:06	132 KB	

Figure 12-1 Picture Search Interface

### Steps:

1. Select the desired channel number.
2. Select the file type from the dropdown list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection are selectable.
3. Select the start time and end time.
4. Click **Search** to search the matched pictures.
5. Check the checkbox of the pictures and then click **Download** to download the selected pictures.

### Note:

Up to 4000 pictures can be displayed at one time.



# Appendix

## Appendix 1 SADP Software Introduction

### ● Description of SADP

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

### ● Search active devices online

#### ◆ Search online devices automatically

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

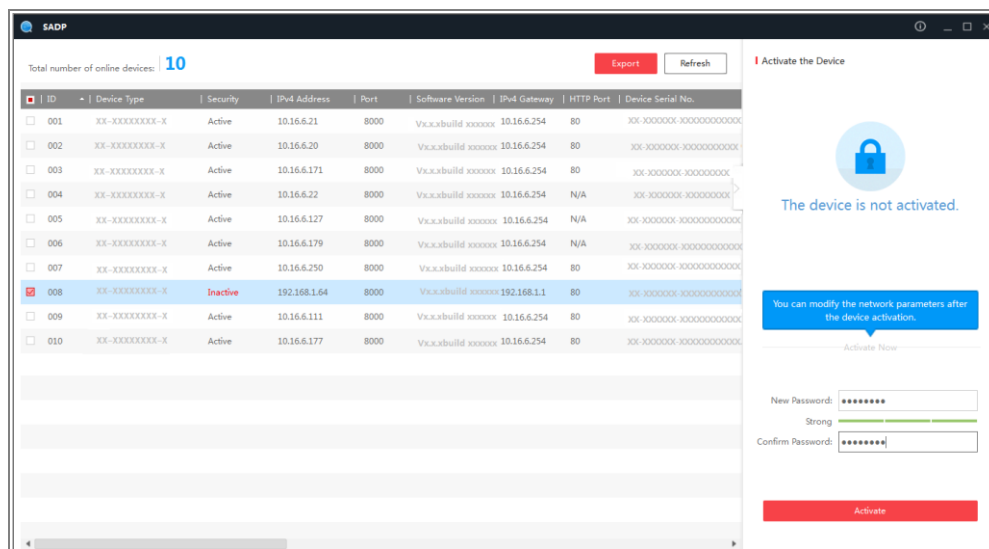



Figure A.1.1 Searching Online Devices





### **Note:**

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

#### ◆ Search online devices manually

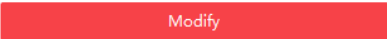
You can also click  to refresh the online device list manually. The newly searched devices will be added to the list.



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

## ● **Modify network parameters**

### *Steps:*

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

### Modify Network Parameters

Enable DHCP

Device Serial No.:

IP Address:

Port:

Subnet Mask:

Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

HTTP Port:

---

Security Verification

Admin Password:

[Modify](#)

[Forgot Password](#)

Figure A.1.2 Modify Network Parameters

## Appendix 2 Port Mapping

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

### Steps:

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

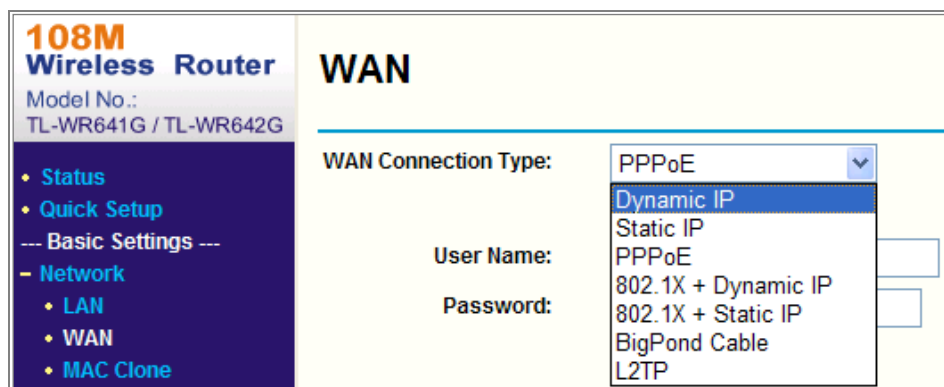


Figure A.2.1 Select the WAN Connection Type

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

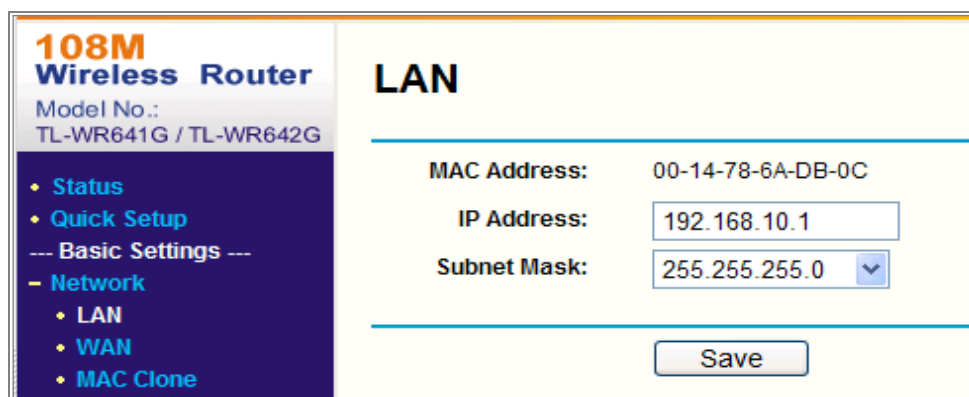


Figure A.2.2 Set the LAN parameters

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

### Example:

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

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

**Steps:**

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

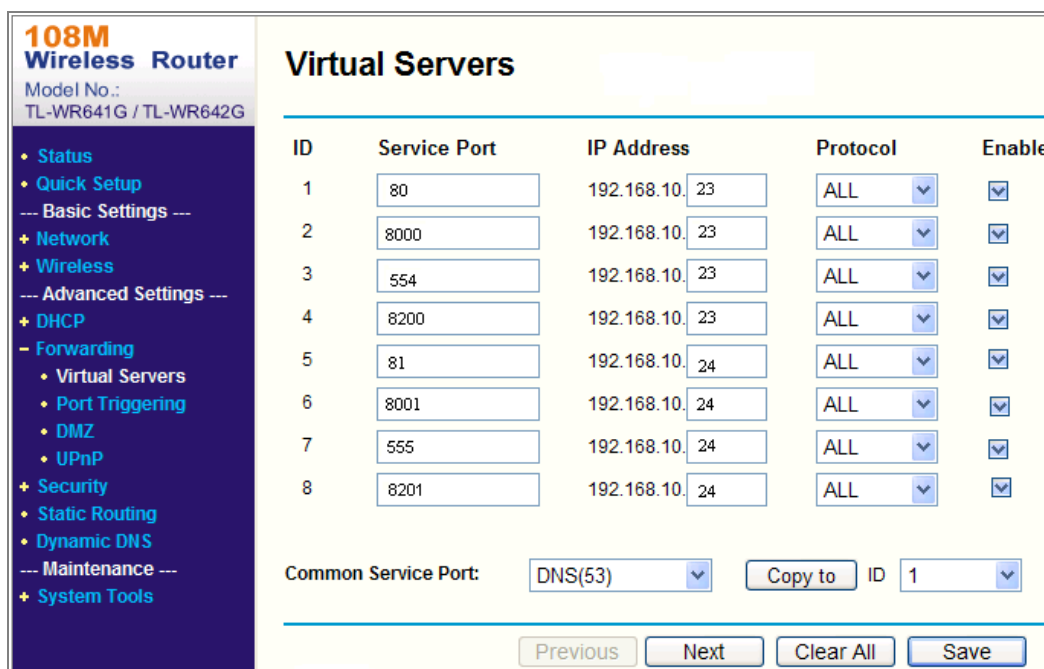


Figure A.2.3 Port Mapping

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



See Far, Go Further