
# Network Camera

## User Manual

UD15501B-A

# Initiatives on the Use of Video Products

## Thank you for choosing Hikvision products.

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

## Please read the following initiatives carefully:

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

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

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

# User Manual



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

## About this Manual

This Manual is applicable to Network 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 RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

**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.

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

 **Warnings:**

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

 **Cautions:**

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (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

# Chapter 1 System Requirement

**Operating System**

Microsoft Windows XP SP1 and above version

**CPU**

2.0 GHz or higher

**RAM**

1G or higher

**Display**

1024×768 resolution or higher

**Web Browser**

**For camera that supports plug-in free live view**

Internet Explorer 8 – 11, Mozilla Firefox 30.0 and above version and Google Chrome 41.0 and above version.

***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.

**For camera that does NOT support plug-in free live view**

Internet Explorer 8 – 11, Mozilla Firefox 30.0 – 51, and Google Chrome 41.0 – 44.

# 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.

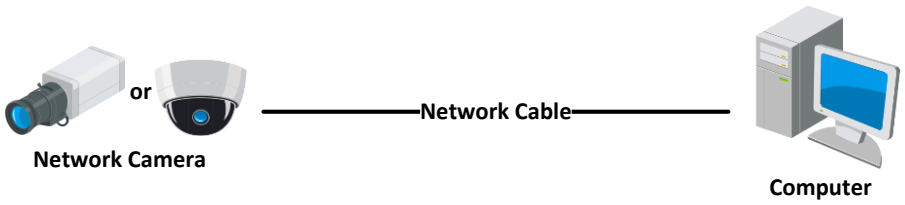



Figure 2-1 Connecting Directly

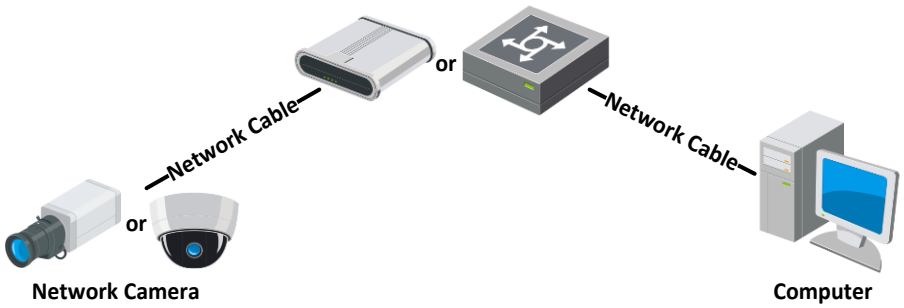



Figure 2-2 Connecting via a Switch or a Router

### 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.

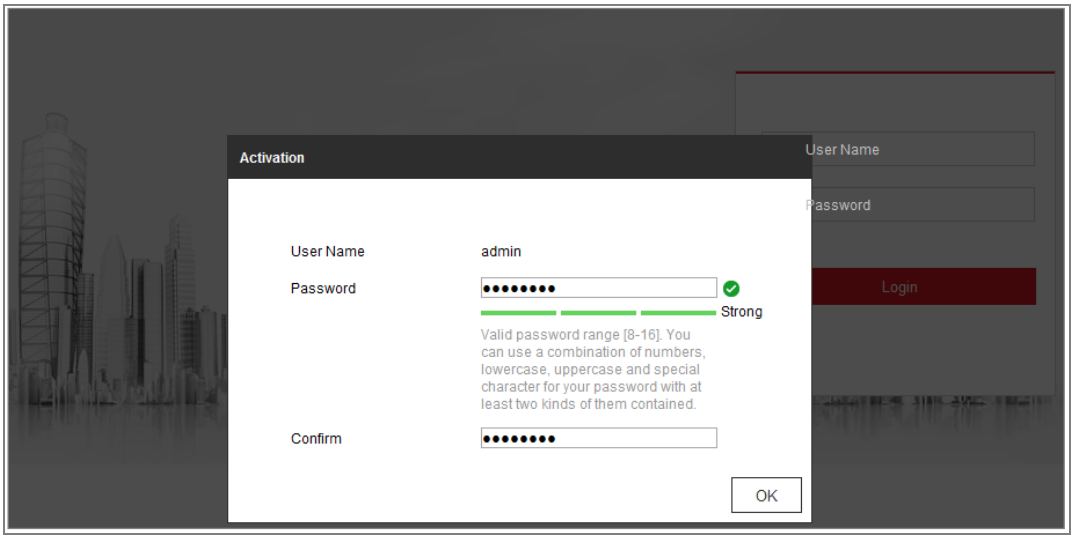



Figure 2-3 Activation via Web Browser

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.

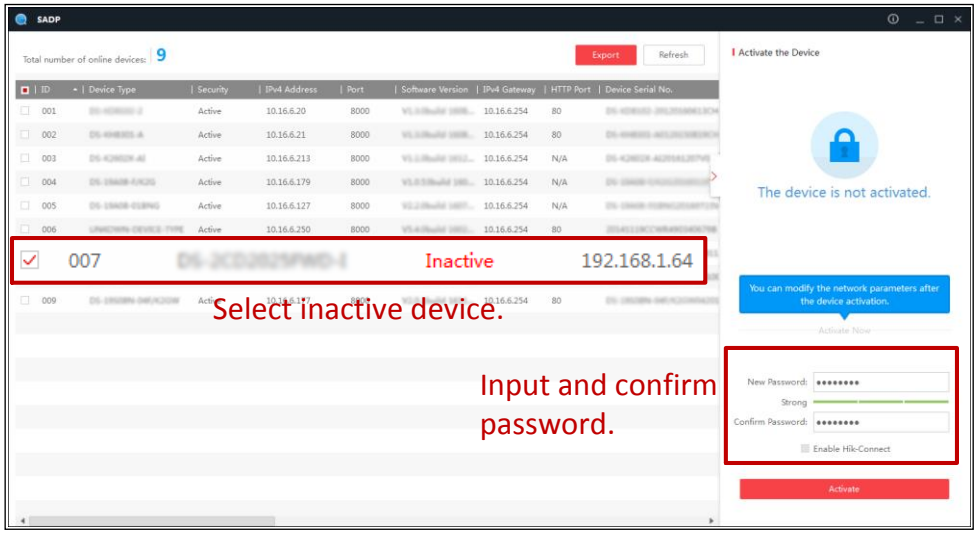



Figure 2-4 SADP Interface

***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.

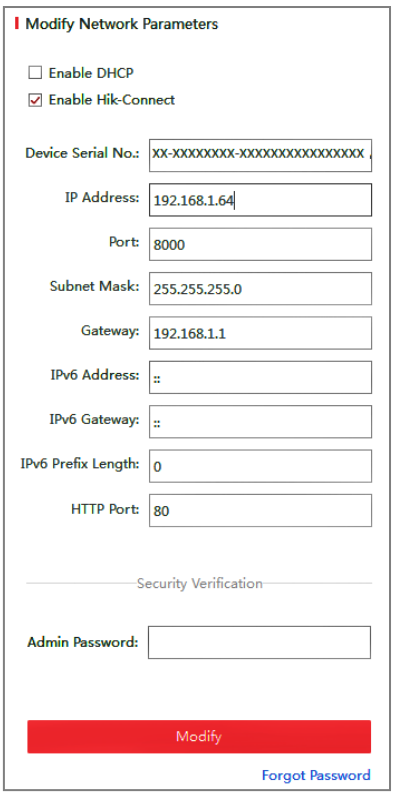



Figure 2-5 Modify the IP Address

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.

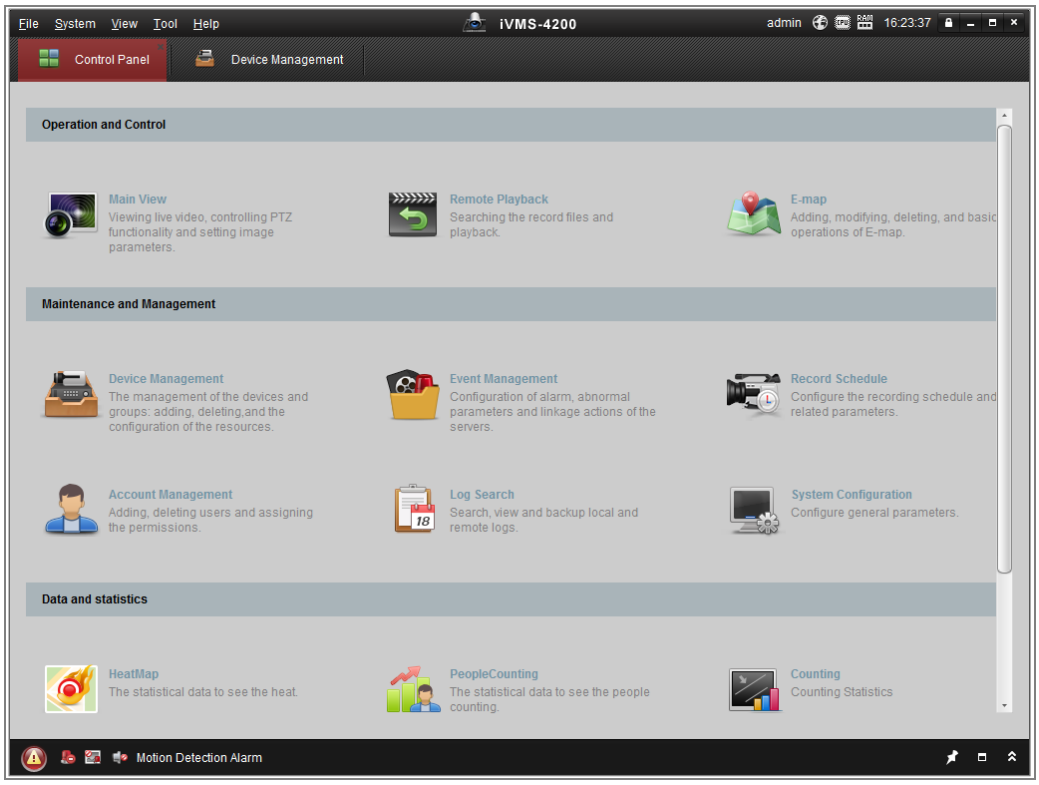



Figure 2-6 Control Panel

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

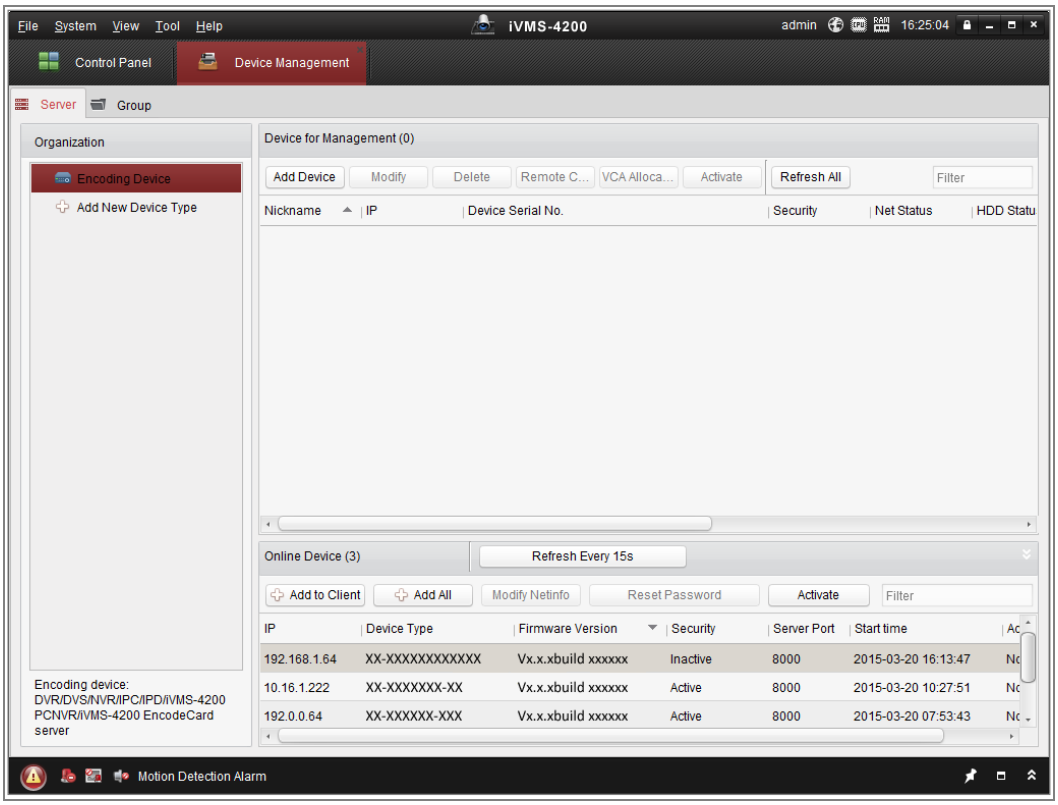



Figure 2-7 Device Management Interface

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.

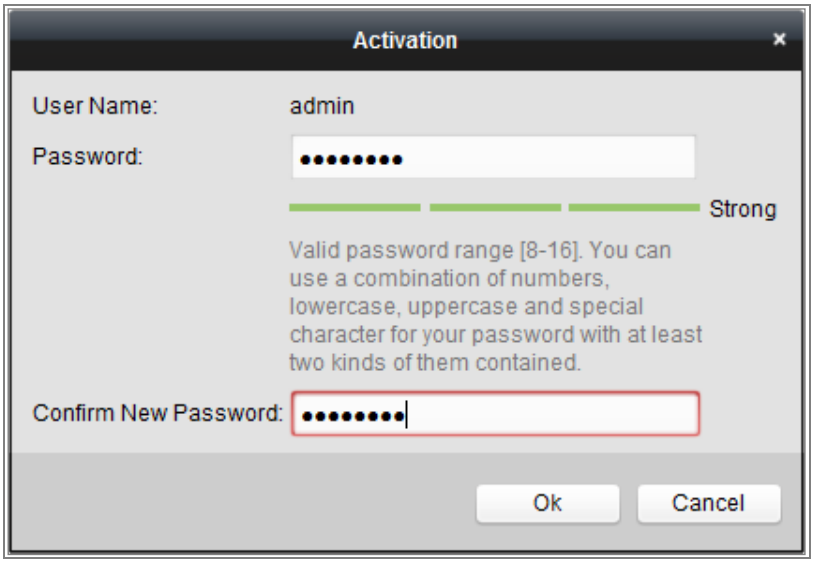



Figure 2-8 Activation Interface (Client Software)

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.

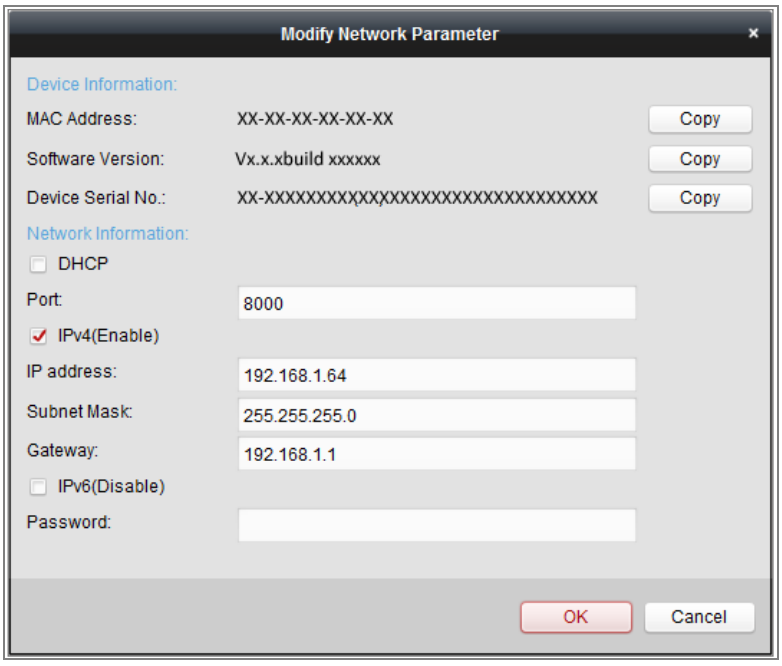



Figure 2-9 Modifying the Network Parameters

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.

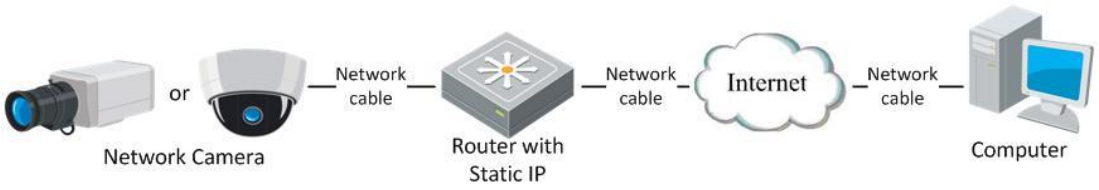



Figure 2-10 Accessing the Camera through Router with Static IP

- **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.

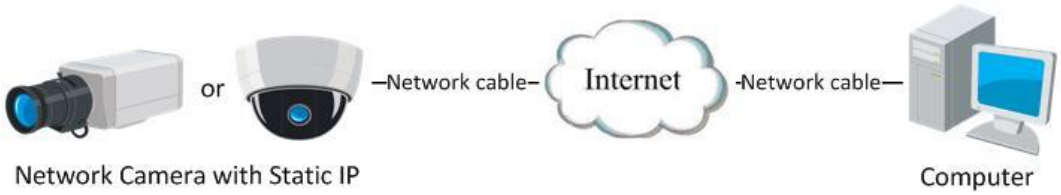



Figure 2-11 Accessing the Camera with Static IP Directly

### 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 7.1.3* ***Configuring PPPoE Settings*** for detailed configuration.

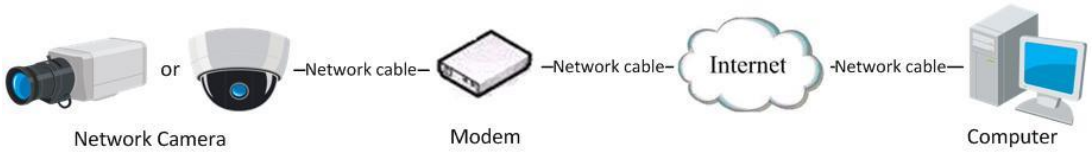



Figure 2-12 Accessing the Camera with Dynamic IP

***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

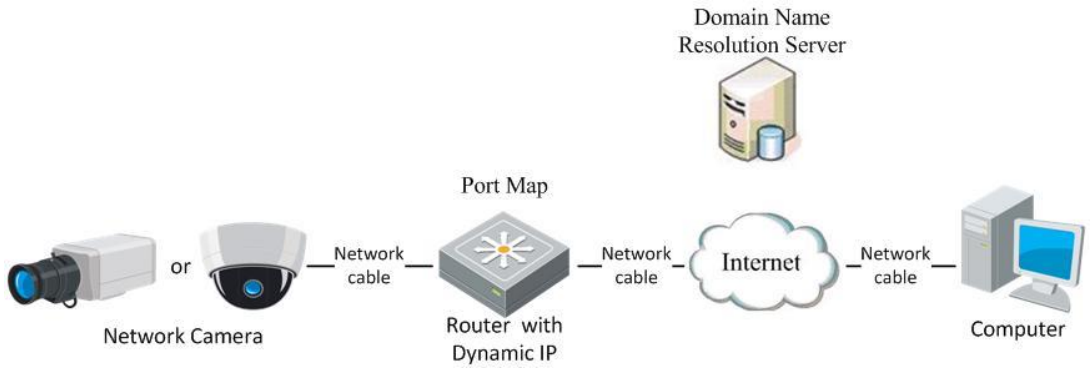



Figure 2-13 Normal Domain Name Resolution

***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 7.1.2* ***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 *7.2.5 HTTPS Settings.*

***Steps:***

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

   ***Note:***

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

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

   ***Note:***

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


Figure 3-1 Login Interface

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

***Note:***

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

## 3.2 Accessing by Client Software

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

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

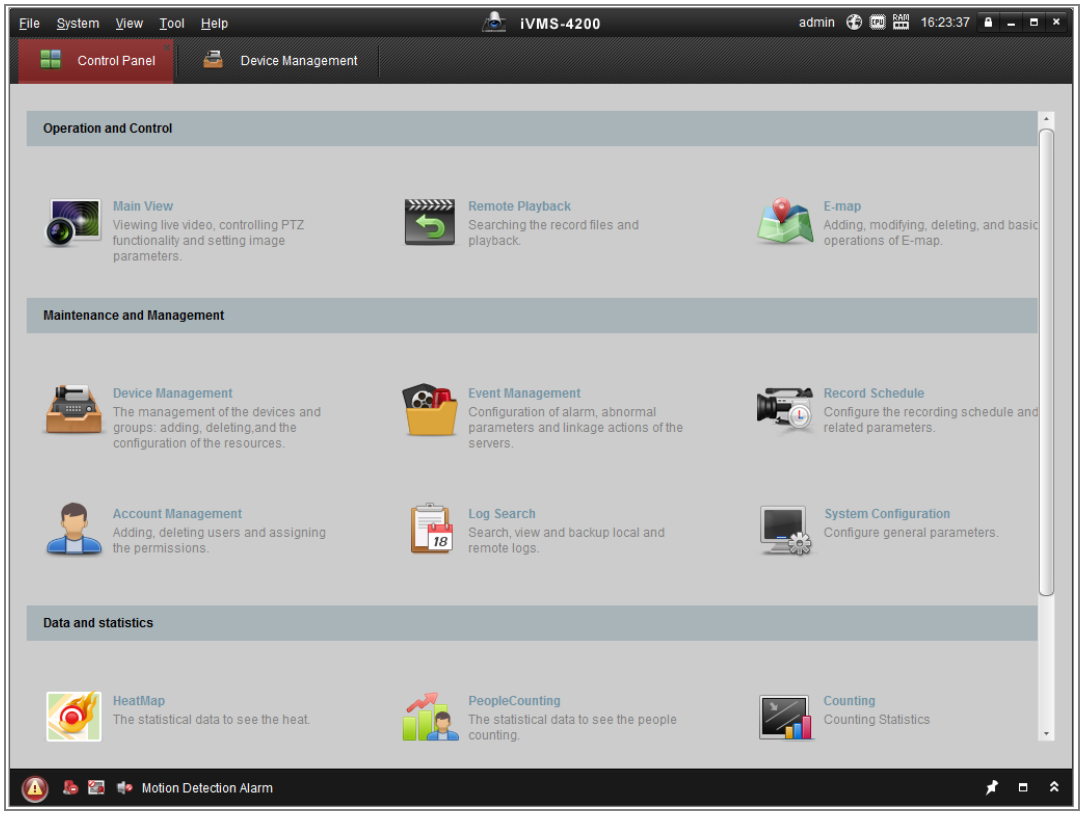


Figure 3-2 iVMS-4200 Control Panel

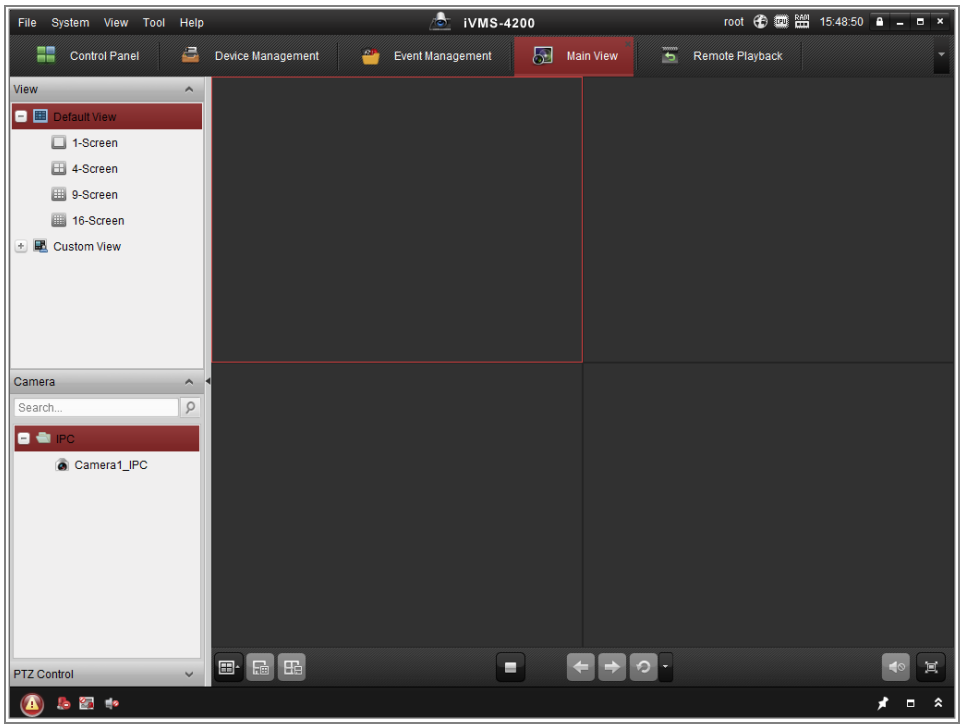



Figure 3-3 iVMS-4200 Main View

# Chapter 4 Wi-Fi Settings

***Purpose:***

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

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

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

***Purpose:***

Two connection modes are supported. Choose a mode as desired and perform the steps to configure the Wi-Fi.

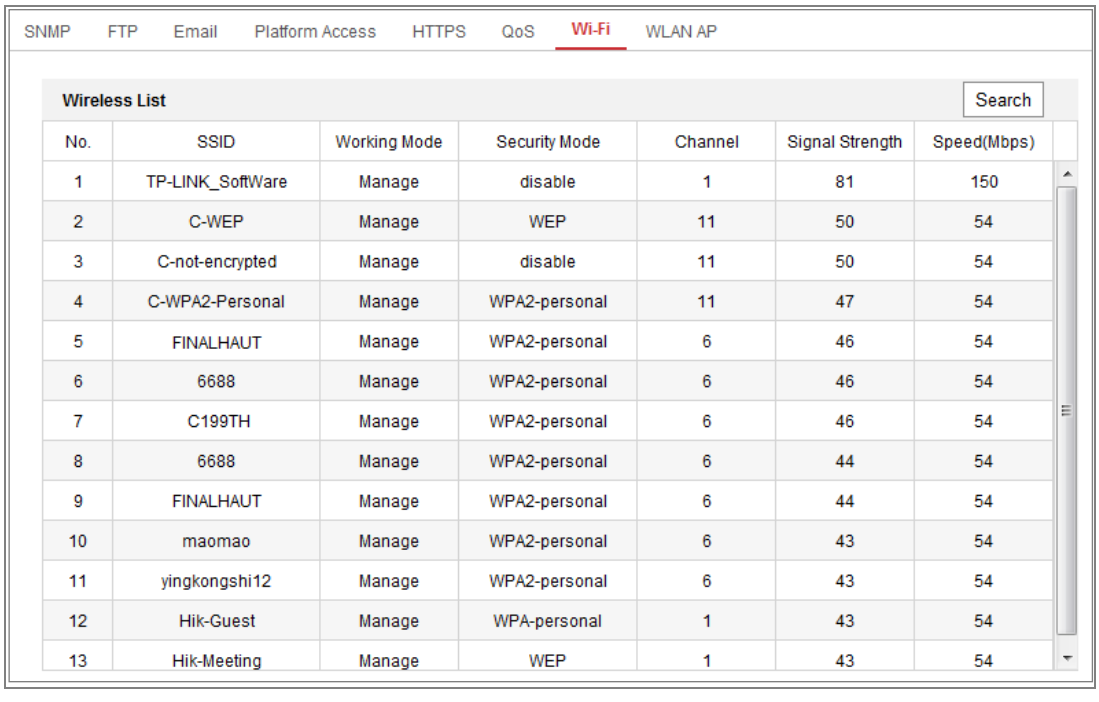
**Wireless Connection in Manage Mode**

***Steps:***

1. Enter the Wi-Fi configuration interface.

   **Configuration> Network> Advanced Settings> Wi-Fi**

2. Click **Search** to search the online wireless connections.




| No. | SSID | Working Mode | Security Mode | Channel | Signal Strength | Speed(Mbps) |
|---|---|---|---|---|---|---|
| 1 | TP-LINK_SoftWare | Manage | disable | 1 | 81 | 150 |
| 2 | C-WEP | Manage | WEP | 11 | 50 | 54 |
| 3 | C-not-encrypted | Manage | disable | 11 | 50 | 54 |
| 4 | C-WPA2-Personal | Manage | WPA2-personal | 11 | 47 | 54 |
| 5 | FINALHAUT | Manage | WPA2-personal | 6 | 46 | 54 |
| 6 | 6688 | Manage | WPA2-personal | 6 | 46 | 54 |
| 7 | C199TH | Manage | WPA2-personal | 6 | 46 | 54 |
| 8 | 6688 | Manage | WPA2-personal | 6 | 44 | 54 |
| 9 | FINALHAUT | Manage | WPA2-personal | 6 | 44 | 54 |
| 10 | maomao | Manage | WPA2-personal | 6 | 43 | 54 |
| 11 | yingkongshi12 | Manage | WPA2-personal | 6 | 43 | 54 |
| 12 | Hik-Guest | Manage | WPA-personal | 1 | 43 | 54 |
| 13 | Hik-Meeting | Manage | WEP | 1 | 43 | 54 |

Figure 4-1 Wi-Fi List

3. Click to choose a wireless connection on the list.

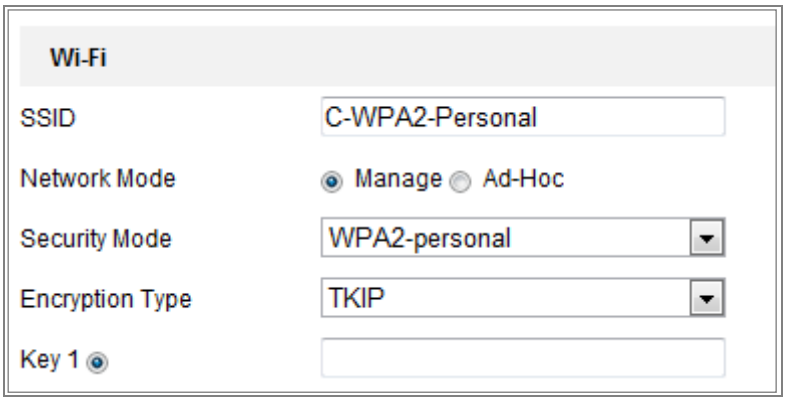



Figure 4-2 Wi-Fi Setting- Manage Mode

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

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

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

**Wireless Connection in Ad-hoc Mode**

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

***Steps:***

1. Choose Ad-hoc mode.

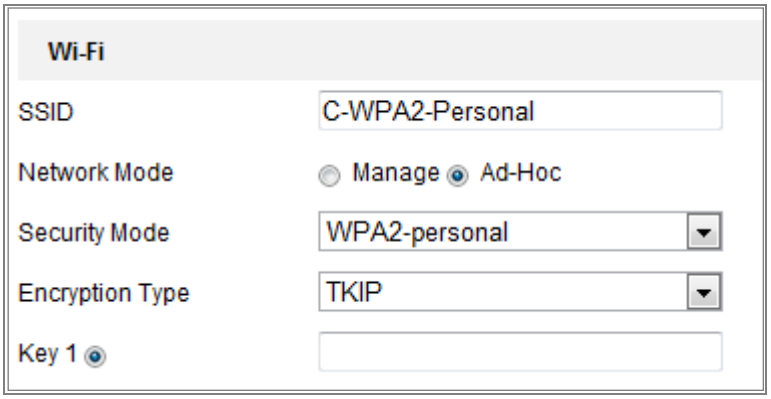



Figure 4-3 Wi-Fi Setting- Ad-hoc

2. Customize a SSID for the camera.
3. Choose the Security Mode of the wireless connection.
4. Enable the wireless connection function for your PC.
5. On the PC side, search the network and you can see the SSID of the camera listed.


Figure 4-4 Ad-hoc Connection Point

6. Choose the SSID and connect.

**Security Mode Description:**

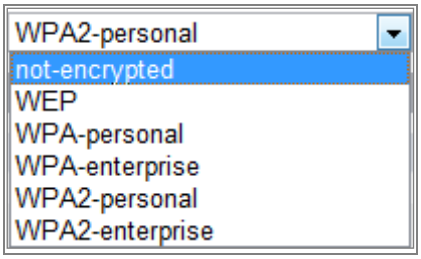



Figure 4-5 Security Mode

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

WEP mode:

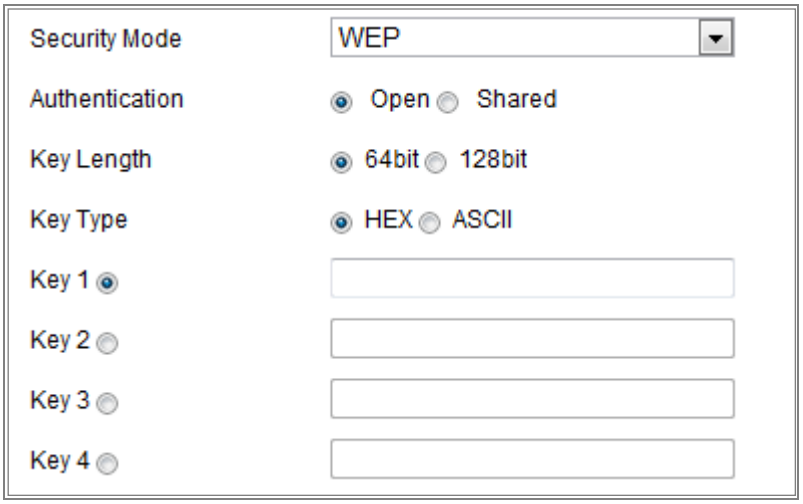



Figure 4-6 WEP Mode

- Authentication - Select Open or Shared Key System Authentication, depending on the method used by your access point. Not all access points have this option, in which case they probably use Open System, which is sometimes known as SSID Authentication.
- Key length - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key length can sometimes be shown as 40/64 and 104/128.
- Key type - The key types available depend on the access point being used. The following options are available:

  HEX - Allows you to manually enter the hex key.

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

WPA-personal and WPA2-personal Mode:

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

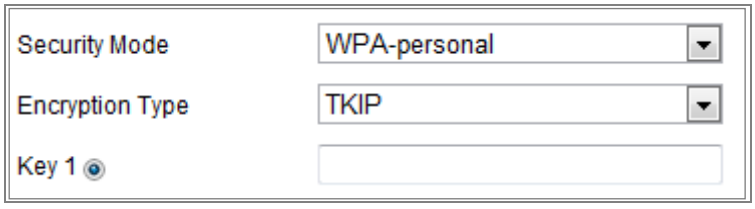



Figure 4-7 Security Mode- WPA-personal

WPA- enterprise and WPA2-enterprise Mode:

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

EAP-TLS

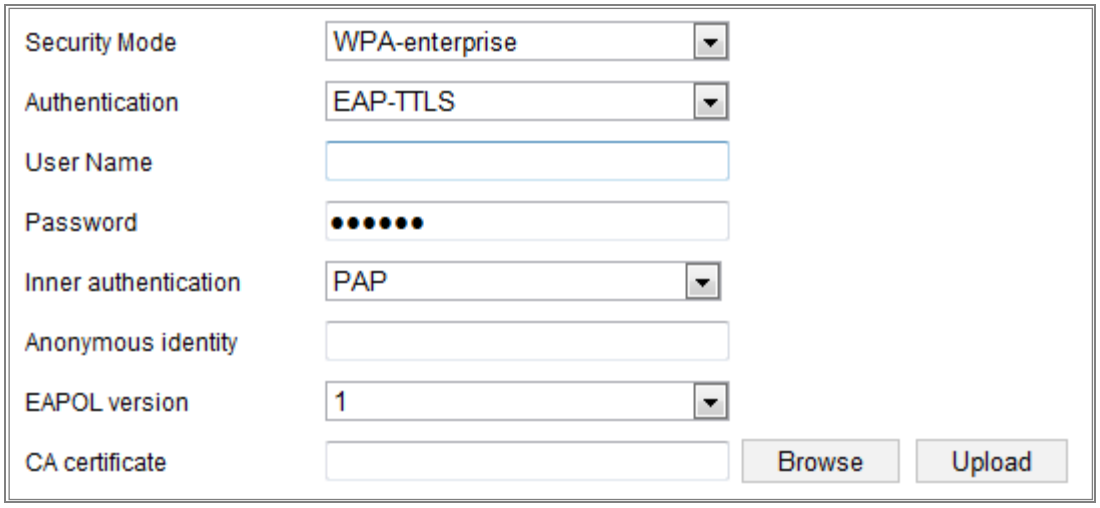



Figure 4-8 EAP-TLS

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

EAP-PEAP:

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

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

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

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

## 4.2 Easy Wi-Fi Connection with WPS function

***Purpose:***

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

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

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

***Steps:***

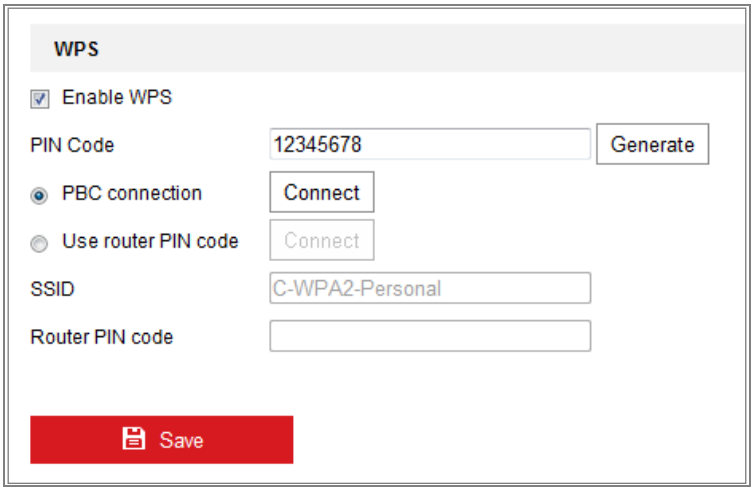
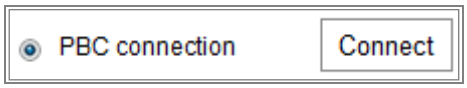



Figure 4-9 Wi-Fi Settings - WPS

***PBC*** Mode**:**

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

1. Check the checkbox of Enable WPS to enable WPS.
2. Choose the connection mode as PBC.




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

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

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

5. Click **Connect** button.

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

**PIN Mode:**

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

***Steps:***

1. Choose a wireless connection on the list and the SSID is loaded automatically.
2. Choose **Use route PIN code**.

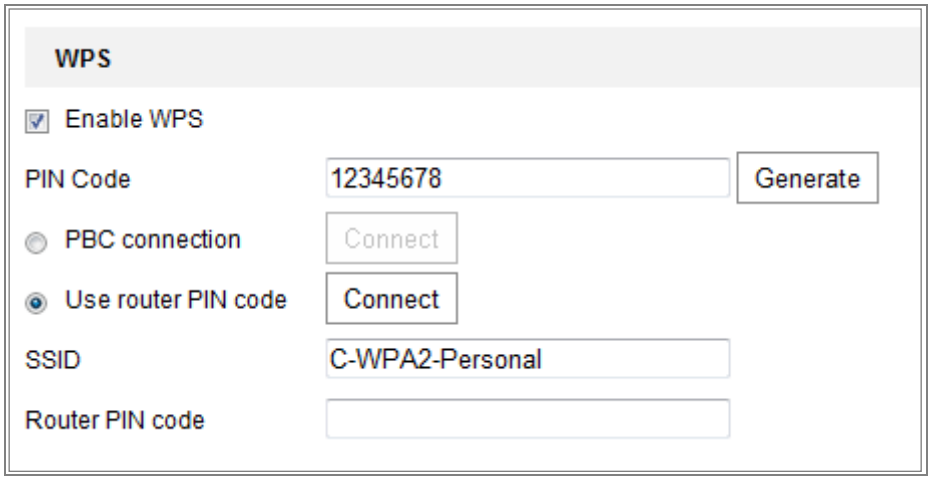



Figure 4-10 Use PIN Code

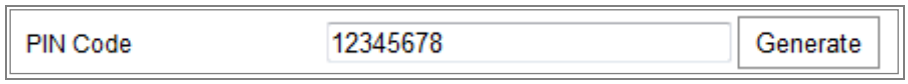
If the PIN code is generated from the router side, you should enter the PIN code you get from the router side in the **Router PIN code** field.

3. Click **Connect**.

Or

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

1. Click **Generate**.




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

## 4.3 IP Property Settings for Wireless Network Connection

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

***Steps:***

1. Enter the TCP/IP configuration interface.

   Configuration> Network> Basic Settings > TCP/IP

2. Select the Wlan tab.

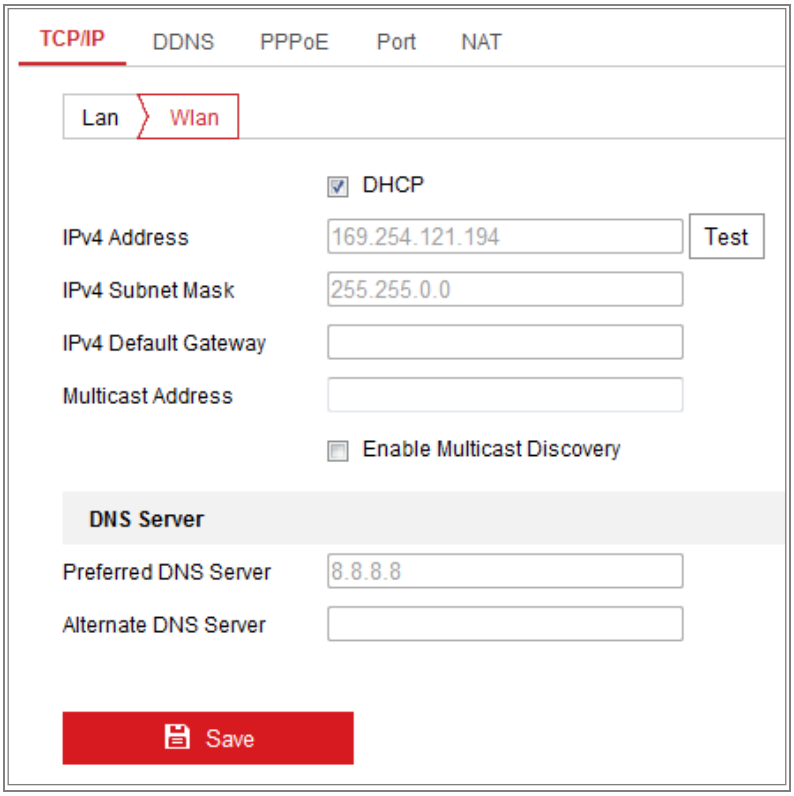



Figure 4-11 Setting WLAN Parameters

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

   The setting procedure is the same with that of LAN.

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

# Chapter 5 Live View

## 5.1 Live View Page

***Purpose:***

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

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

**Descriptions of the live view page:**

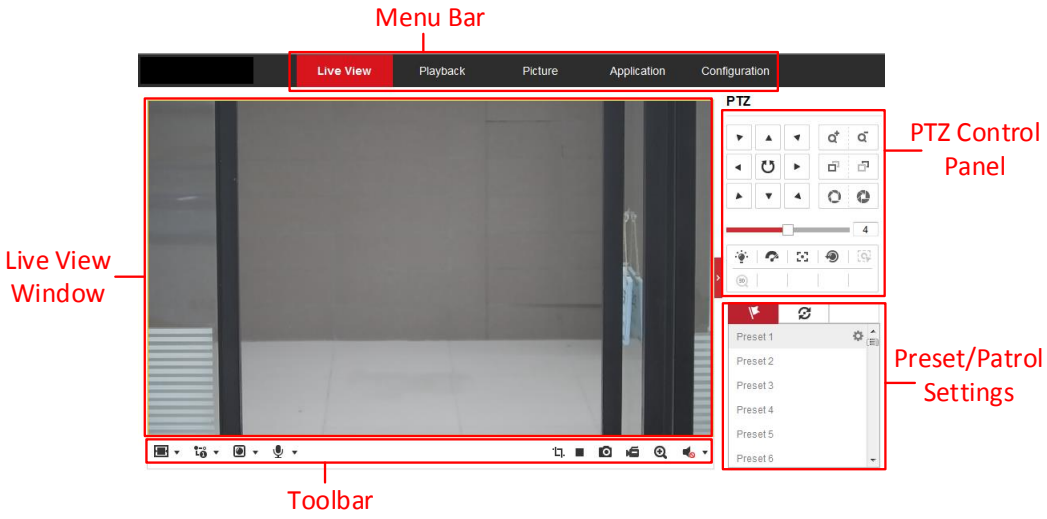



Figure 5-1 Live View Page

**Menu Bar:**

Click each tab to enter Live View, Playback, Picture, Application, 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:***

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

## 5.2 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.

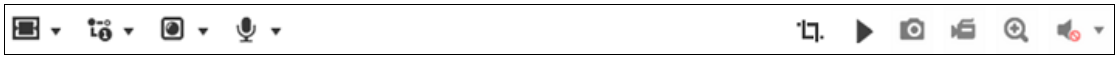


Figure 5-2 Live View Toolbar

Table 5-1 Descriptions of the Toolbar

| Icon | Description |
|---|---|
| ▶/■ | Start/Stop live view. |
| 4:3 | The window size is 4:3. |
| 16:9 | The window size is 16:9. |
| 1× | The original widow size. |
| | Self-adaptive window size. |
| , , , etc. | Live view with the different video streams.<br>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. |
| / | Start/stop pixel counter |

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

**Pixel Counter:**

1. Click **Start Pixel Counter** button to enable the function.
2. Drag the mouse on the image to select the desired rectangle area. The width pixel and height pixel is displayed on the bottom of the web.
3. Click the button again to stop the function.

***Note:***

The pixel counter is only supported under the main stream and only one rectangle are supported.

## 5.3 Recording and Capturing Pictures Manually

In the live view interface, click on the toolbar to capture the live pictures or click to record the live view. The saving paths of the captured pictures and clips can be set on the **Configuration > Local** 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.

## 5.4 Live View Quick Setup

It allows quick setup of image/video related parameters on live view page.

***Steps:***

1. Click button on the right of the live view window to show the PTZ control

panel. Click  to hide it.

2. Specify PTZ, Display, OSD and Video/Audio and VCA resource parameters. For more settings, go to **Configuration** > **Image** and **Configuration** > **Video/Audio**.

- **Display Settings**
  - **Scene:** Select a scene according to actual installation environment. (Only certain camera models support.)
  - **WDR:** The WDR (Wide Dynamic Range) function helps the camera provide clear images even under back light circumstances. When there are both very bright and very dark areas simultaneously in the field of view, WDR balances the brightness level of the whole image and provide clear images with details. You can enable or disable the WDR function and set the level.
  - **HLC:** High Light Compensation makes the camera identify and suppress the strong light sources that usually flare across a scene. This makes it possible to see the detail of the image that would normally be hidden.
- **OSD (On Screen Display)**

  Set text information displayed on screen. Alignment adjustment is available for Text Overlay. Save the settings after configuration.
- **Video/Audio**

  Resolution and Max. Bit rate are adjustable. Click  to change stream.
- **VCA Resource**

  VCA Resource offers options to enable certain VCA functions and hide others. It helps allocate more resources to the wanted functions. A reboot is required after setting the VCA Resource.

  ***Note:***
  - VCA Resource function varies according to different camera models.
  - VCA options are mutually exclusive.
  - The function may not be supported by some camera models.

# 5.5 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 6.2.4* ***RS485 Settings***.

## 5.5.1 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.

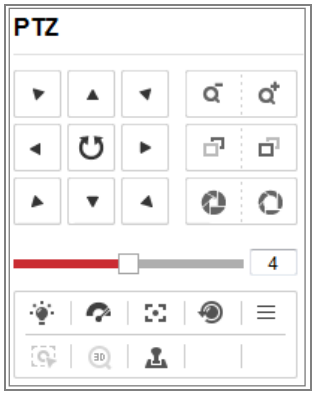



Figure 5-3 PTZ Control Panel

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 5-2 Descriptions of PTZ Control Panel

| Icon | Description |
|---|---|

| | |
|---|---|
| | Zoom in/out |
| | Focus near/far |
| | Iris +/- |
| 4 | 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 |

## 5.5.2 Setting/Calling a Preset

- **Setting a Preset:**

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

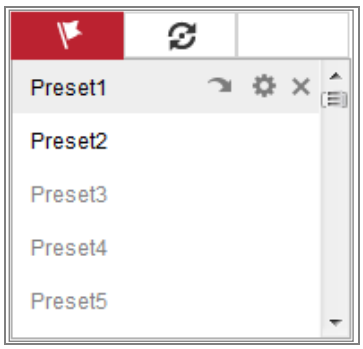



Figure 5-4 Setting a Preset

4. 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.
5. Click to finish the setting of the current preset.
6. 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.

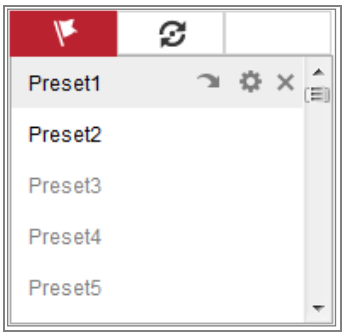



Figure 5-5 Calling a Preset

### 5.5.3 Setting/Calling a Patrol

***Note:***

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

***Steps:***

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

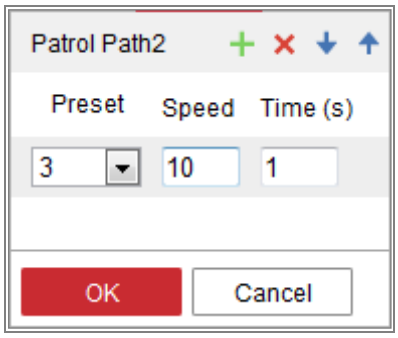



Figure 5-6 Add Patrol Path

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

# Chapter 6 Network Camera Configuration

## 6.1 Configuring Local Parameters

***Purpose:***

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

***Steps:***

1. Enter the Local Configuration interface: **Configuration** > **Local**.
2. Configure the following settings:

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

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

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

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

    **MULTICAST:** It's recommended to select 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 live view performance to Shortest Delay, Balanced, Fluent or Custom. For Custom, you can set the frame rate for live view.
  - **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.

- **Display POS Information:** Enable the function, feature information of the detected target is dynamically displayed near the target in the live image. The feature information of different functions are different. For example, ID and waiting time for Queue Management, height for People Counting, etc.

  ***Note:***

  Display POS Information is only available for certain camera models.

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

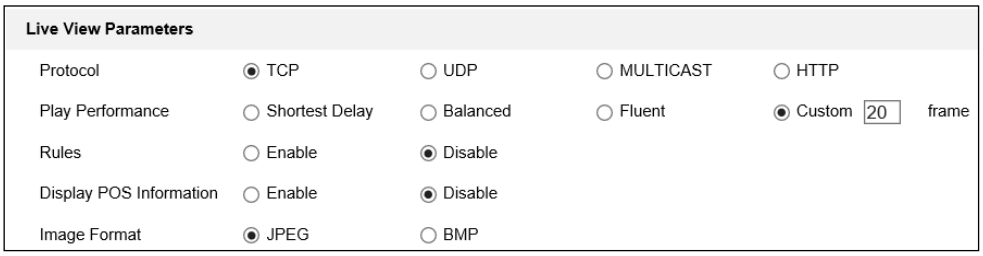



Figure 6-1 Live View Parameters

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

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

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

# 6.2 Configure System Settings

***Purpose:***

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

## 6.2.1 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.

## 6.2.2 Configuring Time Settings

***Purpose:***

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

***Steps:***

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

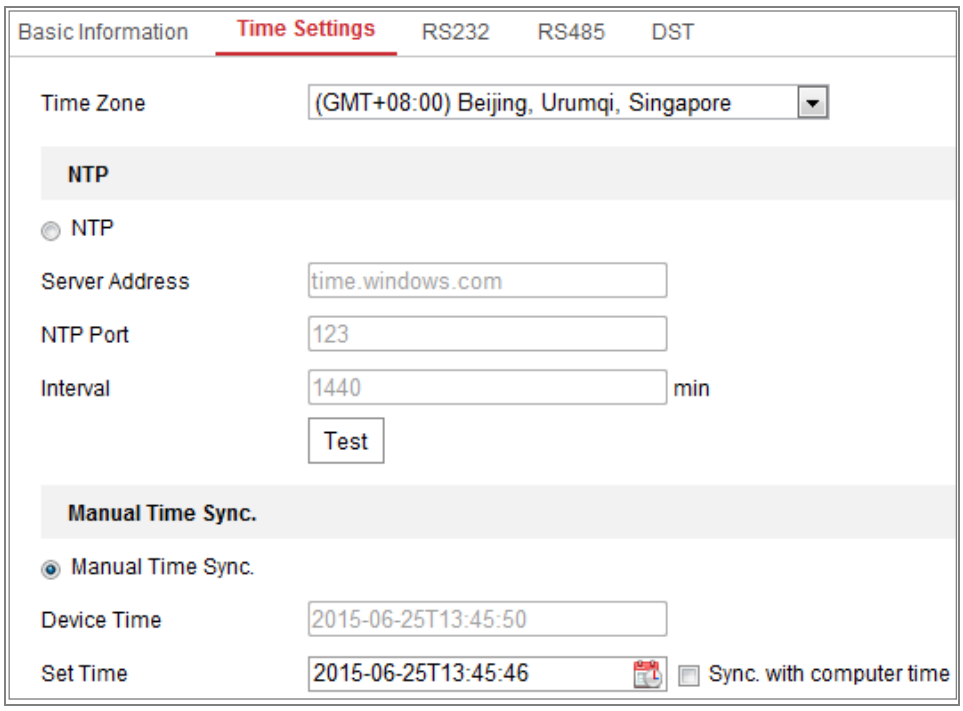



Figure 6-2 Time Settings

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

(1) Click to enable the **NTP** function.

(2) Configure the following settings:

**Server Address:** IP address of NTP server.

**NTP Port:** Port of NTP server.

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

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

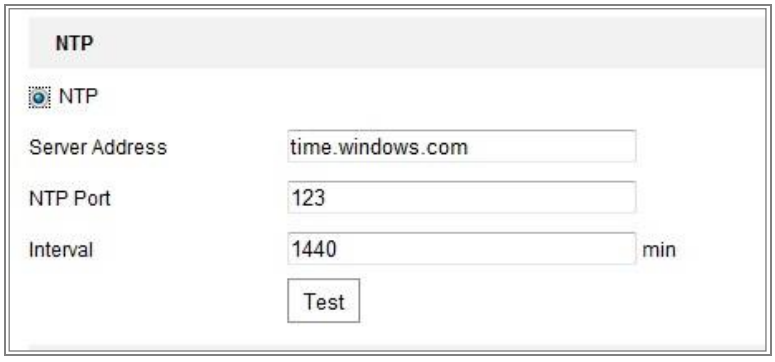



Figure 6-3 Time Sync by NTP Server

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

- 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 6-4 Time Sync Manually

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

## 6.2.3 Configuring RS232 Settings

The RS232 port can be used in two ways:

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

***Steps:***

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

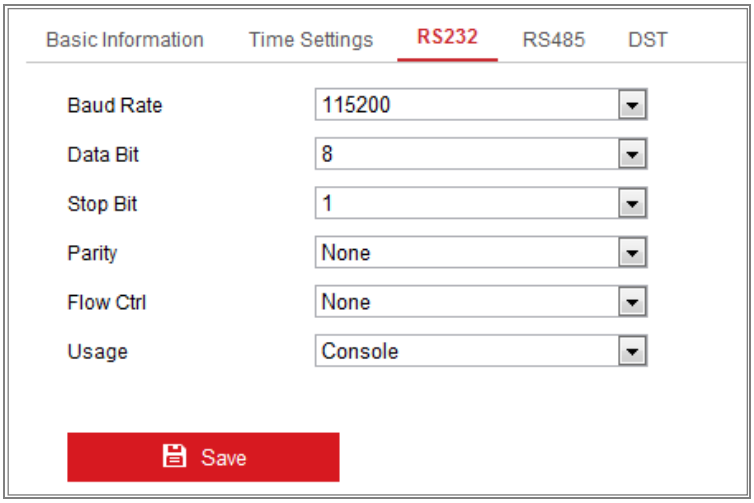



Figure 6-5 RS232 Settings

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

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

### 6.2.4 Configuring RS485 Settings

***Purpose:***

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

***Steps:***

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

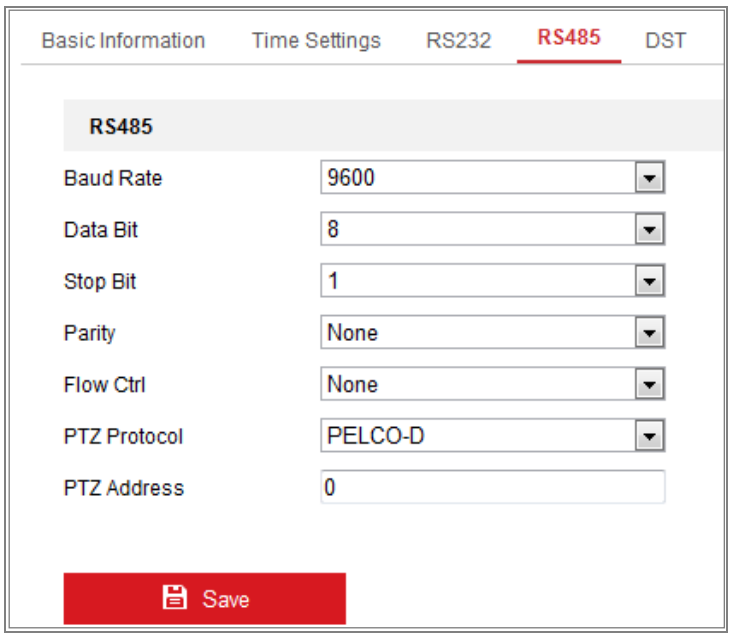



Figure 6-6 RS-485 Settings

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

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

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

### 6.2.5 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**

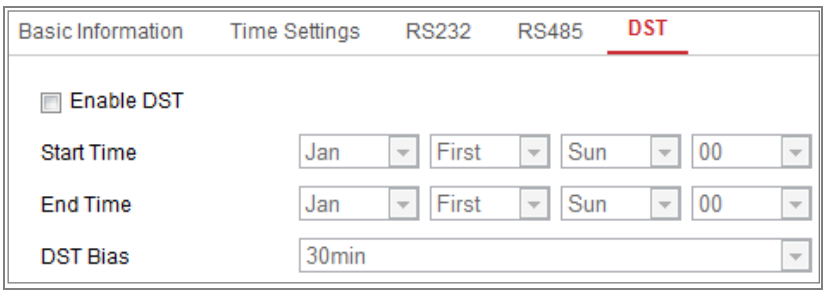



Figure 6-7 DST Settings

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

### 6.2.6 Configuring External Devices

***Purpose:***

For the device supported external devices, including the wiper on the housing or the LED light, you can control them via the Web browser. External devices vary according to the different camera models.

***Steps:***

1. Enter the External Device configuration interface.

   **Configuration** > **System** > **System Settings** > **External Device**

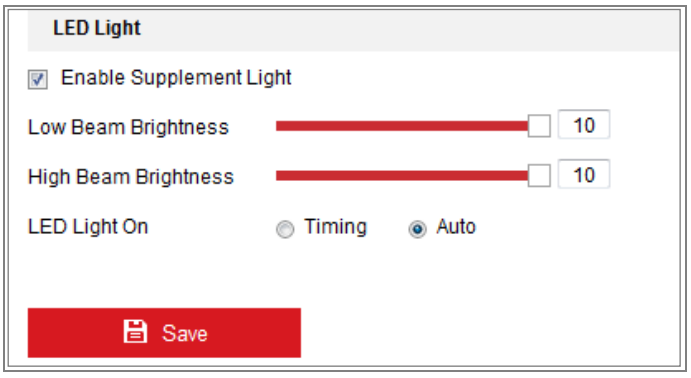



Figure 6-8 External Device Settings

2. Check the Enable Supplement Light checkbox to enable the LED Light.
3. Move the slider to adjust the low beam brightness and high bean brightness.
4. Select the mode for LED light. Timing and Auto are selectable.
   - **Timing:** The LED will be turned on by the schedule you set. You should set

the Start Time and End Time.

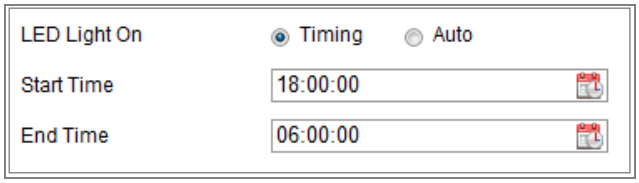



Figure 6-9 Set Schedule

- **Auto:** The LED will be turned on according to the environment illumination.

5. Click Save to save the settings.

### 6.2.7 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.**

## 6.3 Maintenance

### 6.3.1 Upgrade & Maintenance

***Purpose:***

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

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

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

  ***Notes:***

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

- For camera that supports Wi-Fi, wireless dial, or wlan function, **Restore** action does not restore the related settings of mentioned functions to default.

- **Information Export**

  **Device Parameters:** click to export the current configuration file of the camera. This operation requires admin password to proceed.

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

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

- **Import Config. File**

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

  ***Steps:***

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

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

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

  ***Steps:***

  1. Select firmware or firmware directory to locate the upgrade file.

     Firmware: Locate the exact path of the upgrade file.

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

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

### 6.3.2 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**.

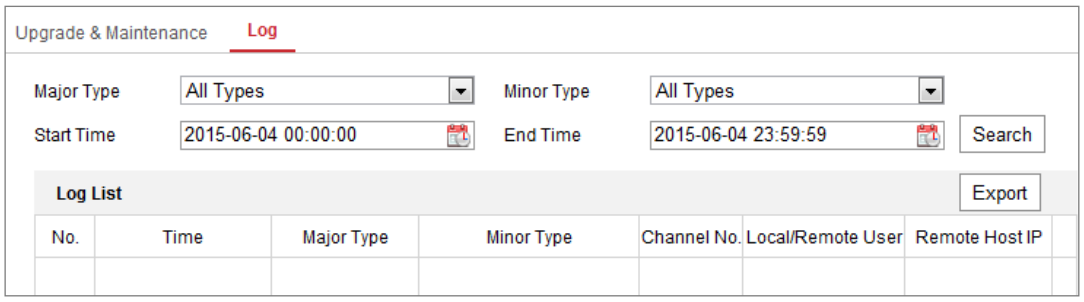



Figure 6-10 Log Searching Interface

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.

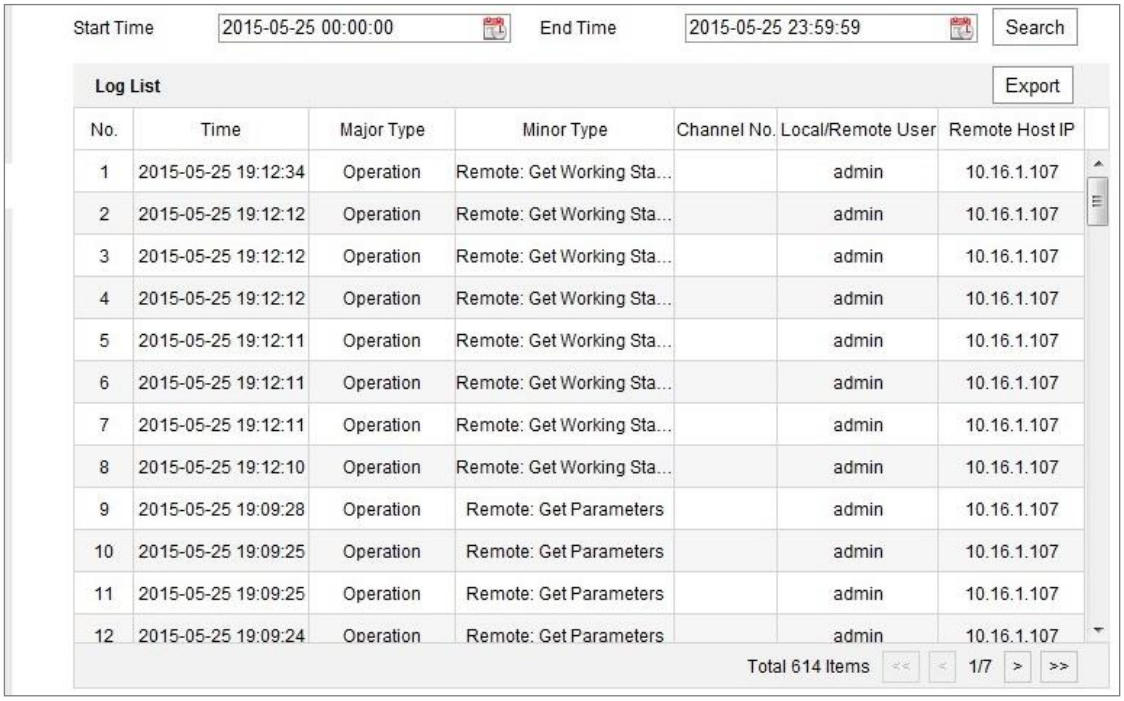



Figure 6-11 Log Searching

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

### 6.3.3 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.

## 6.4 Security Settings

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

### 6.4.1 Authentication

***Purpose:***

You can specifically secure the stream data of live view.

***Steps:***

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

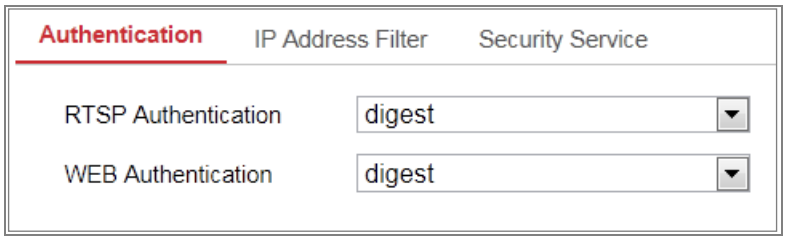


Figure 6-12 Authentication

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

   ***Caution:***

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

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

### 6.4.2 IP Address Filter

***Purpose:***

This function makes it possible for access control.

***Steps:***

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

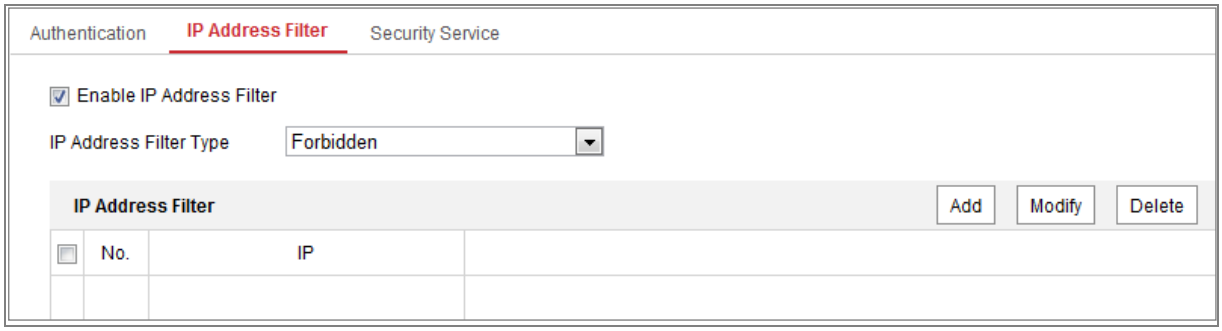



Figure 6-13 IP Address Filter Interface

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

     ***Steps:***

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

     (2) Input the IP Adreess.


Figure 6-14 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 6-15 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.

### 6.4.3 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**.

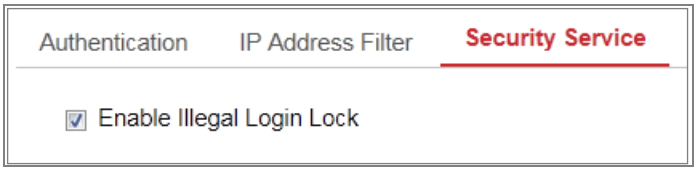



Figure 6-16 Security Service

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.

# 6.5 User Management

## 6.5.1 User Management

- **As Administrator**

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

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

  ***Note:***

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

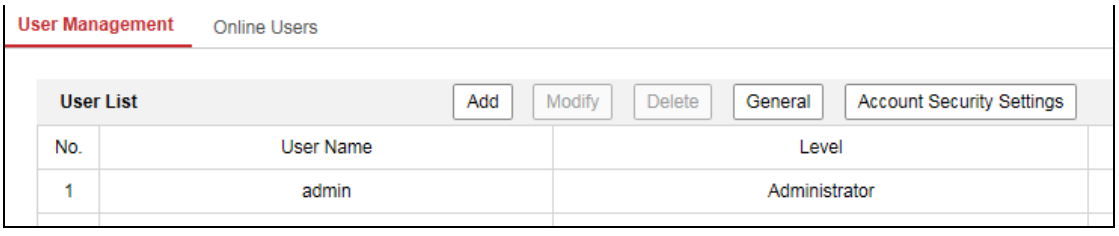



**Figure 6-17** User Management Interface

- **Adding a User**

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

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

***Steps:***

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

   ***Notes:***

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

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

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

- **Modifying a User**

***Steps:***

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

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

3. You can check or uncheck the permissions.

4. Click **OK** to finish the user modification.

- **Deleting a User**

***Steps:***

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

- **Setting Simultaneous Login**

***Steps:***

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

- **As Operator or User**

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

### 6.5.2 Online Users

***Purpose:***

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

Click **Refresh** to refresh the list.

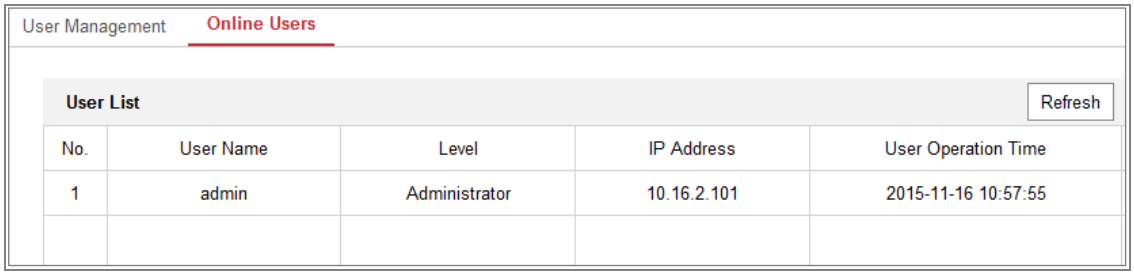



Figure 6-18 View the Online Users

# Chapter 7 Network Settings

***Purpose:***

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

## 7.1 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.

### 7.1.1 Configuring TCP/IP Settings

***Purpose:***

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

***Steps:***

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

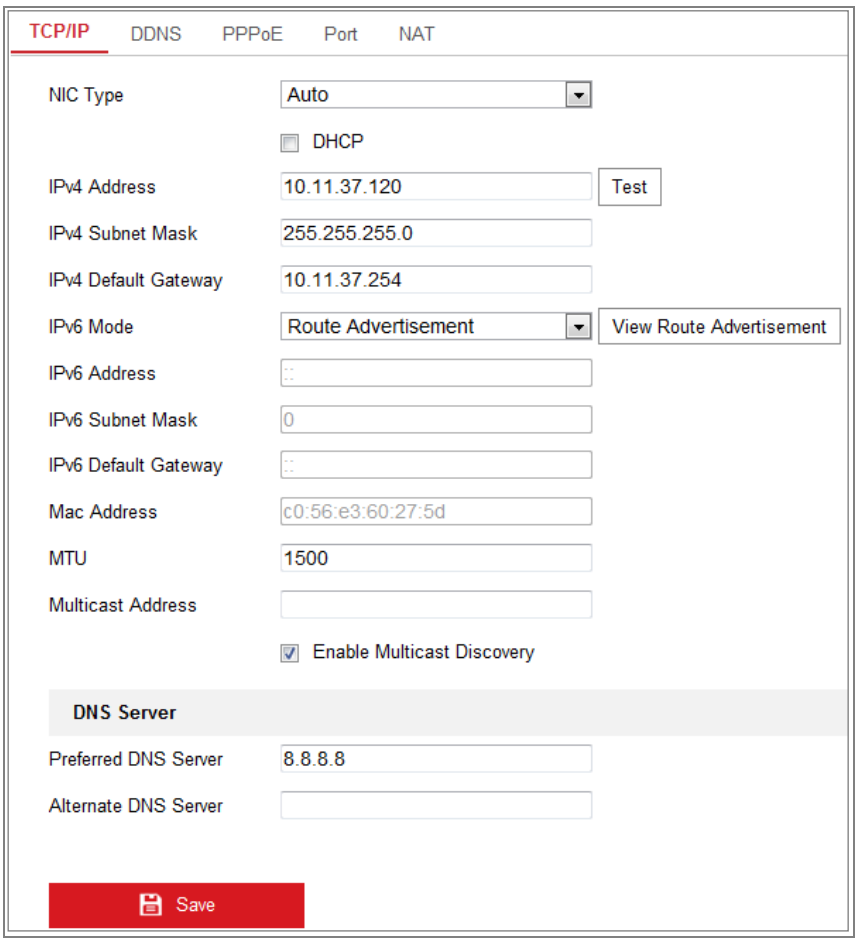



Figure 7-1 TCP/IP Settings

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

***Notes*:**

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

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

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

### 7.1.2 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.

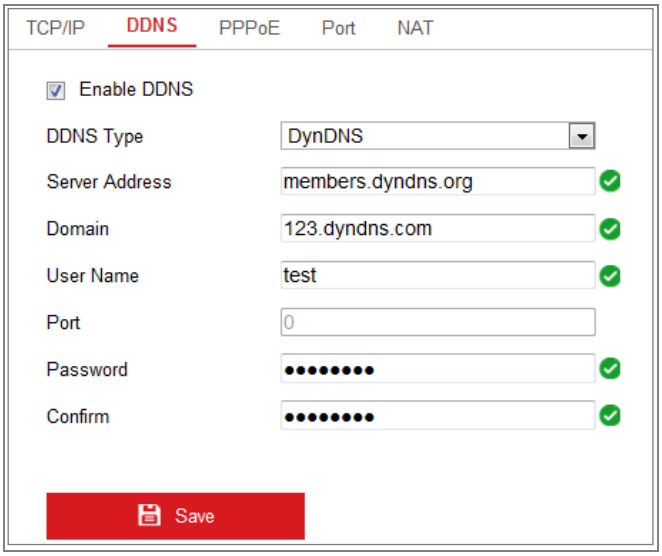



Figure 7-2 DynDNS Settings

- NO-IP:

***Steps:***

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

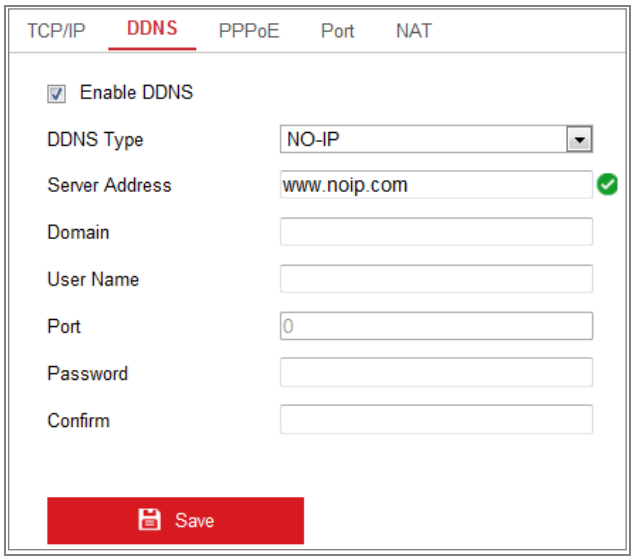



Figure 7-3 NO-IP DNS Settings

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

(3) Enter the Domain name you registered.

(4) Enter the User Name and Password.

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

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

### 7.1.3 Configuring PPPoE Settings

***Steps:***

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

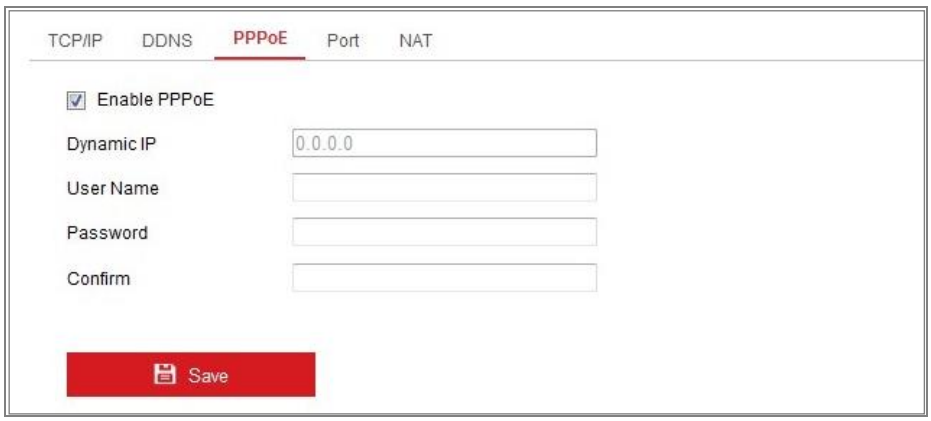



Figure 7-4 PPPoE Settings

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.

### 7.1.4 Configuring Port Settings

***Purpose:***

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

***Steps:***

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

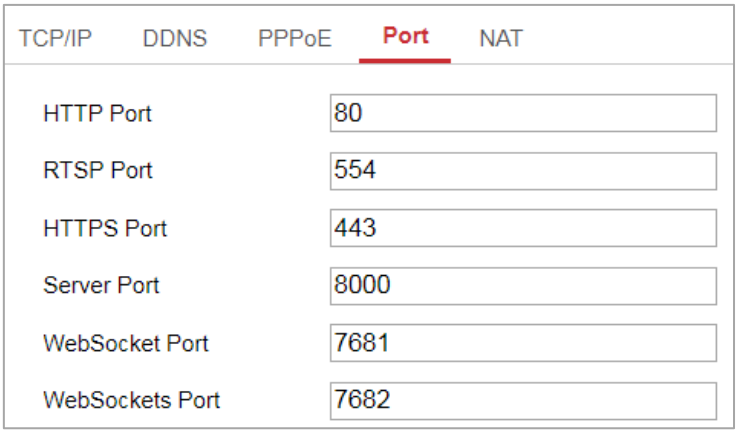



Figure 7-5 Port Settings

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 *7.2.9*.

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

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

### 7.1.5 Configure NAT (Network Address Translation) Settings

***Purpose:***

NAT interface allows you to configure the UPnP™ parameters.

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

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

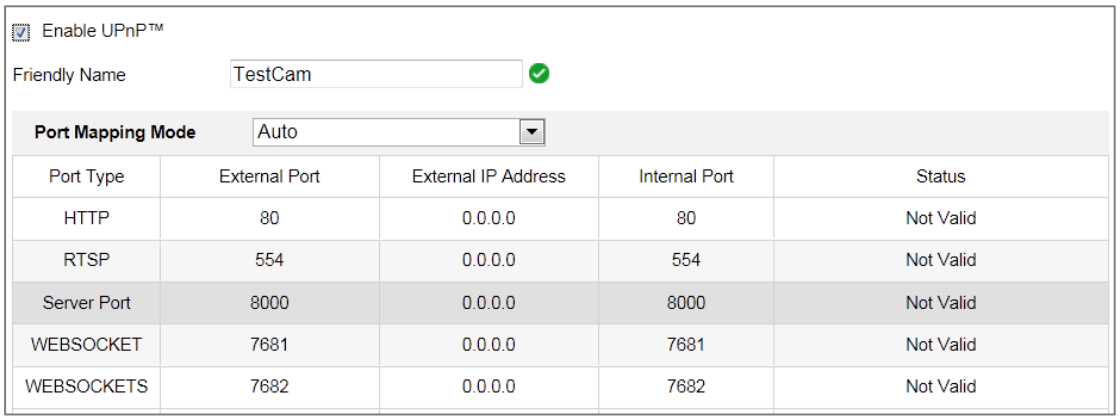



Figure 7-6 UPnP Settings

***Steps:***

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

***Note:***

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

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

   ***Note:***

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

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

## 7.2 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.

### 7.2.1 Configuring SNMP Settings

***Purpose:***

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

***Before you start:***

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

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

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

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

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

***Steps:***

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

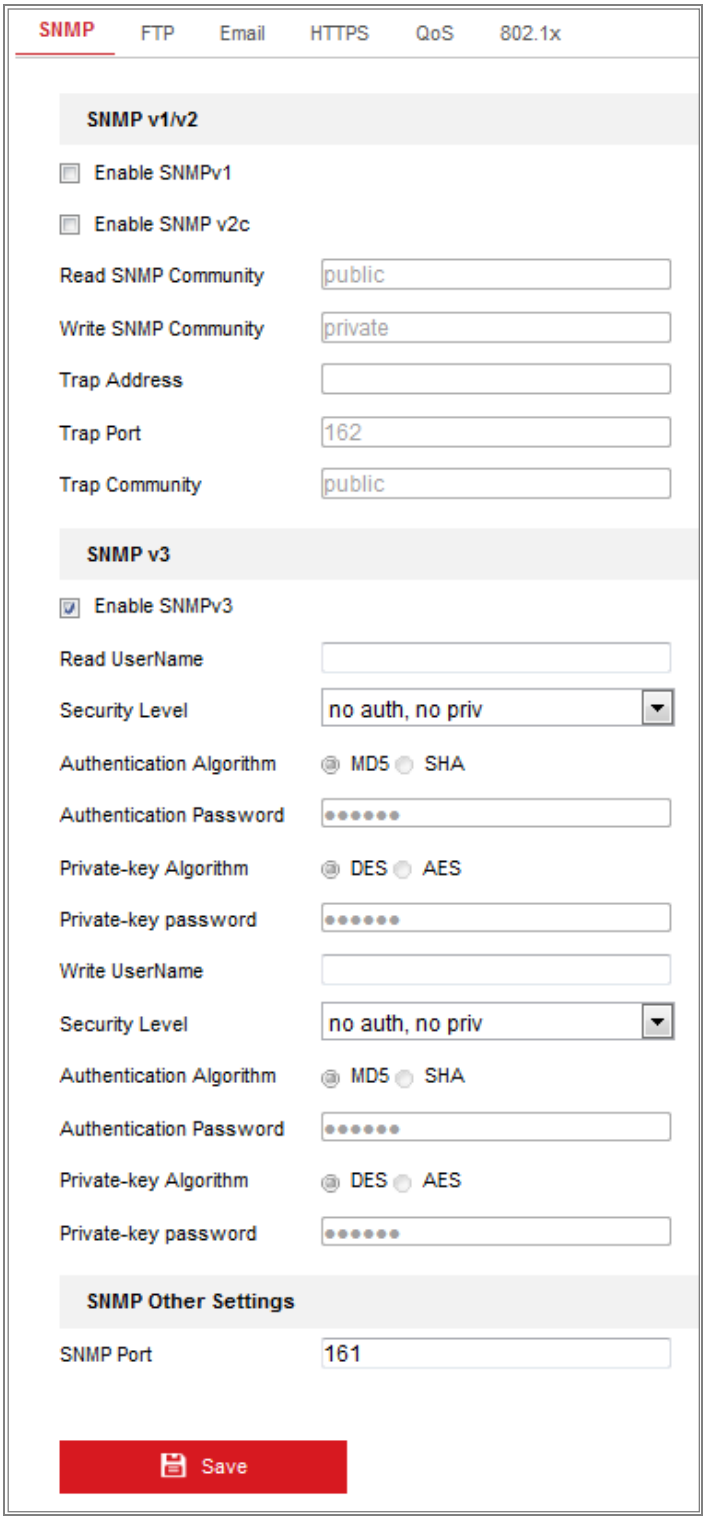



Figure 7-7 SNMP Settings

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.

## 7.2.2 Configuring FTP Settings

***Purpose:***

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

***Steps:***

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

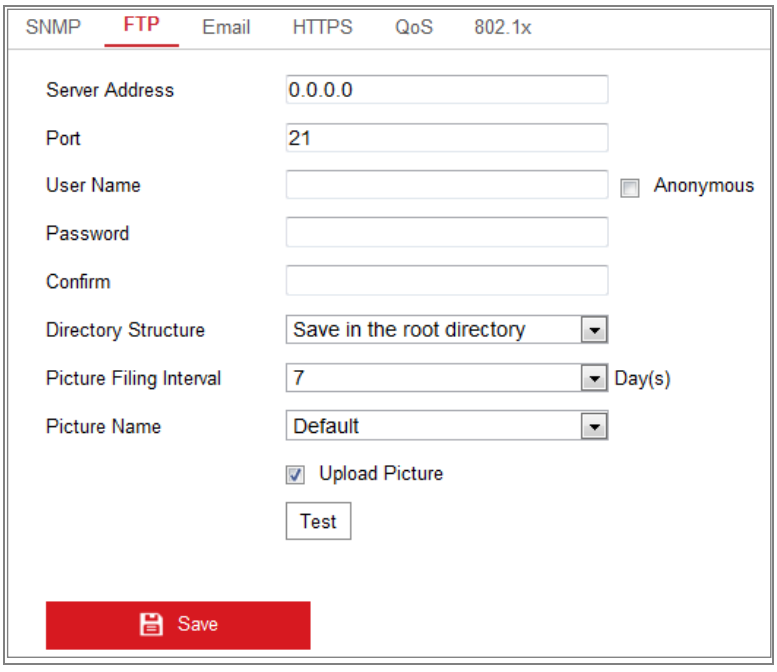



Figure 7-8 FTP Settings

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.

### 7.2.3 Configuring Email Settings

***Purpose:***

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

***Before you start:***

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

***Steps:***

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

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

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

3. Configure the following settings:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

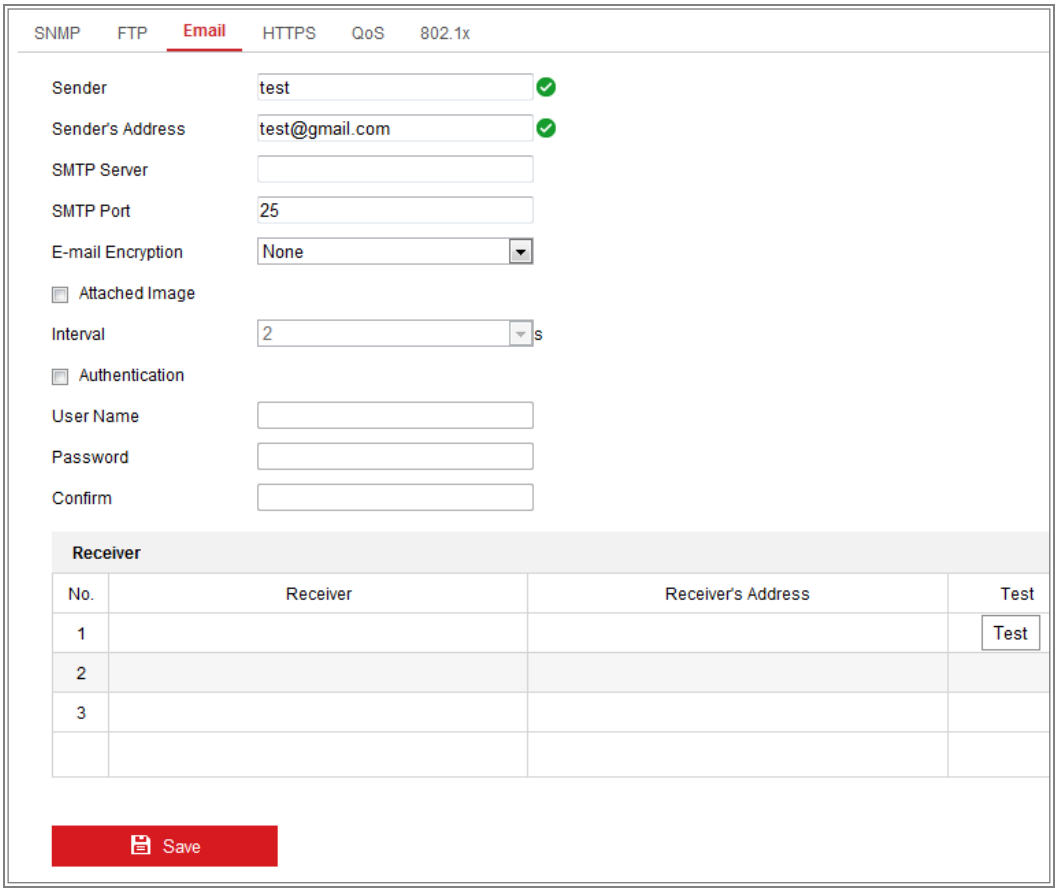



Figure 7-9 Email Settings

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

## 7.2.4 Platform Access

***Purpose:***

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

***Steps:***

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

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

If you select Platform Access Mode as Hik-Connect,

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

***Note:***

- The verification code is required when you add the camera to Hik-Connect app.
- For more information about the Hik-Connect app, refer to Hik-Connect Mobile Client User Manual.

4. You can use the default server address. Or you can check the Custom checkbox on the right and input a desired server address.
5. Click **Save** to save the settings.

### 7.2.5 HTTPS Settings

***Purpose:***

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

***Note:***

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

***Steps:***

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

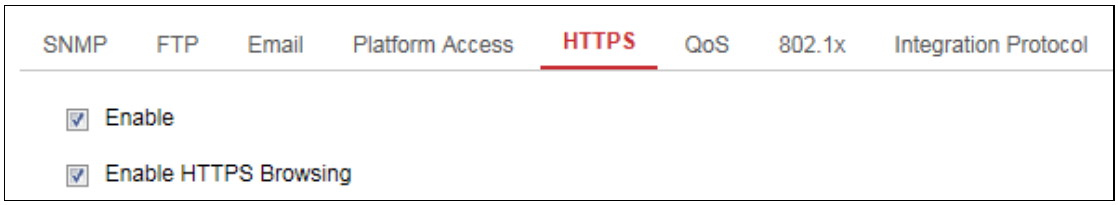



Figure 7-10 HTTPS Configuration Interface

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

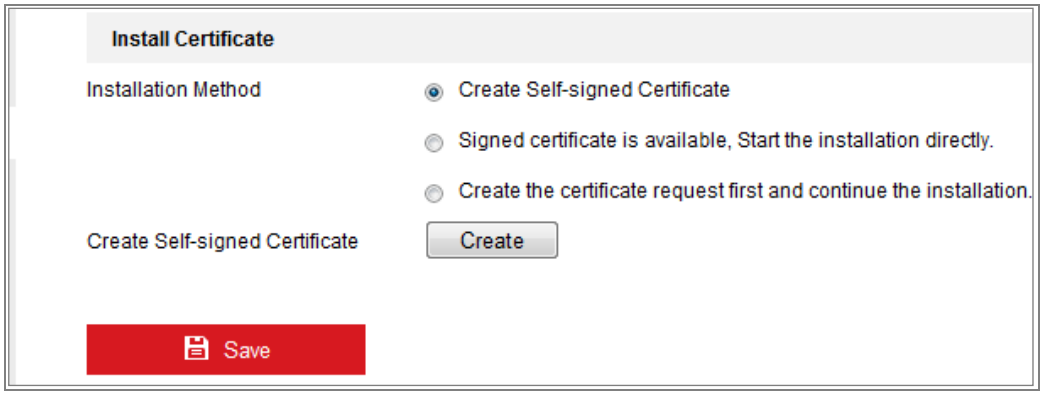



Figure 7-11 Create Self-signed Certificate

- Create the self-signed certificate

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

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

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

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

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

- Create the request and import the authorized certificate

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

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

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

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

a) Select **Signed certificate is available, Start the installation directly**.

Click **Browse** and **Install** to import the certificate to the device.

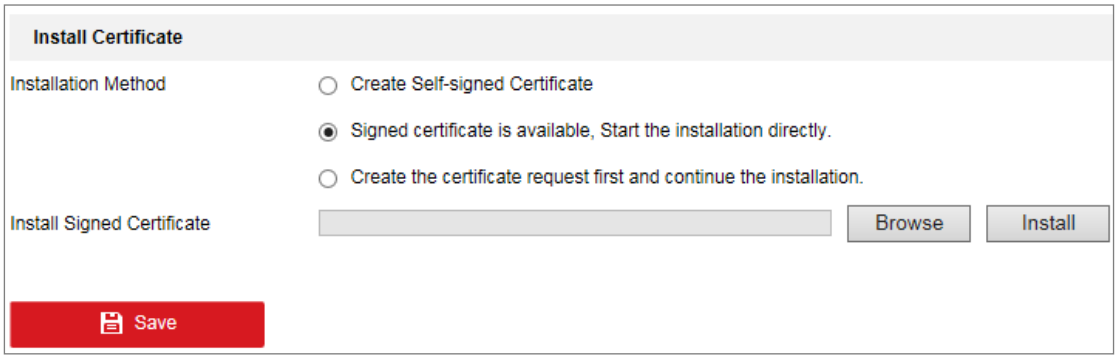



Figure 7-12 Import the Certificate (1)

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

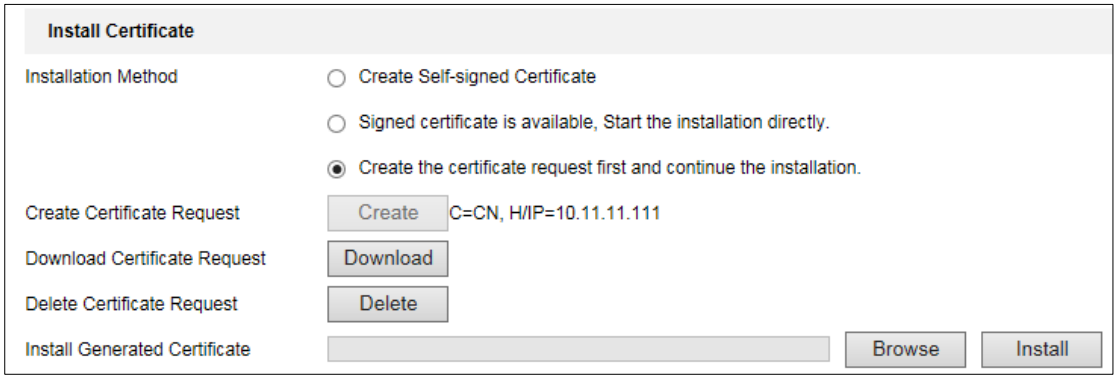



Figure 7-13 Import the Certificate (2)

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


Figure 7-14 Installed Certificate

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

***Note:***

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

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

## 7.2.6 Configuring QoS Settings

***Purpose:***

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

***Steps:***

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

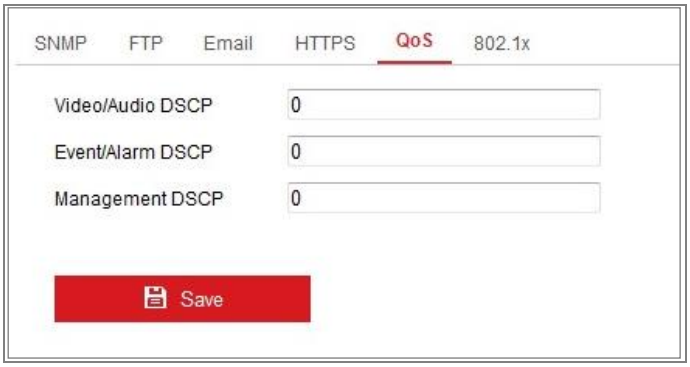



Figure 7-15 QoS Settings

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.

### 7.2.7 Configuring 802.1X Settings

***Purpose:***

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

***Before you start:***

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

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

***Steps:***

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

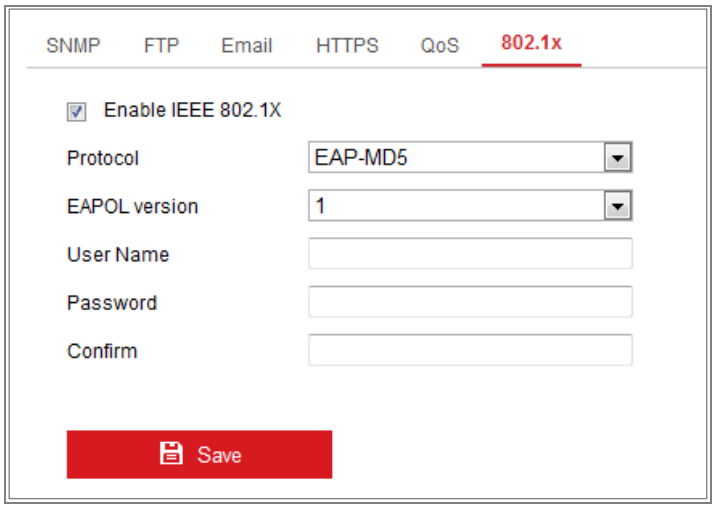


Figure 7-16 802.1X Settings

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.

### 7.2.8 Integration Protocol

***Purpose:***

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

- **CGI**

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

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

- **ONVIF**

  ***Steps:***

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

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

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

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

### 7.2.9 Network Service

You can control the ON/OFF status of certain protocol that the camera supports.

***Note:***

- Keep unused function OFF for security concern.
- Supported function varies according to camera models.

**WebSocket** and **WebSockets**

WebSocket or WebSockets protocol should be enabled if you use Google Chrome 45 and its above version or Mozilla Firefox 52 and its above version to visit your camera. Otherwise, live view, image capture, and digital zoom function can not be used.

If the camera uses HTTP, enable **WebSocket**.

If the camera uses HTTPS, enable **WebSockets**.

**SDK Service** and **Enhanced SDK Service**

If you want to add the device to the client software, you should enable SDK Service or Enhanced SDK Service.

**SDK Service:** SDK protocol is used.

**Enhanced SDK Service:** SDK over TLS protocol is used. Communication between the device and the client software is secured by using TLS (Transport Layer Security) protocol.

**TLS (Transport Layer Security)**

The device offers TLS 1.1 and TLS 1.2. Enable one or more protocol versions according to your need.

### 7.2.10 Configuring HTTP Listening

***Purpose:***

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

***Before you start:***

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

***Steps:***

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

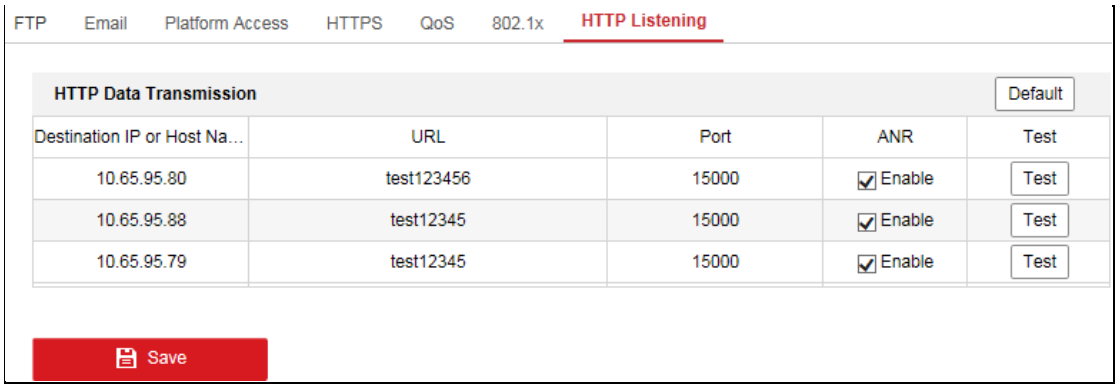



Figure 7-17 HTTP Listening

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

# Chapter 8 Video/Audio Settings

***Purpose:***

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

## 8.1 Configuring Video Settings

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

***Steps:***

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

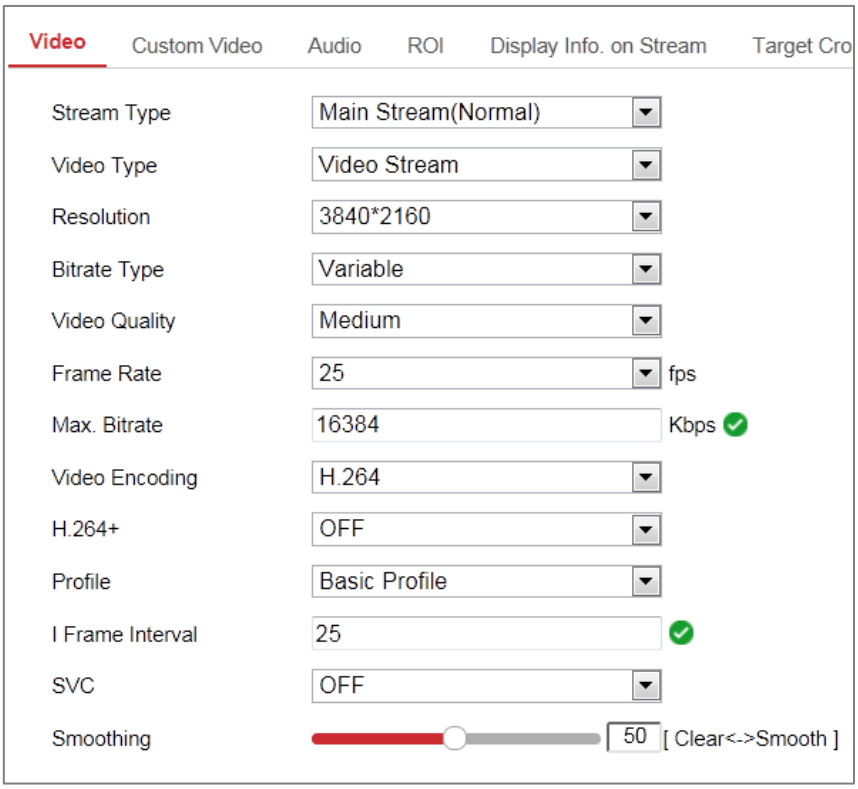



Figure 8-1 Video Settings

2. Select the Stream Type.

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

   ***Notes:***

   - For some models, the **Third Stream** is not enabled by default. Go to **System > Maintenance > System Service> Software** to enable the function is required.

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

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

**Video Type**:

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

**Resolution:**

Select the resolution of the video output.

**Bitrate Type:**

Select the bitrate type to constant or variable.

**Video Quality:**

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

**Frame Rate:**

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

**Max. Bitrate:**

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

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

**Video Encoding:**

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

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

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

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

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

***Notes:***

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

**Max. Average Bitrate:**

When you set a maximum bitrate, its corresponding recommended maximum average bitrate will be shown in the Max. Average Bitrate box. You can also set the

maximum average bitrate manually from 32 Kbps to the value of the set maximum bitrate.

**Profile:**

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

**I Frame Interval:**

Set I Frame Interval from 1 to 400.

**SVC:**

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

**Smoothing:**

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

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

***Note:***

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

## 8.2 Configuring Audio Settings

***Steps:***

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

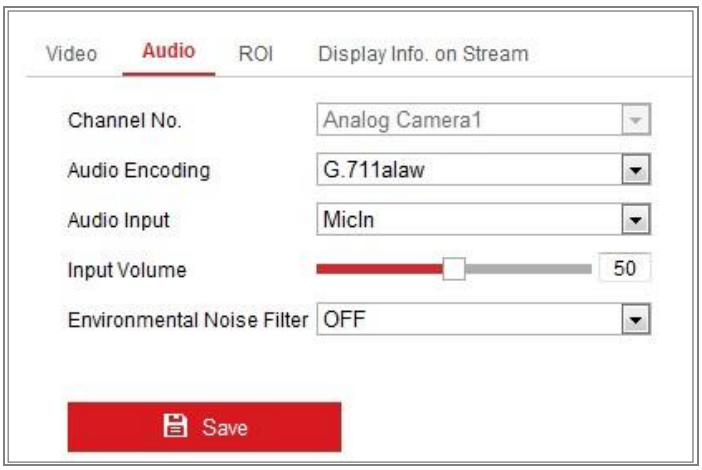



Figure 8-2 Audio Settings

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.

# 8.3 Configuring ROI Encoding

***Purpose:***

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

***Note:*** ROI function varies according to different camera models.

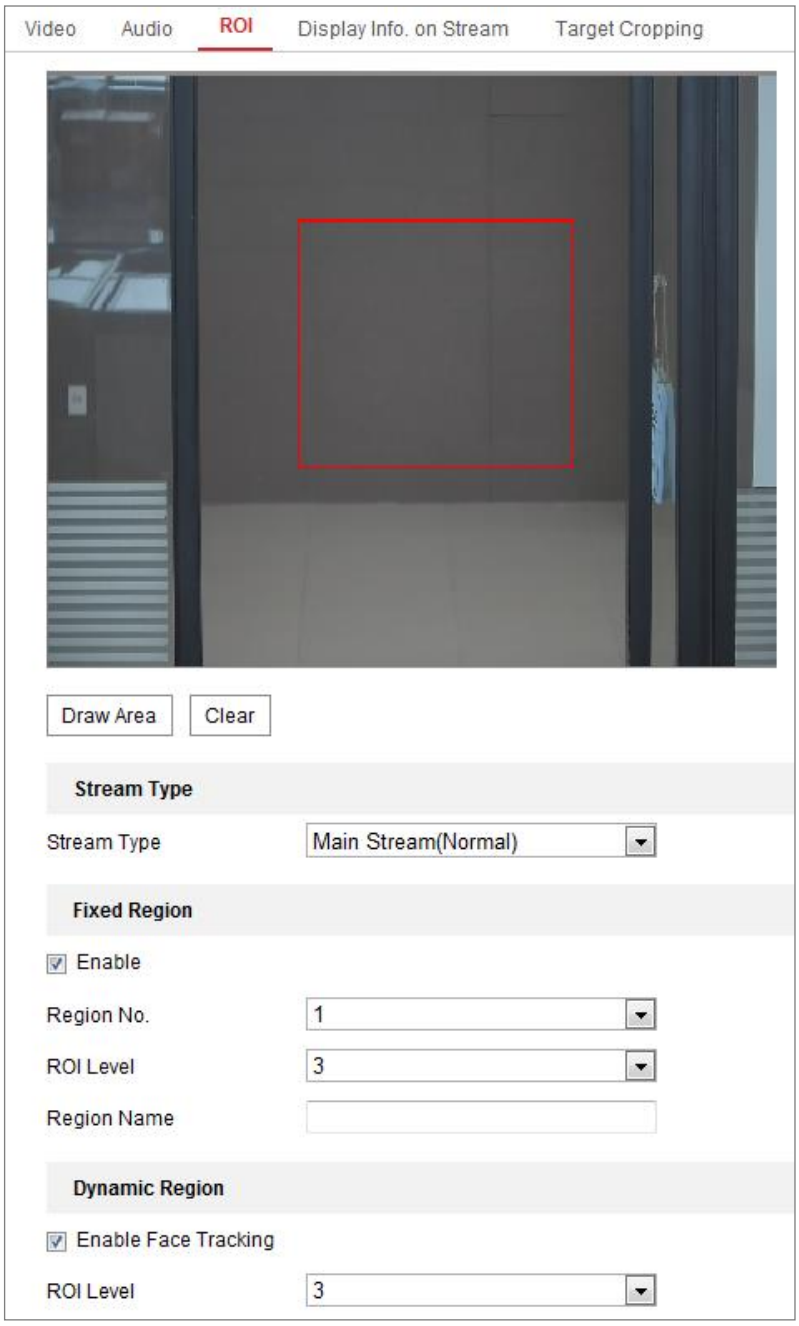



Figure 8-3 Region of Interest Settings

***Steps:***

1. Enter the ROI settings interface: **Configuration > Video/Audio > ROI**.
2. Select the Stream Type for ROI encoding.
3. Check the checkbox of **Enable** under Fixed Region item.
4. Set **Fixed Region** for ROI.
   (1) Select the Region No. from the drop-down list.
   (2) Check the **Enable** checkbox to enable ROI function for the chosen region.

(3) Click **Drawing**. Click and drag the mouse on the view screen to draw a red rectangle as the ROI region. You can click **Clear** to cancel former drawing. Click **Stop Drawing** when you finish.

(4) Select the ROI level.

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

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

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

5. Set **Dynamic Region** for ROI.

(1) Check the checkbox to enable **Face Tracking**.

***Note:*** To enable face tracking function, the face detection function should be supported and enabled.

(2) Select the ROI level.

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

***Note:*** ROI level means the image quality enhancing level. The larger the value is, the better the image quality would be.

# Chapter 9 Image Settings

***Purpose:***

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

## 9.1 Configuring Display Settings

***Purpose:***

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

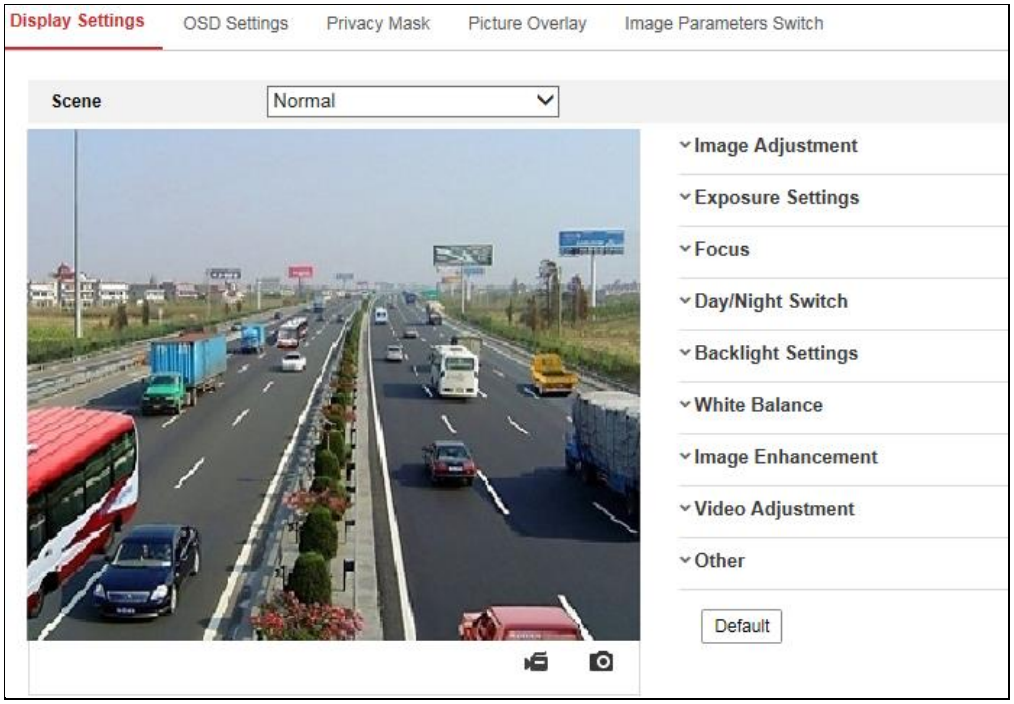



Figure 9-1 Display Settings

2. Select the desired scene.
3. Set the image parameters of the camera.

- **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.

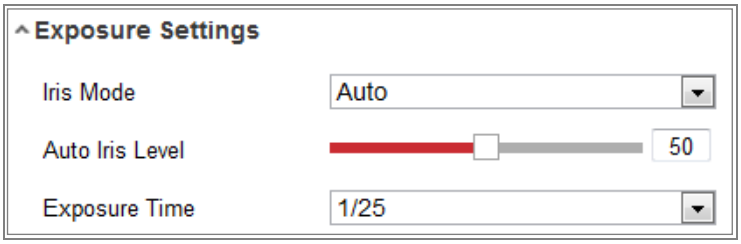



Figure 9-2 Exposure Settings

- **Focus**

  For camera support motor-driven lens, you can set the focus mode as Auto, Manual or Semi-auto.

  **Auto:** Camera focus is adjusted automatically according to the actual monitoring scenario.

  **Manual:** You can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus manually.

  **Semi-Auto:** Camera will focus automatically when you adjust the zoom parameters.

- **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.

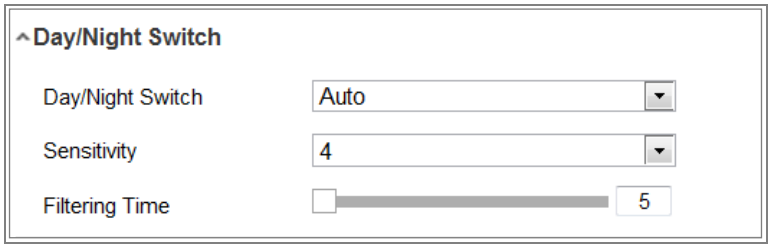



Figure 9-3 Day/Night Switch

**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 as 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 supplement by adjusting the distance. E.g., 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.

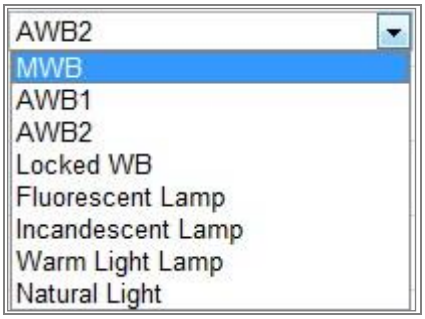



Figure 9-4 White Balance

- **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.

## 9.2 Configuring OSD Settings

***Purpose:***

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


Figure 9-5 OSD Settings

***Steps:***

1. Enter the OSD Settings interface: **Configuration > Image > OSD Settings**.
2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format and date format.
5. Select from the drop-down list to set the time format, date format, display mode, OSD size and OSD color.
6. 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.
7. Adjust the position and alignment of text frames.

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

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

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

## 9.3 Configuring Privacy Mask

***Purpose:***

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

***Steps:***

1. Enter the Privacy Mask Settings interface: **Configuration** > **Image** > **Privacy Mask**.
2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.

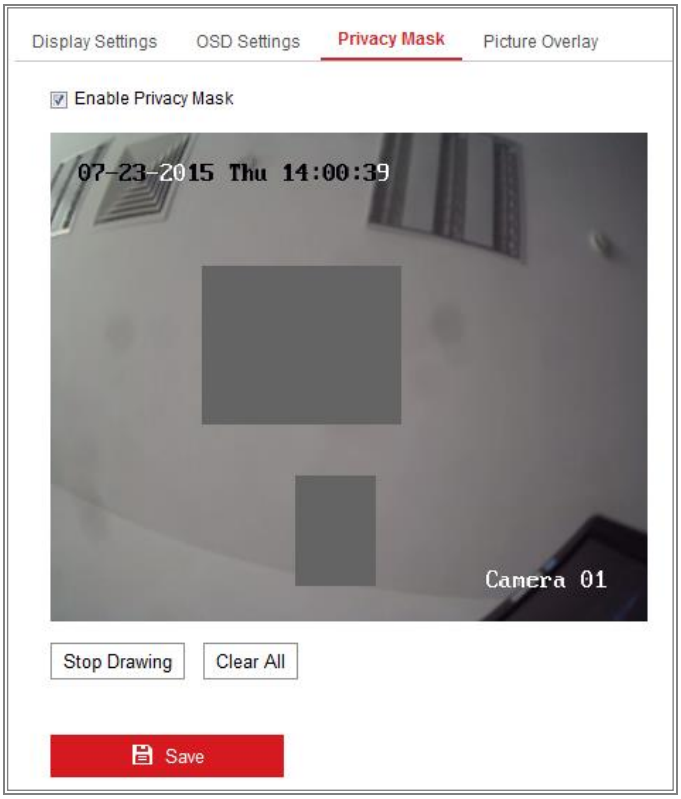



Figure 9-6 Privacy Mask Settings

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

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

5. Click **Stop Drawing** to finish drawing or click **Clear All** to clear all of the areas

you set without saving them.

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

## 9.4 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**.

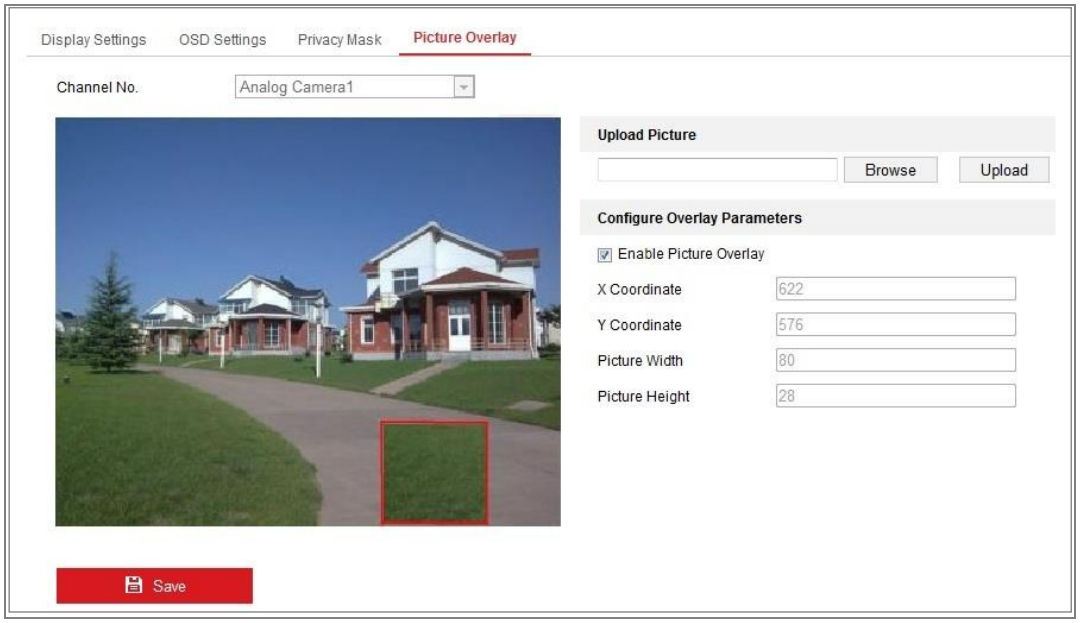



Figure 9-7 Picture Overlay

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

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

# 9.5 Configuring Image Parameters Switch

***Purpose:***

Image parameters scheduled-switch configuration interface enables you to set the time period and linked scene and it will go to the linked scene in the configured time period when you check the corresponding checkbox.

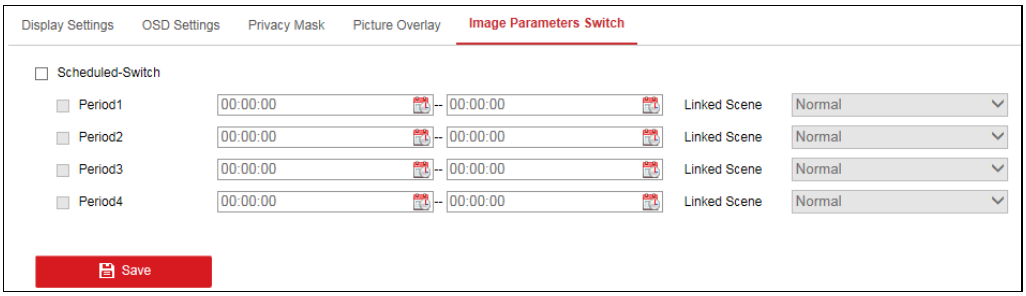



Figure 9-8 Scheduled-Switch Configuration Interface

***Steps:***

1. Enter Image Parameters Switch interface, **Configuration** > **Image** > **Image Parameters Switch**.
2. Check **Scheduled-Switch**.
3. Set the time period and the linked scene. Up to four periods can be configured.
4. Click **Save**.

# Chapter 10 Event Settings

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

## 10.1 Basic Events

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

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

### 10.1.1 Configuring Motion Detection

***Purpose:***

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

In order to detect the moving objects accurately and reduce the false alarm rate, normal configuration and expert configuration are selectable for different motion detection environment.

- **Normal Configuration**

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

***Tasks 1: Set the Motion Detection Area***

***Steps:***

1. Enter the motion detection settings interface: **Configuration > Event > Basic Event > Motion Detection**.
2. Check the checkbox of **Enable Motion Detection**.

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

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

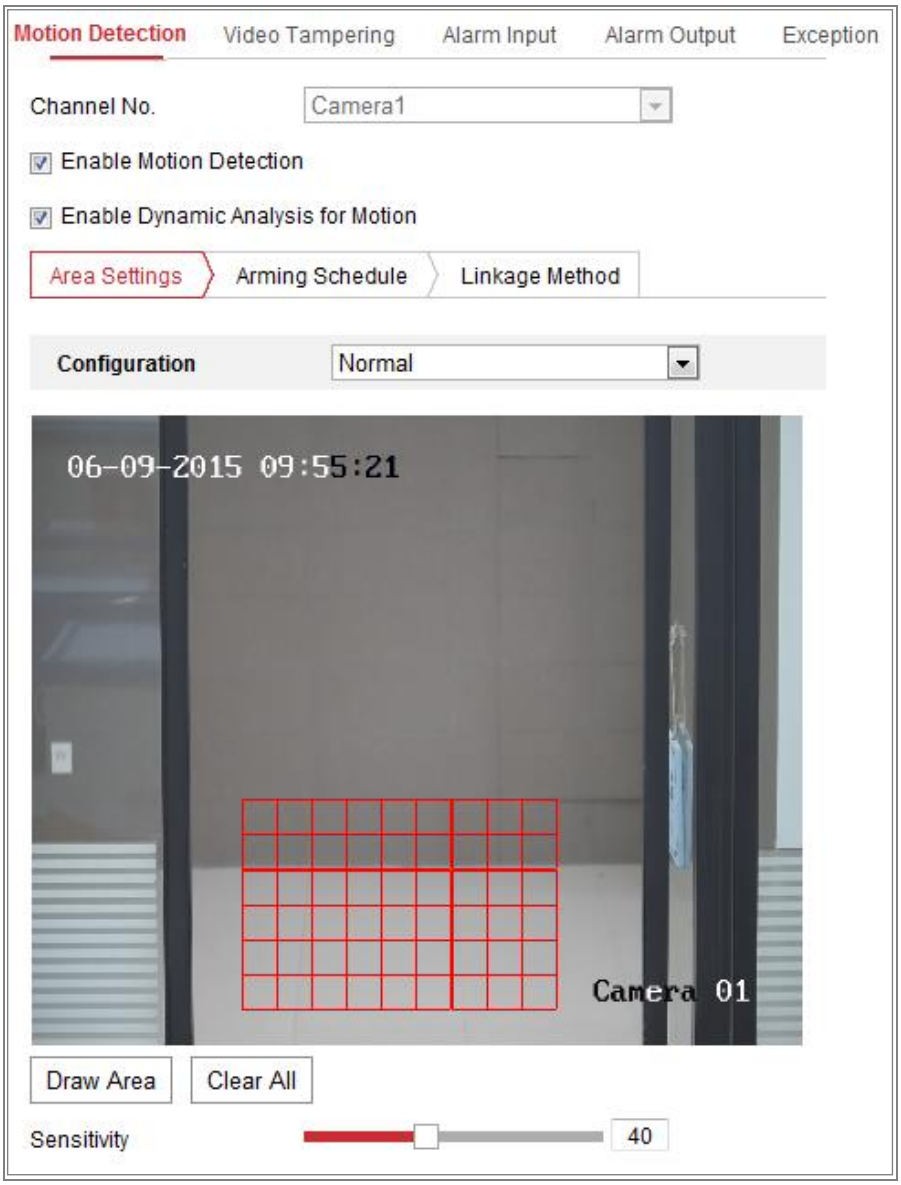



Figure 10-1 Enable Motion Detection

4. Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area. Click **Stop Drawing** to finish drawing one area.
5. (Optional) Click **Clear All** to clear all of the areas.
6. (Optional) Move the slider to set the sensitivity of the detection.

### *Task 2: Set the Arming Schedule for Motion Detection*


Figure 10-2 Arming Schedule

***Steps:***

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

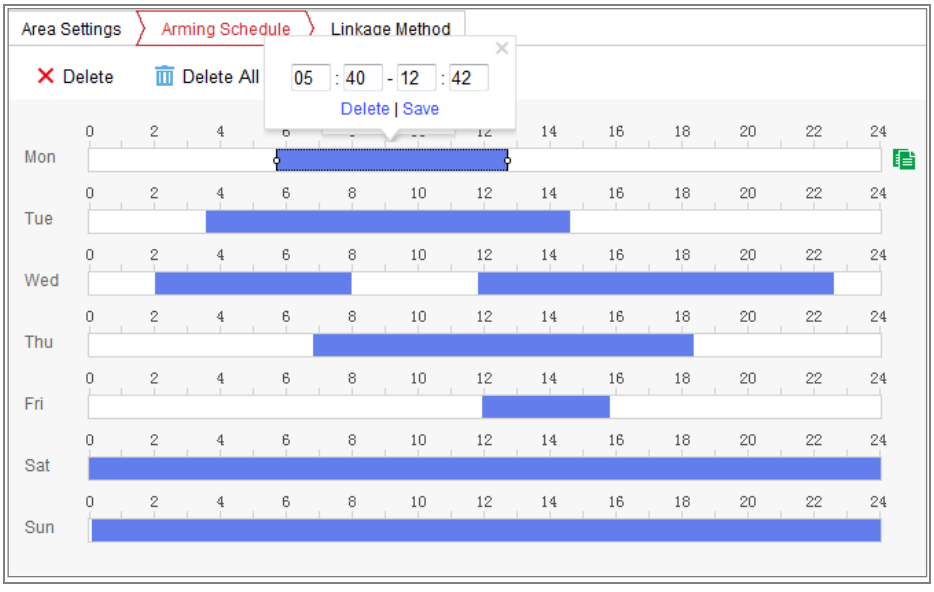



Figure 10-3 Arming Schedule

***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.

***Task 3: Set the Linkage Method for Motion Detection***

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.

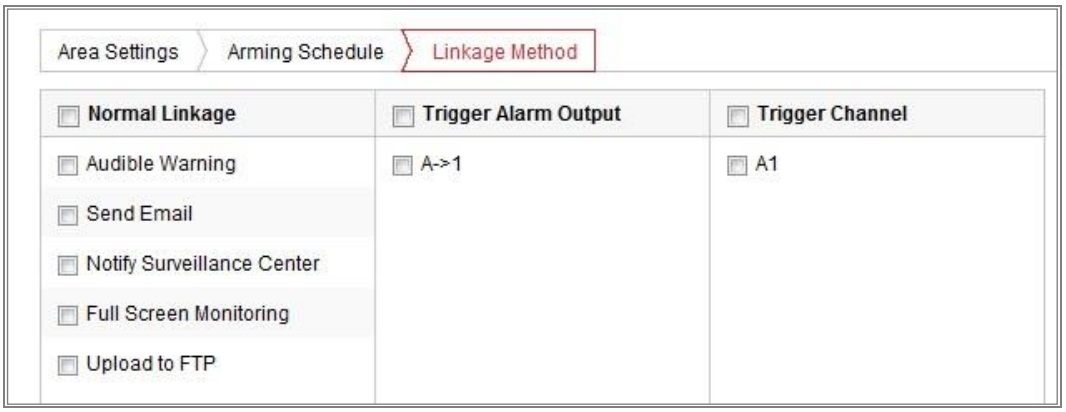



Figure 10-4 Linkage Method

***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 7.2.2* ***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 *Section 10.1.4* ***Configuring Alarm Output*** to set the related parameters.

- **Expert Configuration**

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

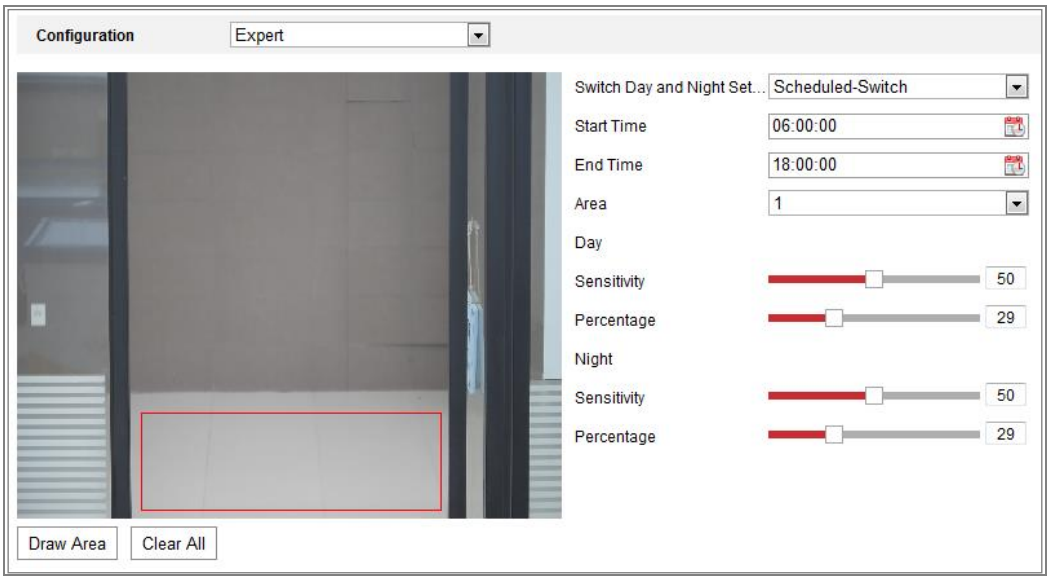



Figure 10-5 Expert Mode of Motion Detection

- Day/Night Switch OFF

***Steps:***

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **OFF** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area.
5. Set the arming schedule and linkage method as in the normal configuration mode.
6. Click **Save** to save the settings.

- Day/Night Auto-Switch

***Steps:***

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Auto-Switch** for **Switch Day and Night Settings**.
3. Select the area by clicking the area No.
4. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.

6. Set the arming schedule and linkage method as in the normal configuration mode.
7. Click **Save** to save the settings.

- Day/Night Scheduled-Switch

***Steps:***

1. Draw the detection area as in the normal configuration mode. Up to 8 areas are supported.
2. Select **Scheduled-Switch** for **Switch Day and Night Settings**.


Figure 10-6 Day/Night Scheduled-Switch

3. Select the start time and the end time for the switch timing.
4. Select the area by clicking the area No..
5. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area in the daytime.
6. Slide the cursor to adjust the sensitivity and proportion of object on the area for the selected area at night.
7. Set the arming schedule and linkage method as in the normal configuration mode.
8. Click **Save** to save the settings.

### 10.1.2 Configuring Video Tampering Alarm

***Purpose:***

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

Detection area for this alarm is the whole screen.

***Steps:***

1. Enter the video tampering Settings interface, **Configuration > Event > Basic Event > Video Tampering**.

2. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
3. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 10.1.1*.
4. Check the checkbox to select the linkage method taken for the video tampering. Please refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 10.1.1*.
5. Click **Save** to save the settings.

### 10.1.3 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).

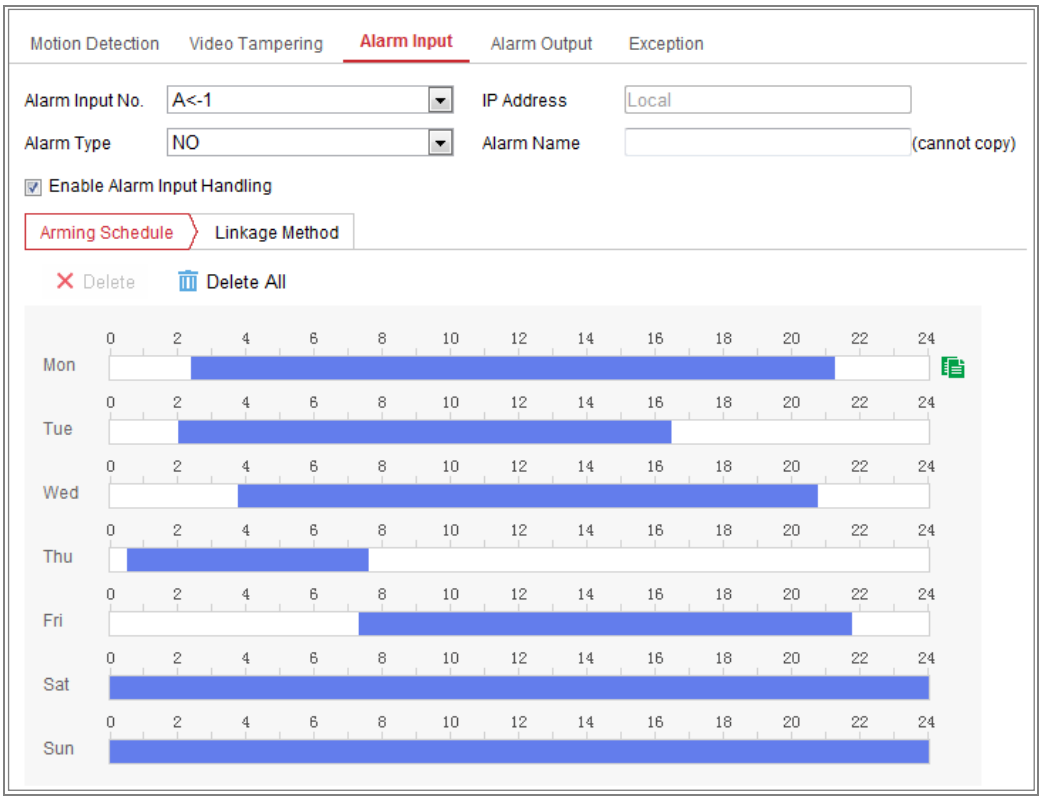



Figure 10-7 Alarm Input Settings

3. Click **Arming Schedule** to set the arming schedule for the alarm input. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 10.1.1*.
4. Click **Linkage Method** and check the checkbox to select the linkage method taken for the alarm input. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 10.1.1*.
5. You can copy your settings to other alarm inputs.
6. Click **Save** to save the settings.

## 10.1.4 Configuring Alarm Output

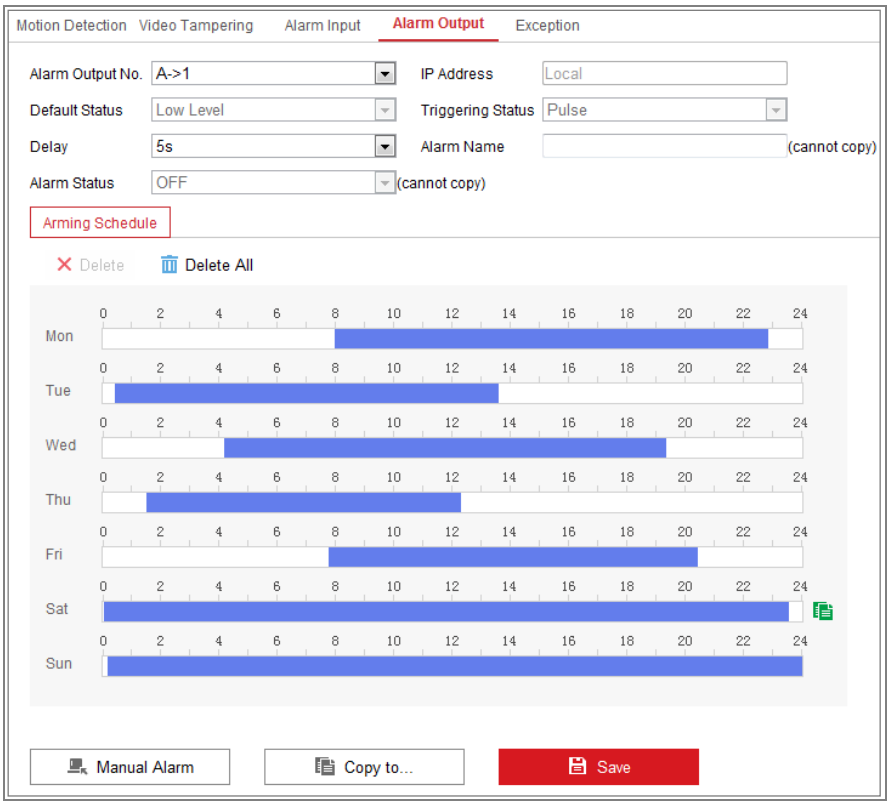



Figure 10-8 Alarm Output Settings

***Steps:***

1. Enter the Alarm Output Settings interface: **Configuration> Event > Basic Event > Alarm Output**.
2. Select one alarm output channel in the **Alarm Output** drop-down list. You can also set a name for the alarm output (optional).
3. The Delay time can be set to 5sec, 10sec, 30sec, 1min, 2min, 5min, 10min or Manual. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
4. Click **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 2: Set the Arming Schedule for Motion Detection*** in *Section 10.1.1*.
5. You can copy the settings to other alarm outputs.

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

### 10.1.5 Handling Exception

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

***Steps:***

1. Enter the Exception Settings interface: **Configuration > Event > Basic Event > Exception**.
2. Check the checkbox to set the actions taken for the Exception alarm. Refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 10.1.1*.
3. Click **Save** to save the settings.

## 10.2 Smart Events

You can configure the smart events by following the instructions in this section, including audio exception detection, defocus detection, scene change detection, intrusion detection, and line crossing detection, etc. These events can trigger the linkage methods, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

### 10.2.1 Configuring Audio Exception Detection

***Purpose:***

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

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

***Steps:***

1. Enter the Audio Exception Detection settings interface, **Configuration > Event >**

**Smart Event > Audio Exception Detection**.

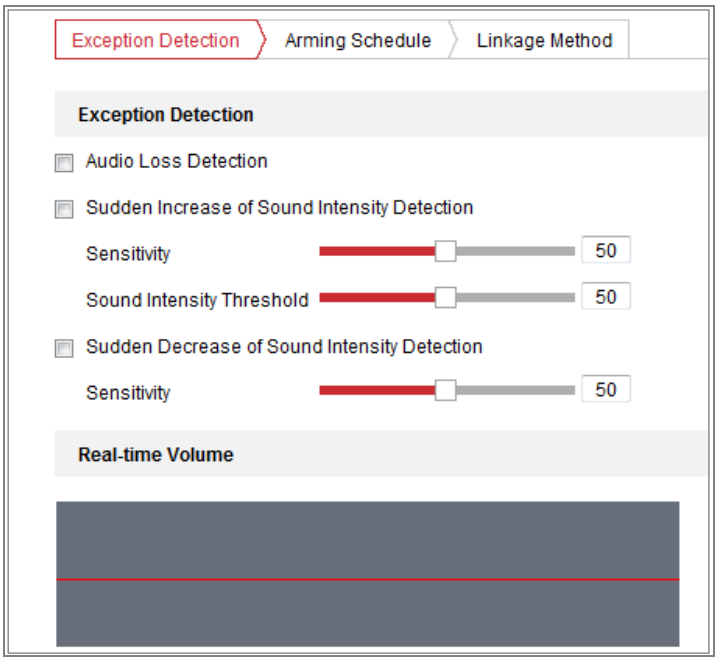



Figure 10-9 Audio Exception Detection

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

   ***Notes:***

   - Sensitivity: Range [1-100], the smaller the value is, the more severe the change should be to trigger the detection.
   - Sound Intensity Threshold: Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the real environment.
   - You can view the real-time volume of the sound on the interface.
5. Click **Arming Schedule** to set the arming schedule. Refer to ***Task 2 Set the Arming Schedule for Motion Detection*** in *Section 10.1.1* for detailed steps.

6. Click **Linkage Method** and select the linkage methods for audio exception, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel for recording and Trigger Alarm Output.
7. Click **Save** to save the settings.

### 10.2.2 Configuring Defocus Detection

***Purpose:***

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

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

***Steps:***

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

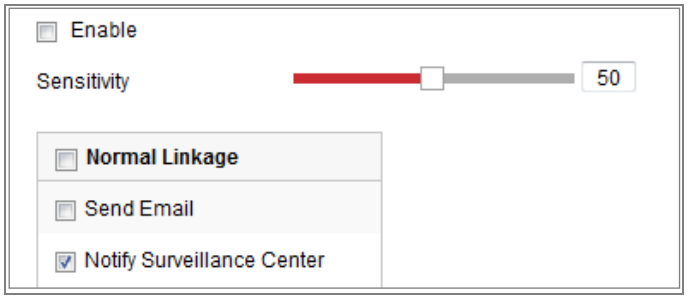



Figure 10-10 Configuring Defocus Detection

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

### 10.2.3 Configuring Scene Change Detection

***Purpose:***

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

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

***Steps:***

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

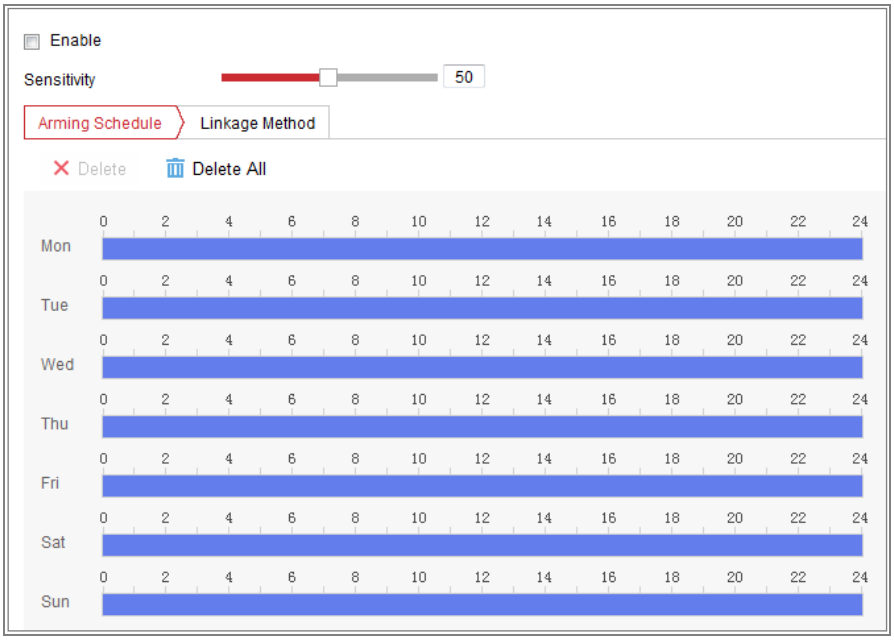



Figure 10-11 Scene Change Detection

2. Check the checkbox of **Enable** to enable the function.
3. Click-and-drag the slider to set the detection sensitivity. The sensitivity value ranges from 1 to 100, and the higher the value is, the more easily the change of scene can trigger the alarm.
4. Click **Arming Schedule** to set the arming schedule. Refer to *Task 2* ***Set the Arming Schedule for Motion Detection*** in *Section 10.1.1* for detailed steps.
5. Click **Linkage Method** to select the linkage methods for scene change, including Notify Surveillance Center, Send Email, Upload to FTP/Memory Card/NAS, Trigger Channel and Trigger Alarm Output.
6. Click **Save** to save the settings.

# Chapter 11 People Counting

***Purpose:***

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

***Before you start:***

The camera is recommended to be installed right above the entrance/exit, and make sure it is installed properly.

Refer to *Quick Start Guide of Dual-Lens People Counting Camera* for installation advice.

***About the task:***

Configuration for Mobile Model and Non-Mobile Model are different:

To complete the configuration, you should:

- Set rule
- Set shield region
- Set data uploading
- Set overlay and capture parameters
- Set advanced parameters

## 11.1 Set the Rule

### 11.1.1 Rule

**For Non-Mobile Models**

***Steps:***

1. Enter the People Counting Configuration interface: **VCA** > **VCA Resource** > **People Counting**.

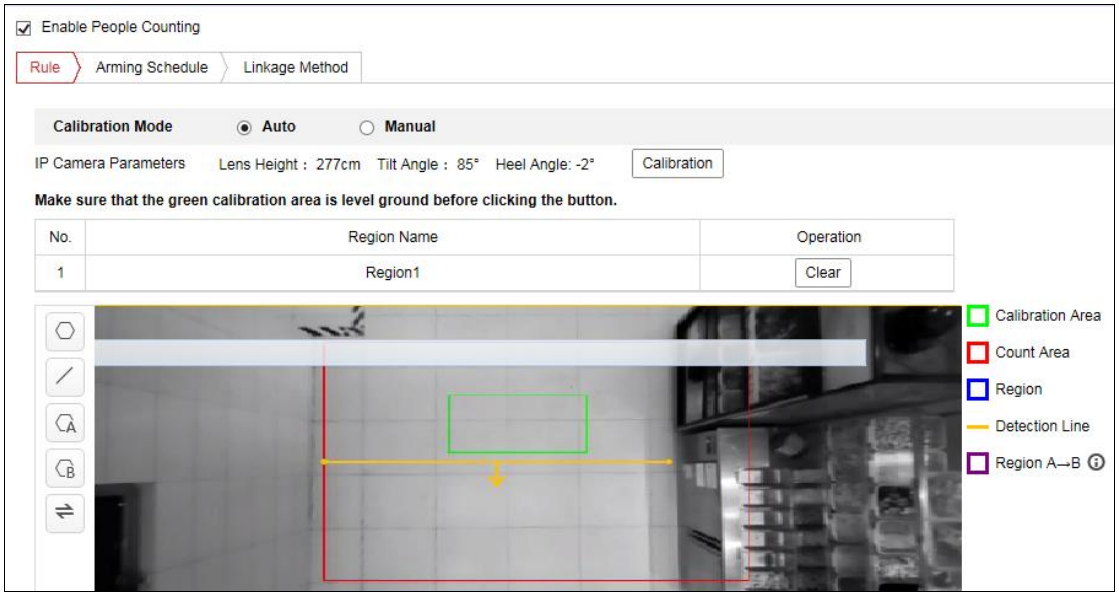



Figure 11-1 People Counting Configuration

2. Check **Enable People Counting** checkbox to enable the function.
3. Select the calibration mode and then click **Calibration**.

   Auto calibration and manual calibration are selectable.

   **Auto:** The camera automatically calculates the lens height, tilt angle and heel angle.

   Select the calibration area and drag it to the level ground.

   ***Note:***

   To increase the accuracy and success rate of the automatic calibration, follow the rule below to select the calibration area.

   - Select the level ground with rich texture as the calibration area.
   - Select the area with uniformity of brightness as the calibration area.
   - Select the middle of the image as the calibration area.

   **Manual:** Measure and input the lens height, tilt angle and heel angle.

   ***Note:***

   - It is recommended to use manual calibration if the ground area is less than 25% of the whole image.
   - To increase the success rate of the manual calibration, make sure the lens height is the true value in vertical direction between the lens and the ground.
   - After the area is successfully calibrated, then the camera generates the

detection area and starts people counting.

4. Click on the left of the live view image to draw a detection region.
5. Click on the left of the live view image to draw the detection line. The arrow stands for the direction of entering, you can click to change the direction.
   - If the target crosses the counting area along the entering direction and crosses the detection line, then it is counted as the entering number.
   - If the target crosses the counting area along the exiting direction and crosses the detection line, then it is counted as the exiting number.
6. Click and to draw A and B area. Make sure the two areas don't overlap. You can click to change the direction.
   - If the target enters from A region to B region, then it is counted as the entering number
   - If the target enters from B region to A region, then it is counted as the exiting number.

**For Mobile Models**

***Steps:***

1. Enter the People Counting Configuration interface: **VCA** > **VCA Resource** > **People Counting**.
2. Check **Enable People Counting** checkbox to enable the function.
3. Click **Calibration**. Measure and input the lens height from entry/exit area, tilt angle and heel angle.

   ***Note:***
   - To increase the success rate of the manual calibration, make sure the lens height from entry/exit area is the true value in vertical direction between the lens and the entry/exit area.
   - After the area is successfully calibrated, then the camera generates the detection area and starts people counting.
4. Click on the left of the live view image to draw a entry/exit area.
5. Click on the left of the live view image to draw a detection region.
6. Click on the left of the live view image to draw the detection line. The arrow

stands for the direction of entering, you can click ⇌ to change the direction.

- If the target crosses the counting area along the entering direction and crosses the detection line, then it is counted as the entering number.
- If the target crosses the counting area along the exiting direction and crosses the detection line, then it is counted as the exiting number.

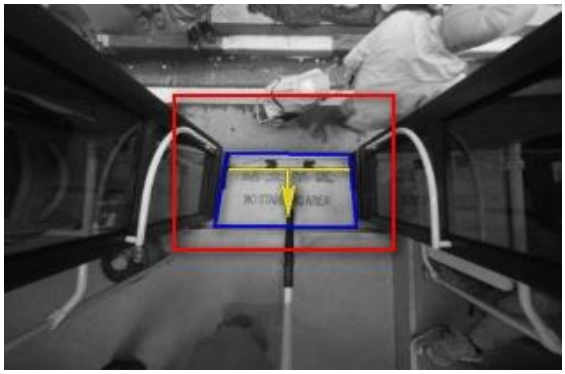


Figure 11-2 An Example of Detection Line and Entry/Exit Area

### 11.1.2 Arming Schedule

***Steps:***

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

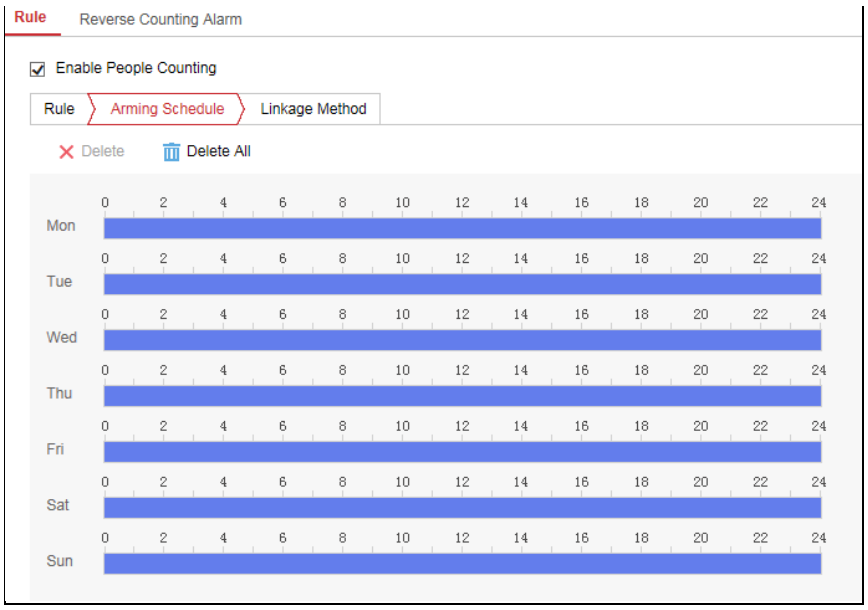



Figure 11-3 Arming Schedule

***Note:*** Click on the selected time period, you can adjust the time period to the

desired time by either moving the time bar or input the exact time period.

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

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

### 11.1.3 Linkage Method

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

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

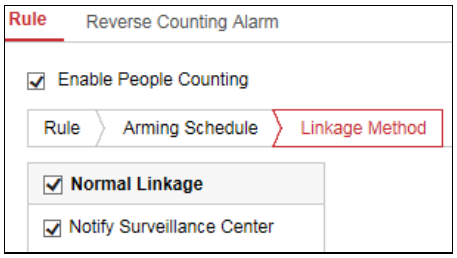



Figure 11-4 Linkage Method

- **Notify Surveillance Center**

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

### 11.1.4 (Optional) Reverse Counting Alarm

***Steps:***

1. Check **Enable Reverse Entering Alarm** to enable the function. An alarm is enabled when the target leaves the region.
2. Set the arming schedule and linkage method.

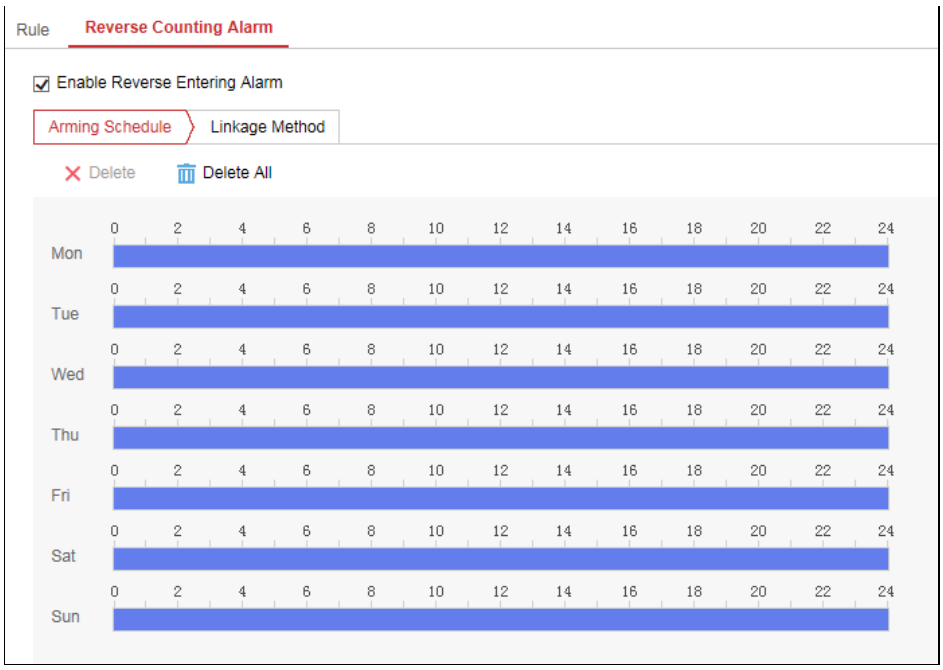



Figure 11-5 Reverse Counting Alarm

## 11.2 Set the Shield Region

Set the shield region. Click to draw a polygon shield region. You can click to clear all the shield regions.

## 11.3 Set the Data Uploading

**For Non-Mobile Models**

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

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

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

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

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

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

  Select report type (daily report, weekly report, monthly report, and annual report)

and report format to activate the function.

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

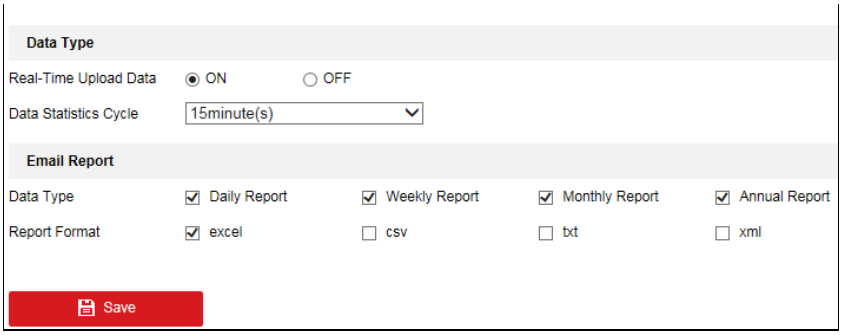



Figure 11-6 Data Uploading

**For Mobile Models**

Select a trigger counting mode. None, or trigger by alarm input.

- **None:** Camera keeps counting, unaffected by door status.

  When you select None, people counting data is sent to surveillance center and client software through SDK (default) and HTTP (if configured).

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

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

- **Trigger by Alarm Input:** Camera judges the door status by alarm input signals. Counting only happens when the door status is considered as open.

  1. Select **Alarm Input Signal Type** according to the actual signal type of the vehicle.

     ***Note:*** Alarm input should be configured. Go to Event > Basic Event > Alarm Input.

     **Level Signal:** If high level is door open and low level is door closed, set the alarm type as NO. If high level is door closed and low level is door open, set the alarm type as NC.

     **Pulse Signal:** Set the alarm type of both alarm input No. A<-1 and alarm input No. A<-2 as NO.

  2. (Optional) If RS-485 data transmission is required, select ON.

     Then you should set RS-485 parameters at System > System Settings >

RS485

3. (Optional) If data uploading by HTTP is required, set up the **HTTP Data Transmission** parameters.

## 11.4 Set the Overlay and Capture

- **Display VCA info. on Stream**

  The green frames will be displayed on the target if in a live view or playback.

- **Display Target info. on Alarm Picture**

  There will be a frame on the target on the uploaded alarm picture if the checkbox is checked.

- **Display Rule info. on Alarm Picture**

  The captured target and the configured area will be framed on the alarm picture.

- **Snapshot Settings**

  You can set the quality and resolution for the captured picture. Check the checkbox of Background Upload to upload the background image. Select the resolution from the drop-down list.

- Flow **Overlay**

  You can overlay the flow statistics on the live view image. You can select the number of the people entering, leaving, entering and leaving, and the number of adults or children to overlay. The overlay can only count the number of people on that day. Restarting the device can reset the number or the number reset automatically on 0:00. You can click Manual Reset to reset the counted people flow statistics.

***Note:*** Background upload is only available for face capture camera, and resolution selection is only available for behavior analysis camera.

## 11.5 Set the Advanced Parameters

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

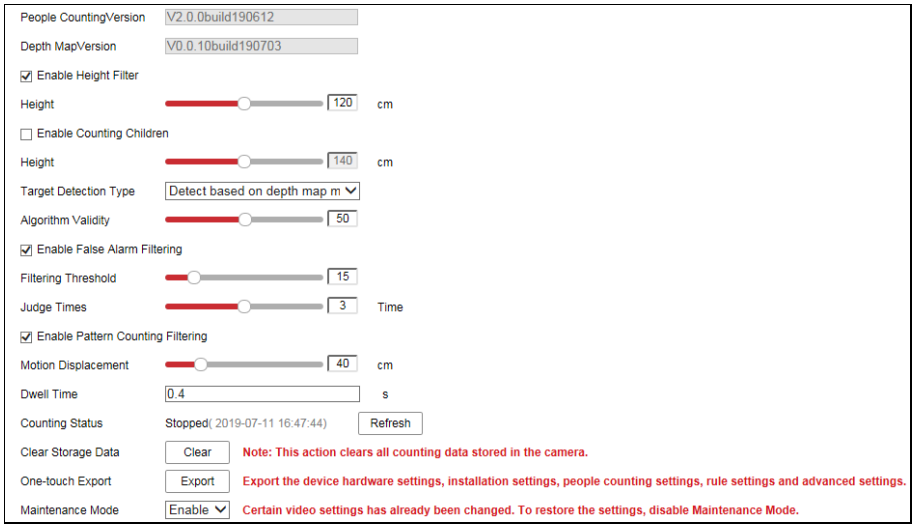



Figure 11-7 Advanced Parameters

- **Enable Height Filter:**

  Enable the function and set a height value. Persons and objects shorter than the set value are not counted as a valid target.

  Enable Counting Children: Enable the function and set a height value to calculate the number of the children higher than the set value.

- **Target Detection Type**

  You can select to detect based on the tracking algorithm only, depth map only, tracking algorithm mainly and depth map secondarily, and depth map mainly and tracking algorithm secondarily.

  Algorithm Validity: It refers to the validity of the detection. The higher the value is, the less easier to detect the target but the higher the detection accuracy is.

- **Enable Pattern Counting Filtering**

  It refers to filter the invalid target based on the motion and event. You can set the motion displacement and dwell time. If the motion displacement of the target is less than the set value, or the dwell time is less than the set value, the target will not be counted.

- **Counting Status**

  It displays the current status of the camera. You can click the Refresh button to refresh the status.

- **Door Status (only available for mobile camera)**

It displays the vehicle door status. Click **Refresh** to update the status.

- **Clear Storage Data**

  To clear stored data on camera, you can click the Clear button. Always do the operation with caution. Deleted data cannot be restored.

- **One-touch Export**

  Click the button to export the camera configuration parameters.

- **Maintenance Mode**

  If the function is enabled, certain camera settings will be changed, such as the resolution, frame rate and bit rate.

***Note:***

The people counting statistics will be calculated under **Application** tab. Go to **Application** to check the people counting statistics.

# Chapter 12 Storage Settings

***Before you start:***

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

## 12.1 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**.

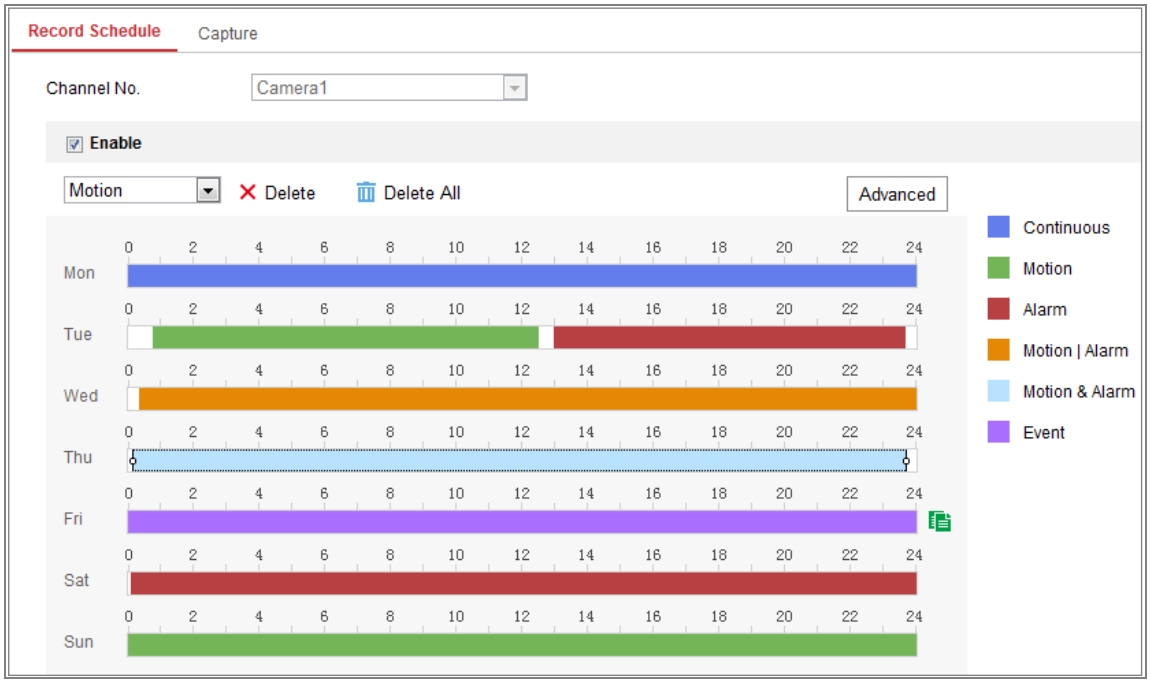



Figure 12-1 Recording Schedule Interface

2. Check the checkbox of **Enable** to enable scheduled recording.
3. Click **Advanced** to set the camera record parameters.

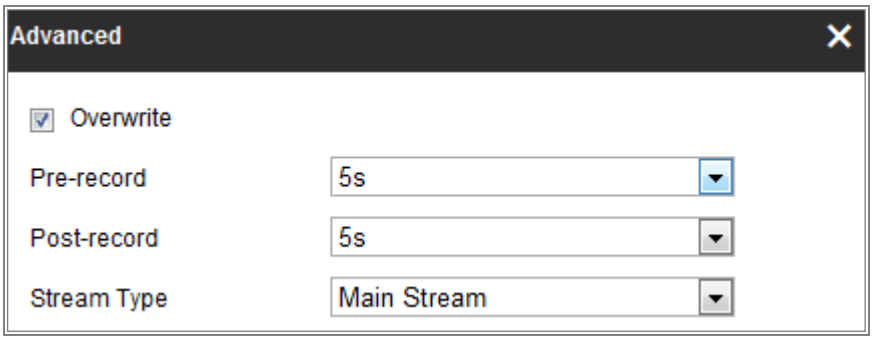



Figure 12-2 Record Parameters

- 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.

4. 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 10.1.1*.

- **Record Triggered by Alarm**

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

  Besides configuring the recording schedule, you have to set the **Alarm Type** and check the checkbox of **Trigger Channel** in the **Linkage Method** of **Alarm Input Settings** interface. For detailed information, please refer to *Section 10.1.3*.

- **Record Triggered by Motion & Alarm**

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

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 10.1.1*.and *Section 10.1.3* for detailed information.

- **Record Triggered by Motion | Alarm**

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

  Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 10.1.1*.and *Section 10.1.3* 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.

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

## 12.2 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**.

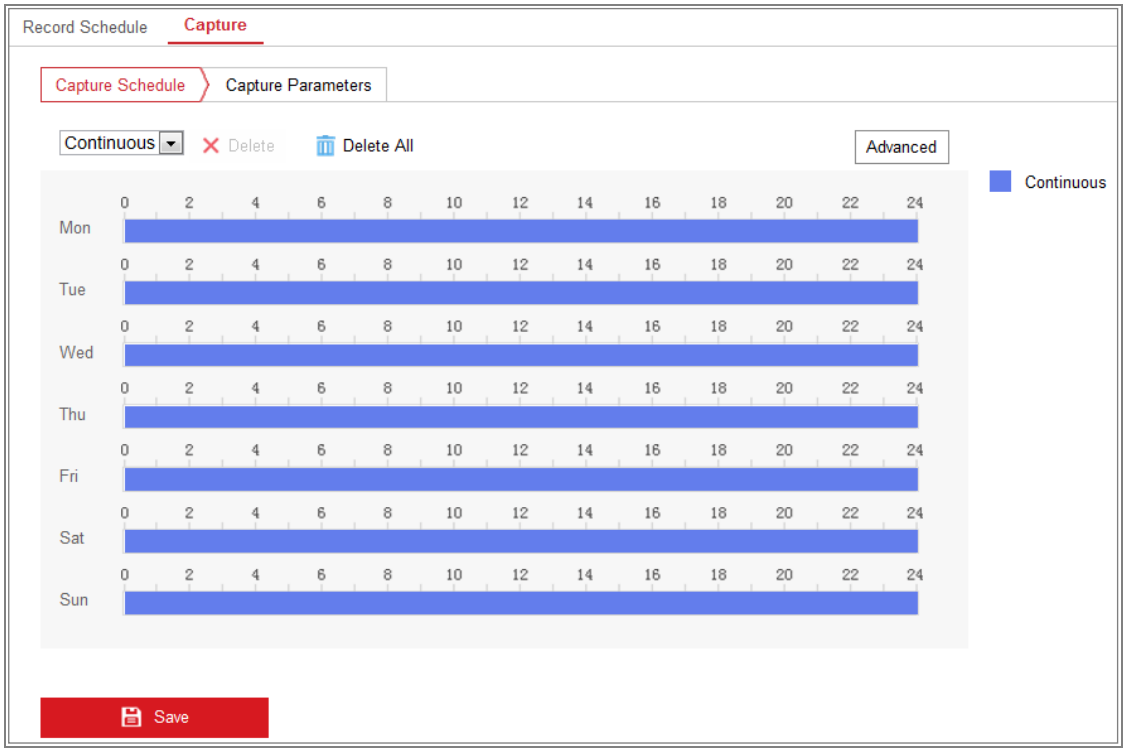



Figure 12-3 Capture Configuration

2. 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.
3. Click **Advanced** to select stream type.

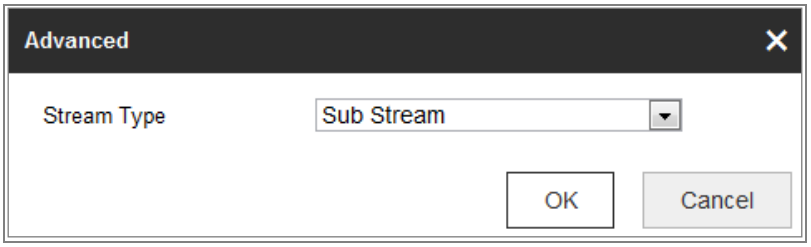



Figure 12-4 Advanced Setting of Capture Schedule

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

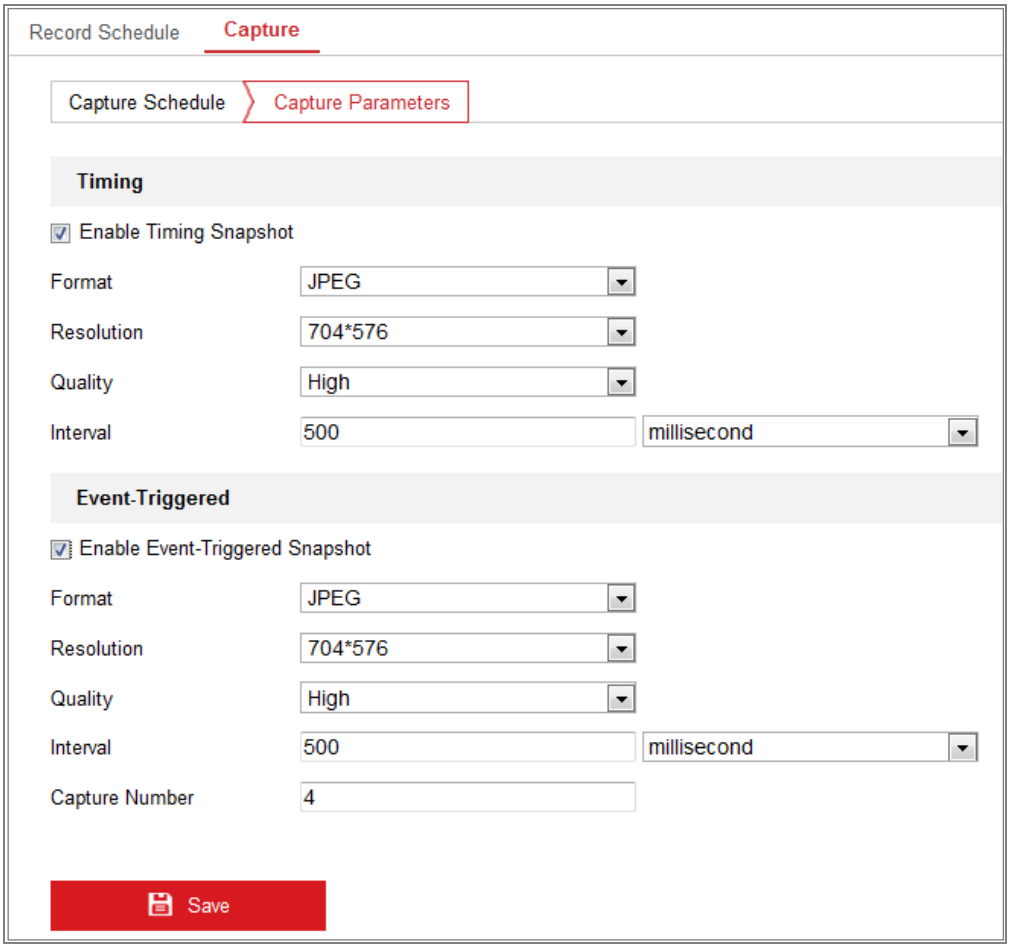



Figure 12-5 Set Capture Parameters

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

## 12.3 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**.

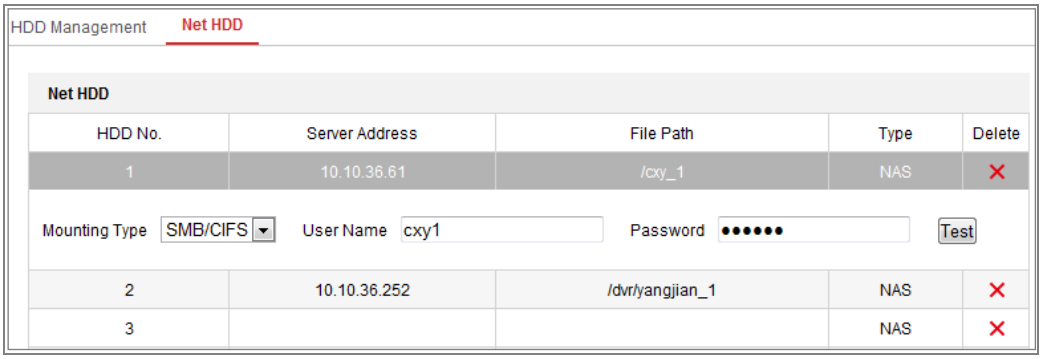



Figure 12-6 Add Network Disk

   (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.

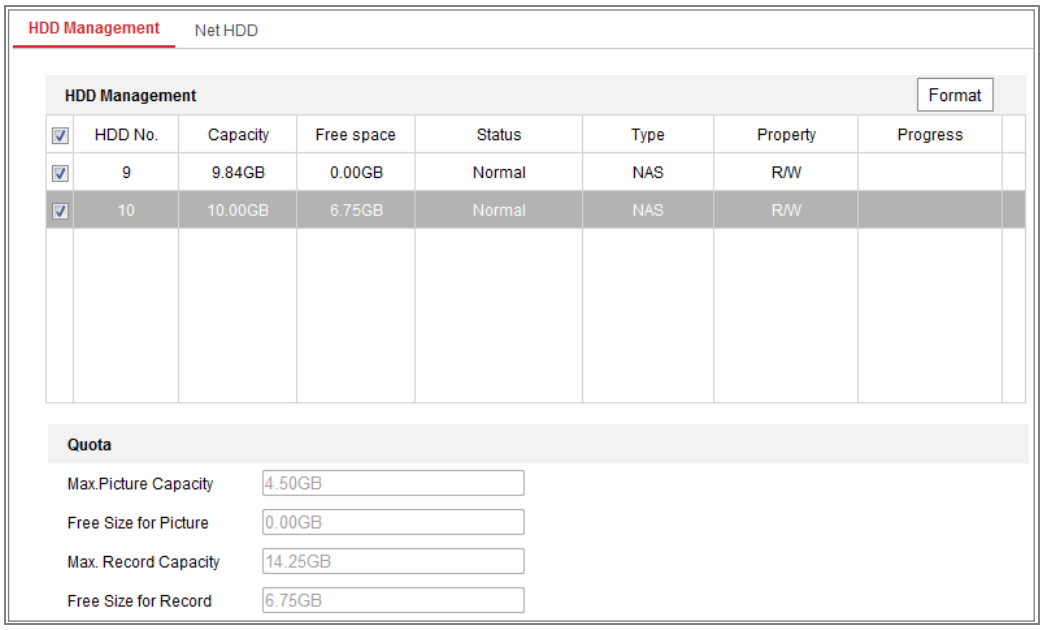



Figure 12-7 Storage Management Interface

(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.**

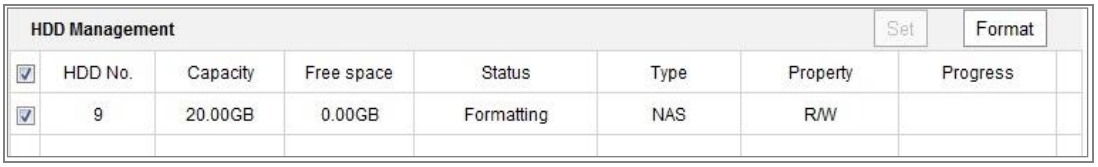



Figure 12-8 View Disk Status

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.

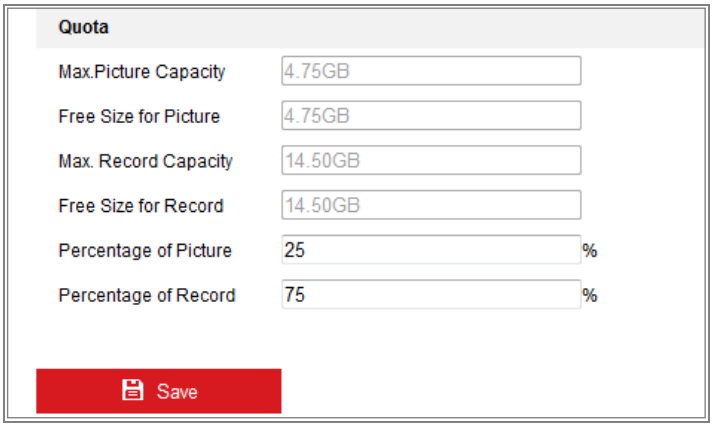



Figure 12-9 Quota Settings

***Note:***

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

# Chapter 13 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.

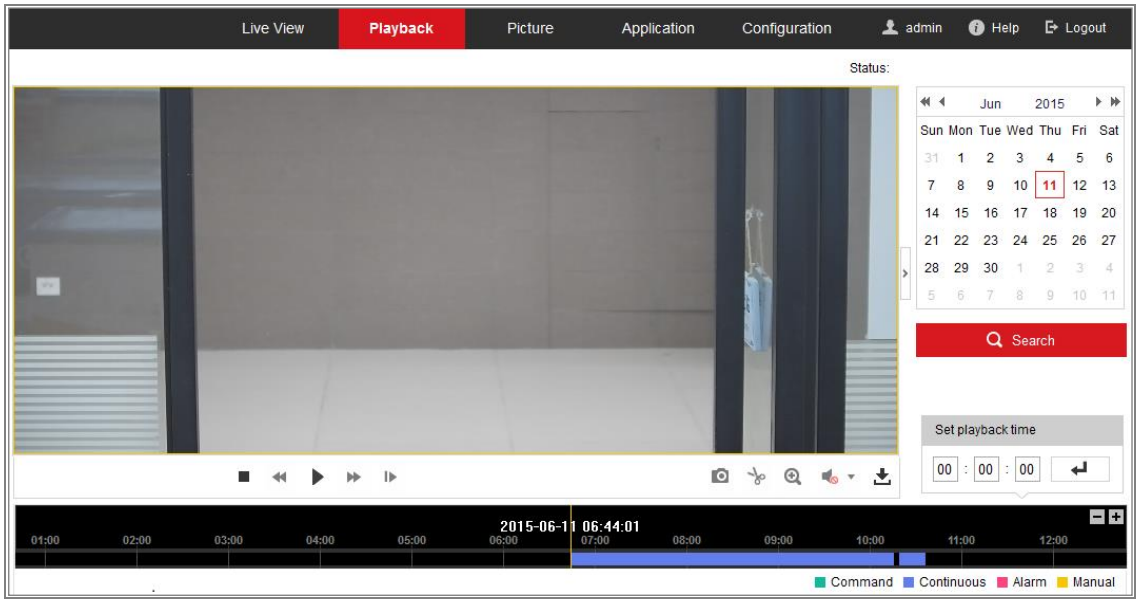



Figure 13-1 Playback Interface

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


Figure 13-2 Search Video

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

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

Figure 13-3 Playback Toolbar

Table 13-1 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.

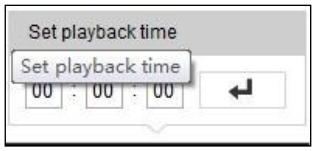



Figure 13-4 Set Playback Time

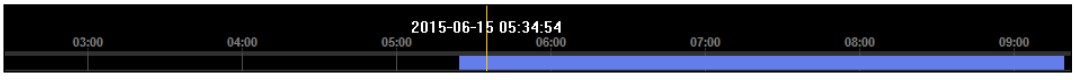



Figure 13-5 Progress Bar

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

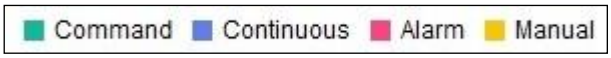



Figure 13-6 Video Types

# Chapter 14 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.

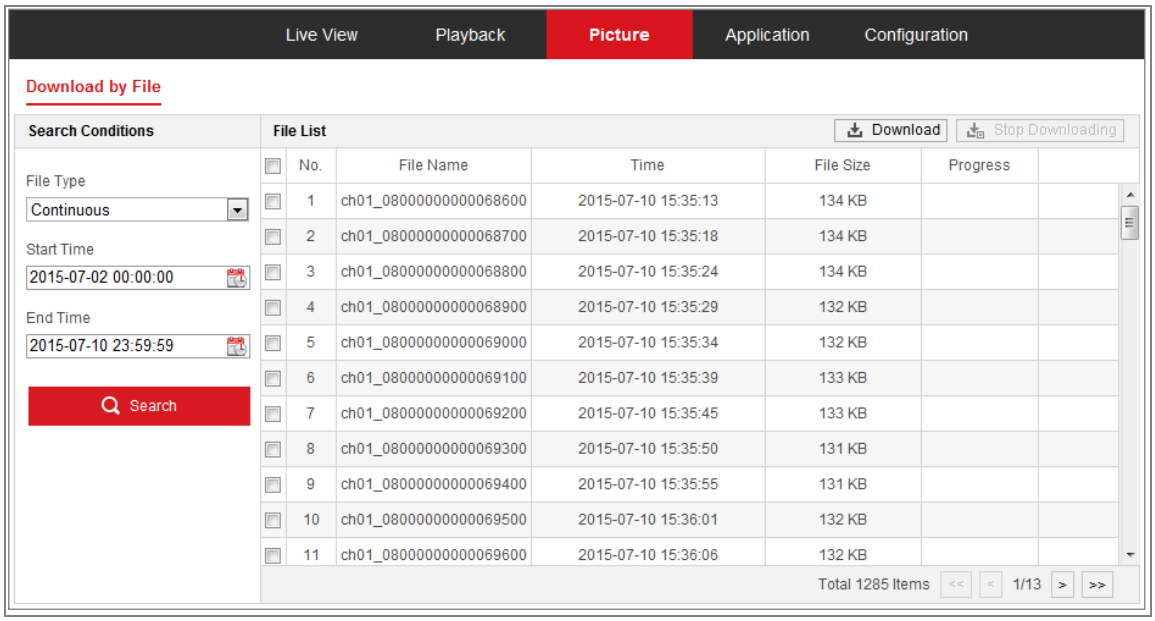



Figure 14-1 Picture Search Interface

***Steps:***

1. Select the file type from the dropdown list. Continuous, Motion, Alarm, Motion | Alarm, Motion & Alarm, Line Crossing, Intrusion Detection, and Scene Change Detection are selectable.
2. Select the start time and end time.
3. Click **Search** to search the matched pictures.
4. 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.

# Chapter 15 Application

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

***Note:*** Application function varies according to the different camera models.

## 15.1 People Counting Statistics

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

***Steps:***

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

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

2. Select the statistics type. People Entered, People Exited and All are selectable.
3. Select the start time.
4. (Optional) Check **Counting Children Statistics**.
5. Click **Counting**.

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

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

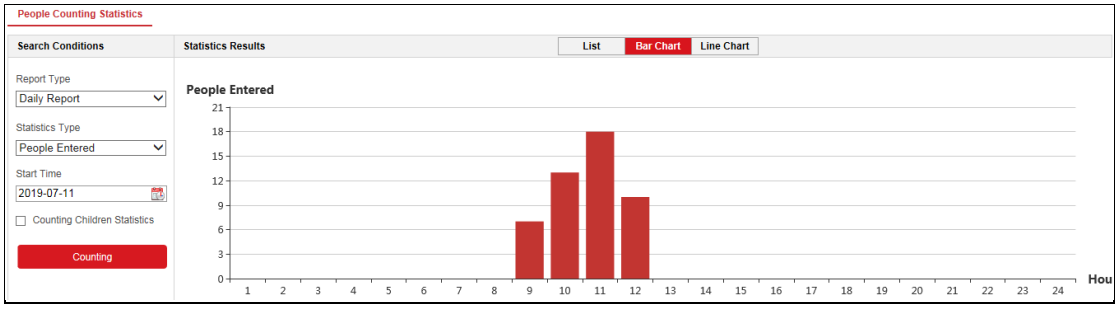


Figure 15-1 People Counting

# Appendix

## Appendix 1 SADP Software Introduction

- **Description of SADP**

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

- **Search active devices online**

♦ **Search online devices automatically**

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

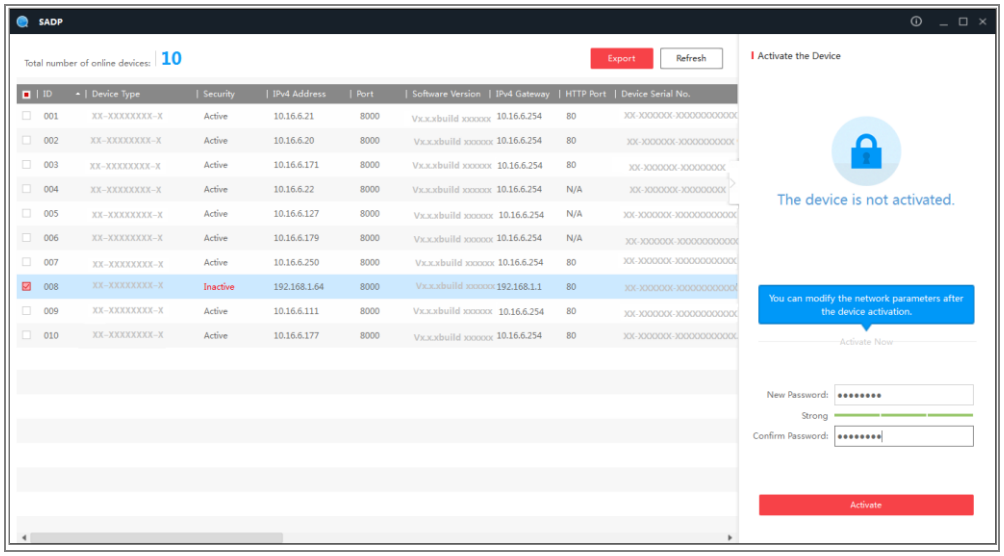



Figure A.1.1 Searching Online Devices

***Note:***

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

♦ **Search online devices manually**

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

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

## ● Modify network parameters

***Steps:***

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

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

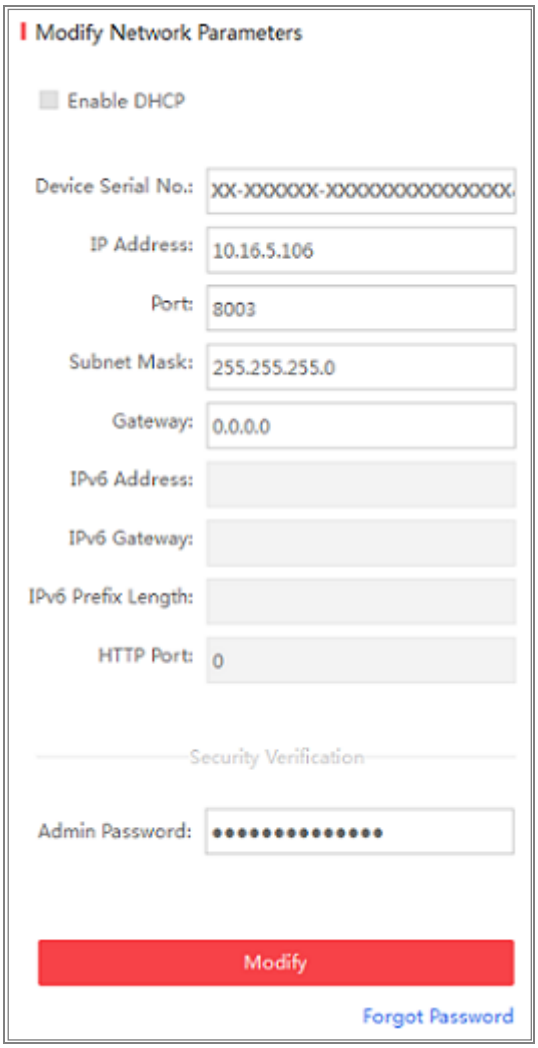



Figure A.1.2 Modify Network Parameters

# Appendix 2 Port Mapping

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

***Steps:***

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

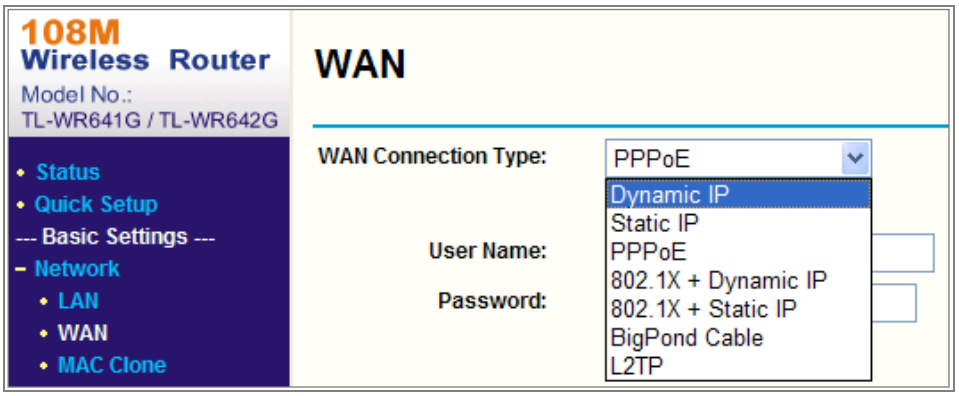



Figure A.2.1 Select the WAN Connection Type

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

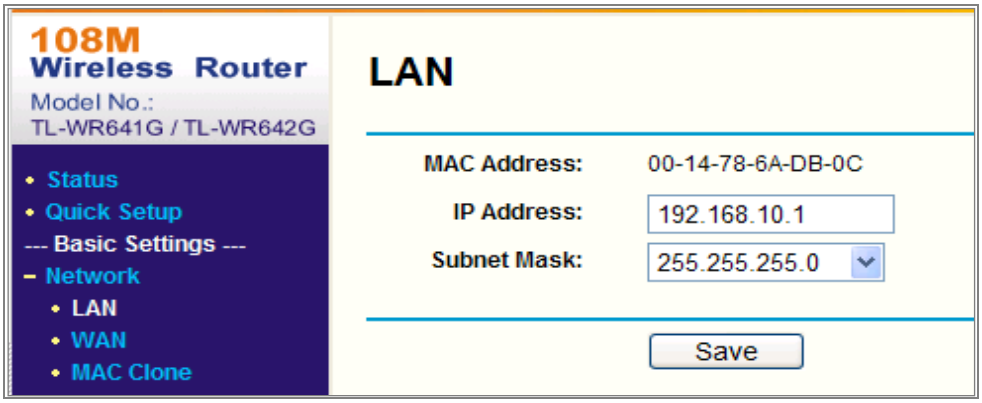



Figure A.2.2 Set the LAN parameters

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

***Example:***

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

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

***Steps:***

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

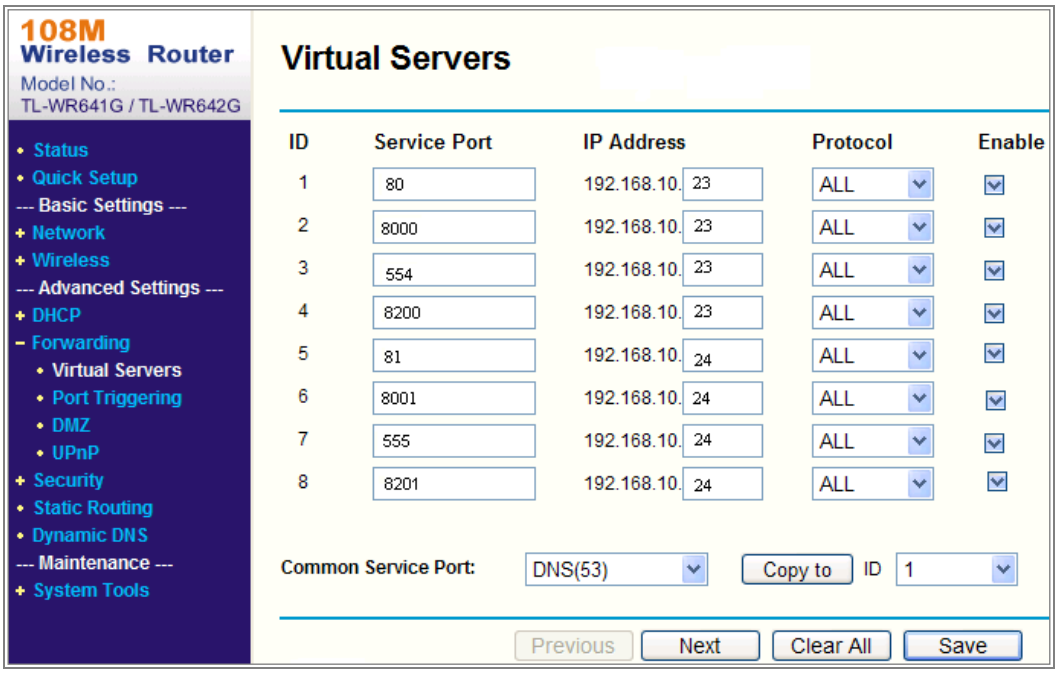



Figure A.2.3 Port Mapping

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


See Far, Go Further