Network Camera

User Manual

User 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.

Please use this user manual under the guidance of professionals.

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 OUR COMPANY 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 OUR COMPANY, 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 OUR COMPANY 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. OUR COMPANY 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, OUR COMPANY 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. OUR COMPANY SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

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

Regulatory Information

FCC Information

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

FCC Conditions

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

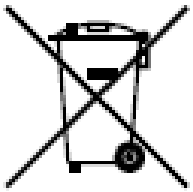
1. This device may not cause harmful interference.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

CE This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2004/108/EC, the RoHS Directive 2011/65/EU.

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



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

Industry Canada ICES-003 Compliance

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

Safety Instruction

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

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

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

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

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

Warnings:

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

Cautions:

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

- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C to +60°C, or -40°C to +60°C if the camera model has an “H” in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, 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 10

Chapter 2 Network Connection 11

2.1 Setting the Network Camera over the LAN 11

2.1.1 Wiring over the LAN 11

2.1.2 Activating the Camera 12

2.2 Setting the Network Camera over the WAN 18

2.2.1 Static IP Connection 18

2.2.2 Dynamic IP Connection 19

Chapter 3 Access to the Network Camera 22

3.1 Accessing by Web Browsers 22

3.1.1 User Login 22

3.2 Accessing by Client Software 24

Chapter 4 Wi-Fi Settings 26

4.1 Configuring Wi-Fi Connection in Manage and Ad-hoc Modes 26

4.2 Easy Wi-Fi Connection with WPS function 30

4.3 IP Property Settings for Wireless Network Connection 32

Chapter 5 Live View 34

5.1 Live View Page 34

5.2 Starting Live View 35

5.3 Recording and Capturing Pictures Manually 36

5.4 Operating PTZ Control 36

5.4.1 PTZ Control Panel 36

5.4.2 Setting / Calling a Preset 37

5.4.3 Setting / Calling a Patrol 38

Chapter 6 Network Camera Configuration 40

6.1 Configuring Local Parameters 40

6.2 Configure System Settings 42

6.2.1 Configuring Basic Information 42

6.2.2 Configuring Time Settings 43

6.2.3 Configuring RS232 Settings 45

6.2.4 Configuring RS485 Settings 45

6.2.5 Configuring DST Settings 46

6.3 Maintenance 47

6.3.1 Upgrade & Maintenance 47

6.3.2 Log 48

6.4 Security Settings 49
6.4.1 Authentication 50
6.4.2 IP Address Filter 50
6.4.3 Security Service 52
6.5 User Management 52
Chapter 7 Network Settings 56
7.1 Configuring Basic Settings 56
7.1.1 Configuring TCP/IP Settings 56
7.1.2 Configuring DDNS Settings 58
7.1.3 Configuring PPPoE Settings 60
7.1.4 Configuring Port Settings 61
7.1.5 Configure NAT (Network Address Translation) Settings 61
7.2 Configure Advanced Settings 62
7.2.1 Configuring SNMP Settings 63
7.2.2 Configuring FTP Settings 64
7.2.3 Email Settings 66
7.2.4 HTTPS Settings 68
7.2.5 Configuring QoS Settings 70
7.2.6 Configuring 802.1X Settings 71
Chapter 8 Video/Audio Settings 73
8.1 Configuring Video Settings 73
8.2 Configuring Audio Settings 75
8.3 Configuring ROI Encoding 76
8.4 Display Info. on Stream 78
8.5 Configuring Target Cropping 78
Chapter 9 Image Settings 80
9.1 Configuring Display Settings 80
9.1.1 Day/Night Auto-Switch 80
9.1.2 Day/Night Scheduled-Switch 83
9.2 Configuring OSD Settings 84
9.3 Configuring Privacy Mask 85
9.4 Configuring Picture Overlay 86
Chapter 10 Event Settings 88
10.1 Basic Events 88
10.1.1 Configuring Motion Detection 88
10.1.2 Configuring Video Tampering Alarm 94
10.1.3 Configuring Alarm Input 96
10.1.4 Configuring Alarm Output 97

10.1.5 Handling Exception 98

10.2 Smart Events 99

10.2.1 Configuring Intrusion Detection 99

10.2.2 Configuring Line Crossing Detection 101

10.2.3 People Counting 103

Chapter 11 Storage Settings 106

11.1 Configuring Record Schedule 106

11.2 Configure Capture Schedule 109

11.3 Configuring Net HDD 110

11.4 Configuring Lite Storage 112

Chapter 12 Playback 114

Chapter 13 Picture 116

Chapter 14 Application 117

14.1 People Counting Statistics 117

Appendix 118

Appendix 1 SADP Software Introduction 118

Appendix 2 Port Mapping 121

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

Chapter 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 NVMS7000 software to search and change the IP of the network camera.

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

2.1.1 Wiring over the LAN

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

Purpose:

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.

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

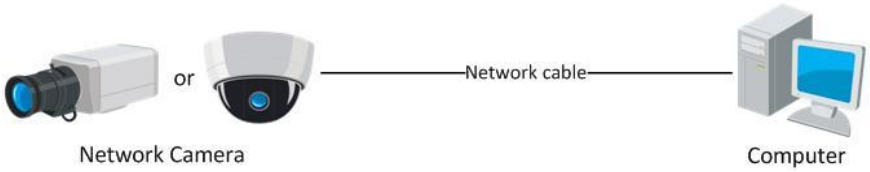


Figure 2-1 Connecting Directly

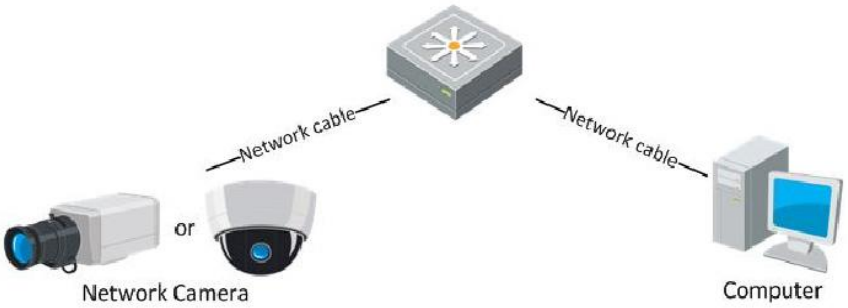


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Camera

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

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

❖ Activation via Web Browser

Steps:

1. Power on the camera, and connect the camera to the network.

2. Input the IP address into the address bar of the web browser, and click Enter to enter the activation interface.

Notes:

- The default IP address of the camera is 192.168.1.64.
- For the camera enables the DHCP by default, the IP address is allocated automatically. And you need to activate the camera via SADP software. Please refer to the following chapter for Activation via SADP.

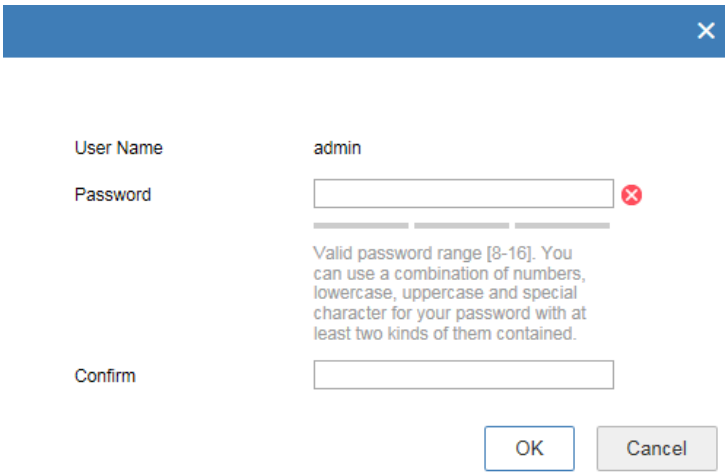


Figure 2-3 Activation via Web Browser

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

STRONG PASSWORD RECOMMENDED–We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including 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.

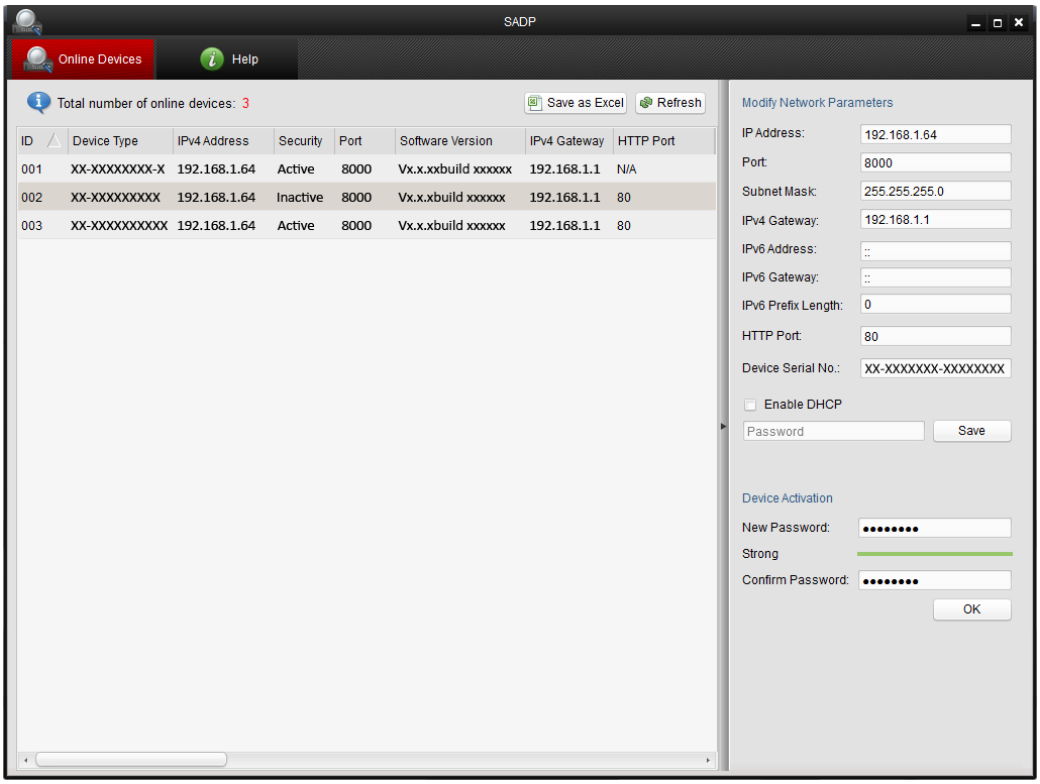


Figure 2-4 SADP Interface

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

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

4. Click **OK** to save the password.

You can check whether the activation is completed on the popup window. If activation failed, please make sure that the password meets the requirement and try again.

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

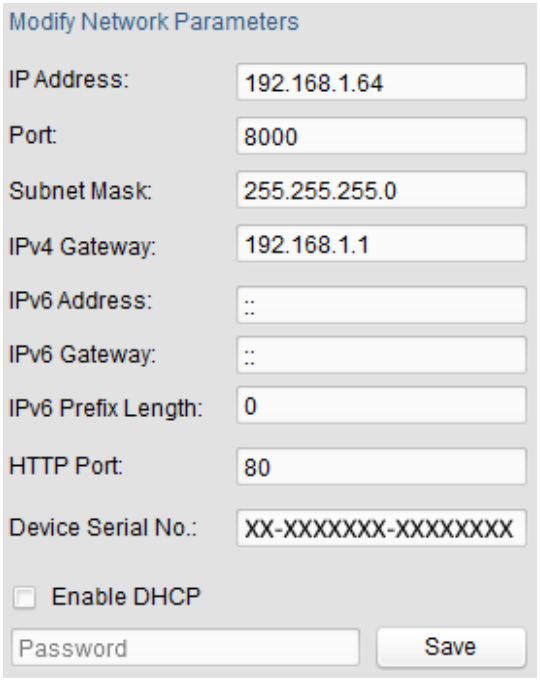


Figure 2-5 Modify the IP Address

6. Input the password and click the **Save** button to activate your IP address modification.

❖ Activation via Client Software

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

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

Steps:

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

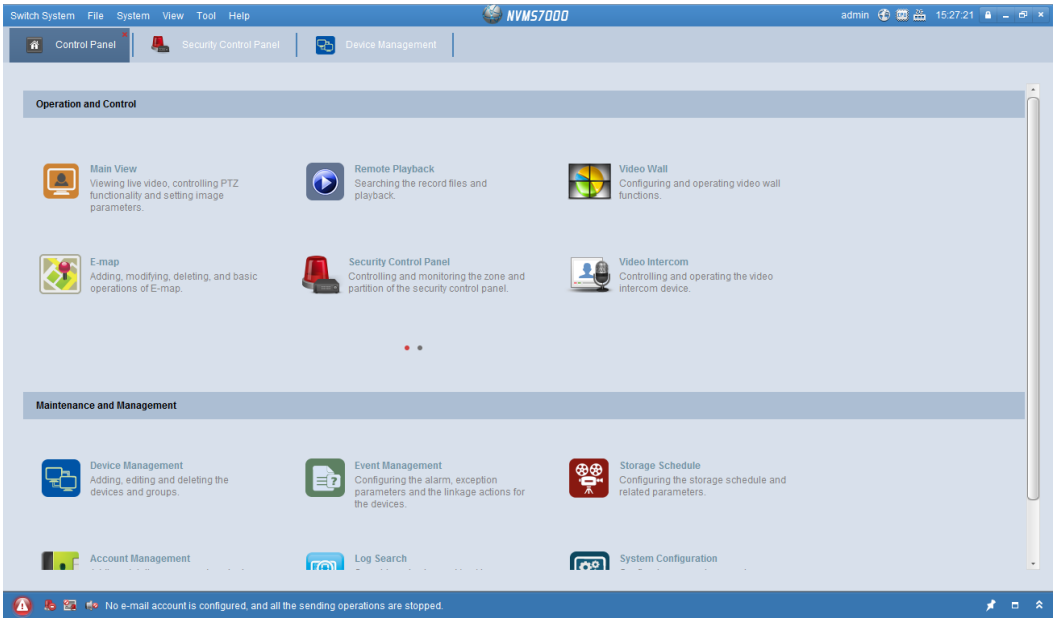


Figure 2-6 Control Panel

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

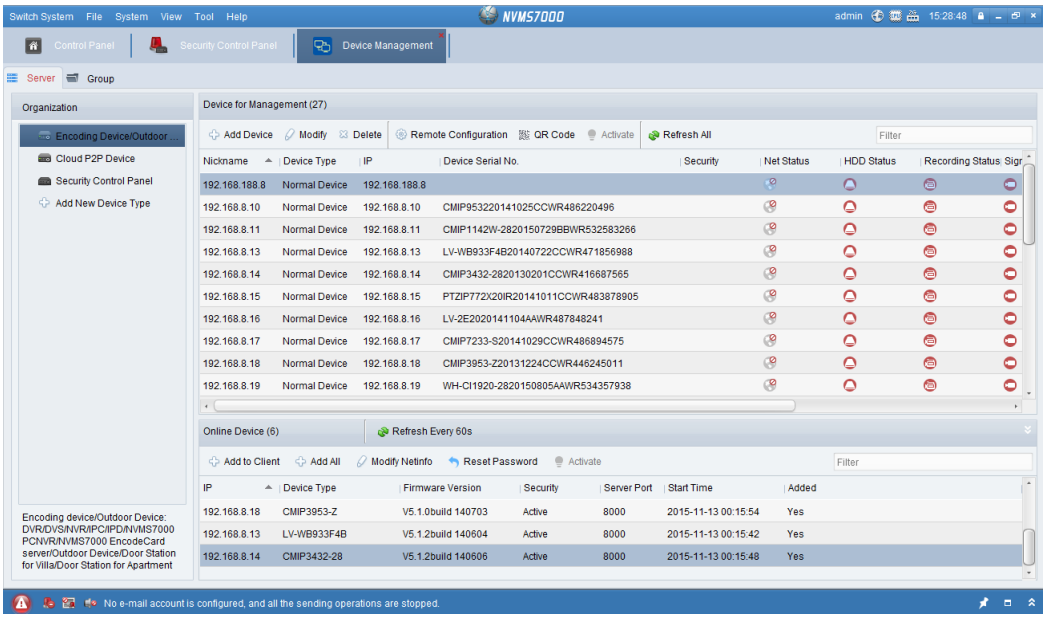


Figure 2-7 Device Management Interface

3. Check the device status from the device list, and select an inactive device.

4. Click the **Activate** button to pop up the Activation interface.

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

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

Figure 2-8 Activation Interface (Client Software)

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

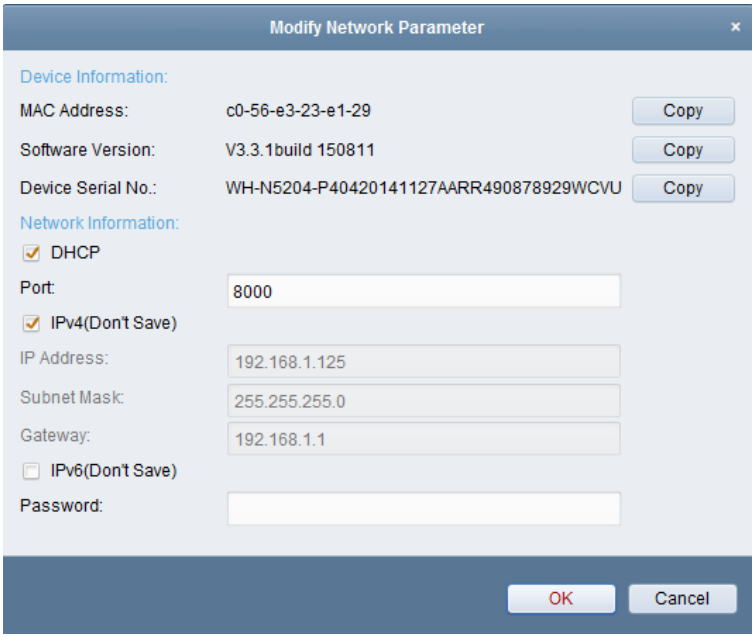


Figure 2-9 Modifying the Network Parameters

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

9. Input the password to activate your IP address modification.

2.2 Setting the Network Camera over the WAN

Purpose:

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

2.2.1 Static IP Connection

Before you start:

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

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

Steps:

1. Connect the network camera to the router.

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

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

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

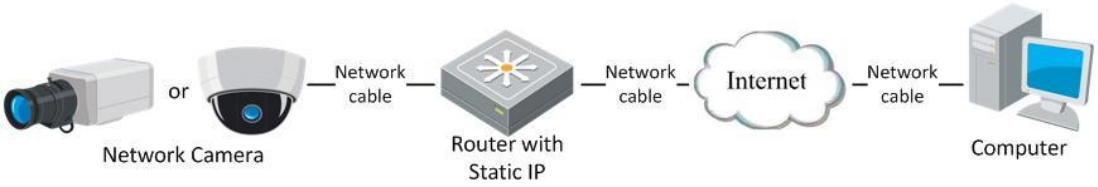


Figure 2-10 Accessing the Camera through Router with Static IP

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

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

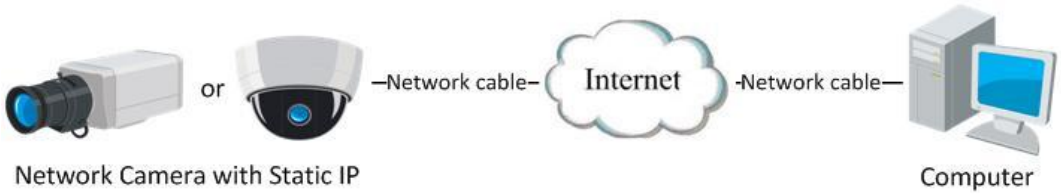


Figure 2-11 Accessing the Camera with Static IP Directly

2.2.2 Dynamic IP Connection

Before you start:

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

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

Steps:

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

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

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

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

Purpose:

This camera supports the PPPoE auto dial-up function. The camera gets a public IP address by ADSL dial-up after the camera is connected to a modem. You need to configure the PPPoE parameters of the network camera. Refer to *Section 6.3.3* ***Configuring PPPoE Settings*** for detailed configuration.

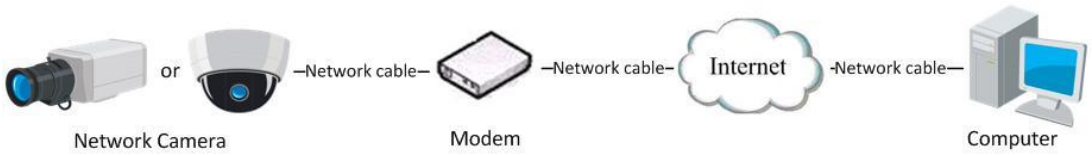


Figure 2-12 Accessing the Camera with Dynamic IP

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

♦ Normal Domain Name Resolution

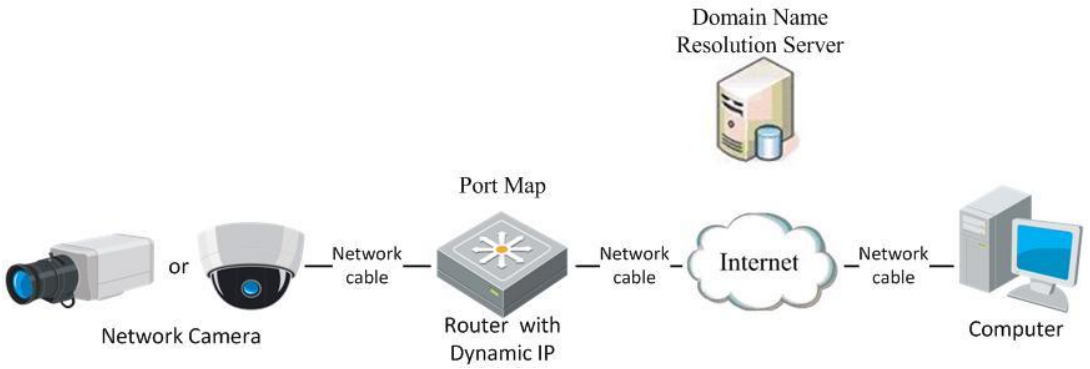


Figure 2-13 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network camera. Refer to *Section 6.3.4* ***Configuring DDNS Settings*** for detailed configuration.
3. Visit the camera via the applied domain name.

♦ Private Domain Name Resolution

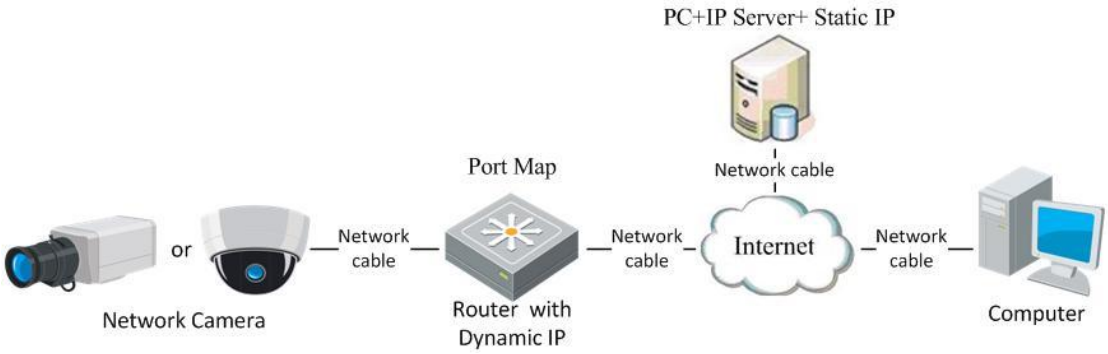


Figure 2-14 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.
2. Access the network camera through the LAN with a web browser or the client software.
3. Enable DDNS and select IP Server as the protocol type. Refer to *Section 6.3.4* ***Configuring DDNS Settings*** for detailed configuration.

Chapter 3 Access to the Network Camera

3.1 Accessing by Web Browsers

3.1.1 User Login

Steps:

1. Open the web browser.
2. In the browser address bar, input the IP address of the network camera, and press the **Enter** key to enter the login interface.
3. Activate the network camera for the first time using, refer to the section 2.1.2 for details.

   Note:

   - The default IP address is 192.168.1.64.
   - If the camera is not activated, please activate the camera first according to Chapter 2.1.2.

4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click **Login**.

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

   Note:

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

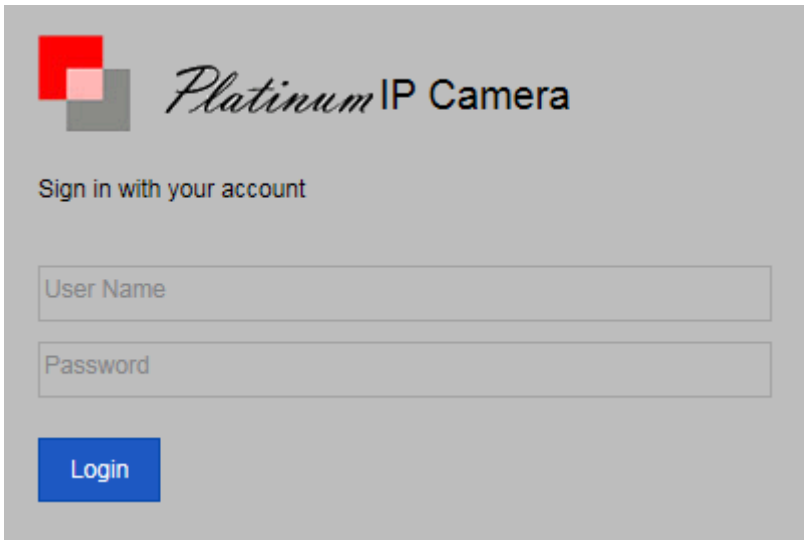


Figure 3-1 Login Interface

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

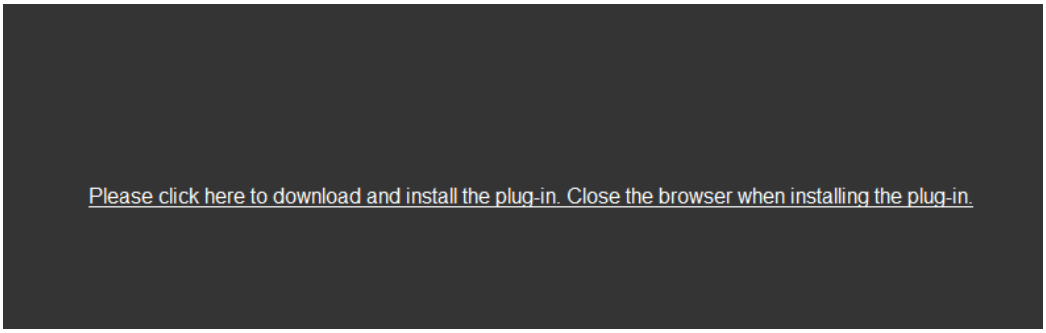


Figure 3-2 Download and Install Plug-in

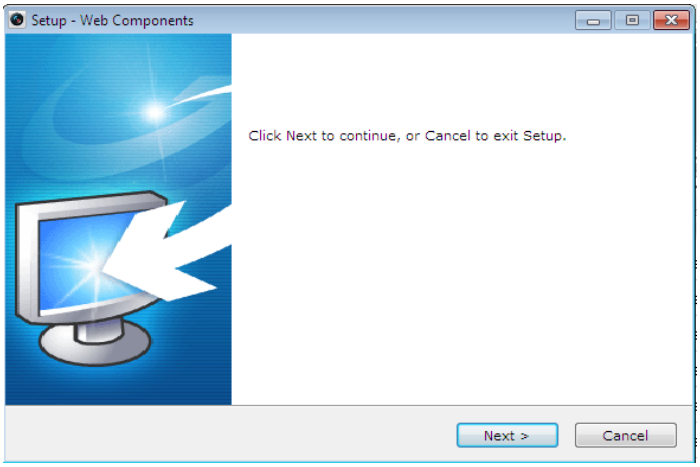


Figure 3-3 Install Plug-in (1)

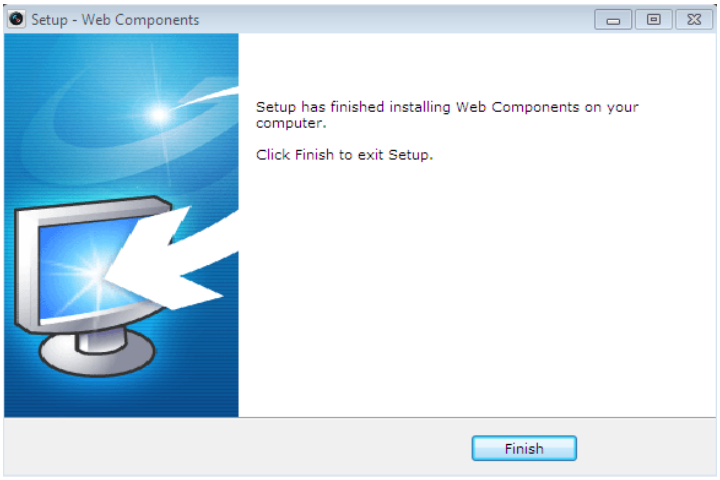


Figure 3-4 Install Plug-in (2)

Note: You may have to close the web browser to install the plug-in. Please reopen the web browser and log in again after installing the plug-in.

3.2 Accessing by Client Software

The product CD contains the NVMS7000 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 NVMS7000 client software are shown as below.

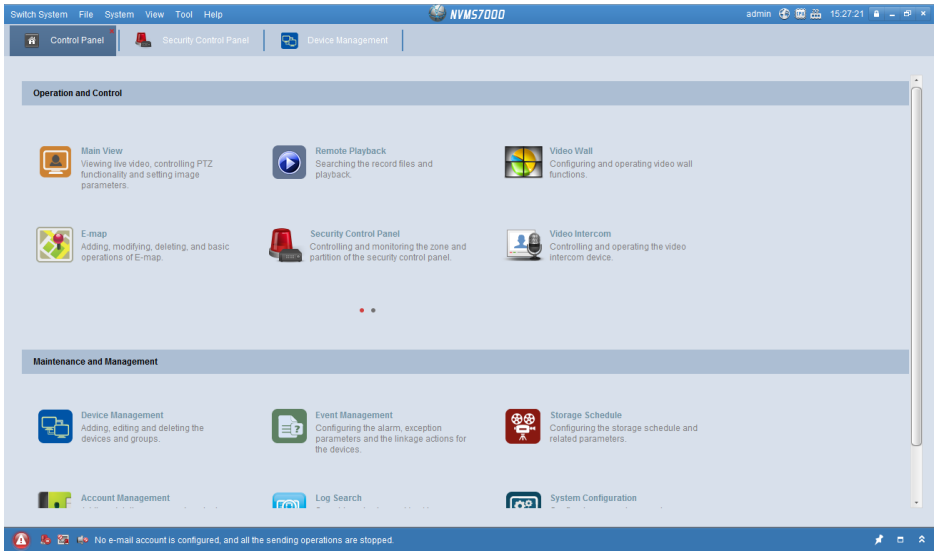


Figure 3-5 NVMS7000 Control Panel

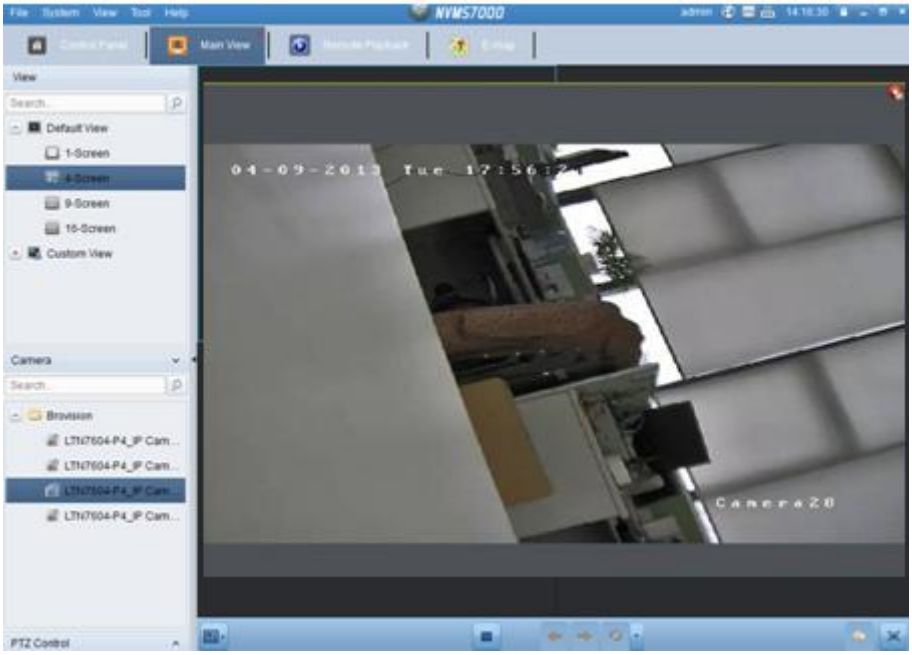


Figure 3-6 NVMS7000 Main View

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.

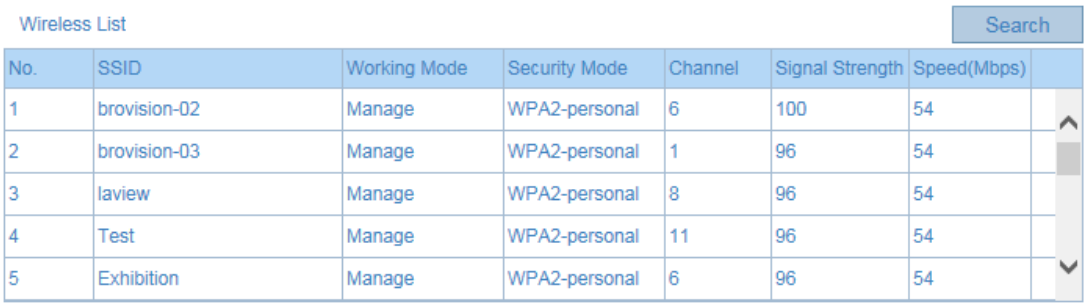


Figure 4-1 Wi-Fi List

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

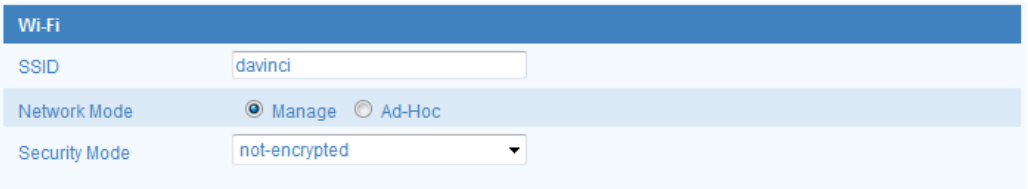


Figure 4-2 Wi-Fi Setting- Manage Mode

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.

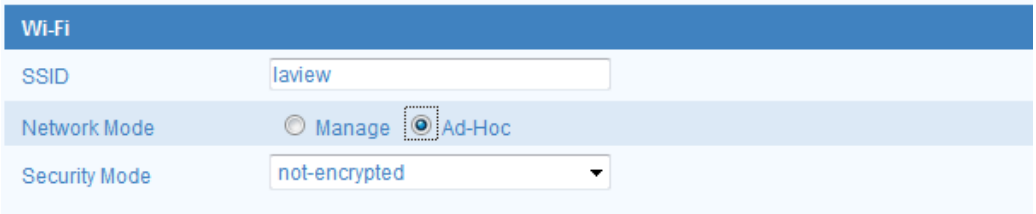


Figure 4-3 Wi-Fi Setting- Ad-hoc

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.

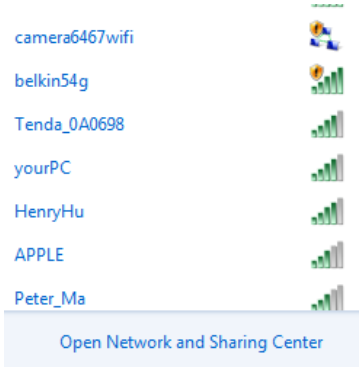


Figure 4-4 Ad-hoc Connection Point

6. Choose the SSID and connect.

Security Mode Description:

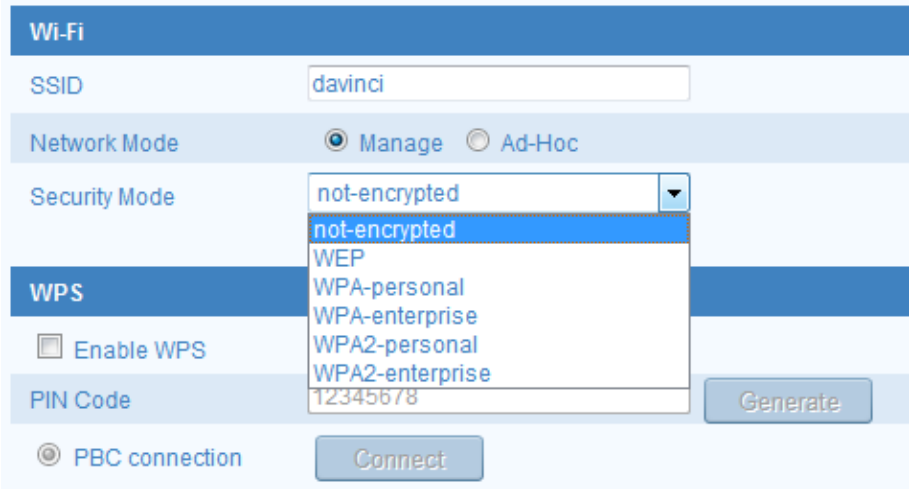


Figure 4-5 Security Mode

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

WEP mode:

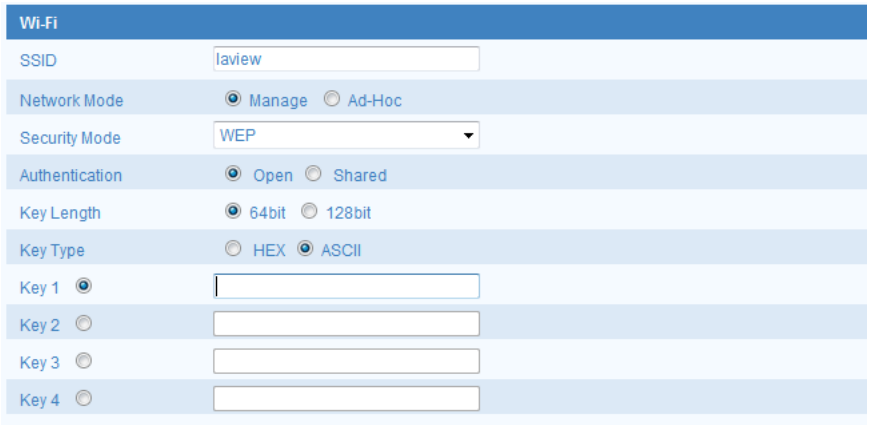


Figure 4-6 WEP Mode

- 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.

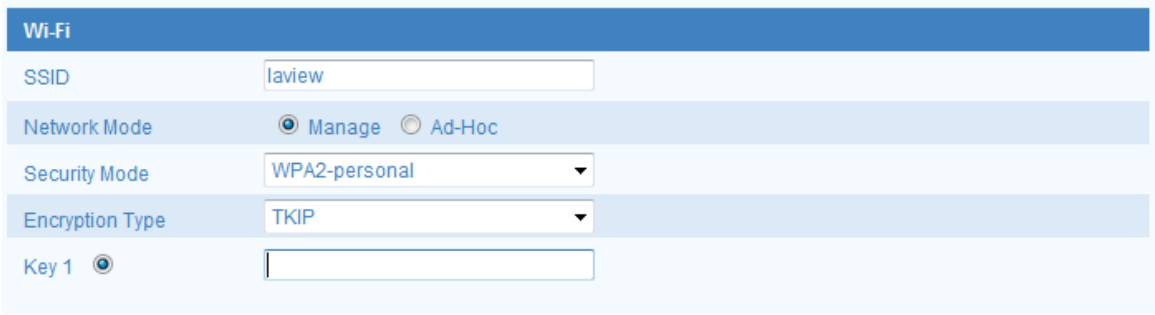


Figure 4-7 Security Mode- WPA-personal

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

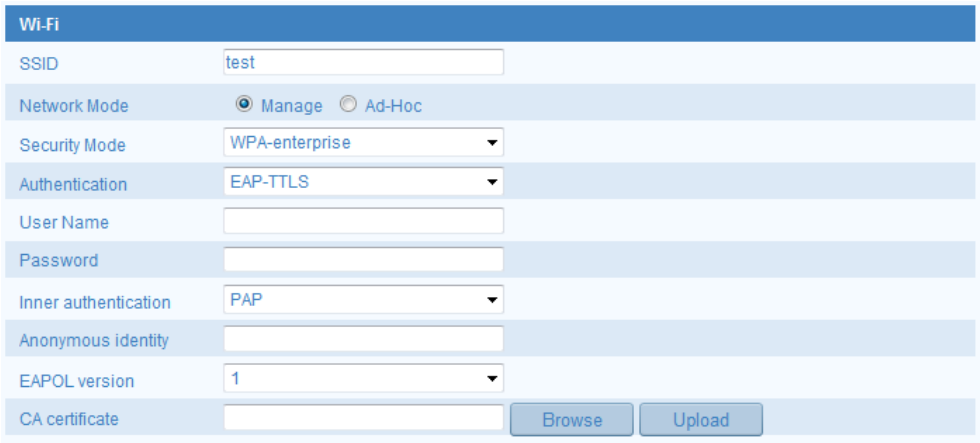


Figure 4-8 EAP-TLS

- 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:

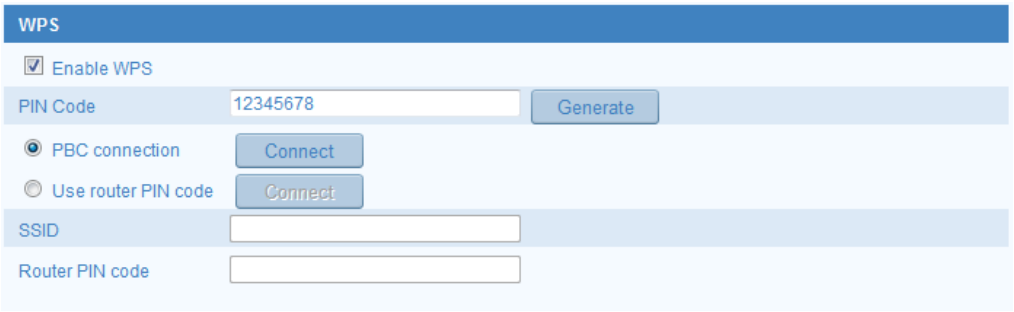
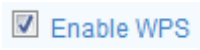


Figure 4-9 Wi-Fi Settings - WPS

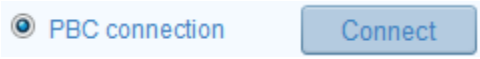
PBC Mode**:**

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

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 

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**.

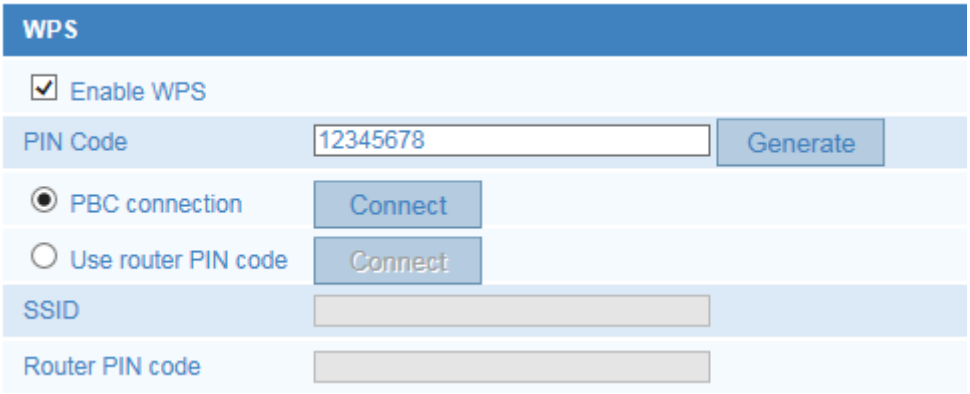


Figure 4-10 Use PIN Code

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.

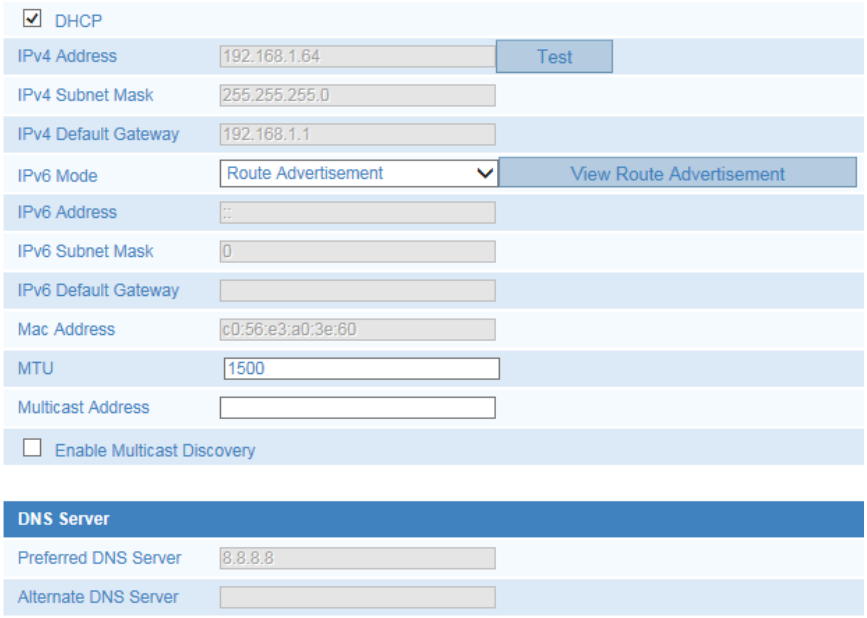


Figure 4-11 Setting WLAN Parameters

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:

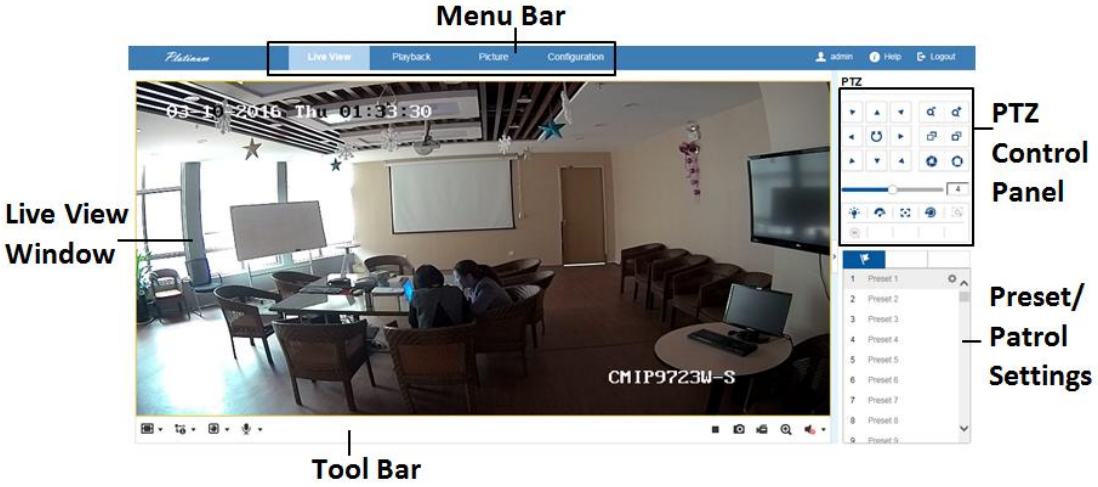


Figure 5-1 Live View Page

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, 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 is selectable if they are supported by the web browser.

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 5-2, 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.
	Live view with the main stream.
	Live view with the sub stream.
	Live view with the third stream.
	Click to select the third-party plug-in.
	Manually capture the picture.
/	Manually start/stop recording.
/	Audio on and adjust volume /Mute.
/	Turn on/off microphone.
/	Turn on/off digital zoom function.

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

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 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***.

5.4.1 PTZ Control Panel

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

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

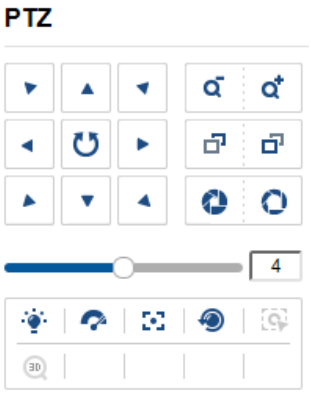


Figure 5-3 PTZ Control Panel

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 +/-
	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

5.4.2 Setting / Calling a Preset

- **Setting a Preset:**

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

Figure 5-4 Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.

   • Pan the camera to the right or left.

- Tilt the camera up or down.
- Zoom in or out.
- Refocus the lens.

3. Click to finish the setting of the current preset.
4. You can click to delete the preset.

- **Calling a Preset:**

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

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

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

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

Figure 5-5 Calling a Preset

5.4.3 Setting / Calling a Patrol

Note:

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

Steps:

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

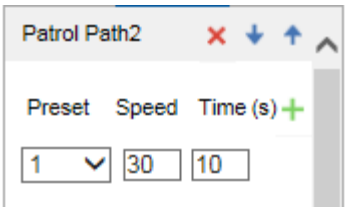


Figure 5-6 Add Patrol Path

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**.

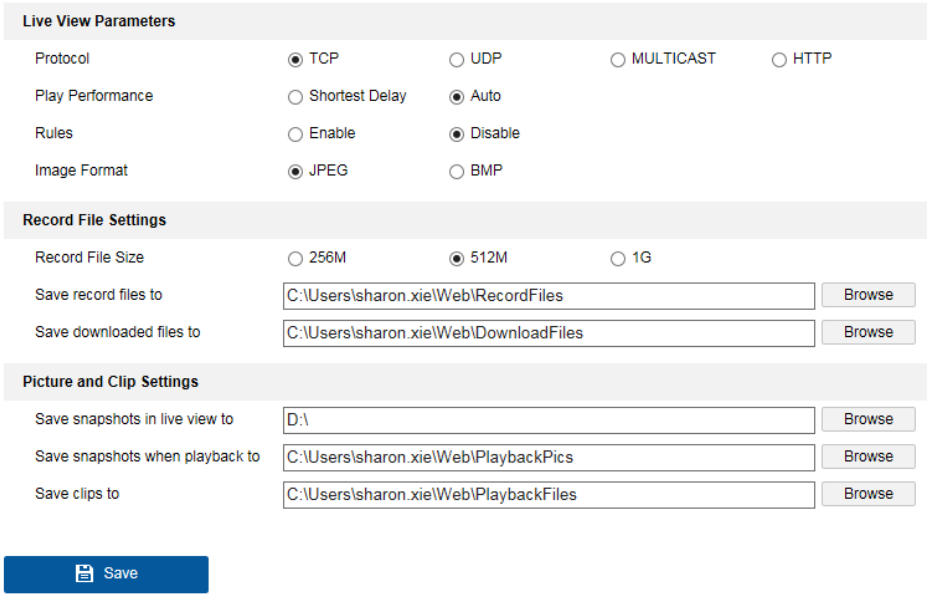


Figure 6-1 Local Configuration Interface

2. Configure the following settings:

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

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

UDP: Provides real-time audio and video streams.

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

MULTICAST: It's recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to *Section 6.1.1* ***Configuring TCP/IP Settings****.*

- **Live View Performance:** Set the live view performance to Shortest Delay or Auto.
- **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, face detection, or intrusion detection is triggered. E.g., enabled as the rules are, and the face detection is enabled as well, when a face is detected, it will be marked with a green rectangle on the live view.
- **Image Format:** Choose the image format for picture capture.

- **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.

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.

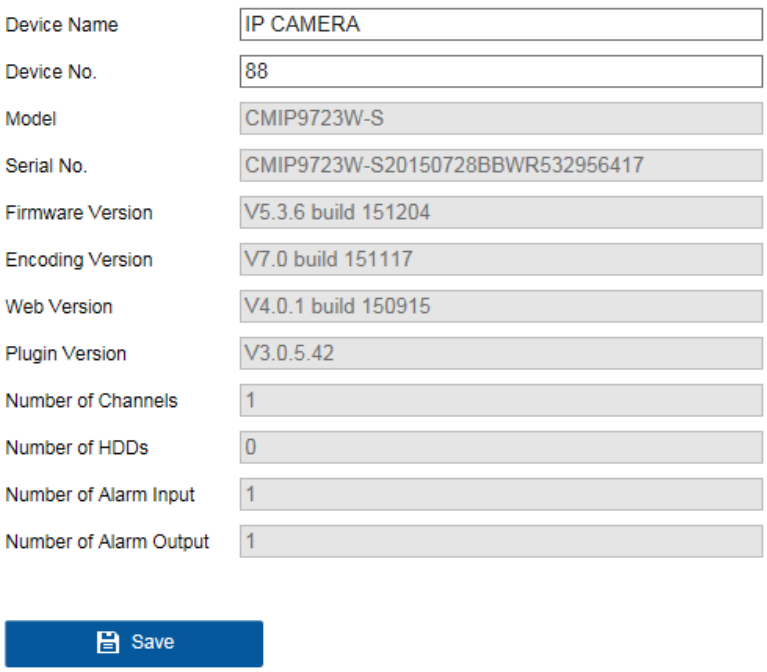


Figure 6-2 Basic Information

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**.

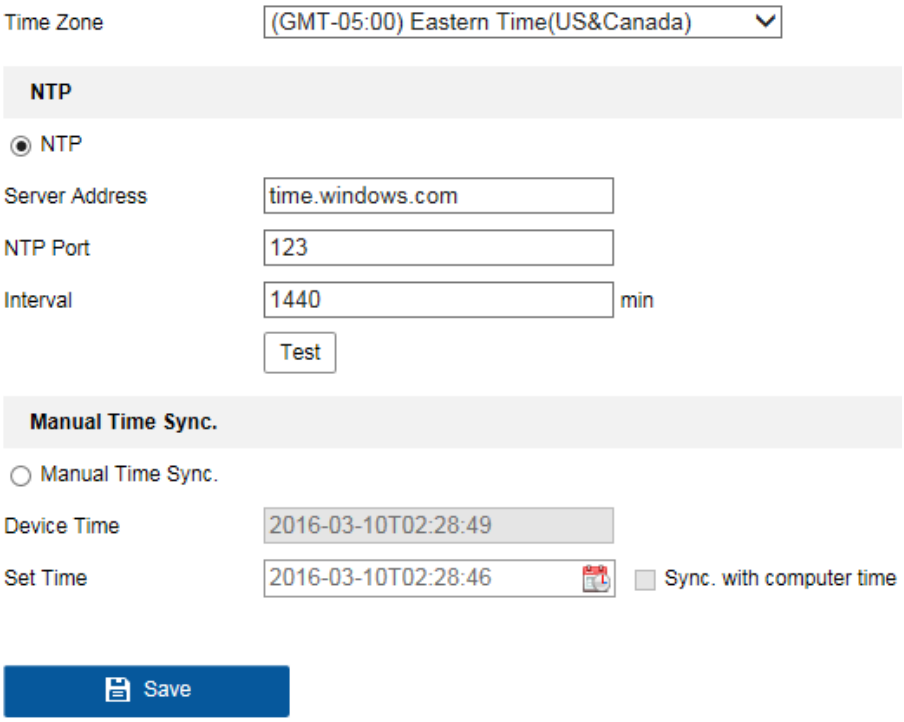


Figure 6-3 Time Settings

2. Select the Time Zone of your location from the drop-down menu.
3. Configure the NTP settings.
   (1) Click to enable the **NTP** function.
   (2) Configure the following settings:

   Server Address: IP address of NTP server.

   NTP Port: Port of NTP server.

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

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

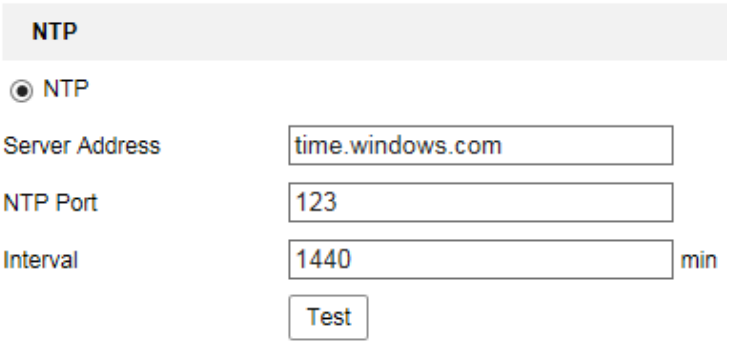


Figure 6-4 Time Sync by NTP Server

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

- Configure the manual time synchronization.

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

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

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

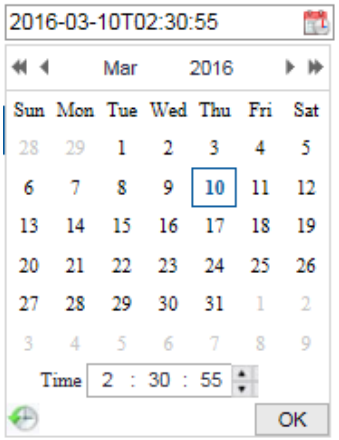


Figure 6-5 Time Sync Manually

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

6.2.3 Configuring RS232 Settings

The RS232 port can be used in two ways:

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

Steps:

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

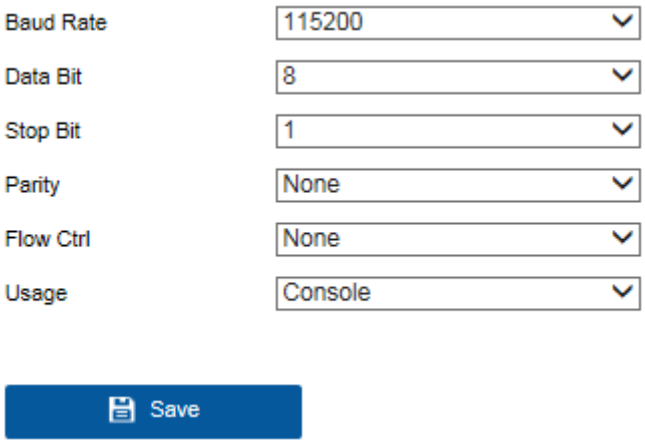


Figure 6-6 RS232 Settings

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

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

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**.

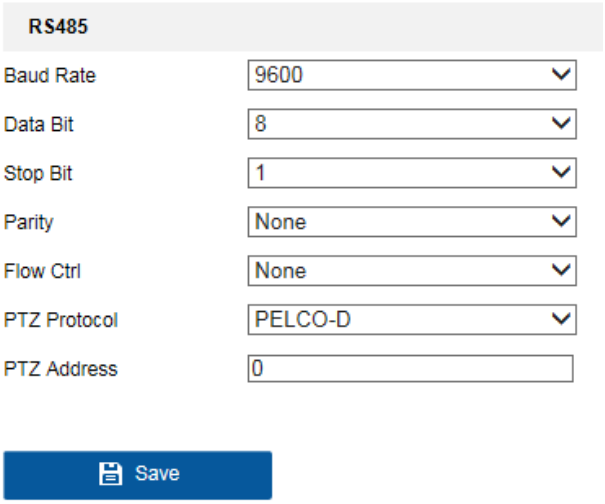


Figure 6-7 RS-485 Settings

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

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

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

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**

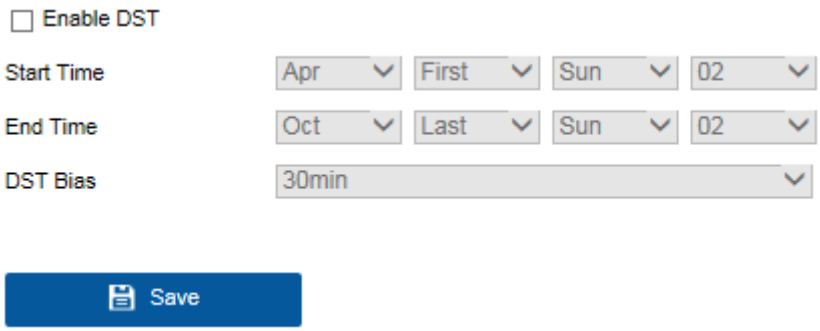


Figure 6-8 DST Settings

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

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.

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

- **Export/Import Config. File:** Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:

1. Click **Device Parameters** to export the current configuration file, and save it to certain place.
2. Click **Browse** to select the saved configuration file and then click **Import** to start importing configuration file.

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

- **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**.

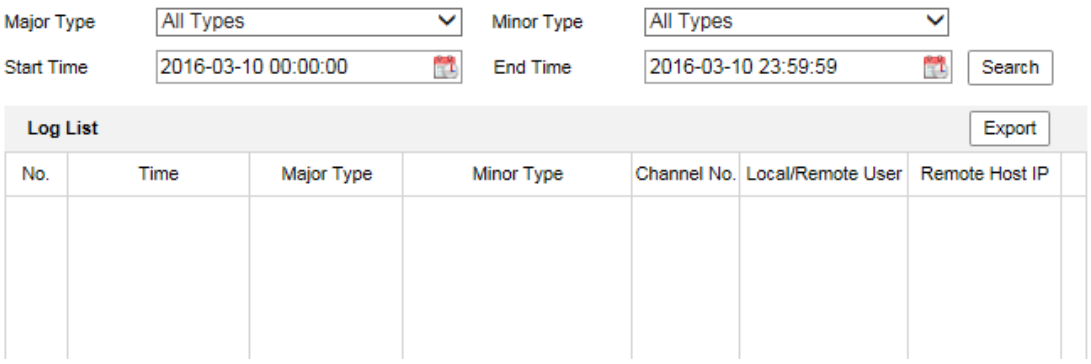


Figure 6-9 Log Searching Interface

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.

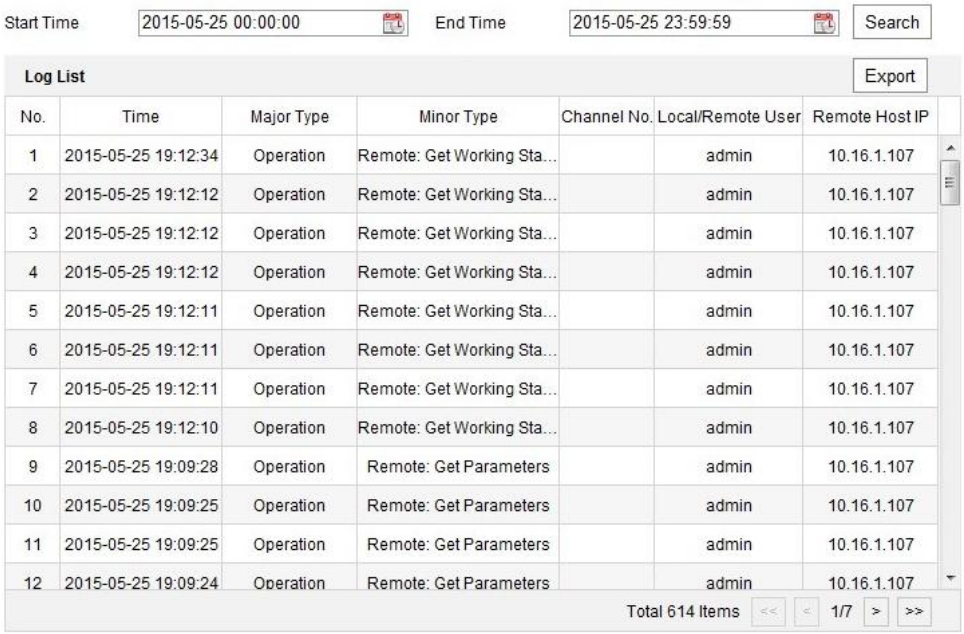


Figure 6-10 Log Searching

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

6.4 Security Settings

Configure the parameters, including Authentication, Anonymous Visit, 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.**

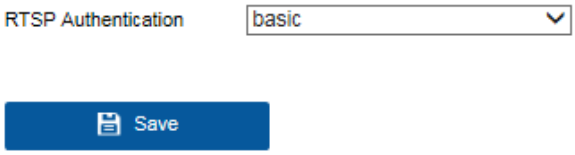


Figure 6-11 RTSP Authentication

2. Select the RTSP **Authentication** type **basic** or **disable** in the drop-down list to enable or disable the RTSP authentication.

Note: If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol via the IP address.

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

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**

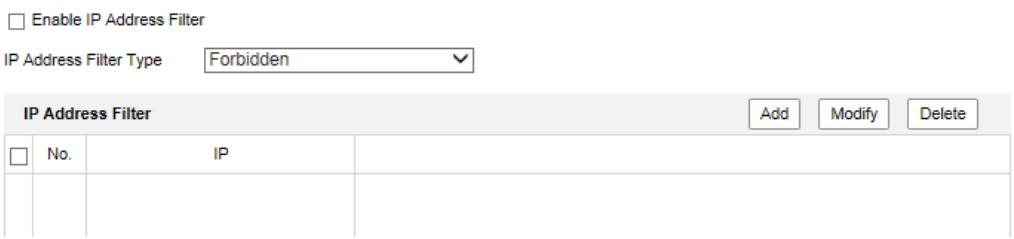


Figure 6-12 IP Address Filter Interface

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.

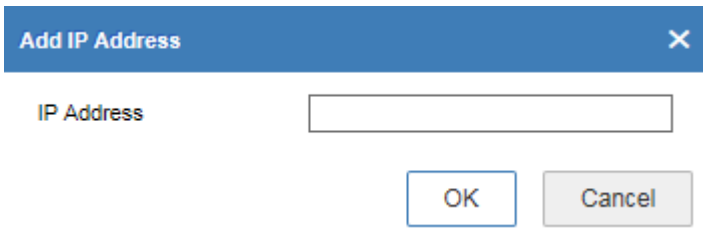


Figure 6-13 Add an IP

     (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.

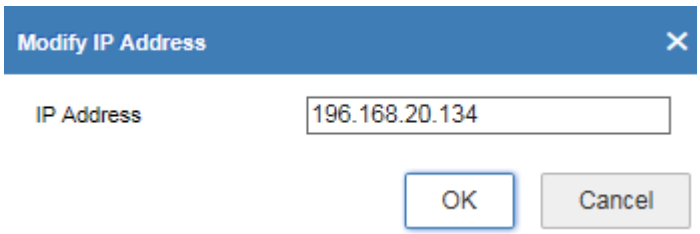


Figure 6-14 Modify an IP

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

   - Delete an IP Address

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

   - Delete all IP Addresses

     Click **Clear** to delete all the IP addresses.

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**.

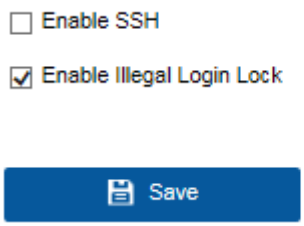


Figure 6-15 Security Service

2. Check the checkbox of **Enable SSH** to enable the data communication security, and uncheck the checkbox to disable the SSH.
3. Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/password attempts (5 times for the operator/user).

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

6.5 User Management

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

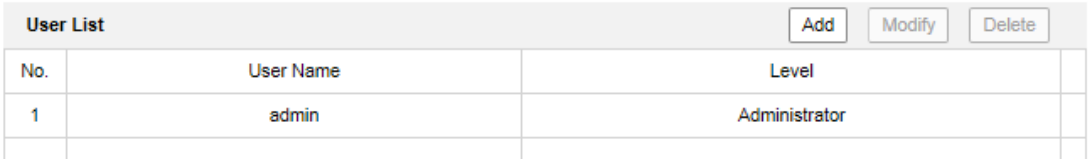


Figure 6-16 User Management Interface

- **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 **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.

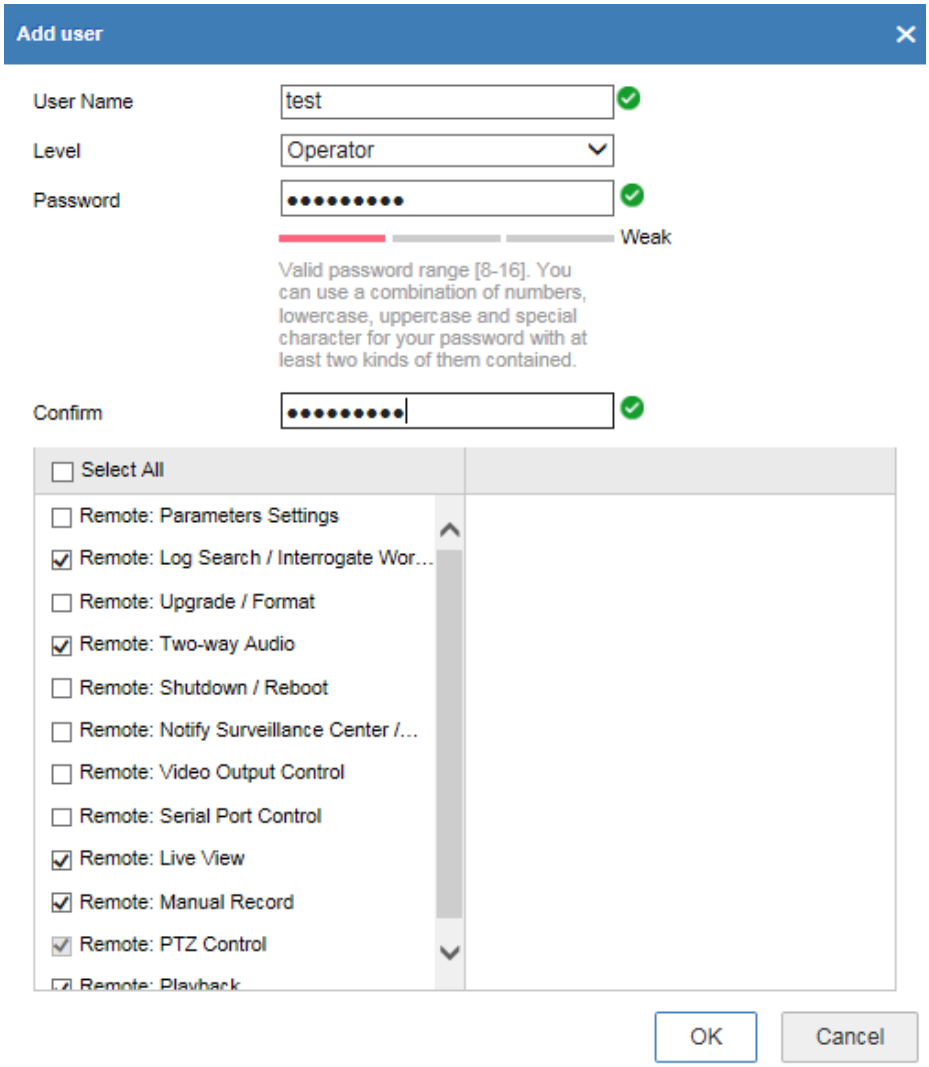


Figure 6-17 Add a User

- **Modifying a User**

Steps:

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

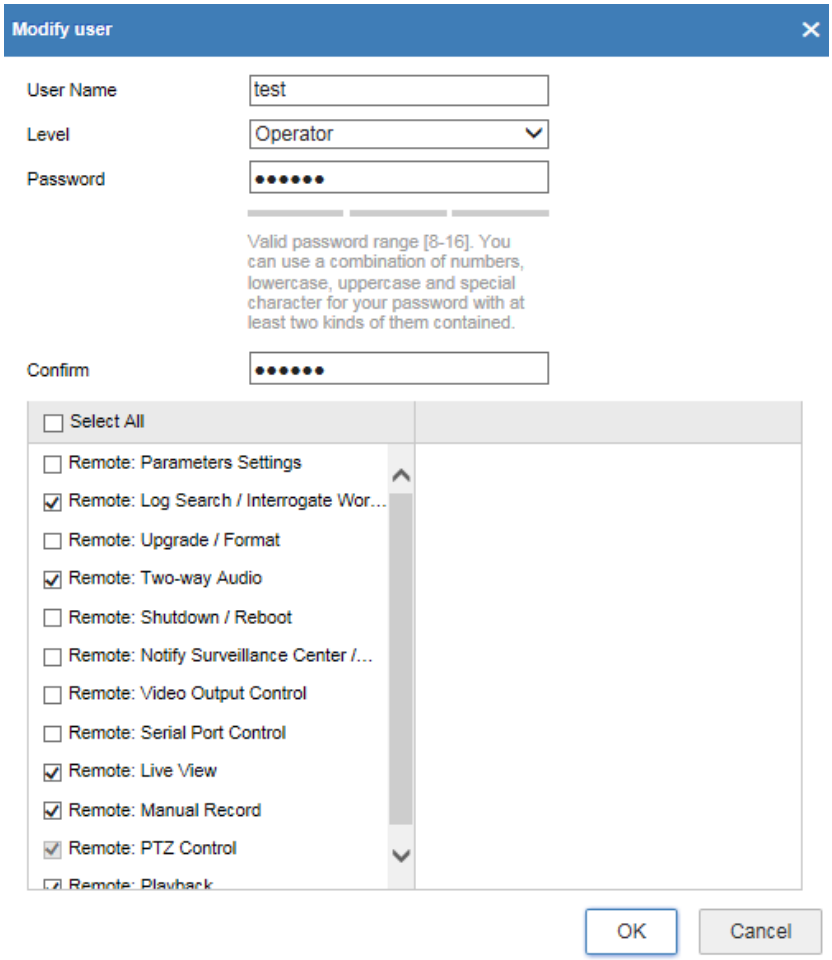


Figure 6-18 Modify a User

- **Deleting a User**

Steps:

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

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**

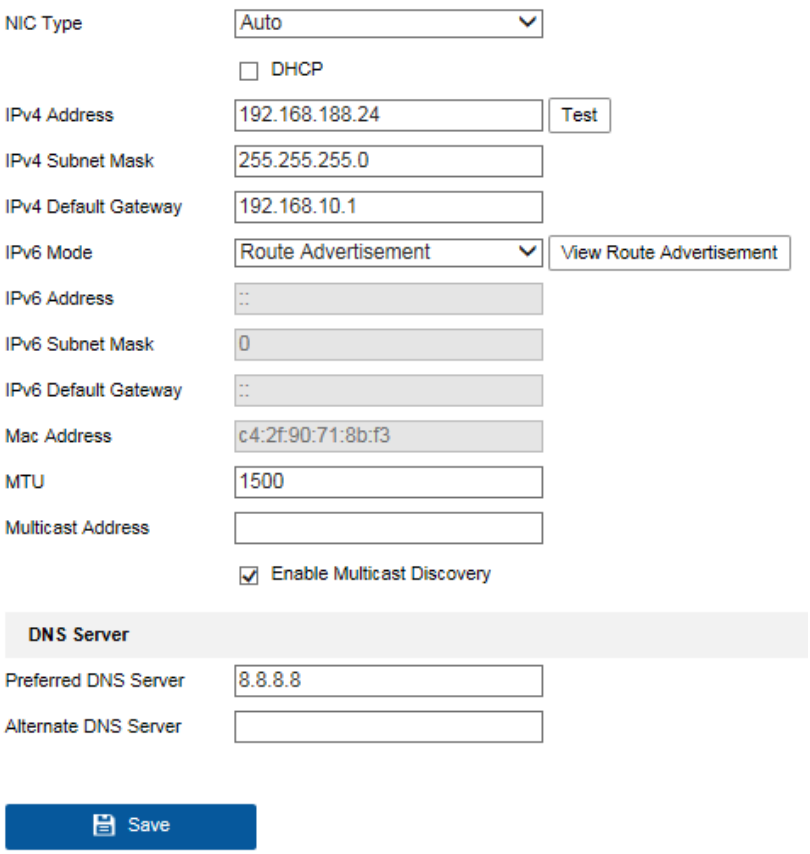


Figure 7-1 TCP/IP Settings

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 ~ 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**. HiDDNS and IPServer are selectable.
   - IP Server:

   Steps:

   (1) Enter the Server Address of the IP Server.

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

   Note: For the IP Server, you have to apply a static IP, subnet mask, gateway and preferred DNS from the ISP. The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software.

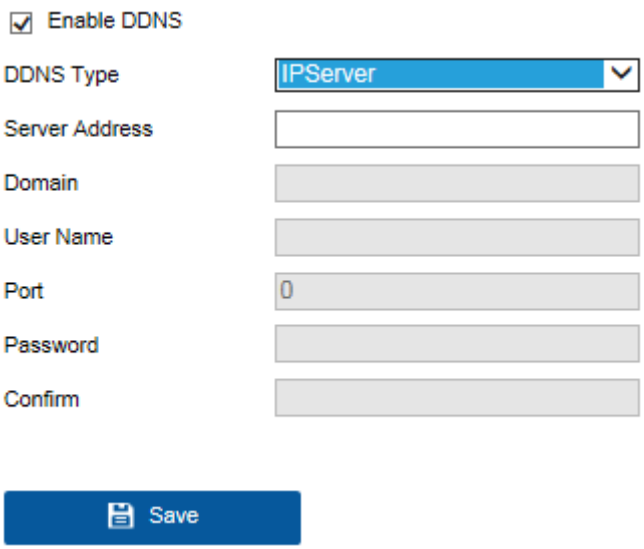


Figure 7-2 IP Server Settings

Note: For the US and Canada area, you can enter 173.200.91.74 as the server address.

- HiDDNS

Steps:

(1) Choose the DDNS Type as HiDDNS.

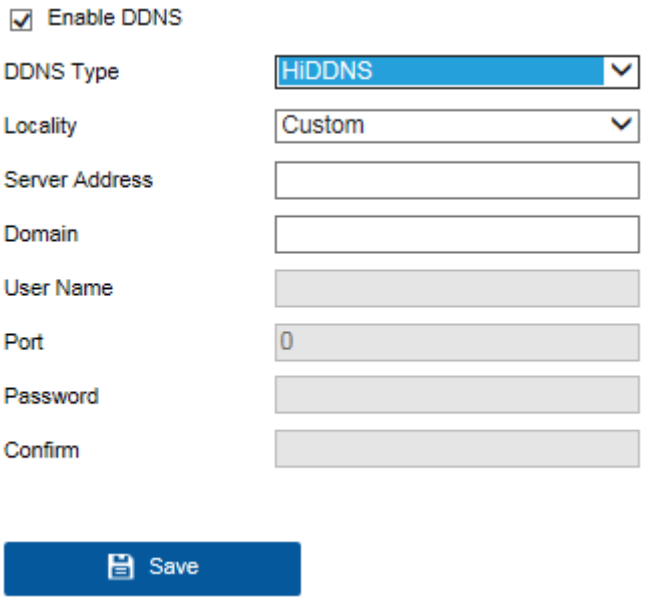


Figure 7-3 HiDDNS Settings

(2) Select the location and the country that the device is located in.

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

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

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

7.1.3 Configuring PPPoE Settings

Steps:

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

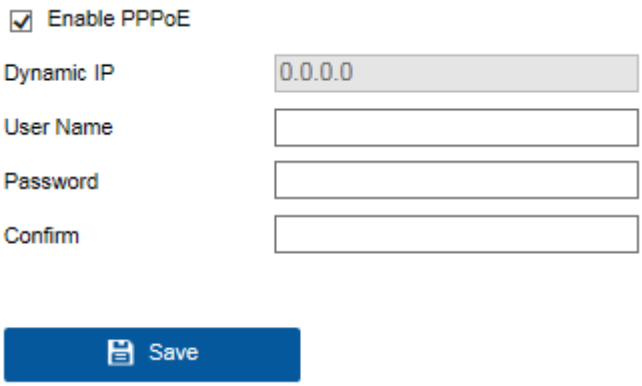


Figure 7-4 PPPoE Settings

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**

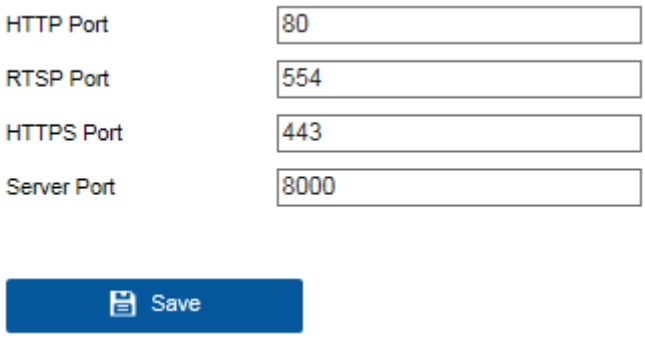


Figure 7-5 Port Settings

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

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

   RTSP Port: The default port number is 554 and it can be changed to any port No. ranges from 1024 to 65535.

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

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

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

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

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.

Steps:

1. Enter the NAT settings interface. **Configuration > Network > Basic Settings > NAT.**
2. Check the checkbox to enable the UPnP™ function.
3. Choose a nickname for the camera, or you can use the default name.
4. Select the port mapping mode. Manual and Auto are selectable. And for manual port mapping, you can customize the value of the external port.
5. Click **Save** to save the settings.

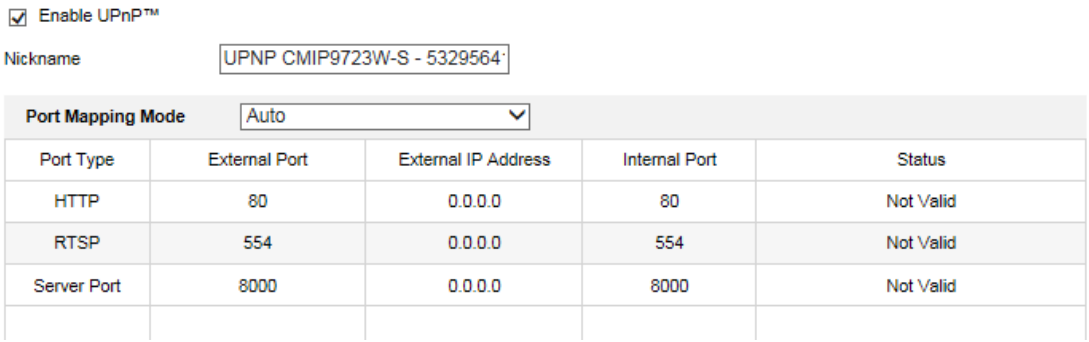


Figure 7-6 UPnP Settings

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**.

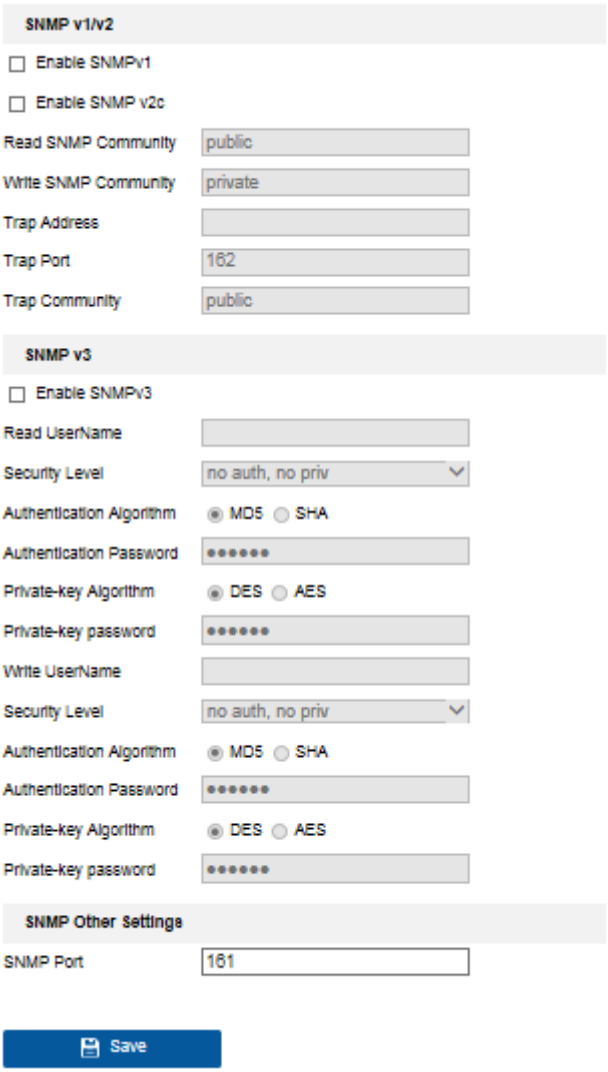


Figure 7-7 SNMP Settings

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.

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

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**.

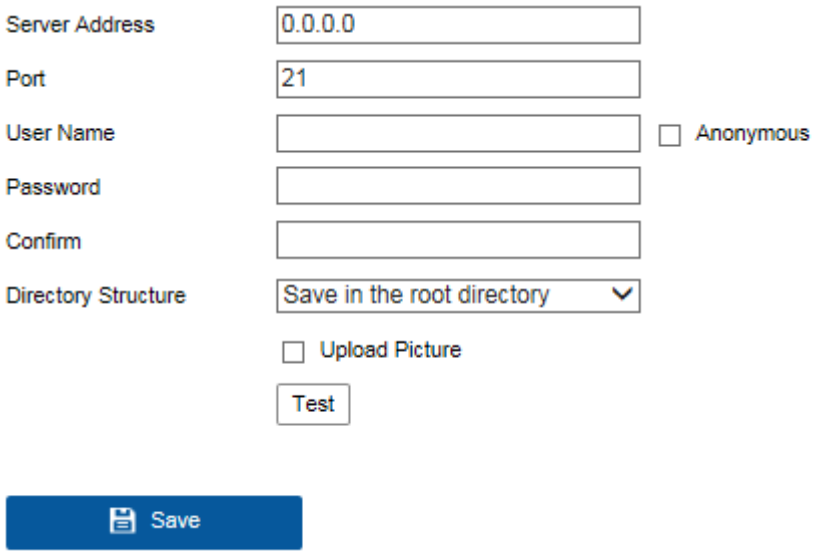


Figure 7-8 FTP Settings

2. 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.*

Directory: In the **Directory Structure** field, you can select the root directory,

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

Upload 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.

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

7.2.3 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 6.1.1* ***Configuring TCP/IP Settings*** for detailed information.

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

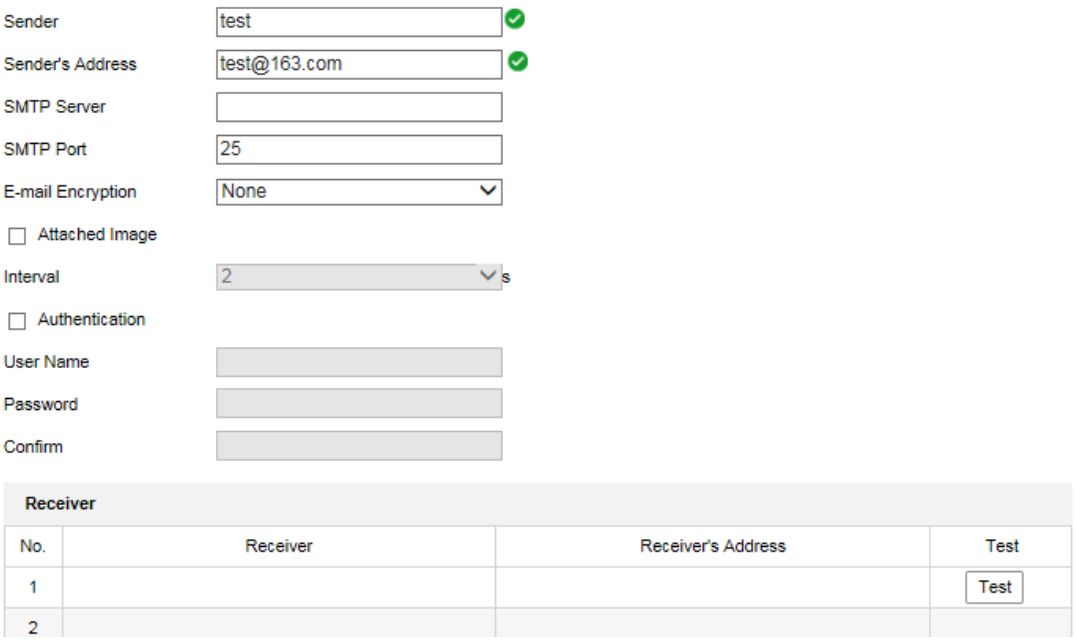


Figure 7-9 Email Settings

3. Configure the following settings:

Sender: The name of the email sender.

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

SMTP Server: 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: Select the Email Encryption method in the dropdown list.**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.

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

7.2.4 HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and its associated web server, which protects against Man-in-the-middle attacks. Perform the following steps to set the port number of https.

E.g., If you set the port number as 443 and the IP address is 192.168.1.64, you may access the device by inputting https://192.168.1.64:443 via the web browser.

Steps:

1. Enter the HTTPS settings interface. **Configuration > Network > Advanced Settings > HTTPS**.
2. Check the checkbox of Enable to enable the function.

Figure 7-10 HTTPS Configuration Interface

3. Create the self-signed certificate or authorized 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.

Figure 7-11 Create Self-signed Certificate

(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 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) Download the certificate request and submit it to the trusted certificate authority for signature.

(4) After receiving the signed valid certificate, import the certificate to the device.

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

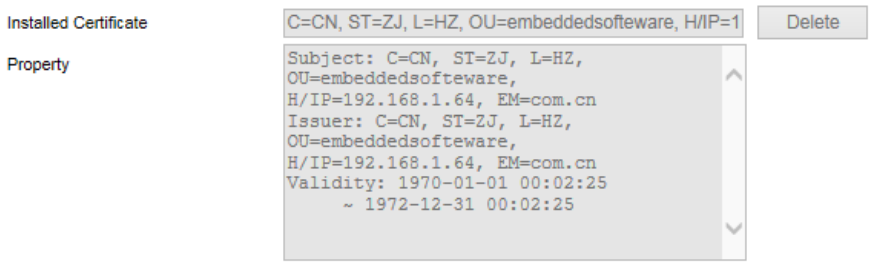


Figure 7-12 Installed Certificate

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

7.2.5 Configuring QoS Settings

Purpose:

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

Steps:

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

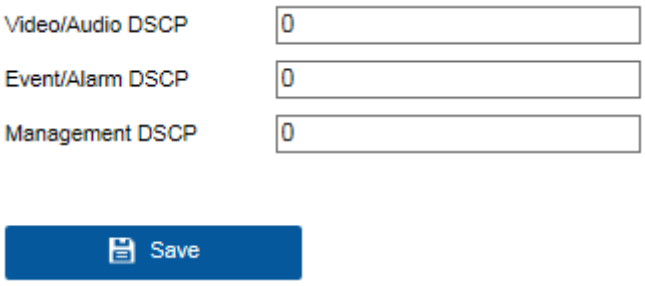


Figure 7-13 QoS Settings

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.

7.2.6 Configuring 802.1X Settings

Purpose:

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

Before you start:

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

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

Steps:

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

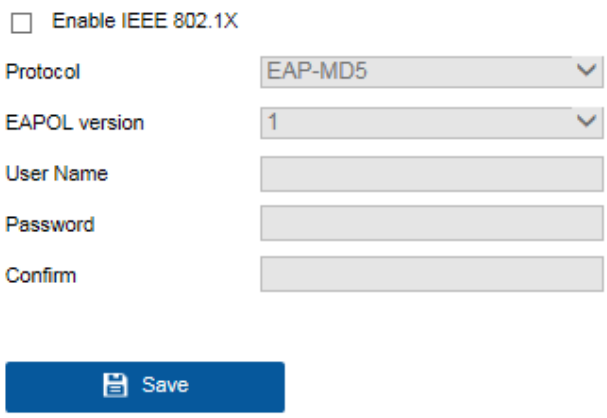


Figure 7-14 802.1X Settings

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.

Chapter 8 Video/Audio Settings

Purpose:

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

8.1 Configuring Video Settings

Steps:

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

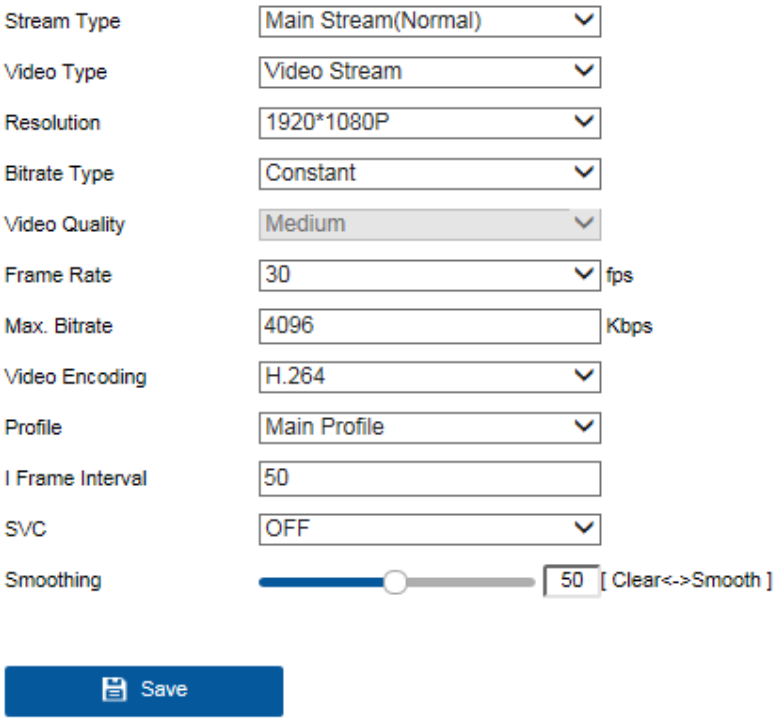


Figure 8-1 Video Settings

2. Select the Stream Type of the camera to main stream, sub-stream, or Third Stream.

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

3. You can customize the following parameters for the selected main stream or sub-stream:

   Video Type:

Select the stream type to video stream, or video & audio composite stream. The 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 from 1/16 to 25 fps. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate:

Set the max. bitrate 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:

If the Stream Type is set to main stream, H.264 and MPEG4 are selectable. If the Stream Type is set to sub stream or third stream, H.264, MJPEG, and MPEG4 are selectable.

If you set the Main Stream as the Stream Type, and H.264 as the video coding, you can see H.264+ is available. H.264+ is an advanced compression coding technology. By enabling H.264+, users can calculate the HDD consumption by its average bitrate, and save the storage by lowering the bitrate as well. You need to reboot the camera if you want to turn on or turn off the H.264+. When the H.264+ is enabled and the Bitrate Type is selected as Variable, the Average Bitrate

is configurable, and you can calculate the HDD consumption according to the average bitrate, or you can set the average bitrate manually, which should be smaller than max. bitrate.

Note: With H.264+ enabled, the parameters such as Profile, I Frame Interval, SVC, Max. Bitrate are greyed out if the Bitrate Type is variable. And the Video Quality, Profile, I Frame Interval, and SVC are greyed out if you set the Bitrate Type as constant.

Profile:

Basic profile, Main Profile, and High Profile for coding are selectable.

I Frame Interval:

Set I Frame Interval from 1 to 400.

SVC:

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

Smoothing:

It refers to the smoothness of the stream. The higher value of the smoothing 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**.

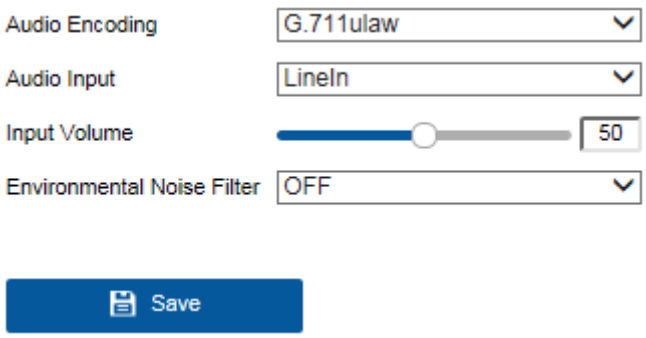


Figure 8-2 Audio Settings

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.

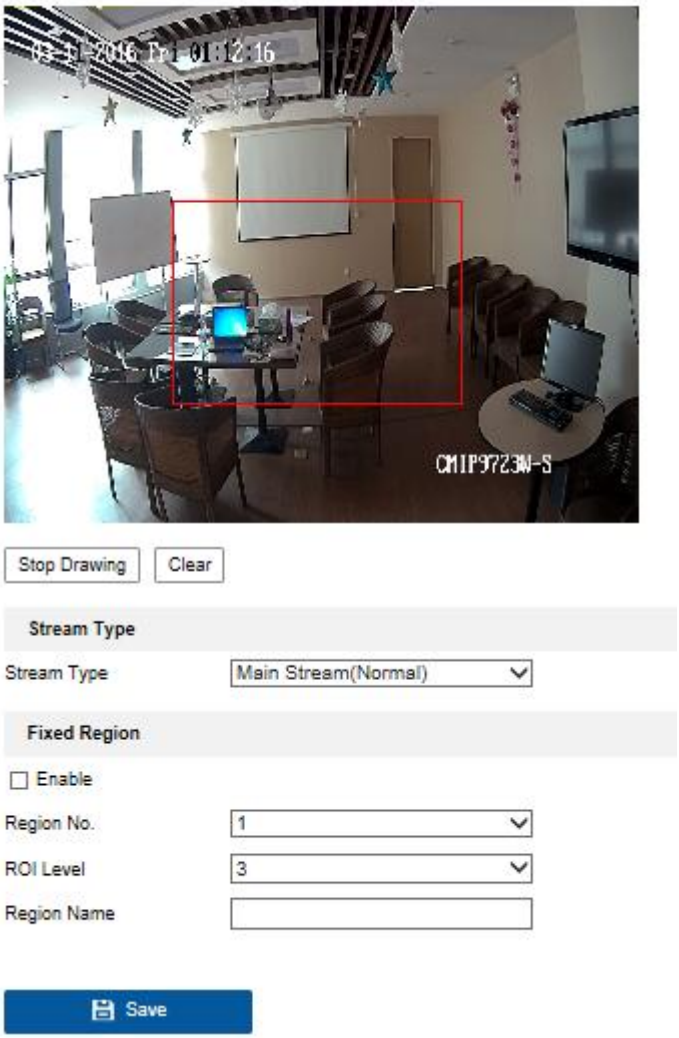


Figure 8-3 Region of Interest Settings

Configuring Fixed Region for ROI:

Steps:

1. Enter the ROI settings interface: **Configuration > Video/Audio> ROI**.
2. Check the checkbox of **Enable** under Fixed Region item.
3. Select the Stream Type for ROI encoding.
4. Select the region from the drop-down list for ROI settings. There are four fixed regions selectable.
5. Click the **Draw Area** button, and then click-and-drag the mouse to draw the region of interest on the live video.
6. Select the ROI Level to set the image quality enhancing level. The larger the value is, the better the image quality is.

7. Input the region name for ROI as desired.
8. Click **Save** to save the settings.

Configuring Dynamic Region for ROI:

1. Enter the ROI settings interface: **Configuration > Video/Audio > ROI**
2. Check the checkbox of **Enable Face Tracking**, and then the captured face picture is set as region of interest.

   Note: To enable face tracking function, the face detection function should be supported and enabled.
3. Respectively set the ROI level. The larger the value is, the better the image quality is.
4. Click **Save** to save the settings.

8.4 Display Info. on Stream

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

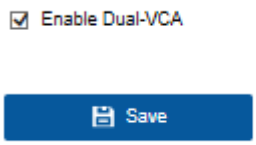


Figure 8-4 Display Info. on Stream

8.5 Configuring Target Cropping

Purpose:

You can specify a target area on the live video, and then the specified video area can be displayed via the third stream in certain resolution, providing more details of the target area if needed.

Note: Target cropping function varies according to different camera models.

Steps:

1. Enter the **Target Cropping** settings interface.
2. Check **Enable Target Cropping** checkbox to enable the function.
3. Set Third Stream as the stream type.
4. Select the cropping resolution for the video display of target area. A red rectangle is displayed on the live video to mark the target area, and you can click-and-drag the rectangle to locate the target area as desired.
5. Click **Save** to save the settings.

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.

9.1.1 Day/Night Auto-Switch

Steps:

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

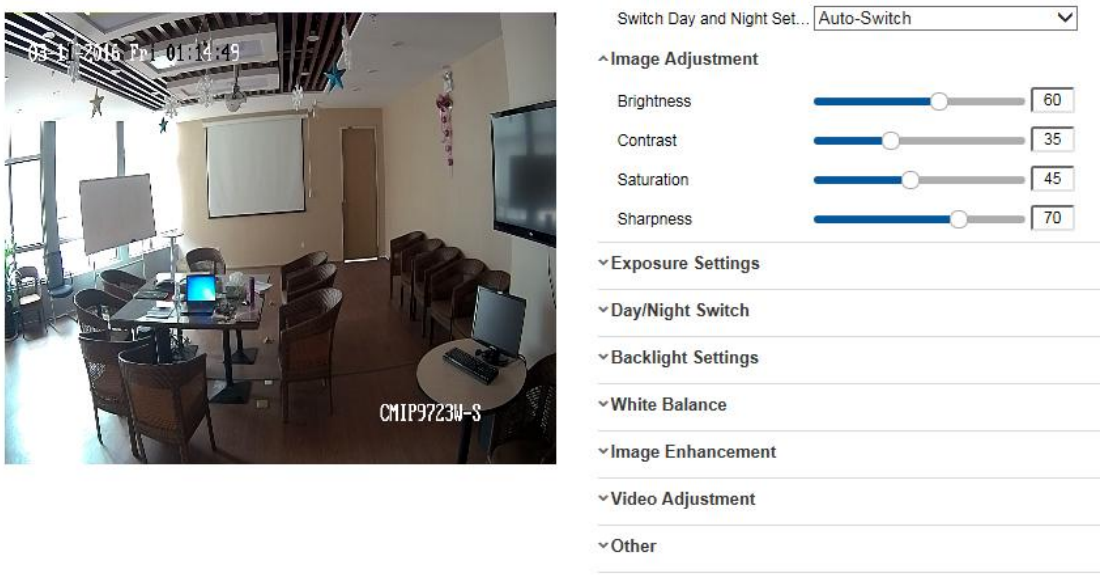


Figure 9-1 Display Settings of Day/Night Auto-Switch

2. Set the image parameters of the camera.

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

- **Image Adjustment**

  Brightness describes bright of the image, which ranges from 1 to100, and the default value is 50.

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

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

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

- **Exposure Settings**

  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.

- **Day/Night Switch**

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

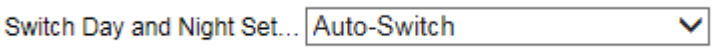


Figure 9-2 Day/Night Switch

Auto, Scheduled-Switch are selectable for day/night switch.

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.

- **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 and Customize are selectable.

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

- **White Balance**

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

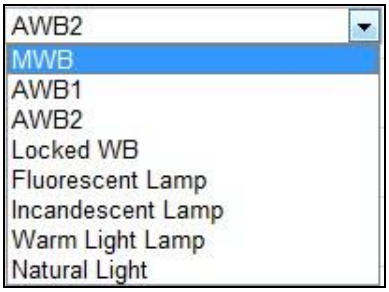


Figure 9-3 White Balance

- **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, and the default value is 50 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.

Capture Mode: It's the selectable video input mode to meet the different demands of field of view and resolution.

- **Others**

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

9.1.2 Day/Night Scheduled-Switch

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

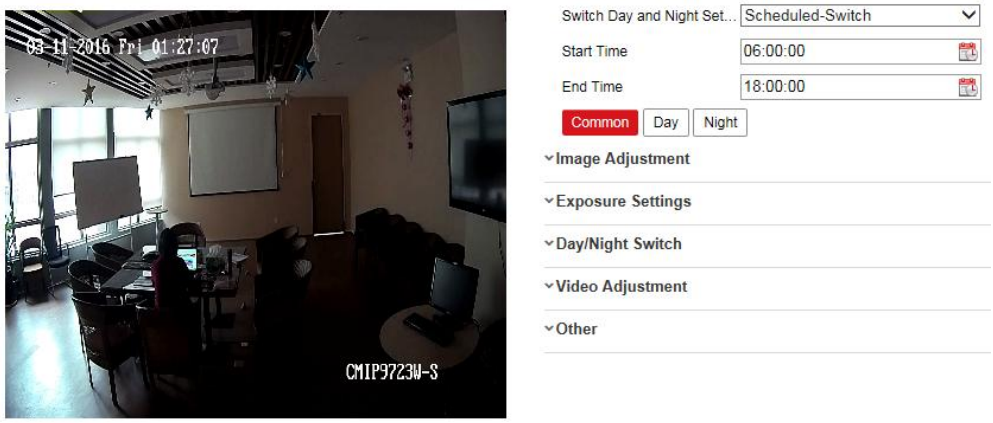


Figure 9-4 Day/Night Scheduled-Switch Configuration Interface

Steps:

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

   Note: For the detailed information of each parameter, please refer to *Section 8.1.1 Day/Night Auto-Switch.*
3. Click Day tab to configure the parameters applicable for day mode.
4. Click Night tab to configure the parameters applicable for night mode.

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

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.

Steps:

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

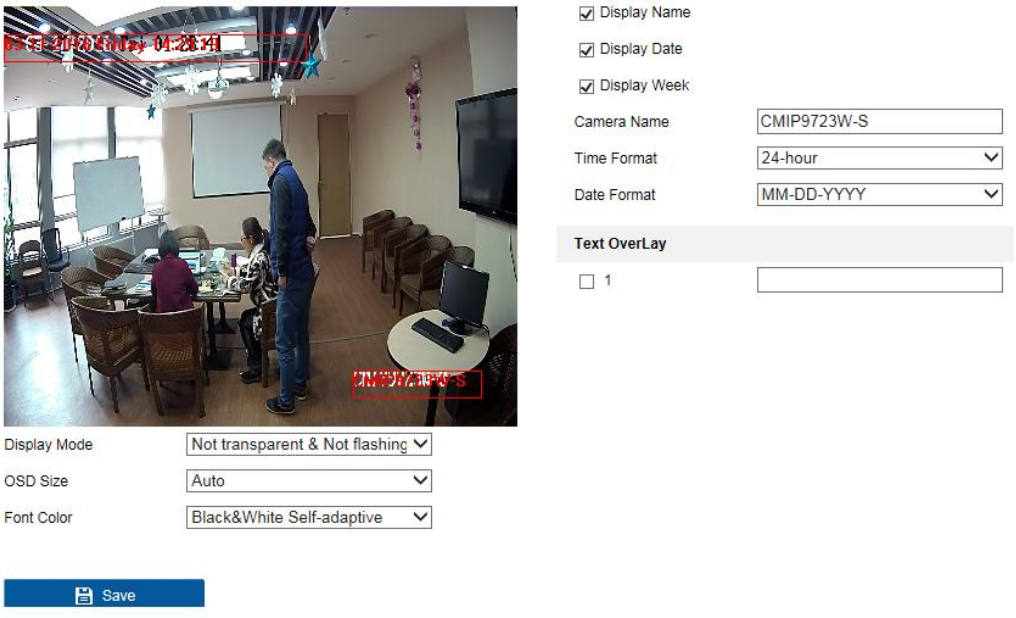


Figure 9-5 OSD Settings

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. You can use the mouse to click and drag the text frame in the live view window to adjust the OSD position.
6. Configure the text overlay settings.

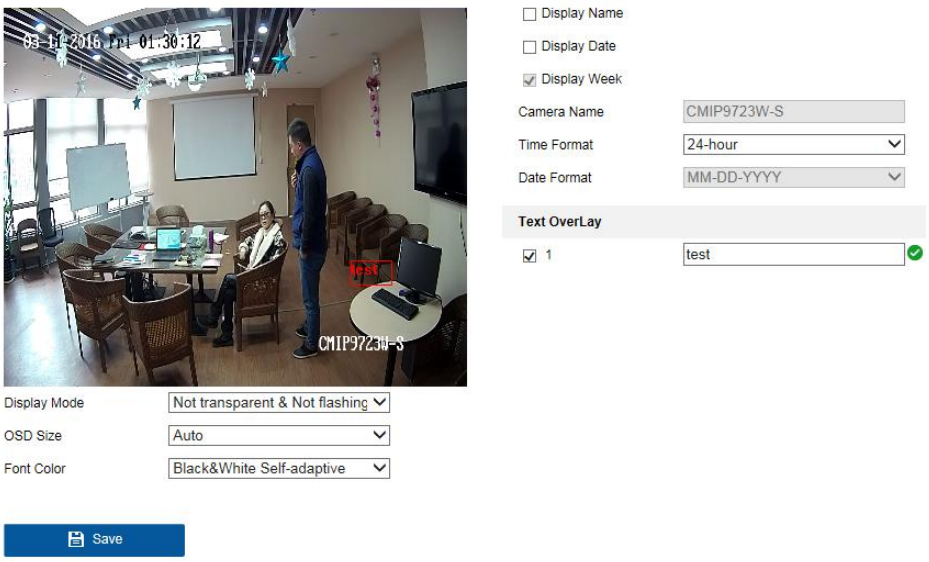


Figure 9-6 Text Overlay

(1) Check the checkbox in front of the textbox to enable the on-screen display.

(2) Input the characters in the textbox.

(3) (Optional) Use the mouse to click and drag the red text frame in the live view window to adjust the text overlay position.

Note: Up to 8 text overlays are configurable.

7. 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**.

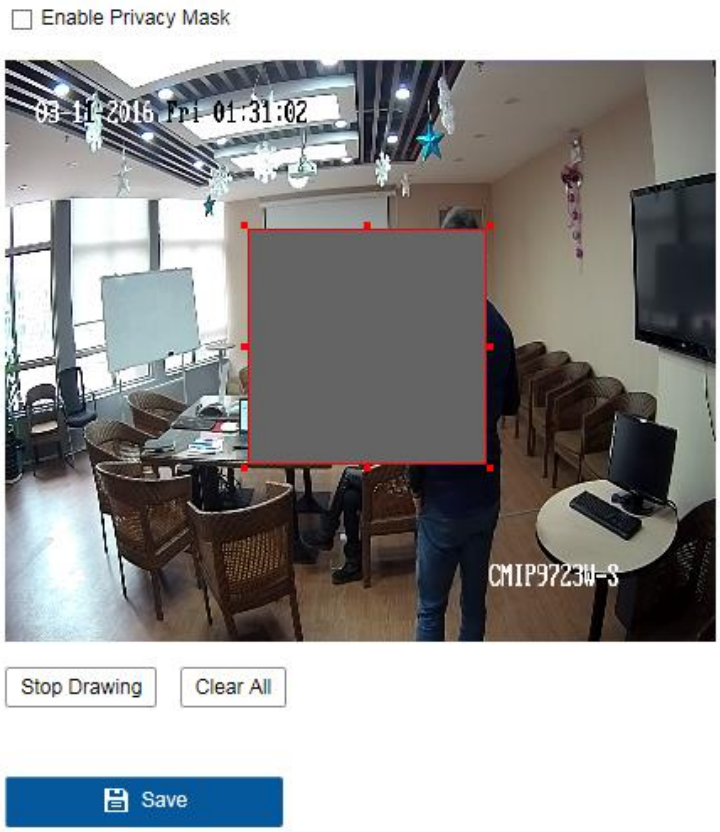


Figure 9-7 Privacy Mask Settings

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 9-8 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.

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**.

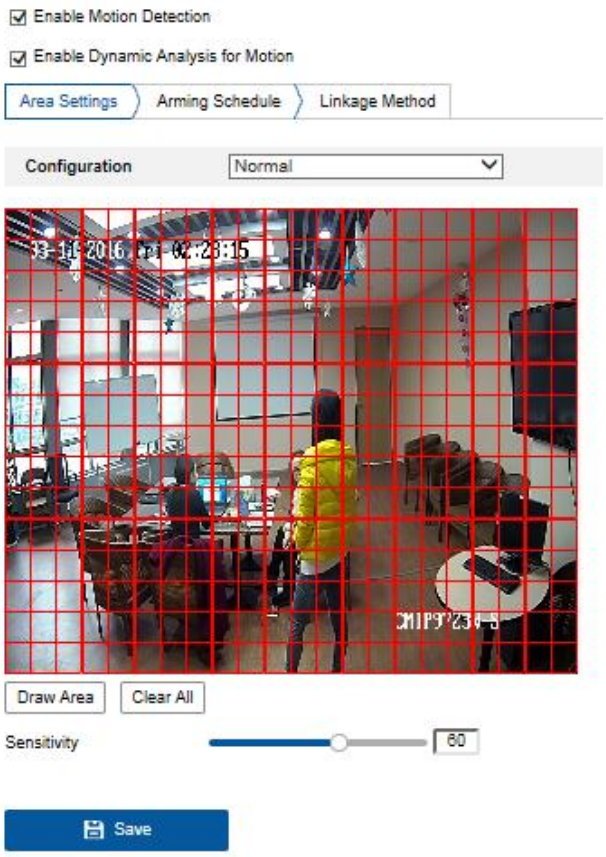


Figure 10-1 Enable Motion Detection

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

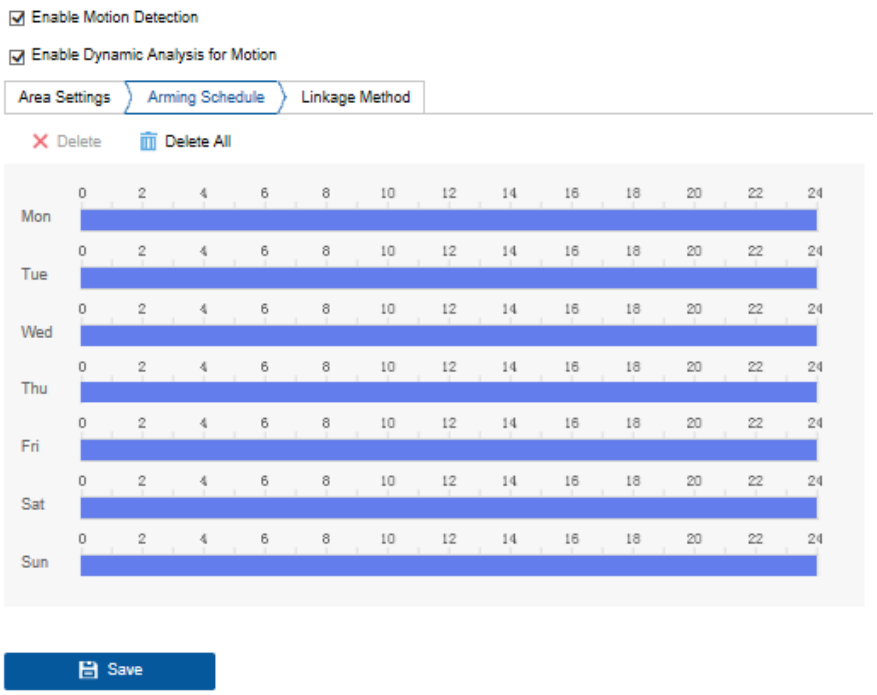


Figure 10-2 Arming Schedule

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.

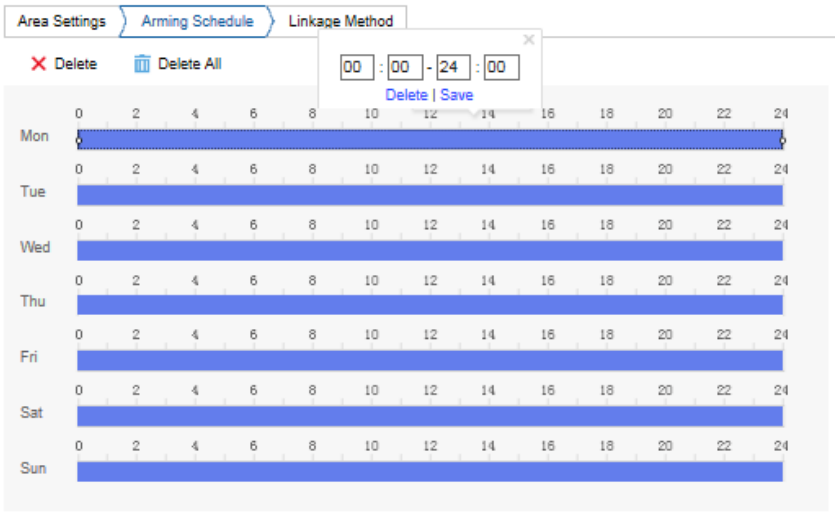


Figure 10-3 Arming Schedule

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, Trigger Channel and Trigger Alarm Output are selectable. You can specify the linkage method when an event occurs.

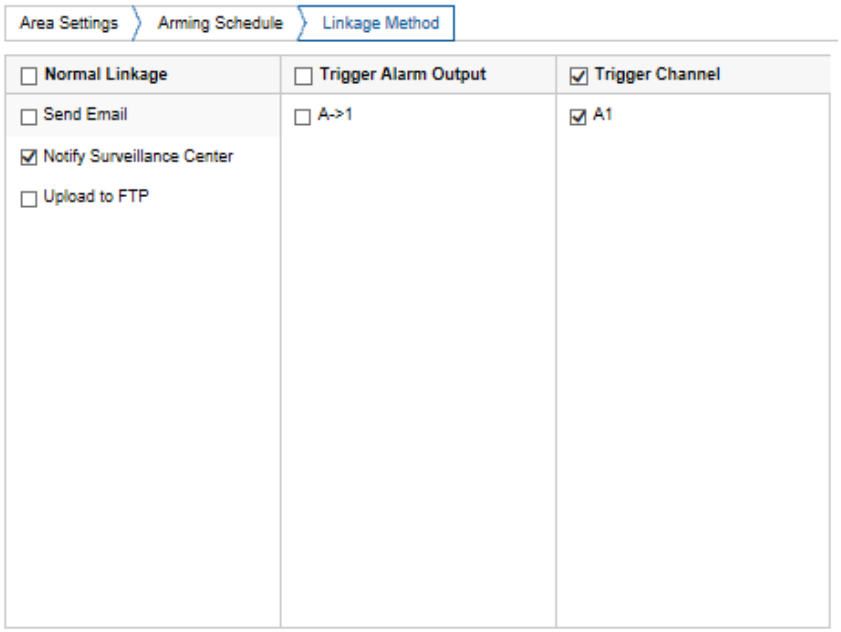


Figure 10-4 Linkage Method

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 6.2.3* to complete Email setup in advance.

- **Upload to FTP**

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

  Notes:

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

- **Trigger Channel**

  The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 10.1* 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 9.1.4* ***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.

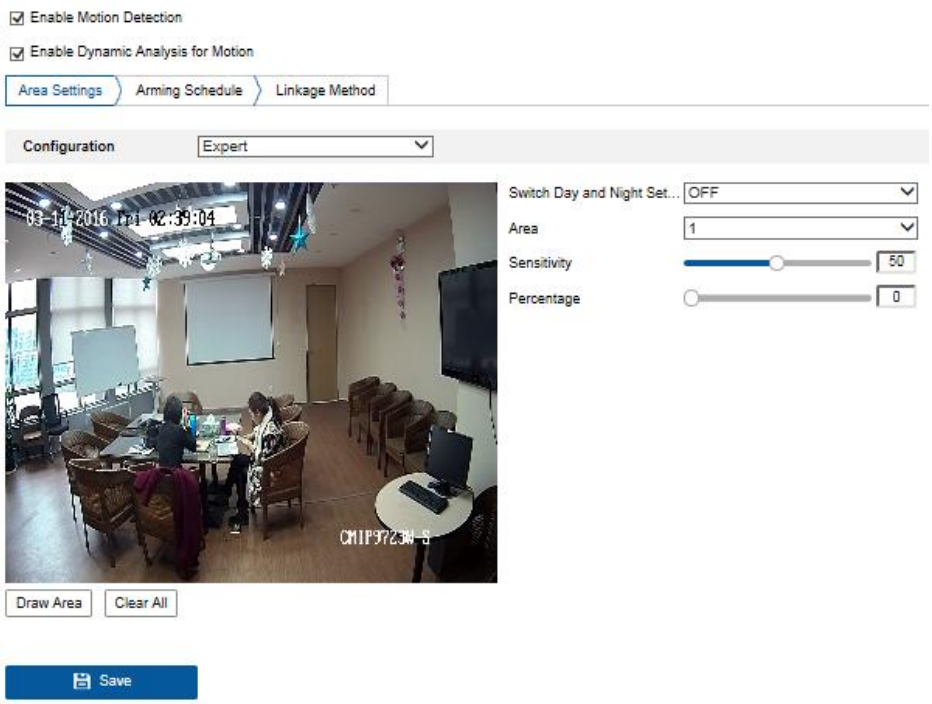


Figure 10-5 Expert Mode of Motion Detection

- 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**.

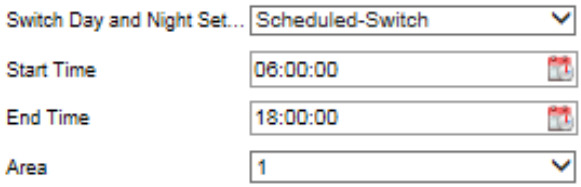


Figure 10-6 Day/Night Scheduled-Switch

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.

Steps:

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

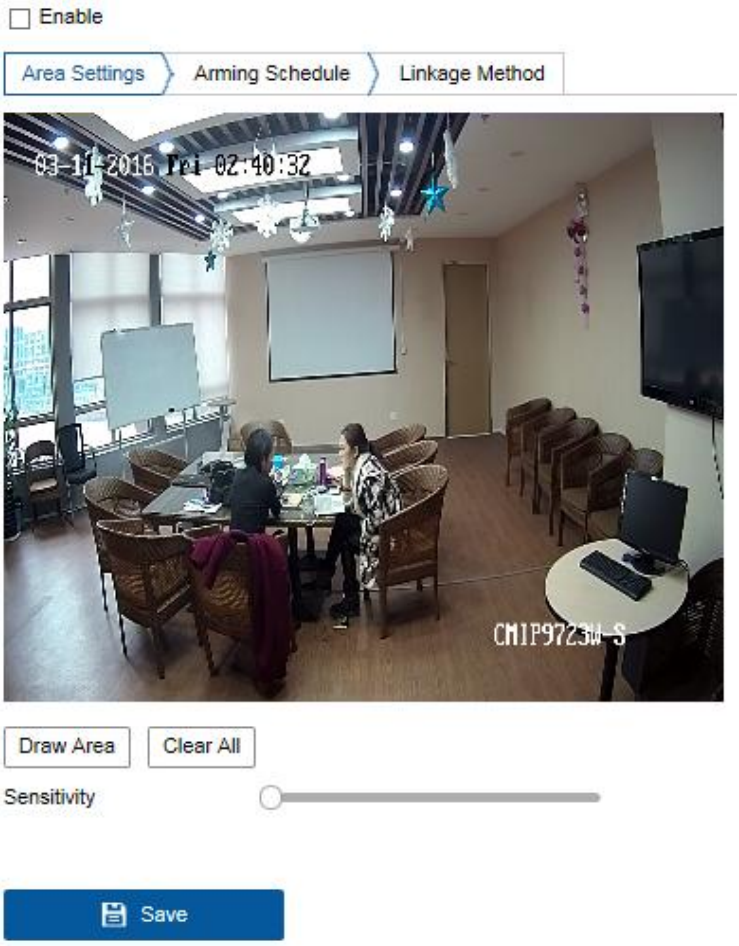


Figure 10-7 Video Tampering Alarm

2. Check **Enable Video Tampering** checkbox to enable the video tampering detection.
3. Set the video tampering area. Refer to ***Task 1: Set the Motion Detection Area*** in *Section 9.1.1.*
4. Click **Edit** to edit the arming schedule for video tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to ***Task 2: Set the Arming Schedule for Motion Detection*** in *Section 9.1.1.*

5. Check the checkbox to select the linkage method taken for the video tampering. Audible warning, notify surveillance center, send email and trigger alarm output are selectable. Please refer to ***Task 3: Set the Linkage Method for Motion Detection*** in *Section 9.1.1.*
6. 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).

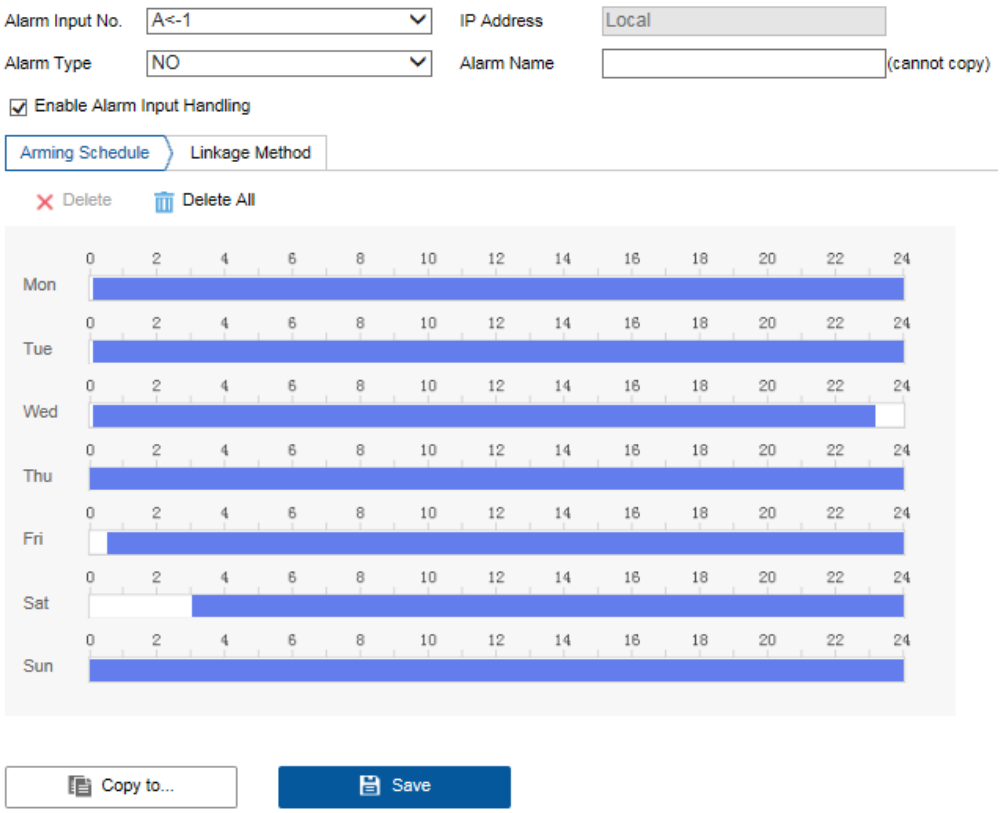


Figure 10-8 Alarm Input Settings

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 9.1.1.*

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 9.1.1.*
5. You can copy your settings to other alarm inputs.
6. Click **Save** to save the settings.

10.1.4 Configuring Alarm Output

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 9.1.1.*
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

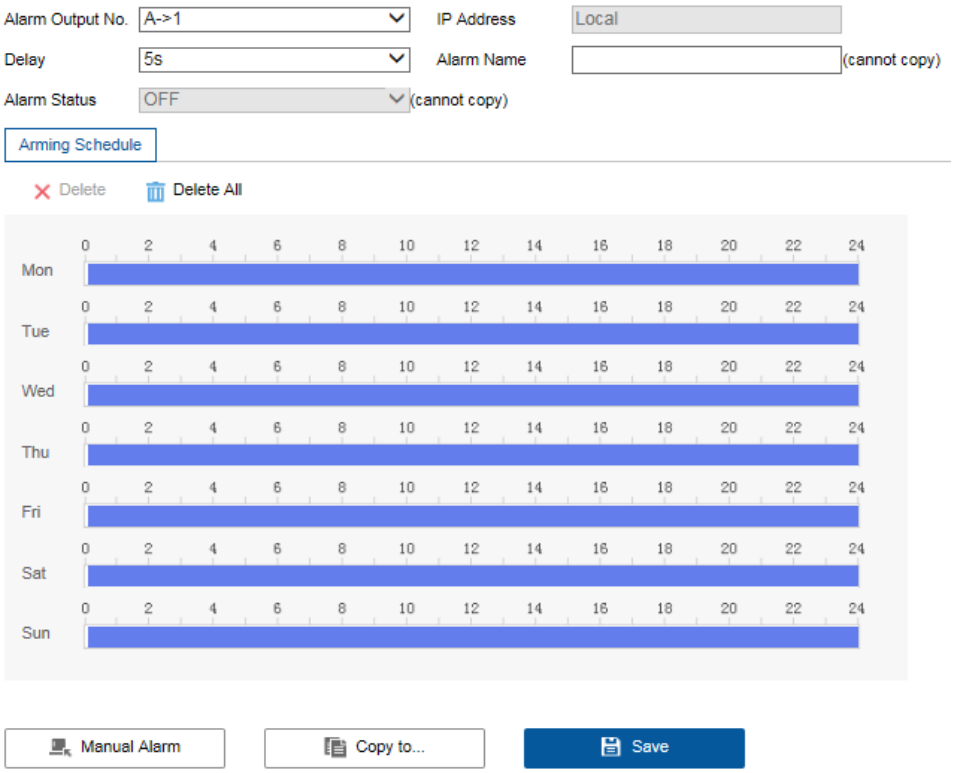


Figure 10-9 Alarm Output Settings

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 9.1.1.*

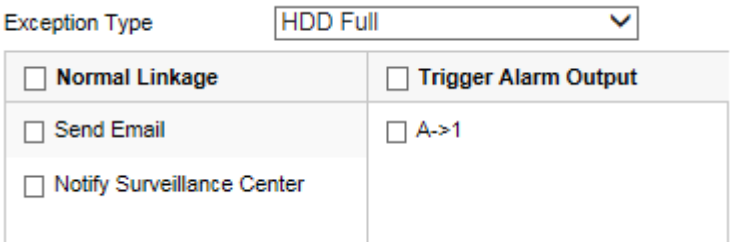


Figure 10-10 Exception Settings

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 Intrusion Detection

Purpose:

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

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

Steps:

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

Figure 10-11 Intrusion Detection

2. Check the checkbox of **Enable Intrusion Detection** to enable the function.
3. Select the region from the drop-down list for detection settings.
4. Click **Area Settings** tab and click **Draw Area** button to start the region drawing.
5. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.
6. Set the time threshold, detection sensitivity and object percentage for intrusion detection.

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

   Sensitivity: Range [1-100]. The value of the sensitivity defines the size of the

object which can trigger the alarm. When the sensitivity is high, a very small object can trigger the alarm.

Percentage: Range [1-100]. Percentage defines the ratio of the in-region part of the object which can trigger the alarm. For example, if the percentage is set as 50%, when the object enters the region and occupies half of the whole region, the alarm is triggered.

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

10.2.2 Configuring Line Crossing Detection

Purpose:

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

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

Steps:

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

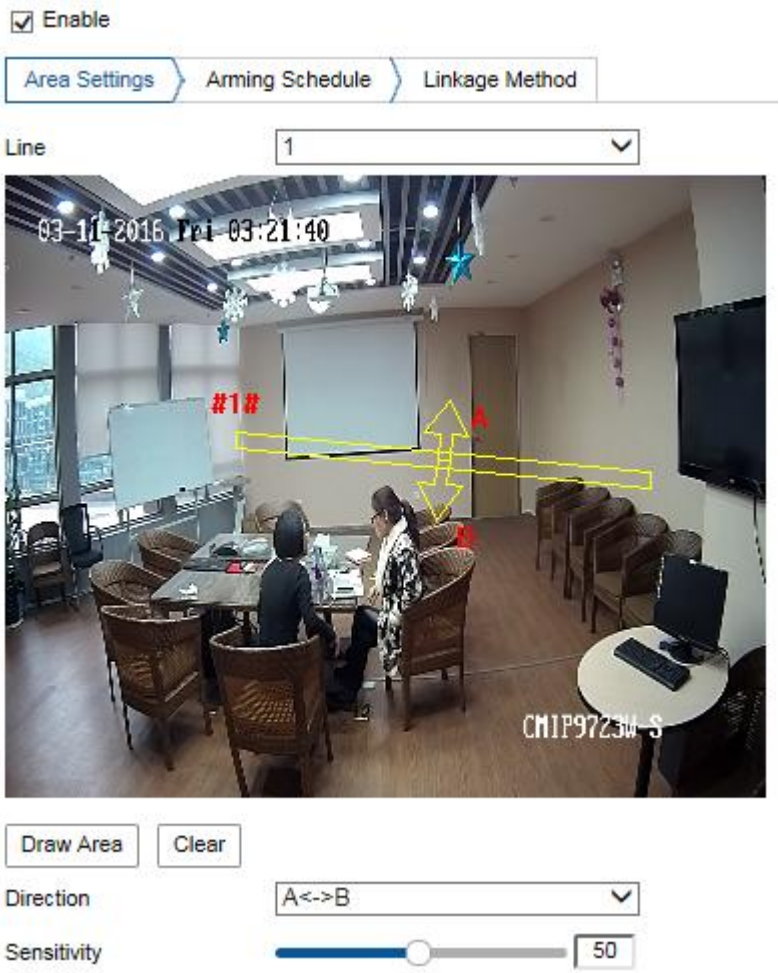


Figure 10-12 Line Crossing Detection

2. Check the checkbox of **Enable Line Crossing Detection** to enable the function.
3. Select the line from the drop-down list for detection settings.
4. Click **Area Settings** tab and click **Draw Area** button, and a virtual line is displayed on the live video.
5. Click-and-drag the line, and you can locate it on the live video as desired. Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.
6. Select the direction for line crossing detection. And you can select the directions as A<->B, A ->B, and B->A.

   A<->B: Only the arrow on the B side shows; when an object going across the plane with both direction can be detected and alarms are triggered.

   A->B: Only the object crossing the configured line from the A side to the B side

can be detected.

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

7. Click-and-drag the slider to set the detection sensitivity.

   Sensitivity: Range [1-100]. The higher the value is, the more easily the line crossing action can be detected.

8. Repeat the above steps to configure other lines. Up to 4 lines can be set. You can click the **Clear** button to clear all pre-defined lines.
9. Click the **Arming Schedule** to set the arming schedule.
10. Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
11. Click **Save** to save the settings.

10.2.3 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.

Notes:

It is recommended to install the camera as right above the entrance/exit as possible, and make sure it is horizontal to improve the counting accuracy.

Steps：

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

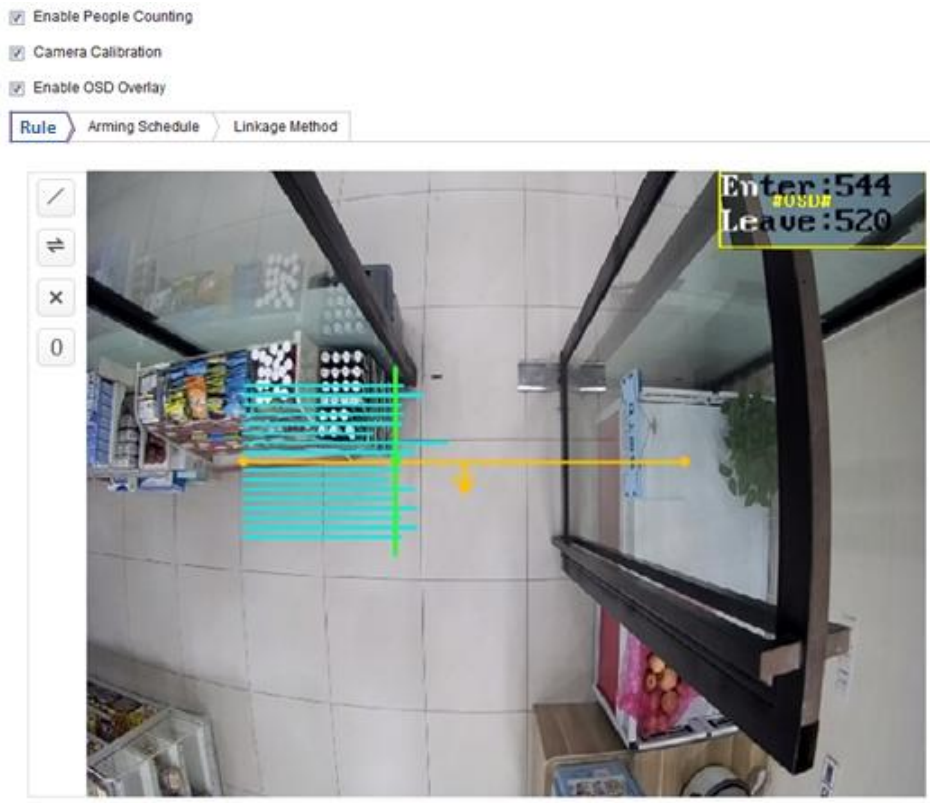


Figure 10-13 People Counting Configuration

2. Check **Enable People Counting** checkbox to enable the function.

3. Check **Enable OSD Overlay** checkbox, and the real-time number of object entered and exited is displayed on the live video.

You can also adjust the OSD position according to the actual needs.

4. Set the detection line.

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

1) Click to draw a detection line, and an orange detection line will appear on the image.

Note:

- The detection line should be drawn at the position right below the camera, and it should cover the whole entrance / exit.
- Draw the detection line at the position don't have many people lingering.

2) Click-and-drag the detection line to adjust its position.

3) Click-and-drag the two end points of the detection line to adjust its length.

4) Click to delete the detection line.

5) Click ⇌ to change the direction.

5. Check **Camera Calibration** checkbox to enable camera calibration.

   A vertical line appears in the configuration window after you enable the calibration. And a horizontal line (blue) appears if one target passed the detection line. Up to 8 horizontal lines can be displayed on one side of the detection line.

   The horizontal line is calculated according to the shoulder width of the target. And you can decide the calibration line position according to the width of the targets. You can click-and-drag to adjust the calibration line position.

6. Click the 0 button, and the number of the people entered and exited will be cleared to zero.

7. Click **Arming Schedule** to enter the arming schedule interface, and click-and-drag the mouse on the time bar to set the time.

8. Check **Linkage Method** tab to select the linkage method.

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

Note:

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

Chapter 11 Storage Settings

Before you start:

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

11.1 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**.

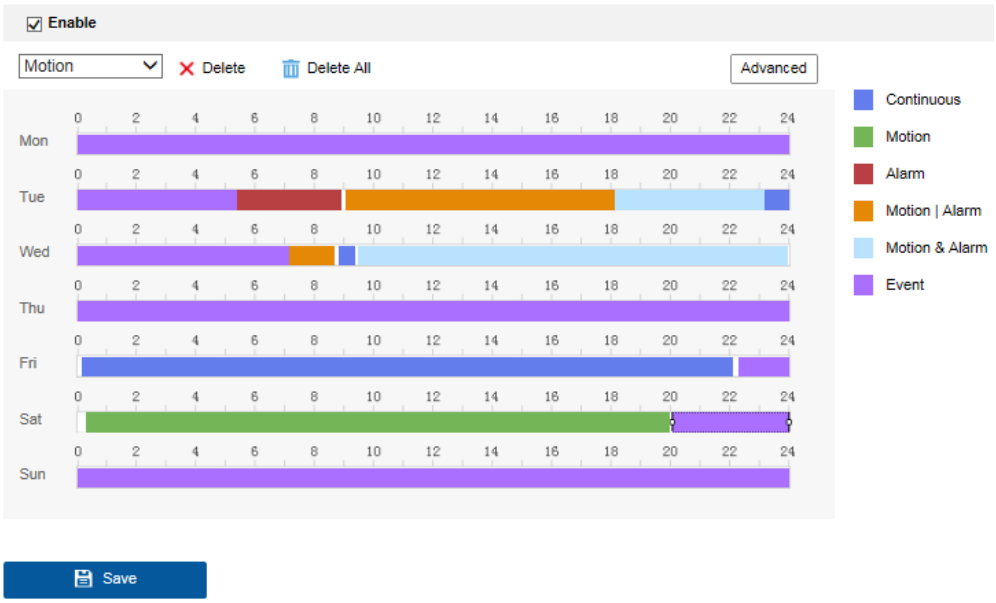


Figure 11-1 Recording Schedule Interface

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

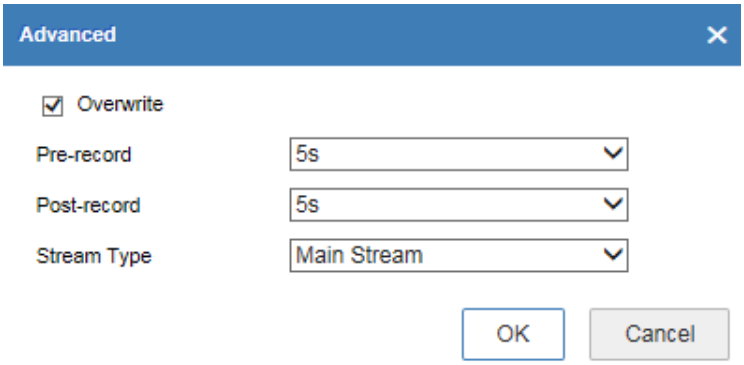


Figure 11-2 Record Parameters

- 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 9.1.1.

- **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 9.1.3*.

- **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 9.1.1* and *Section 9.1.3* 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 9.1.1* and *Section 9.1.3* 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.

11.2 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**.

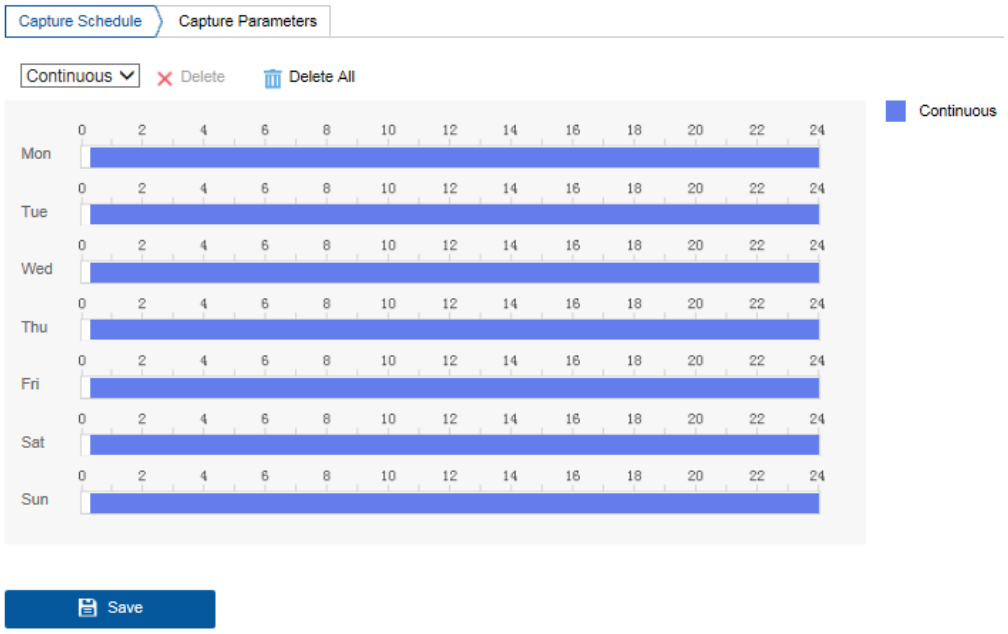


Figure 11-3 Capture Configuration

2. Go to **Capture Schedule** tab to configure the capture schedule by click-and-drag the mouse on the time bar.
3. Click **Save** to save the settings.
4. Go to **Capture Parameters** tab to configure the capture parameters.
   (1) Check the **Enable Timing Snapshot** checkbox to enable continuous 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.

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

11.3 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**.

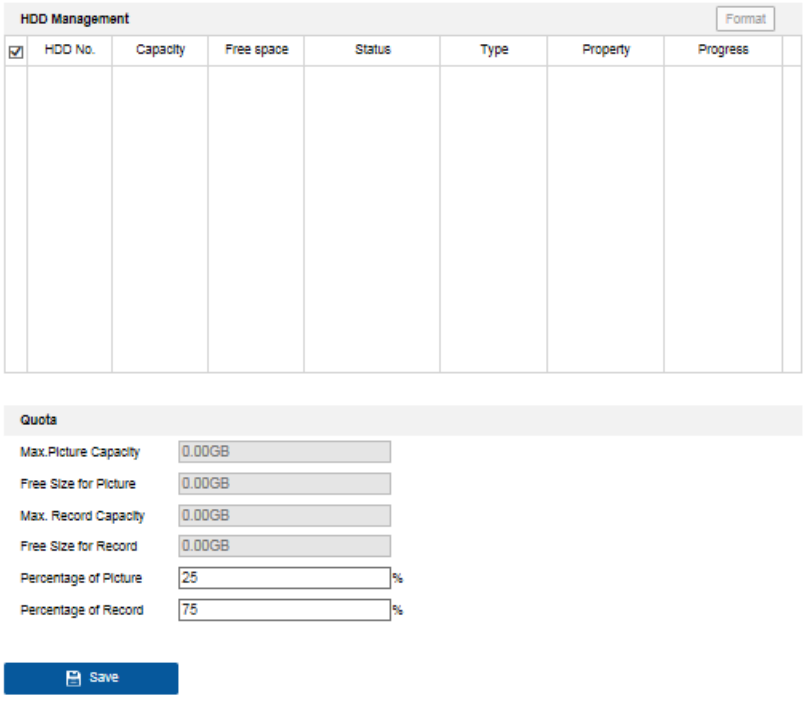


Figure 11-4 Add Network Disk

   (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.

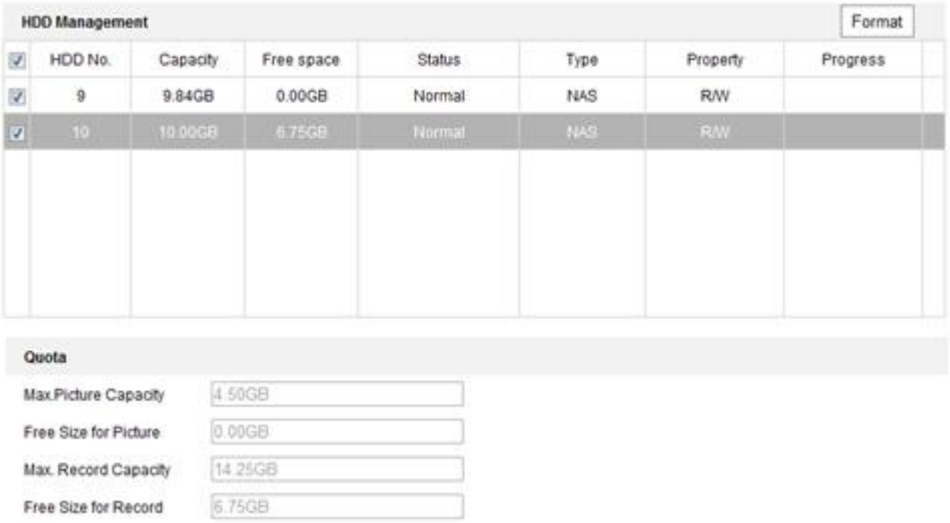


Figure 11-5 Storage Management Interface

(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.**

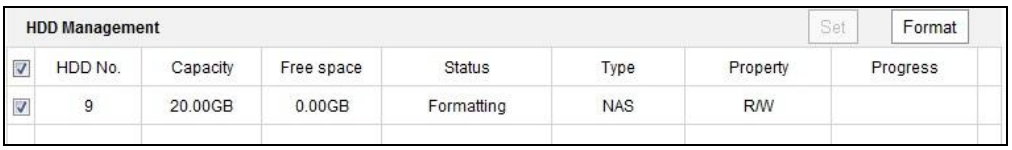


Figure 11-6 View Disk Status

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.

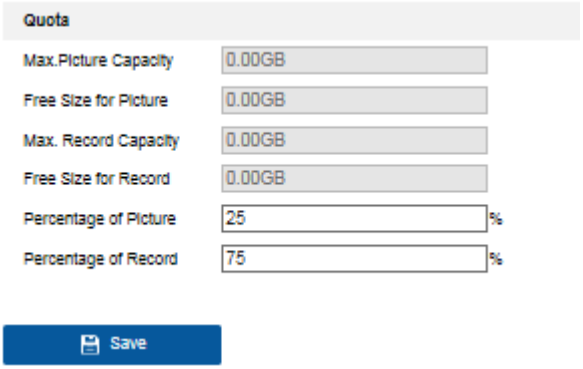


Figure 11-7 Quota Settings

Note:

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

11.4 Configuring Lite Storage

Purpose:

When there is no moving object in the monitoring scenario, the frame rate and bitrate of the video stream can be reduced to lengthen the storage time of the memory card.

Notes:

- Lite storage function varies according to different camera models.
- The video files recorded in lite storage mode will be played back in full frame rate (25fps/30fps), and thus the playback process is speeded up to the eye.

1. Enter the Lite Storage interface:

   Configuration > Storage > Storage Management > Lite Storage.

2. Check the Checkbox of **Enable** to enable the lite storage function.
3. Input the storage time in the text field. You can view the available space of the SD card on the page.
4. Click **Save** to save the settings.

Chapter 12 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.

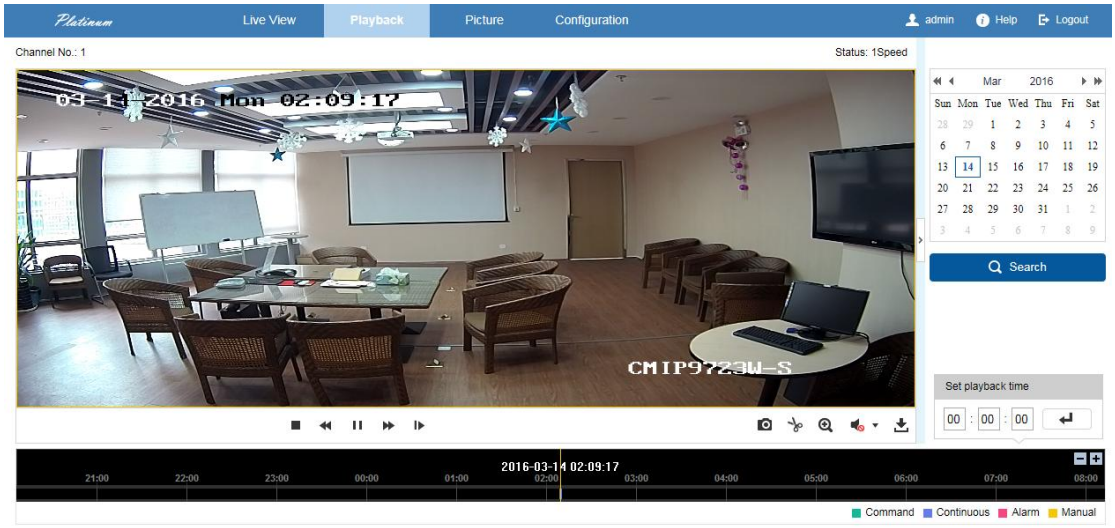


Figure 12-1 Playback Interface

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

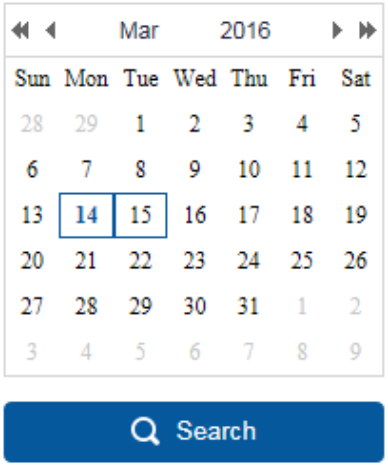


Figure 12-2 Search Video

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 12-3 Playback Toolbar

Table 12-1 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.

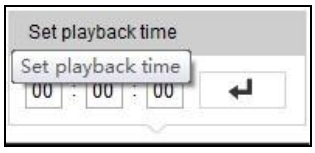


Figure 12-4 Set Playback Time

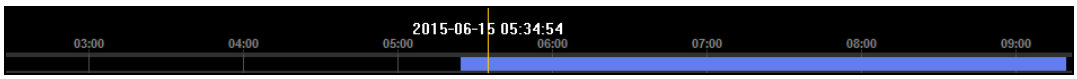


Figure 12-5 Progress Bar

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

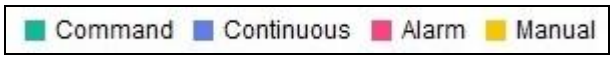


Figure 12-6 Video Types

Chapter 13 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.

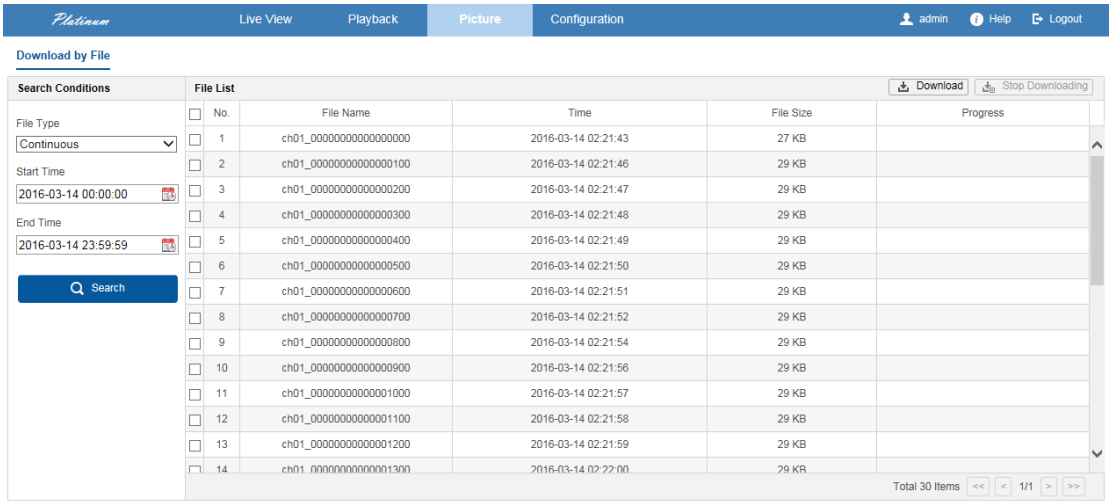


Figure 13-1 Picture Search Interface

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 14 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.

14.1 People Counting Statistics

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

Steps:

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

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

2. Select the statistics type. People Entered, and People Exited are selectable.
3. Select the start time, and click Counting.

   The counting result displays in the statistic result area. Click Table, 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.

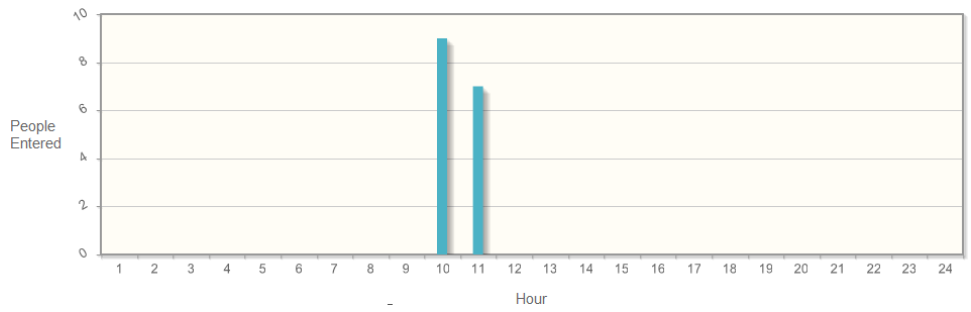


Figure 14-1 People Counting

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.

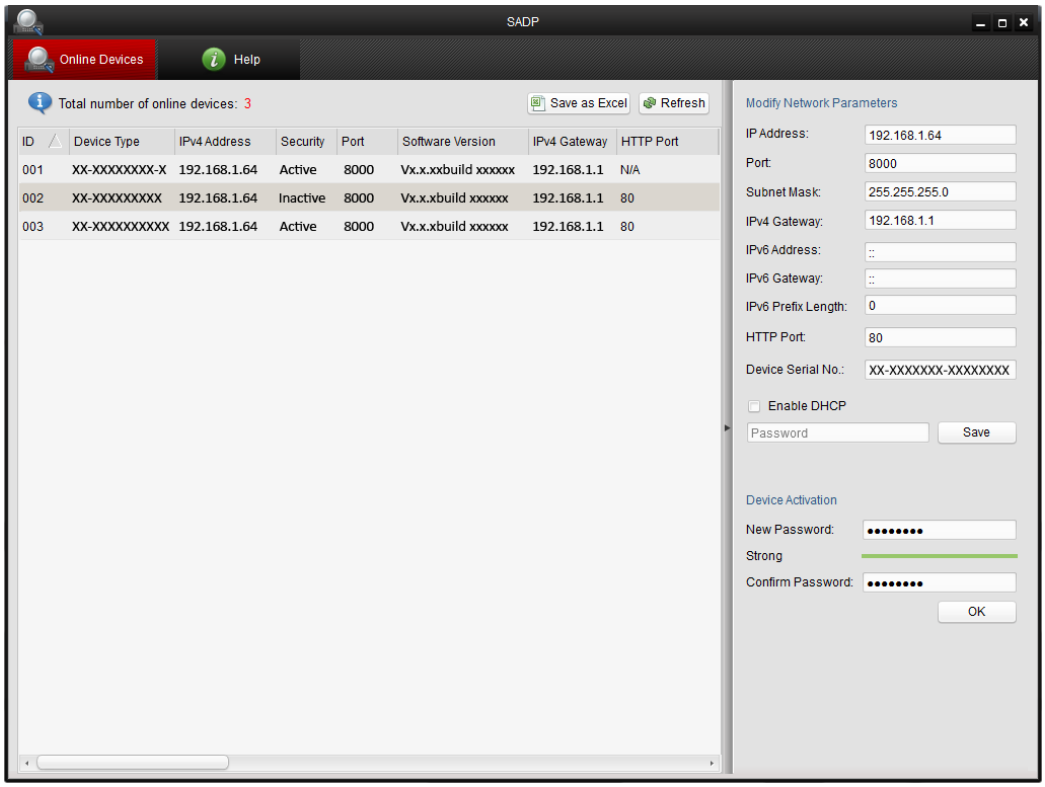


Figure A.1.1 Searching Online Devices

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 **Password** field and click Save 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.*

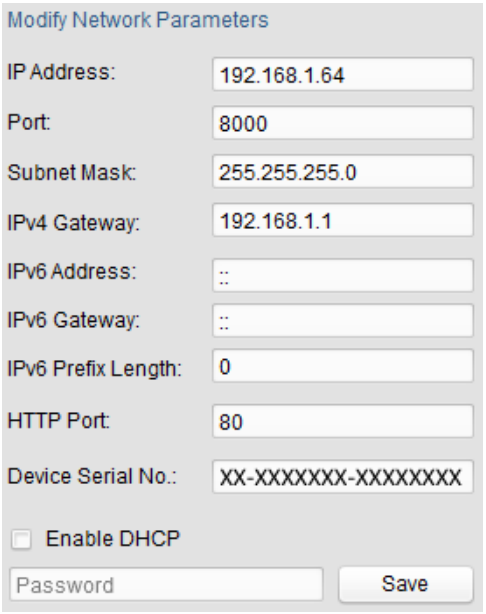


Figure A.1.2 Modify Network Parameters

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:

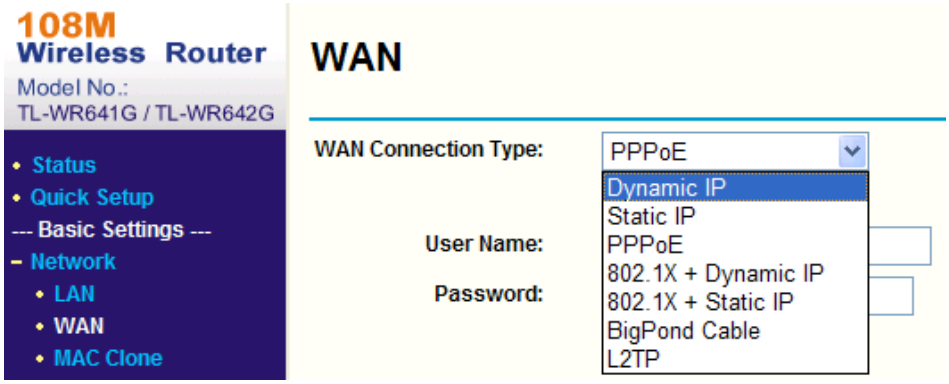


Figure A.2.1 Select the WAN Connection Type

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

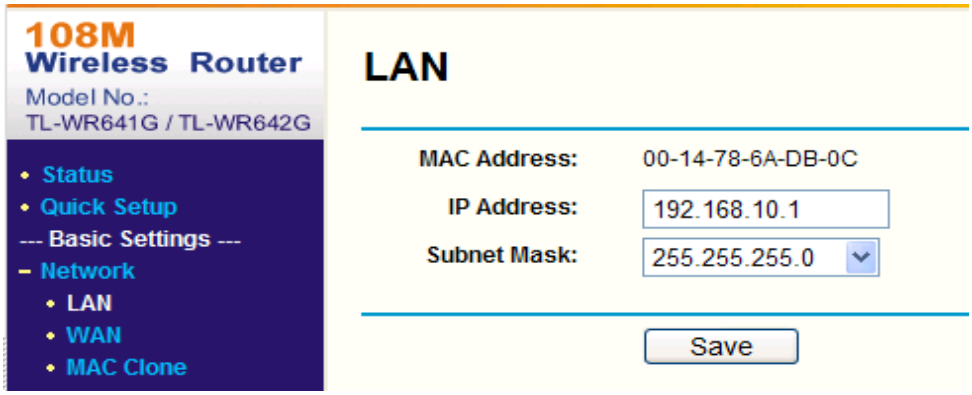


Figure A.2.2 Set the LAN parameters

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.

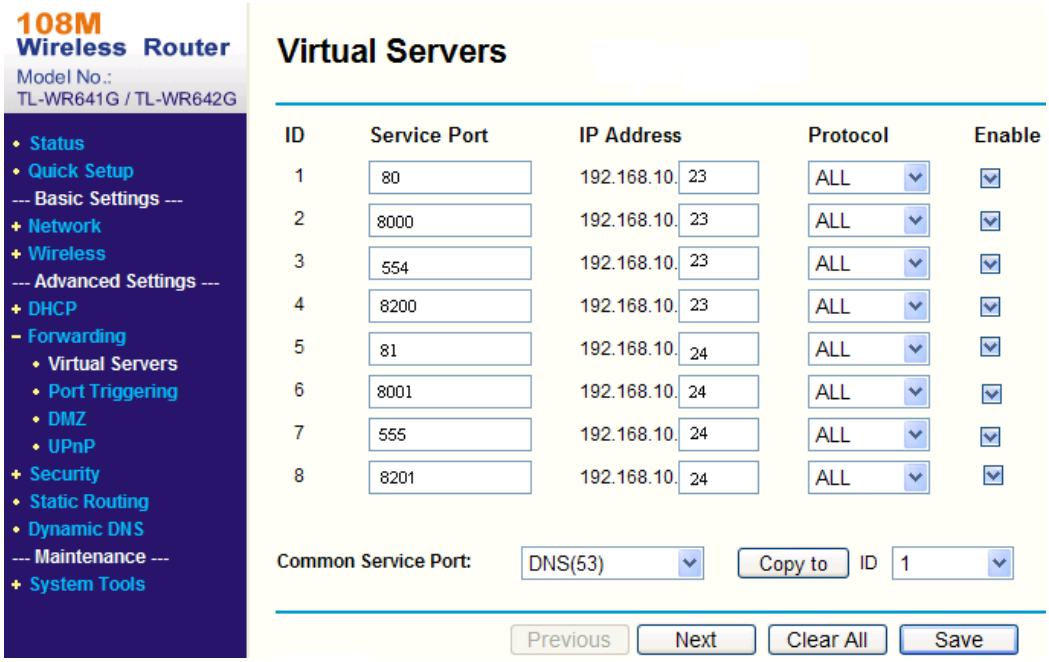


Figure A.2.3 Port Mapping

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.