



IPOB-PR4IR

PRIME SERIES



3yr
Warranty

View From
Anywhere

4MP
Resolution

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 RESPONSIBILITIES 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



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 $-30\text{ }^{\circ}\text{C} \sim 60\text{ }^{\circ}\text{C}$, or $-40\text{ }^{\circ}\text{C} \sim 60\text{ }^{\circ}\text{C}$ if the camera model has an “H” in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed in its original packing.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.

Notes:

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

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

Table of Contents

Chapter 1	System Requirement.....	1
Chapter 2	Network Connection.....	2
2.1	Setting the Network Camera over the LAN.....	2
2.1.1	Wiring over the LAN	2
2.1.2	Creating a Password.....	3
2.2	Setting the Network Camera over the WAN	5
2.2.1	Static IP Connection	5
2.2.2	Dynamic IP Connection.....	6
Chapter 3	Access to the Network Camera.....	9
3.1	Accessing by Web Browsers.....	9
3.2	Accessing by Client Software	11
Chapter 4	Wi-Fi Settings	12
4.1	Configuring Wi-Fi Connection in Manage and Ad-hoc Modes	12
4.2	Easy Wi-Fi Connection with WPS function	17
4.3	IP Property Settings for Wireless Network Connection	19
Chapter 5	Live View	21
5.1	Live View Page.....	21
5.2	Starting Live View	22
5.3	Recording and Capturing Pictures Manually	23
5.4	Operating PTZ Control	23
5.4.1	PTZ Control Panel.....	23
5.4.2	Setting / Calling a Preset	24
5.4.3	Setting / Calling a Patrol.....	26
Chapter 6	Network Camera Configuration	27
6.1	Configuring Local Parameters	27
6.2	Configuring Time Settings	29
6.3	Configuring Network Settings	31
6.3.1	Configuring TCP/IP Settings	31
6.3.2	Configuring Port Settings	32
6.3.3	Configuring PPPoE Settings.....	33
6.3.4	Configuring DDNS Settings.....	34
6.3.5	Configuring SNMP Settings	37
6.3.6	Configuring 802.1X Settings.....	38
6.3.7	Configuring QoS Settings	40
6.3.8	Configuring UPnP™ Settings	40

6.3.9	Configuring Wireless Dial Settings	41
6.3.10	Email Sending Triggered by Alarm	44
6.3.11	Configuring NAT (Network Address Translation) Settings	46
6.3.12	Configuring FTP Settings	47
6.3.13	HTTPS Settings	48
6.4	Configuring Video and Audio Settings	50
6.4.1	Configuring Video Settings	50
6.4.2	Configuring Audio Settings	53
6.4.3	Configuring ROI Encoding	53
6.4.4	Display Information on Stream	55
6.5	Configuring Image Parameters	56
6.5.1	Configuring Display Settings	56
6.5.2	Configuring OSD Settings	61
6.5.3	Configuring Text Overlay Settings	63
6.5.4	Configuring Privacy Mask	64
6.5.5	Configuring Picture Overlay	65
6.6	Configuring and Handling Alarms	66
6.6.1	Configuring Motion Detection	66
6.6.2	Configuring Video Tampering Alarm	72
6.6.3	Configuring Alarm Input	73
6.6.4	Configuring Alarm Output	74
6.6.5	Handling Exception	75
6.6.6	Configuring Other Alarm	76
6.6.7	Configuring Line Crossing Detection	79
6.6.8	Configuring Intrusion Detection	80
Chapter 7	Storage Settings	83
7.1	Configuring NAS Settings	83
7.2	Configuring Recording Schedule	85
7.3	Configuring Snapshot Settings	89
7.4	Configuring Lite Storage	91
Chapter 8	Playback	93
Chapter 9	Log Searching	95
Chapter 10	Others	97
10.1	Managing User Accounts	97
10.2	Authentication	99
10.3	Anonymous Visit	100
10.4	IP Address Filter	101
10.5	Security Service	102

10.6	Viewing Device Information	103
10.7	Maintenance	104
10.7.1	Rebooting the Camera	104
10.7.2	Restoring Default Settings.....	104
10.7.3	Exporting / Importing Configuration File.....	105
10.7.4	Upgrading the System	106
10.8	RS-232 Settings	106
10.9	RS-485 Settings	107
10.10	Service Settings.....	108
Appendix		109
	Appendix 1 SADP Software Introduction	109
	Appendix 2 Port Mapping	112

Chapter 1 System Requirement

Operating System: Microsoft Windows XP SP1 and above version / Vista / Win7 /

Server 2003 / Server 2008 32bits

CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 6.0 and above version, Apple Safari 5.02 and above version, Mozilla Firefox 3.5 and above version and Google Chrome8 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 CMS 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.

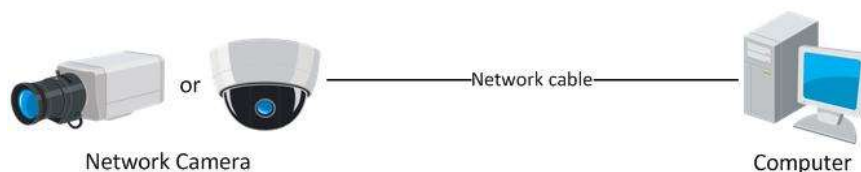


Figure 2-1 Connecting Directly

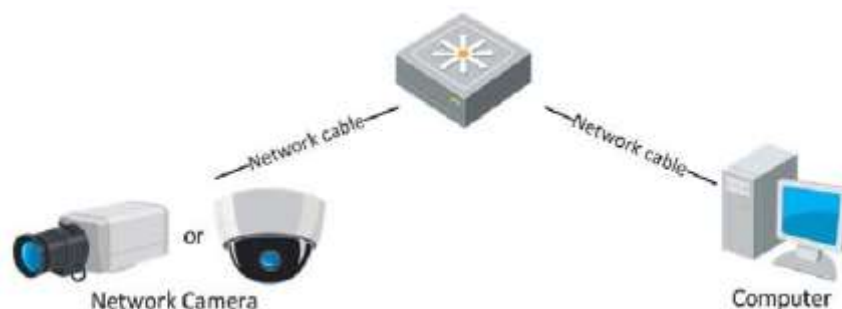


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Creating a Password

For most of the series, the default user name is admin and password is 12345.

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.

For some series, you are required to activate the camera first by setting a strong password for it before you can use the camera.

Creating a Password via Web Browser, Creating a Password via SADP, and Creating a Password via Client Software are all supported. Here we take web browser as an example.

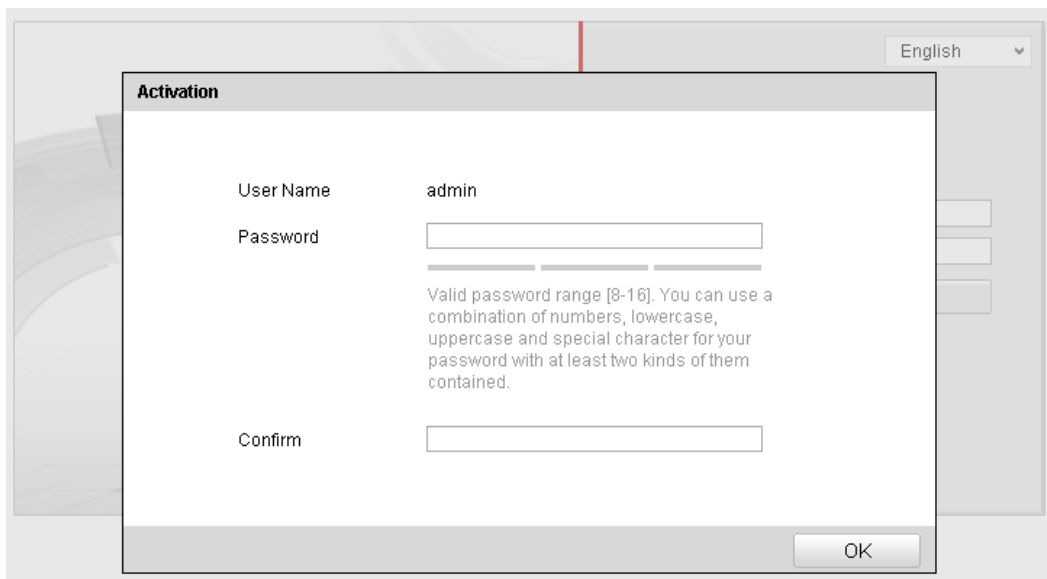
❖ Creating a Password via Web Browser

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. You can refer to the SADP manual for details.



The screenshot shows a web browser window with a language dropdown set to 'English'. The main content area is titled 'Activation'. It contains three input fields: 'User Name' with the value 'admin', 'Password' (empty), and 'Confirm' (empty). Below the password field, there is a text note: 'Valid password range [8-16]. You can use a combination of numbers, lowercase, uppercase and special character for your password with at least two kinds of them contained.' An 'OK' button is located at the bottom right of the activation form.

Figure 2-3 Creating a Password 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.

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.

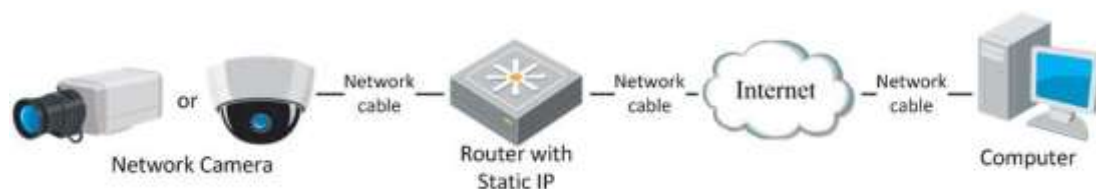


Figure 2-4 Accessing the Camera through Router with Static IP

- **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.

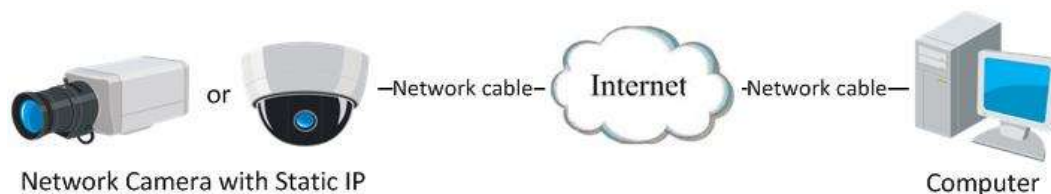


Figure 2-5 Accessing the Camera with Static IP Directly

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.

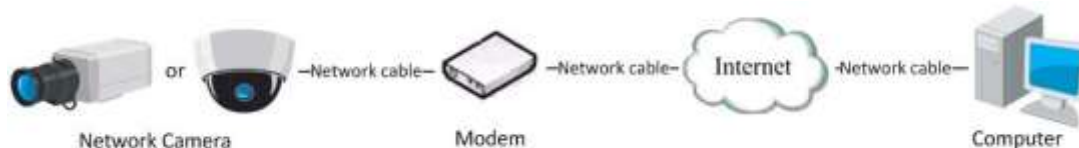


Figure 2-6 Accessing the Camera with Dynamic IP

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

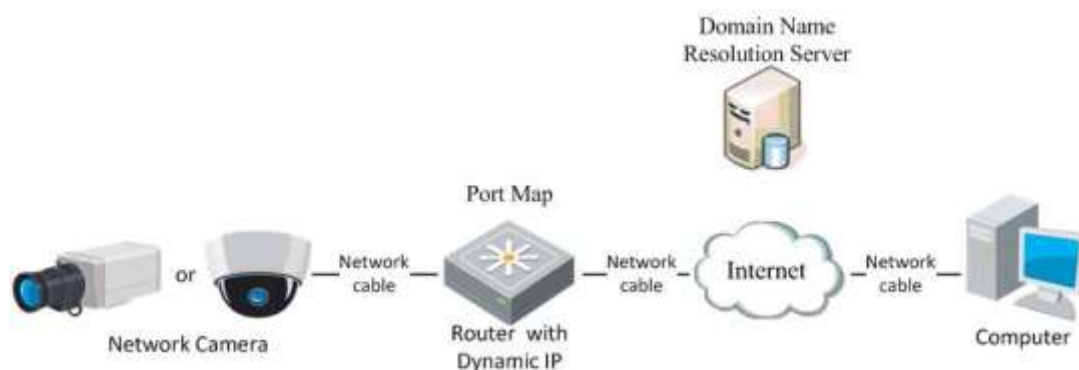


Figure 2-7 Normal Domain Name Resolution

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

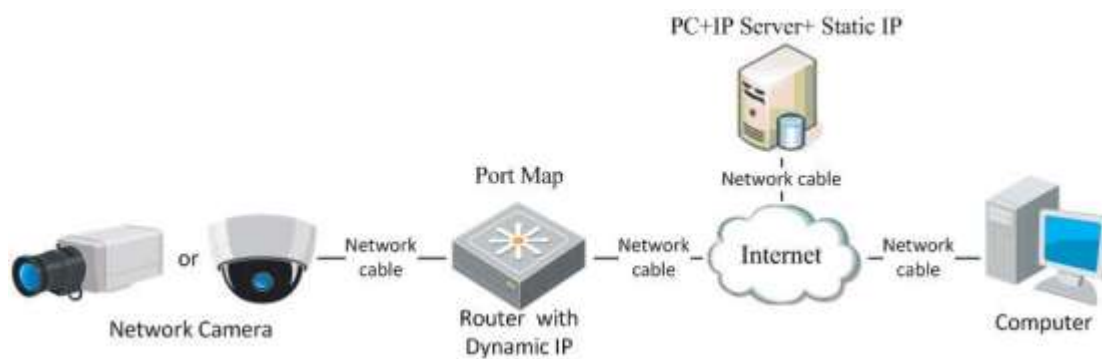


Figure 2-8 Private Domain Name Resolution

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

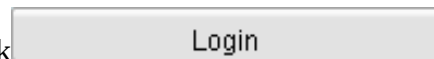
Steps:

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

Note:

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

3. Input the user name and password and click



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

Note:

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



Figure 3-1 Login Interface

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

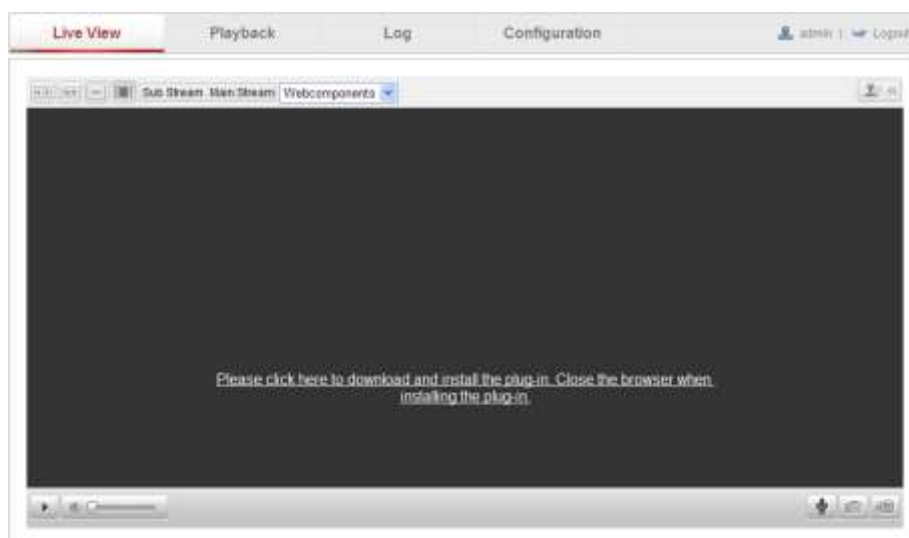


Figure 3-2 Download and Install Plug-in

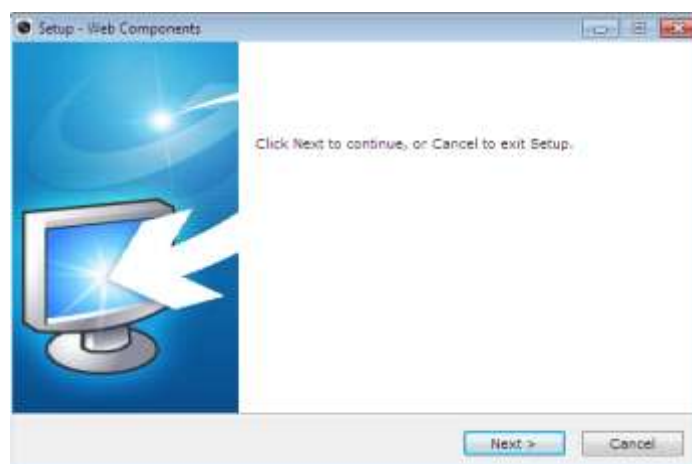


Figure 3-3 Install Plug-in (1)

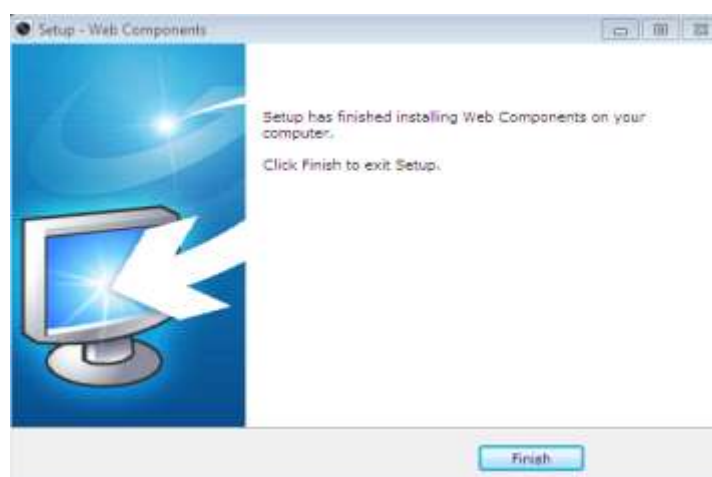


Figure 3-4 Install Plug-in (2)

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 CMS client software. You can view the live video and manage the camera with the software.

Follow the installation prompts to install the software. For detailed information about the software, please refer to the user manual of the CMS.

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

Before you start:

A wireless network must be configured.

Wireless Connection in Manage Mode

Steps:

1. Enter the Wi-Fi configuration interface.

Configuration> Advanced Configuration> Network> Wi-Fi



No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
1	belkin54g	infrastructure	NONE	1	94	54
2	Roy Zhong	infrastructure	WPA2-personal	1	78	54
3	yourPC	infrastructure	WPA2-personal	11	37	150
4	Micheal	infrastructure	WPA2-personal	6	31	150
5	APPLE	infrastructure	WPA2-personal	6	31	150

Figure 4-1 Wireless Network List

2. Click **Search** to search the online wireless connections.
3. Click to choose a wireless connection on the list.



Wi-Fi

SSID: belkin54g

Network Mode: ☒ Manager ☐ Ad-Hoc

Security Mode: not-encrypted

Figure 4-2 Wi-Fi Setting- Manage Mode

4. Check the checkbox 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.

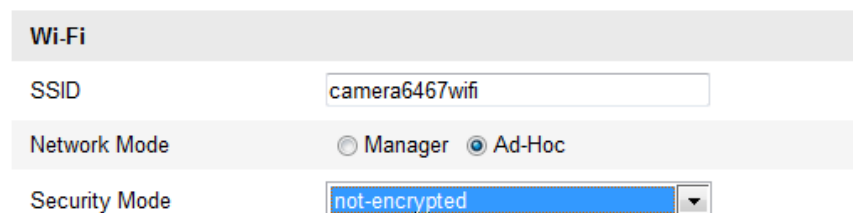
5. Enter the key to connect the wireless network. The key should be that of the wireless network connection you set on the router.

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:

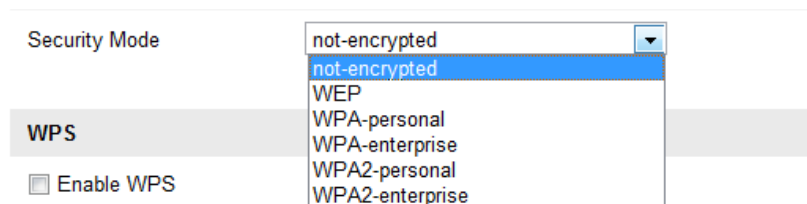
1. Choose Ad-hoc mode.



The image shows a configuration window for Wi-Fi settings in Ad-hoc mode. It includes fields for SSID (set to 'camera6467wifi'), Network Mode (radio buttons for Manager and Ad-Hoc, with Ad-Hoc selected), and Security Mode (a dropdown menu currently showing 'not-encrypted').

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

2. Customize a SSID for the camera.
3. Choose the Security Mode of the wireless connection.



The image shows a configuration window for Security Mode in Ad-hoc Mode. It features a dropdown menu for Security Mode with options: not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise. Below this is a section for WPS with an 'Enable WPS' checkbox.

Figure 4-4 Security Mode- Ad-hoc Mode

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 4-5 Ad-hoc Connection Point

6. Choose the SSID and connect.

Security Mode Description:

Wi-Fi	
SSID	belkin54g
Network Mode	☒ Manager ☐ Ad-Hoc
Security Mode	not-encrypted not-encrypted WEP WPA-personal WPA-enterprise WPA2-personal WPA2-enterprise
WPS ☐ Enable WPS	
PIN Code	99613013 Generate
☒ PBC connection	Connect

Figure 4-6 Security Mode

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

WEP mode:

Wi-Fi	
SSID	belkin54g
Network Mode	☒ Manager ☐ Ad-Hoc
Security Mode	WEP
Authentication	☒ Open ☐ Shared
Key Length	☒ 64bit ☐ 128bit
Key Type	☐ HEX ☐ ASCII
Key 1 ☒	
Key 2 ☐	
Key 3 ☐	
Key 4 ☐	

Figure 4-7 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.

Wi-Fi	
SSID	belkin54g
Network Mode	☒ Manager ☐ Ad-Hoc
Security Mode	WPA-personal
Encryption Type	TKIP
Key 1 ☒	

Figure 4-8 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

Wi-Fi	
SSID	test
Network Mode	☒ Manager ☐ Ad-Hoc
Security Mode	WPA-enterprise
Authentication	EAP-TLS
Identify	
Private key password	
EAPOL version	1
CA certificate	Browse Upload
User certificate	Browse Upload
Private key	Browse Upload

Figure 4-9 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:



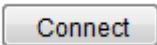
The screenshot shows a web interface for WPS configuration. At the top, there's a 'WPS' section header. Below it, the 'Enable WPS' checkbox is checked. A 'PIN Code' field displays '48167581' with a 'Generate' button to its right. Underneath, there are two radio button options: 'PBC connection' (which is selected) and 'Use router PIN code'. Each option has a 'Connect' button next to it. At the bottom, there are two empty input fields labeled 'SSID' and 'Router PIN code'.

Figure 4-10 Wi-Fi Settings - WPS

PBC Mode:

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

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

 PBC connection

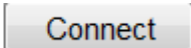
Note: Support of this mode is mandatory for both the Access Points and the connecting devices.

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.

 PBC connection

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 shown.

No.	SSID	Working Mode	Security Mode	Channel	Signal Strength	Speed(Mbps)
10	AP	infrastructure	WPA2-personal	11	13	54
11	Webber	infrastructure	WPA2-personal	11	7	54
12	TP-LINK_PocketAP_DFB048	infrastructure	WPA2-personal	6	7	150
13	AP1	infrastructure	WPA2-personal	11	0	150
14	TP-LINK_PocketAP_C4C218	infrastructure	NONE	6	0	150

Wi-Fi

SSID:

Network Mode: ☒ Manager ☐ Ad-Hoc

Security Mode:

Encryption Type:

Key 1:

WPS

☒ Enable WPS

PIN Code:

☐ PBC connection

☒ Use router PIN code

SSID:

Router PIN code:

Figure 4-11 Wi-Fi Settings – WPS PIN Mode

2. Choose **Use route 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**.

PIN Code:

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.

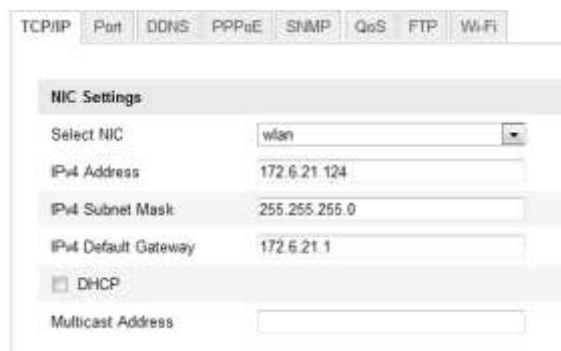
Steps:

1. Enter the TCP/IP configuration interface.

Configuration> Advanced Configuration> Network> TCP/IP

Or

Configuration> Basic Configuration> Network> TCP/IP



The screenshot shows a web-based configuration interface for a network camera. At the top, there is a horizontal menu with tabs: TCP/IP, Port, DDNS, PPPoE, SNMP, QoS, FTP, and Wi-Fi. The 'TCP/IP' tab is selected. Below the tabs, there is a section titled 'NIC Settings'. This section contains several fields: 'Select NIC' with a dropdown menu showing 'wlan'; 'IPv4 Address' with a text box containing '172.6.21.124'; 'IPv4 Subnet Mask' with a text box containing '255.255.255.0'; 'IPv4 Default Gateway' with a text box containing '172.6.21.1'; a checkbox labeled 'DHCP' which is currently unchecked; and 'Multicast Address' with an empty text box.

Figure 4-12 TCP/IP Settings

2. Select the NIC as wlan.
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:

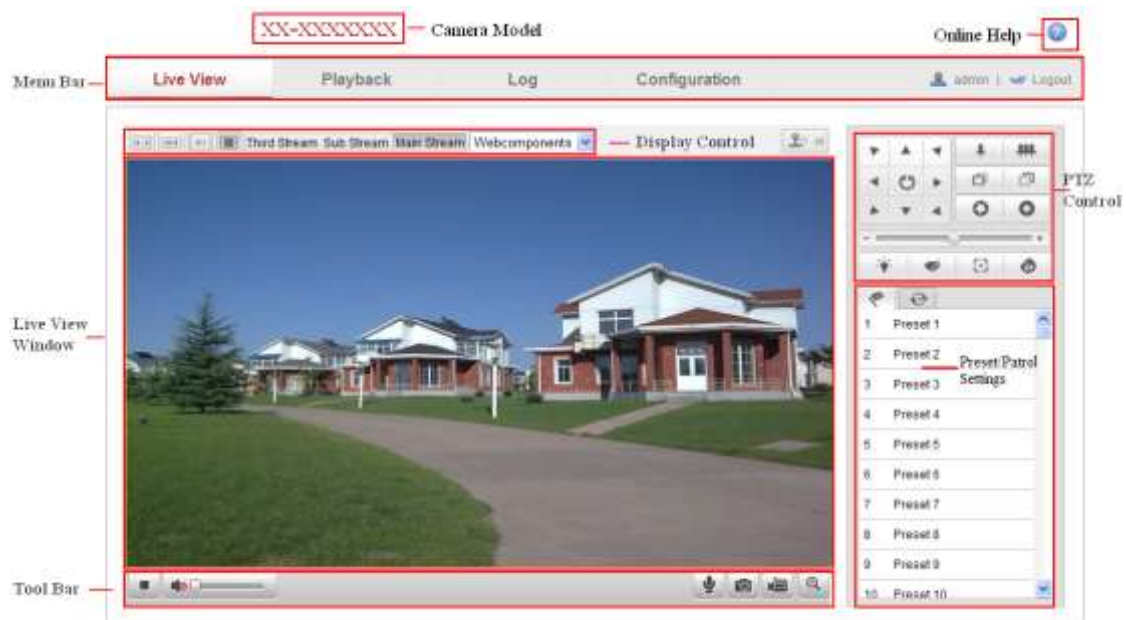


Figure 5-1 Live View Page

Camera Model:

It lists the camera model you are connecting to.

Online Help:

Click  to get the online help, which will guide you through the basic operations for each function.

Menu Bar:

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

Display Control:

Click each tab to adjust the layout and the stream type of the live view. And you can click the drop-down to select the plug-in. For IE (internet explorer) user, webcomponents and quick time are selectable. And for Non-IE user, webcomponents, quick time, VLC or MJPEG is selectable if they are supported by the web browser.

Live View Window:

Display the live video.

Toolbar:

Operations on the live view page, e.g., live view, capture, record, audio on/off, two-way audio, etc.

PTZ Control:

Panning, tilting and zooming actions of the camera and the light and wiper control.
(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

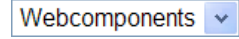
In the live view window as shown in Figure 5-2, click  on the toolbar to start the live view of the camera.



Figure 5-2 Live View Toolbar

Table 5-1 Descriptions of the Toolbar

Icon	Description
	Start/Stop live view.
	The window size is 4:3.
	The window size is 16:9.
	The original widow size.
	Self-adaptive window size.
Main Stream	Live view with the main stream.
Sub Stream	Live view with the sub stream.
Third 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.
	Turn on/off 3D positioning function.

Note: The third stream and 3D positioning require the support of camera.

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 Configuration** page. To configure remote scheduled recording, please refer to *Section 7.2*.

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 a pan/tilt unit has been installed to the camera. Please properly set the PTZ parameters on RS-485 settings page referring to *Section 12.9 RS-485 Settings*.

5.4.1 PTZ Control Panel

On the live view page, click  to show the PTZ control panel or click  to hide it.

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



Figure 5-3 PTZ Control Panel

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

Notes:

- There are 8 direction arrows (▲, ▼, ◀, ▶, ↖, ↗, ↘, ↙) in the live view window when you click and drag the mouse 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 +/-
	Light on/off
	Wiper on/off
	Auxiliary focus
	Initialize lens
	Adjust speed of pan/tilt movements

5.4.2 Setting / Calling a Preset

- **Setting a Preset:**

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

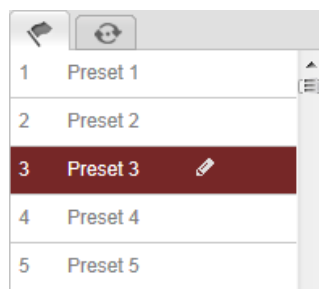


Figure 5-4 Setting a Preset

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.

Note: Up to 16 presets can be configured for the Network Mini PT Camera.

● 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.

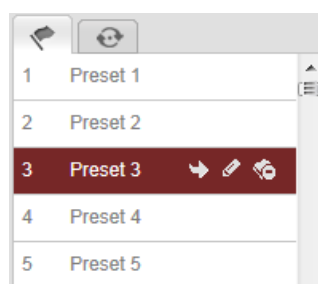


Figure 5-5 Calling a Preset

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.

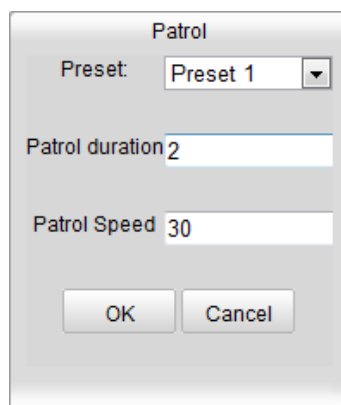


Figure 5-6 Add Patrol Path

6. Click  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

Note: 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 captured 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 Configuration

The screenshot shows the 'Local Configuration' interface with the following sections:

- Live View Parameters**
 - Protocol: ☒ TCP, ☐ UDP, ☐ MULTICAST, ☐ HTTP
 - Live View Performance: ☐ Shortest Delay, ☒ Auto
 - Rules: ☐ Enable, ☐ Disable
 - Image Format: ☒ JPEG, ☐ BMP
- Record File Settings**
 - Record File Size: ☐ 256M, ☒ 512M, ☐ 1G
 - Save record files to:
 - Save downloaded files to:
- Picture and Clip Settings**
 - Save snapshots in live view to:
 - Save snapshots when playback to:
 - Save clips to:

A 'Save' button is located at the bottom right of the interface.

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 6.3.1 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, or intrusion detection is triggered. E.g.: enabled as the rules are, and the motion detection is enabled as well, when a motion 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 captured 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.

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

6.2 Configuring Time Settings

Purpose:

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

Steps:

- Enter the Time Settings interface:

Configuration > Basic Configuration > System > Time Settings

Or **Configuration > Advanced Configuration > System > Time Settings**

Figure 6-2 Time Settings

- Select the Time Zone.

Select the Time Zone of your location from the drop-down menu.

- ◆ Synchronizing Time by NTP Server.

- Check the checkbox to enable the **NTP** function.

- 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.

The screenshot shows the 'Time Sync.' configuration section. The 'NTP' radio button is selected. Below it, there are three input fields: 'Server Address' with the value 'time.windows.com', 'NTP Port' with the value '123', and 'Interval' with the value '1440' followed by a 'min.' label.

Figure 6-3 Time Sync by NTP Server

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

◆ Synchronizing Time Synchronization Manually

Enable the **Manual Time Sync** function and then click  to set the system time from the pop-up calendar.

Note: You can also check the **Sync with computer time** checkbox to synchronize the time of the camera with that of your computer.

The screenshot shows the 'Manual Time Sync.' configuration section. On the left is a calendar for September 2013, with the 22nd highlighted. Below the calendar is a 'Time' display showing '11 : 14 : 33'. To the right of the calendar, the 'Manual Time Sync.' radio button is selected. Below it, there are two input fields: 'Device Time' with the value '2013-09-22T11:32:34' and 'Set Time' with the value '2013-09-22T11:14:33'. To the right of the 'Set Time' field is a checkbox labeled 'Sync. with computer time' which is currently unchecked.

Figure 6-4 Time Sync Manually

- Click the **DST** tab page to enable the DST function and Set the date of the DST period.

The screenshot shows the 'DST' configuration section. The 'Enable DST' checkbox is checked. Below it, there are three rows of settings: 'Start Time' set to 'Apr', 'First', 'Sun', '02' o'clock; 'End Time' set to 'Oct', 'Last', 'Sun', '02' o'clock; and 'DST Bias' set to '30min'.

Figure 6-5 DST Settings

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

6.3 Configuring Network Settings

6.3.1 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 may 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 > Basic Configuration > Network > TCP/IP

Or Configuration > Advanced Configuration > Network > TCP/IP

The screenshot displays the 'TCP/IP Settings' web interface. It is divided into two main sections: 'NIC Settings' and 'DNS Server'.

NIC Settings:

- NIC Type:** A dropdown menu set to 'Auto'.
- DHCP:** An unchecked checkbox.
- IPv4 Address:** A text box containing '10.11.36.159' with a 'Test' button to its right.
- IPv4 Subnet Mask:** A text box containing '255.255.255.0'.
- IPv4 Default Gateway:** A text box containing '10.11.36.254'.
- IPv6 Mode:** A dropdown menu set to 'Route Advertisement' with a 'View Route Advertisement' button to its right.
- IPv6 Address:** A text box containing '::'.
- IPv6 Subnet Mask:** A text box containing '0'.
- IPv6 Default Gateway:** An empty text box.
- Mac Address:** A text box containing '44:19:b6:5e:16:f2'.
- MTU:** A text box containing '1500'.
- Multicast Address:** An empty text box.
- Enable Multicast Discovery:** A checked checkbox.

DNS Server:

- Preferred DNS Server:** A text box containing '8.8.8.8'.
- Alternate DNS Server:** An empty text box.

A 'Save' button is located at the bottom right of the interface.

Figure 6-6 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. Click **Save** to save the above settings.

Notes:

- The valid value range of MTU is 1280 ~ 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router.
- A reboot is required for the settings to take effect.

6.3.2 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 > Basic Configuration > Network > Port

Or **Configuration > Advanced Configuration > Network > Port**

HTTP Port	80
RTSP Port	554
HTTPS Port	443
Server Port	8000

Figure 6-7 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.

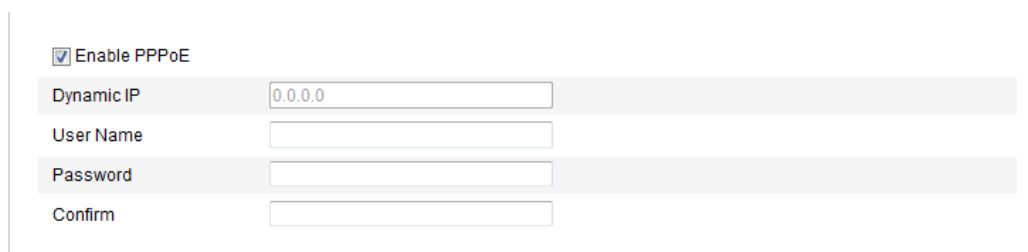
Note: A reboot is required for the settings to take effect.

6.3.3 Configuring PPPoE Settings

Steps:

1. Enter the PPPoE Settings interface:

Configuration > Advanced Configuration > Network > PPPoE



☒ Enable PPPoE	
Dynamic IP	0.0.0.0
User Name	
Password	
Confirm	

Figure 6-8 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.*

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

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

6.3.4 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:

- Enter the DDNS Settings interface:

Configuration > Advanced Configuration > Network > DDNS

Figure 6-9 DDNS Settings

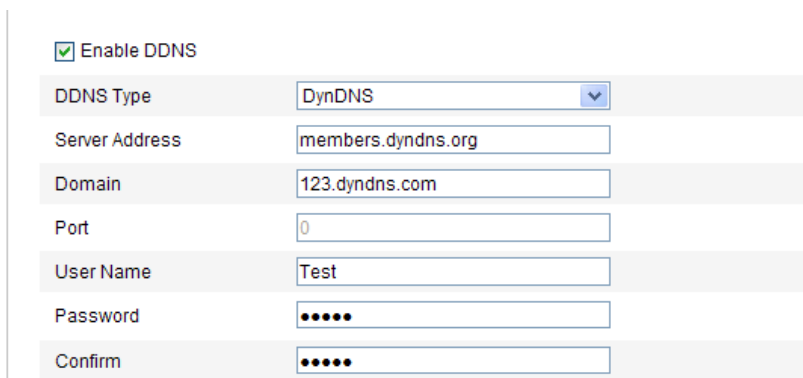
- Check the **Enable DDNS** checkbox to enable this feature.
- Select **DDNS Type**. Four DDNS types are selectable: SIMPLEDDNS, IPServer, NO-IP, and DynDNS.

- DynDNS:

Steps:

- Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
- In the **Domain** text field, enter the domain name obtained from the DynDNS website.

- (3) Enter the **Port** of DynDNS server.
- (4) Enter the **User Name** and **Password** registered on the DynDNS website.
- (5) Click **Save** to save the settings.



☒ Enable DDNS	
DDNS Type	DynDNS
Server Address	members.dyndns.org
Domain	123.dyndns.com
Port	0
User Name	Test
Password	
Confirm	

Figure 6-10 DynDNS Settings

- 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.



☒ Enable DDNS	
DDNS Type	IPServer
Server Address	212.15.10.121
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 6-11 IP Server Settings

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

- NO-IP:

Steps:

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

☒ Enable DDNS	
DDNS Type	NO-IP
Server Address	
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 6-12 NO-IP Settings

- (2) Enter the Server Address as www.noip.com
- (3) Enter the Domain name you registered.
- (4) Enter the Port number, if needed.
- (5) Enter the User Name and Password.
- (6) Click **Save** and then you can view the camera with the domain name.

- SIMPLEDDNS

Steps:

- (1) Choose the DDNS Type as SIMPLEDDNS.

☒ Enable DDNS	
DDNS Type	SIMPLEDDNS
Server Address	www.simpleddns.com
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 6-13 SIMPLEDDNS Settings

- (2) Select the continent/country of the server on which the device is registered.
And if you select the area as Custom, you can input the server address manually.
- (3) Enter the Domain name of the camera. The domain is the same with the device alias in the SIMPLEDDNS server.
- (4) Click **Save** to save the new settings.

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

6.3.5 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 > Advanced Configuration > Network > SNMP

SNMP v1/v2	
Enable SNMPv1	☐
Enable SNMP v2c	☐
Write SNMP Community	private
Read SNMP Community	public
Trap Address	
Trap Port	162
Trap Community	public

SNMP v3	
Enable SNMPv3	☐
Read UserName	
Security Level	no auth, no priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key password	
Write UserName	
Security Level	no auth, no priv
Authentication Algorithm	☒ MD5 ☐ SHA
Authentication Password	
Private-key Algorithm	☒ DES ☐ AES
Private-key password	

SNMP Other Settings	
SNMP Port	161

Figure 6-14 SNMP Settings

- Check the corresponding version checkbox (Enable SNMP SNMPv1 , Enable SNMP v2c , Enable SNMPv3) to enable the feature.

- Configure the SNMP settings.

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

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

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

6.3.6 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 > Advanced Configuration > Network > 802.1X

☒ Enable IEEE 802.1X	
Protocol	EAP-MD5
EAPOL version	1
User Name	
Password	
Confirm	

Figure 6-15 802.1X Settings

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.
3. Configure the 802.1X settings, including EAPOL version, user name and password.

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

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

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

6.3.7 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 > Advanced Configuration > Network > QoS

Video/Audio DSCP	0
Event/Alarm DSCP	0
Management DSCP	0

Figure 6-16 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 0-63. The bigger the DSCP value is, the higher the priority is.

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

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

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

6.3.8 Configuring UPnP™ Settings

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 UPnP™ settings interface.

Configuration > Advanced Configuration > Network > UPnP

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

The name of the device when detected online can be edited.



Figure 6-17 UPnP Settings

6.3.9 Configuring Wireless Dial Settings

Purpose:

Data stream of audio, video and image can be transferred via 3G / 4G wireless network.

Note: The wireless dial function requires the support of the camera.

1. Click the **Wireless Dial** tab to enter the Wireless Dial configuration interface.
2. Check the checkbox of **Enable** to enable the wireless dial settings.
3. Configure the dial parameters.
 - 1) Select the dial mode from the drop-down list. Auto and Manual are selectable. If Auto is selected, you can set the arming schedule for dialing; If Manual is selected, you can set the offline time and manual dialing parameters.
 - 2) Set the access number, user name, password, APN, MTU and verification protocol. You can also leave these parameters blank, and the device will adopt the default settings for dialing after other parameters are configured.
 - 3) Select the network mode from the drop-down list. Auto, 3G and 4G are selectable. If Auto is selected, the network selection priority comes as: 4G >

3G > Wired Network.

- 4) Input the offline time if Manual is selected as the dial mode.
- 5) Input the UIM Number (Mobile Phone Number).
- 6) Click the **Edit** button to set the arming schedule if Auto is selected as the dial mode.
- 7) Click **Save** to save the settings.

^ Dial Parameters

Dial Mode	Auto	▼
Access Number		
User Name		
Password		
APN		
MTU	1400	
Verification Protocol	Auto	▼
Network Mode	Auto	▼
Offline Time	3600	second
UIM Number		

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

Figure 6-18 Dial Parameters

4. View the dial status.
 - 1) Click the **Refresh** button to view the dial status including real-time mode, UIM status, signal strength, etc.
 - 2) If Manual is selected as the dial mode, you can also manually connect / disconnect the wireless network.

^ Dial Status

Real-time Mode	UNKNOWN
UIM Status	UNKNOWN
Signal Strength	0
Dial Status	disconnected
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS Address	0.0.0.0

[Refresh](#)

Figure 6-19 Dial Status

5. Set the white list.

1) Check the checkbox of **Enable SMS Alarm**.

The mobile phone number on the white list can receive the alarm message from the device and reboot the device via SMS.

Note: Up to 8 mobile phone numbers can be added on the white list.

^ White List

☒ Enable SMS Alarm

No.	Mobile Phone Number	Permission
1	18888888888	Edit
2	15968172711	
3		
4		
5		
6		
7		
8		

[Send Test SMS](#)[Save](#)

Figure 6-20 White List Settings

2) Select the item on the white list, and click the **Edit** button to enter the SMS Alarm Settings interface.

Exception	Basic Event	Smart Event
☐ HDD Full	☐ Motion Detection	☐ Line Crossing Detection
☐ Network Disconnected	☐ Video Tampering	☐ Intrusion Detection
☐ HDD Error		
☐ IP Address Conflicted		
☐ Illegal Login		

Figure 6-21 SMS Alarm Settings

- 3) Input the mobile phone number for the white list, check the checkbox of **Reboot via SMS**, select the alarm for SMS push, and click **OK**.

Note: To reboot the device via SMS, send the message "reboot" to the device, and the device will reply a message "reboot success" after rebooting succeeded.

- 4) (Optional) You can click **Send Test SMS** to send a message to the mobile phone for test.
- 5) Click **Save** to save the settings.

6.3.10 Email Sending Triggered by Alarm

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

Steps:

1. Enter the TCP/IP Settings (**Configuration > Basic Configuration > Network > TCP/IP** or **Configuration > Advanced Configuration > Network > TCP/IP**) to

set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.

Note: Please refer to *Section 6.3.1 Configuring TCP/IP Settings* for detailed information.

2. Enter the Email Settings interface:

Configuration > Advanced Configuration > Network > Email

The screenshot shows the 'Email Settings' configuration page. It is organized into two main sections: 'Sender' and 'Receiver'.
Sender Section:
 - 'Sender': Text input field containing 'Test'.
 - 'Sender's Address': Text input field containing 'Test@gmail.com'.
 - 'SMTP Server': Text input field containing 'smtp.263xmail.com'.
 - 'SMTP Port': Text input field containing '25'.
 - 'Enable SSL': A checkbox that is currently unchecked.
 - 'Interval': A dropdown menu showing '2s'.
 - 'Attached Image': A checkbox that is currently unchecked.
 - 'Authentication': A checkbox that is currently unchecked.
 - 'User Name': Text input field.
 - 'Password': Text input field.
 - 'Confirm': Text input field.
Receiver Section:
 - 'Receiver1': Text input field containing 'Test1'.
 - 'Receiver1's Address': Text input field containing 'Test1@gmail.com'.
 - 'Receiver2': Text input field.
 - 'Receiver2's Address': Text input field.
 - 'Receiver3': Text input field.
 - 'Receiver3's Address': Text input field.
 At the bottom right of the form is a 'Save' button.

Figure 6-22 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: The SMTP Server IP address or host name (e.g., smtp.263xmail.com).

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

Enable SSL: Check the checkbox to enable SSL if it is required by the SMTP server.

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 enter the login user Name and password.



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

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

Receiver: The name of the user to be notified.

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

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

6.3.11 Configuring NAT (Network Address Translation) Settings

Purpose:

1. Enter the NAT settings interface.

Configuration > Advanced Configuration > Network > NAT

2. Choose the port mapping mode.

To port mapping with the default port numbers:

Choose Port Mapping Mode as **Auto**.

To port mapping with the customized port numbers:

Choose Port Mapping Mode as **Manual**.

And for manual port mapping, you can customize the value of the port number by yourself.

	Port Type	External Port	External IP Address	Status
☒	HTTP	80	0.0.0.0	Not Valid
☒	RTSP	554	0.0.0.0	Not Valid
☒	Server Port	8000	0.0.0.0	Not Valid

Figure 6-23 Configure NAT Settings

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

6.3.12 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:

- Enter the FTP Settings interface:

Configuration > Advanced Configuration > Network > FTP

Figure 6-24 FTP Settings

- Configure the FTP settings; and the user name and password are required for

login the FTP 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.*

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 type: 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.

Note: If you want to upload the captured pictures to FTP server, you have to enable the timing snapshot or event-triggered snapshot on **Snapshot** page. For detailed information, please refer to the *Section 7.3*.

6.3.13 HTTPS Settings

Purpose:

HTTPS provides authentication of the web site and associated web server that one is communicating with, 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 > Advanced Configuration > Network > HTTPS

2. Check the checkbox of Enable HTTPS to enable the function.
3. Create the self-signed certificate or authorized certificate.

The screenshot shows the 'HTTPS Settings' web interface. At the top, there is a checkbox labeled 'Enable HTTPS'. Below it is a 'Create' section with two buttons: 'Create Self-signed Certificate' and 'Create Certificate Request'. The 'Install Signed Certificate' section has a 'Certificate Path' input field with 'Browse' and 'Upload' buttons. The 'Created Request' section has a 'Created Request' input field with 'Delete' and 'Download' buttons. The 'Installed Certificate' section shows a table with one entry: 'C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=10.11', with a 'Delete' button. Below the table, the 'Property' section displays the certificate details: 'Subject: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=10.11.32.17, EM=com.cn', 'Issuer: C=CN, ST=ZJ, L=HZ, OU=embeddedsoftware, H/IP=10.11.32.17, EM=com.cn', and 'Validity: 2014-05-09 15:45:14 ~ 2017-05-08 15:45:14'.

Figure 6-25 HTTPS Settings

- Create the self-signed certificate

- 1) Click **Create** button to enter the creation interface.
- 2) Enter the country, host name/IP, validity and other information.
- 3) 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) Click **Create** button to create the certificate request.
- 2) Download the certificate request and submit it to the trusted certificate authority for signature.

- 3) After receiving the signed valid certificate, import the certificate to the device.
4. There will be the certificate information after you successfully create and install the certificate.

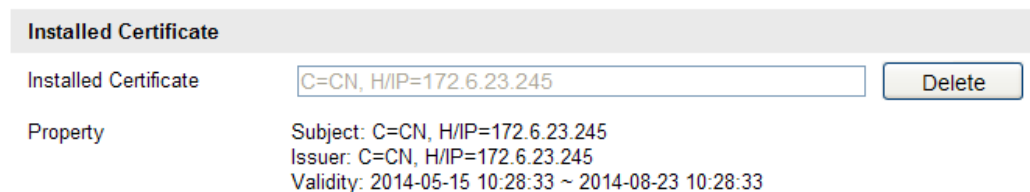


Figure 6-26 Installed Certificate

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

6.4 Configuring Video and Audio Settings

6.4.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface:

Configuration > Basic Configuration > Video / Audio > Video

Or **Configuration > Advanced Configuration > Video / Audio > Video**

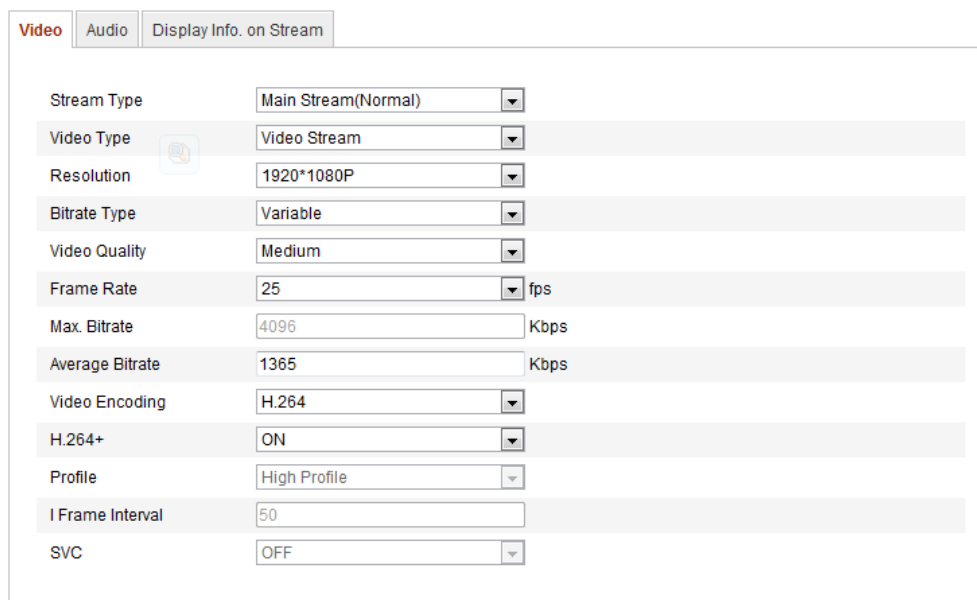


Figure 6-27 Video Settings

2. Select the **Stream Type** of the camera to main stream (normal), sub-stream or third

stream.

The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream and third 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, the parameters are various according to different platform, please refer to the real sample:

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 to 1/16~25 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 to 32~16384 Kbps. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

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

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.

Note: The video encoding type varies according to different camera platforms. For some certain cameras, H.265 is supported while MPEG4 is not.

H.264+:

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+, user 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+.

After H.264+ is enabled, when you set the Variable as the bitrate type, 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.

Profile:

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

I Frame Interval:

Set the I-Frame interval to 1~400.

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

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

6.4.2 Configuring Audio Settings

Steps:

1. Enter the Audio Settings interface

Configuration > Basic Configuration > Video / Audio > Audio

Or Configuration > Advanced Configuration > Video / Audio > Audio

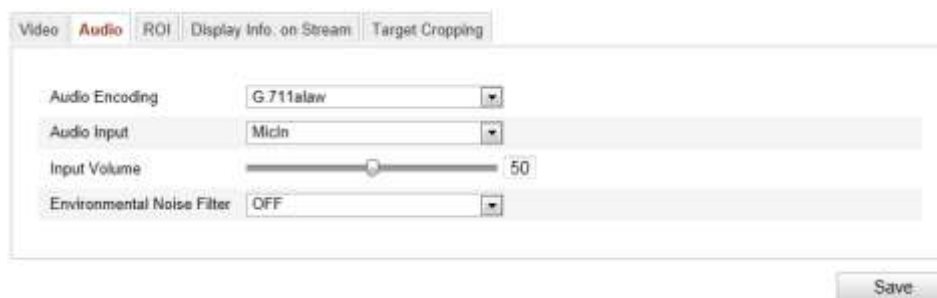


Figure 6-28 Audio Settings

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

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.

6.4.3 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 6-29 Region of Interest Settings

Configuring Fixed Region for ROI:

Steps:

1. Enter the ROI settings interface:
Configuration> Advanced 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> Advanced 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. Check the checkbox of **Enable License Plate Tracking**, and then the captured license plate picture is set as region of interest.
Note: To enable license plate tracking function, the vehicle detection function should be supported and enabled.
4. Respectively set the ROI level. The larger the value is, the better the image quality is.
5. Select the stream type for ROI encoding.
6. Click **Save** to save the settings.

6.4.4 Display Information 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. And then you can set rules on the connected rear-end device to detect the events including line crossing, intrusion, etc.

6.5 Configuring Image Parameters

6.5.1 Configuring Display Settings

Purpose:

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

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

Steps:

1. Enter the Display Settings interface:

Configuration > Basic Configuration> Image> Display Settings

Or Configuration > Advanced Configuration> Image> Display Settings

2. Set the image parameters of the camera.

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

Day/Night Auto-switch

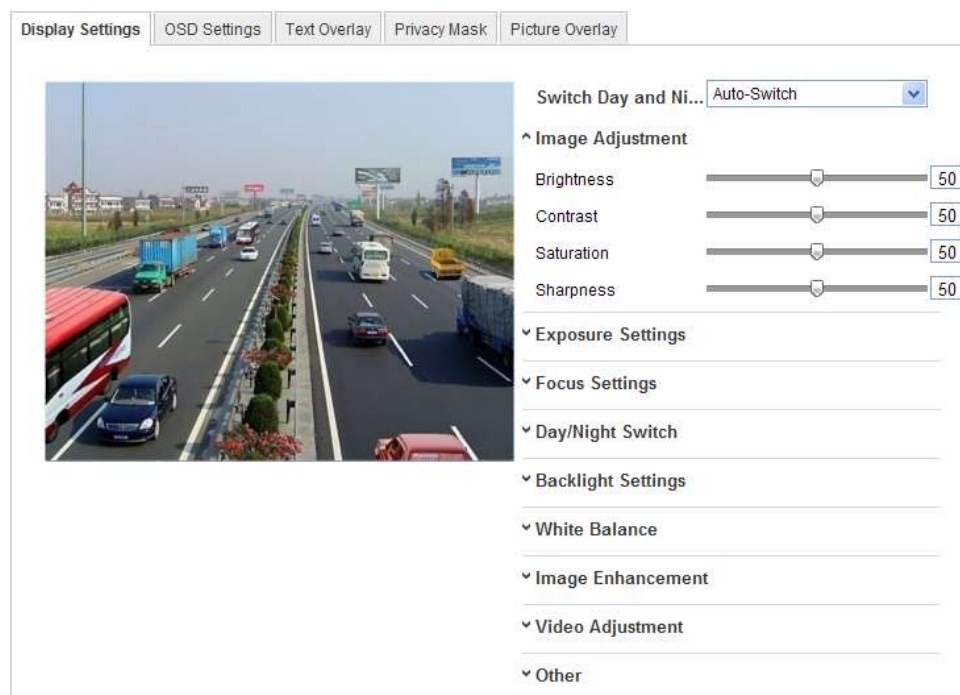


Figure 6-30 Display Settings of Day/night Auto-switch

◆ Image Adjustment

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

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

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

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

For the camera supports **P-Iris** lens, if P-Iris lens is adopted, then the P-Iris lens type is selectable, e.g.: Tamron 2.8-8mm F1.2 (M13VP288-IR), or if DC lens is adopted, then manual and auto are selectable.

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

◆ Focus Settings

For the camera supports electronic lens, you can set the focus mode as Auto, Manual or Semi-auto. If auto is selected, the focus is adjusted automatically according to the actual monitoring scenario; if manual is selected, you can control the lens by adjusting the zoom, focus, lens initialization, and auxiliary focus via the PTZ control interface; if semi-auto is selected, the camera will focus automatically when you adjust the zoom parameters.

◆ Day/Night Switch

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

^ Day/Night Switch

Day/Night Switch	Auto
Sensitivity	4
Filtering Time	5
Smart IR	ON
Mode	Manual
Distance	50

Figure 6-31 Day/Night Switch

Day, night, auto, schedule, and triggered by alarm input are selectable for day/night switch.

Day: the camera stays at day mode.

Night: the camera stays at night mode.

Auto: the camera switches between the day mode and the night mode according to the illumination automatically. The sensitivity ranges from 0~7, 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.

Schedule: Set the start time and the end time to define the duration for day/night mode.

Triggered by alarm input: The switch is triggered by alarm input, and you can set the triggered mode to day or night.

Smart IR: Smart IR function gives user an option to adjust the power of the IR LED, thus providing a clear image that is not overexposed or too dark. Select ON to enable the smart IR, and then Auto and Manual are selectable for IR mode.

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

Select Manual, and you can manually set the value of distance between the IR camera and object, to adjust the power of IR LED. Small distance value indicates the object is near the IR camera, and the device adjusts the IR LED to lower power to avoid

overexposure; large distance value indicates the object is far away, and the device adjusts the IR LED to higher power to avoid too dark image.

◆ Backlight Settings

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

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

◆ White Balance

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

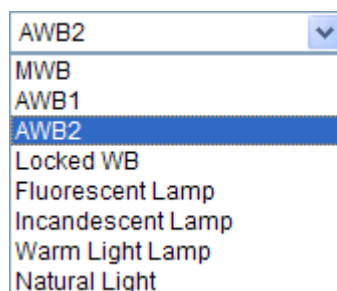


Figure 6-32 White Balance

◆ Image Enhancement

Digital Noise Reduction: DNR reduces the noise in the video stream. OFF, Normal Mode and Expert Mode are selectable. Set the DNR level from 0~100, 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.

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.

Lens Distortion Correction: Select ON / OFF to enable / disable the lens distortion correction. The distorted image caused by the wide-angle lens can be corrected if this function enabled.

◆ Other

Some of the camera supports CVBS, SDI, or HDMI output. Please refer to the actual camera model for details.

Day/Night Scheduled-Switch

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



Figure 6-33 Day/Night Scheduled-Switch Configuration Interface

Steps:

1. Click the time line 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: The detailed information of each parameter please refers to day/night auto switch session.

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.

6.5.2 Configuring OSD Settings

Purpose:

You can customize the camera name and time on the screen.

Steps:

1. Enter the OSD Settings interface:

Configuration > Advanced Configuration > Image > OSD Settings

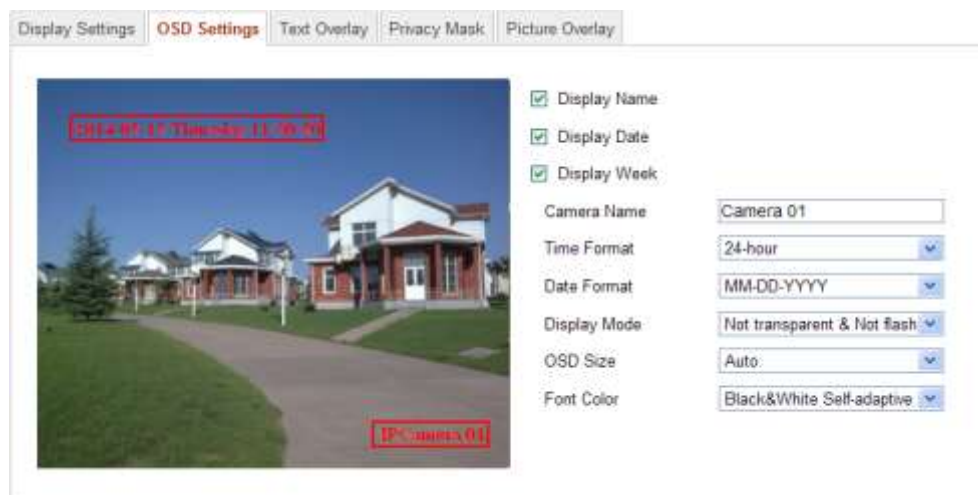


Figure 6-34 OSD Settings

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, date format, display mode and the OSD font size.
5. Define the font color of the OSD by clicking the drop-down, and black & white self-adaptive and custom are selectable.

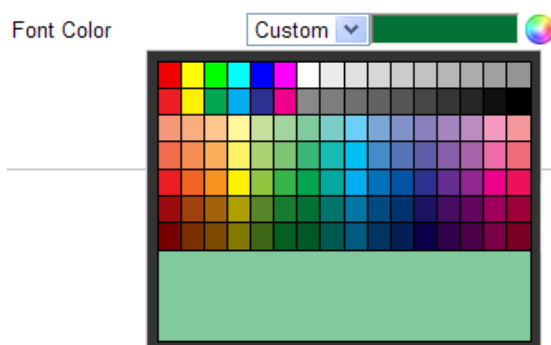


Figure 6-35 Font Color-Custom

6. You can use the mouse to click and drag the text frame **IP Camera 01** in the live view window to adjust the OSD position.

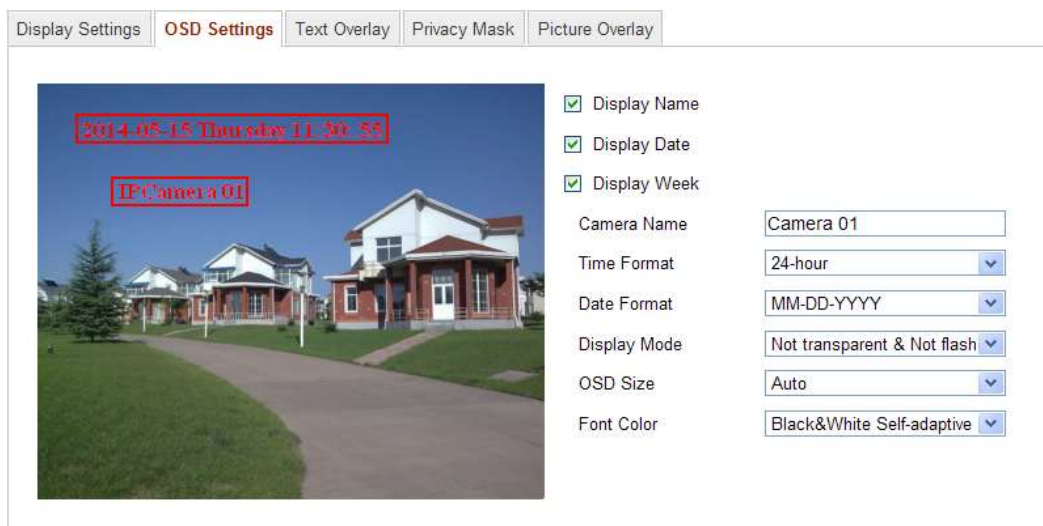


Figure 6-36 Adjust OSD Location

7. Click **Save** to activate the above settings.

6.5.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

1. Enter the Text Overlay Settings interface:

Configuration > Advanced Configuration > Image > Text Overlay

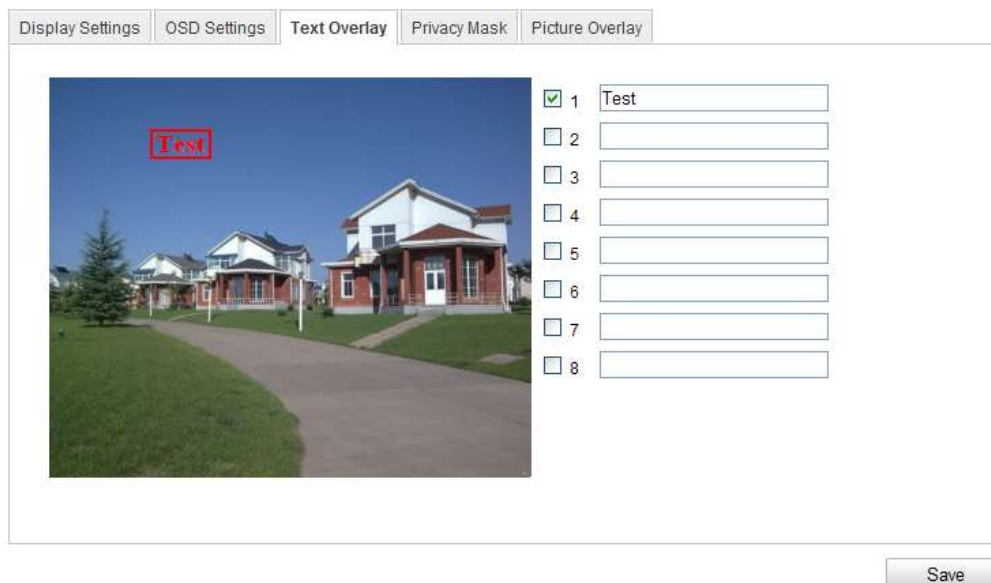


Figure 6-37 Text Overlay

2. Check the checkbox in front of textbox to enable the on-screen display.
3. Input the characters in the textbox.
4. (Optional) Use the mouse to click and drag the red text frame  in the live view window to adjust the text overlay position.
5. Click **Save** to save the settings.

Note: Up to 8 text overlays are configurable.

6.5.4 Configuring Privacy Mask

Purpose:

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

Steps:

1. Enter the Privacy Mask Settings interface:

Configuration > Advanced Configuration > Image > Privacy Mask

2. Check the checkbox of **Enable Privacy Mask** to enable this function.
3. Click **Draw Area**.

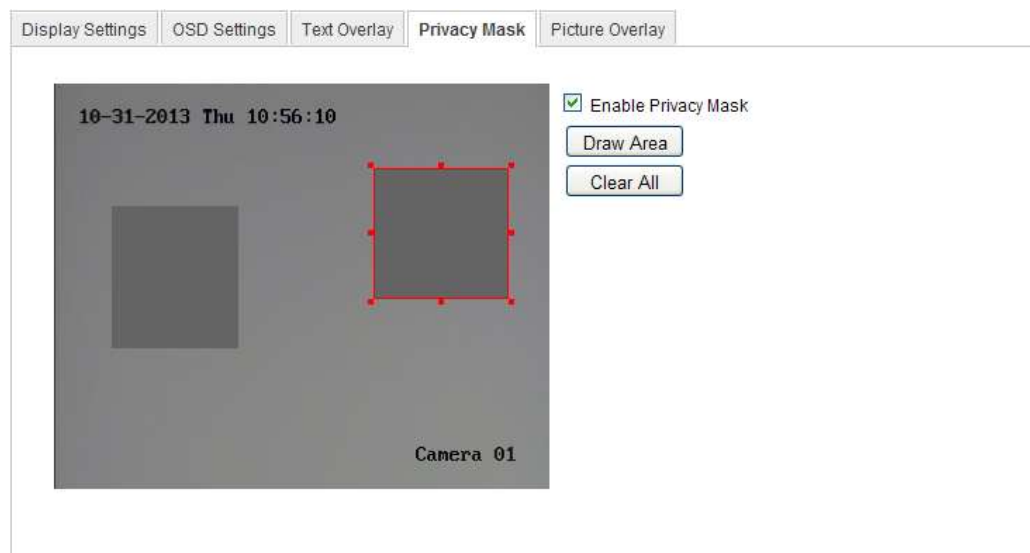


Figure 6-38 Privacy Mask Settings

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.

6.5.5 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.

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

Steps:

1. Enter the Picture Overlay Settings interface:

Configuration > Advanced Configuration > Image > Picture Overlay

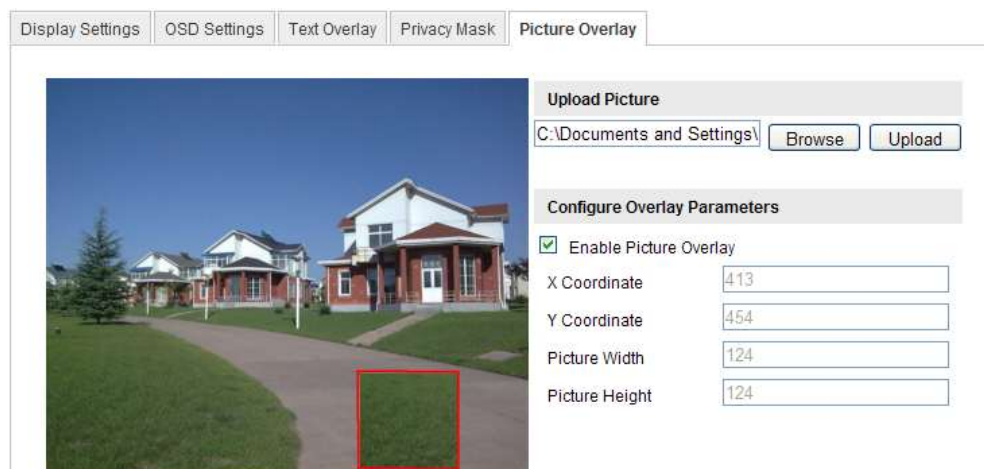


Figure 6-39 Picture Overlay

2. Click **Browse** to select a picture.
3. Click **Upload** to upload it.
4. Check **Enable Picture Overlay** checkbox to enable the function.

X Coordinate and Y Coordinate values are for the location of the picture on the image.

And the Picture width and height shows the size of the picture.

6.6 Configuring and Handling Alarms

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

Notes:

- 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.
- Click  for help when you configure the intelligent functions. A help document will guide you to go through the configuration steps.

6.6.1 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 one 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 > Advanced Configuration> 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 objects displayed with the rectangles. Select disable from **Configuration-Local Configuration-Live View Parameters-rules**.

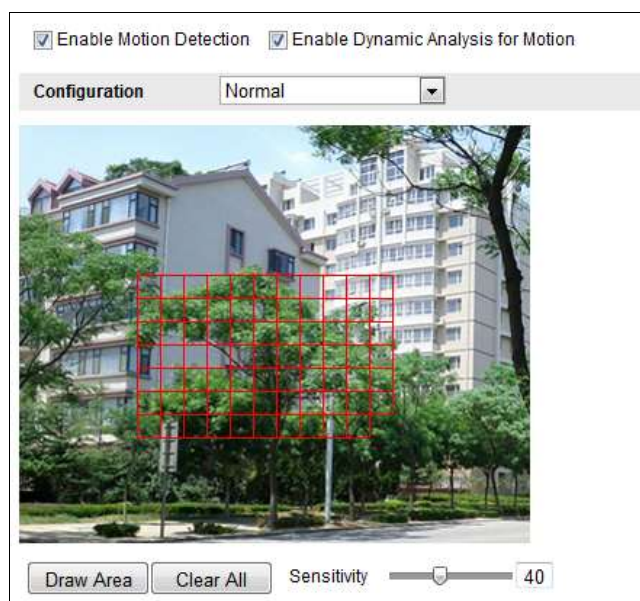


Figure 6-40 Enable Motion Detection

(4) Click **Draw Area**. Click and drag the mouse on the live video to draw a motion detection area.

(5) Click **Stop Drawing** to finish drawing one area.

(6)(Optional) Click **Clear All** to clear all of the areas.

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

2. Set the Arming Schedule for Motion Detection.

Steps:

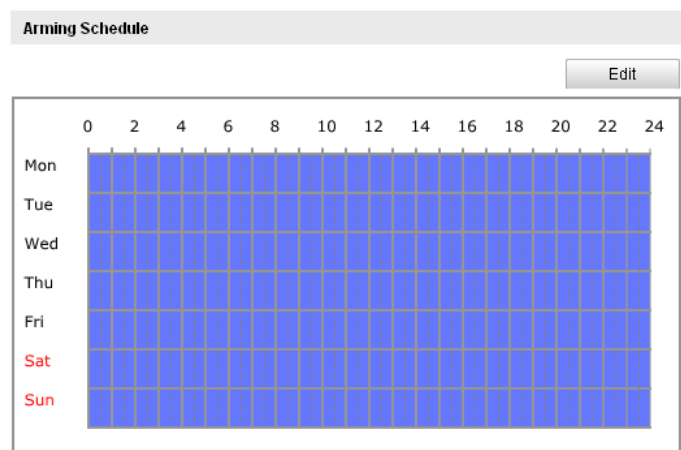


Figure 6-41 Arming Time

- (1) Click **Edit** to edit the arming schedule. The Figure 6-34 shows the editing interface of the arming schedule.
- (2) Choose the day you want to set the arming schedule.
- (3) Click  to set the time period for the arming schedule.
- (4) (Optional) After you set the arming schedule, you can copy the schedule to other days.
- (5) Click **OK** to save the settings.

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

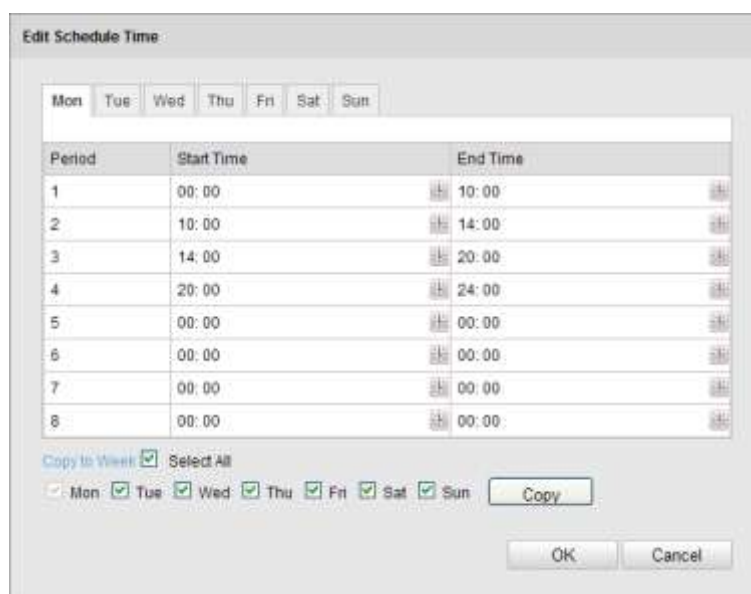


Figure 6-42 Arming Time Schedule

3. Set the Alarm Actions for Motion Detection.

Check the checkbox to select the linkage method. Notify surveillance center, send email, upload to FTP, trigger channel and trigger alarm output are selectable. You can specify the linkage method when an event occurs.

Linkage Method	
Normal Linkage	Other Linkage
☒ Audible Warning ☒ Notify Surveillance Center ☒ Send Email ☒ Upload to FTP ☐ Trigger Channel	Trigger Alarm Output ☐ Select All

Figure 6-43 Linkage Method

● Audible Warning

Trigger the audible warning locally. And it only supported by the device 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, you need to refer to *Section 6.3.10 Email Sending Triggered by Alarm* to set the related parameters.

● 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 6.3.12 Configuring FTP Settings* for detailed information.
- Go to **Advanced Configuration > Storage > Snapshot** 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 7.2* 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 6.6.4 Configuring Alarm Output* to set the related parameters.

➤ Expert Configuration

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

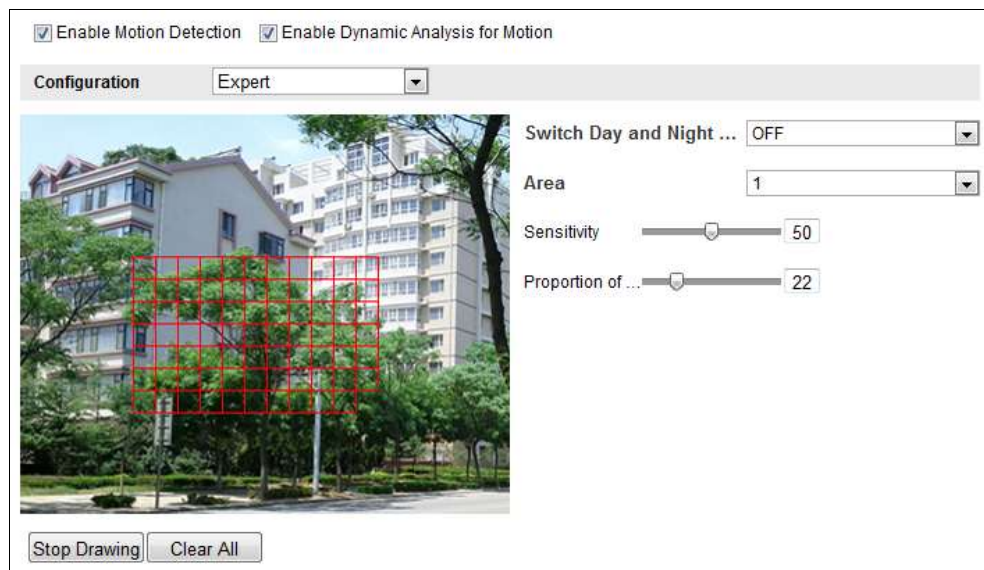


Figure 6-44 Expert Mode of Motion Detection

● 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**.

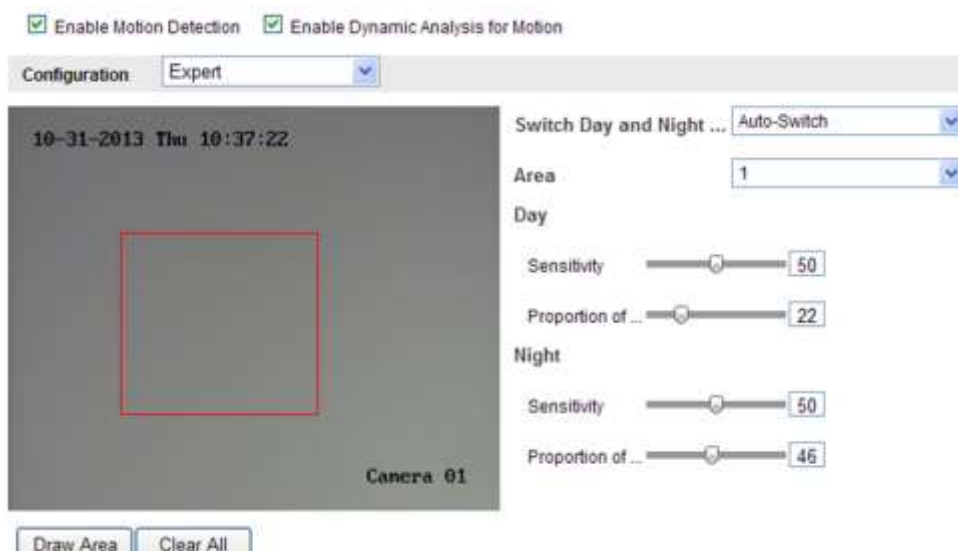


Figure 6-45 Day/Night Auto-Switch

- (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

(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**.

Switch Day and Night ... Scheduled- Switch

Start Time 06:00:00

End Time 18:00:00

Figure 6-46 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.

6.6.2 Configuring Video Tampering Alarm

Purpose:

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

Steps:

1. Enter the video tampering Settings interface:

Configuration > Advanced Configuration > Basic Event > Video Tampering

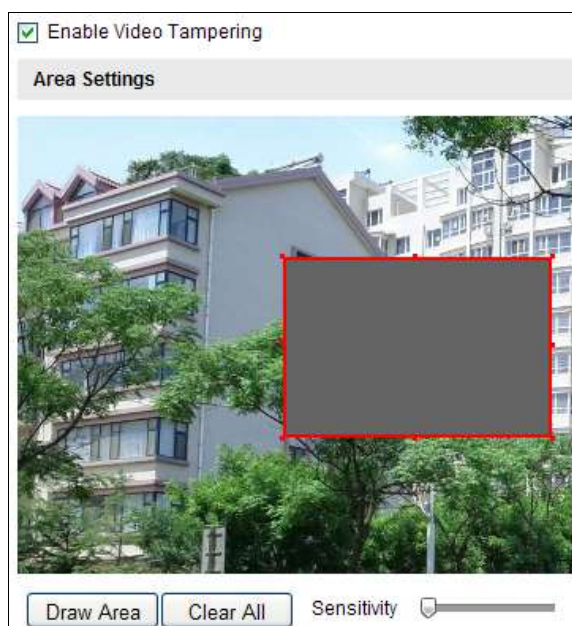


Figure 6-47 Video Tampering Alarm

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 6.6.1*.
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 6.6.1*.
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 Alarm Actions for Motion Detection* in *Section 6.6.1*.
6. Click **Save** to save the settings.

6.6.3 Configuring Alarm Input

Steps:

1. Enter the Alarm Input Settings interface:

Configuration > Advanced Configuration > 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).

Alarm Input No.

Alarm Name (cannot copy)

Alarm Type

Arming Schedule

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

Figure 6-48 Alarm Input Settings

3. Click **Edit** to set the arming schedule for the alarm input. Refer to *Task 2 Set the Arming Schedule for Motion Detection* in Section 6.6.1.
4. Check the checkbox to select the linkage method taken for the alarm input. Refer to *Task 3 Set the Alarm Actions for Motion Detection* in Section 6.6.1.
5. You can also choose the PTZ linking for the alarm input if your camera is installed with a pan/tilt unit. Check the relative checkbox and select the No. to enable Preset Calling, Patrol Calling or Pattern Calling.
6. You can copy your settings to other alarm inputs.
7. Click **Save** to save the settings.

6.6.4 Configuring Alarm Output

Steps:

1. Enter the Alarm Output Settings interface:

Configuration>Advanced Configuration> 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 **Edit** 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 6.6.1*.
5. You can copy the settings to other alarm outputs.
6. Click **Save** to save the settings.

The screenshot displays the 'Alarm Output Settings' interface. At the top, there are three configuration fields: 'Alarm Output' set to 'A->1', 'Alarm Name' with a text box and '(cannot copy)' label, and 'Delay' set to 'Manual'. Below these is a section titled 'Arming Schedule' which contains a 7x24 grid for scheduling. The grid rows are labeled with days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) and the columns are labeled with hours from 0 to 24. The grid cells are currently all blue. An 'Edit' button is located to the right of the grid.

Figure 6-49 Alarm Output Settings

6.6.5 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 > Advanced Configuration > Basic Event > Exception

2. Check the checkbox to set the actions taken for the Exception alarm. Refer to *Task 3 Set the Alarm Actions Taken for Motion Detection* in Section 6.6.1.

Exception Type: HDD Full	
Normal Linkage ☒ Notify Surveillance Center ☒ Send Email	Other Linkage Trigger Alarm Output ☒ Select All ☐ A->1

Save

Figure 6-50 Exception Settings

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

6.6.6 Configuring Other Alarm

Note: Some certain cameras support Wireless Alarm, PIR (passive infrared sensor) Alarm or Emergency Alarm.

● Wireless Alarm

Purpose:

When wireless alarm signal is sent to the camera from the detector, such as the wireless door contact, the wireless alarm is triggered and a series of response actions can be taken.

Steps:

1. Enter the Wireless Alarm Settings interface:
Configuration > Advanced Configuration > Basic Event > Other Alarm
2. Select the wireless alarm number.
Up to 8 channels of external wireless alarm input are supported.
3. Check the checkbox of **Enable Wireless Alarm** to activate the wireless alarm.
4. Input the alarm name in the text field as desired.
5. Check the checkbox to select the linkage methods taken for the wireless alarm.

6. Click **Save** to save the settings.
7. Locate the external wireless device beside the camera, and go to **Configuration > Advanced Configuration> System> Remote Control** to arm the camera and study the wireless alarm.

Wireless Alarm

Select Wireless Alarm: 1

☒ Enable Wireless Alarm

Alarm Name:

Normal Linkage	Other Linkage
☒ Audible Warning	Trigger Alarm Output ☐ Select All
☒ Notify Surveillance Center	☐ A->1
☒ Send Email	Trigger Wireless Alarm
☒ Upload to FTP	☐ Wireless audible and visual alarm
☒ Trigger Channel	

Save

Figure 6-51 Configuring Wireless Alarm Settings

● PIR Alarm

Purpose:

A PIR (Passive Infrared) alarm is triggered when an intruder moves within the detector's field of view. The heat energy dissipated by a person, or any other warm blooded creature such as dogs, cats, etc., can be detected.

Steps:

1. Enter the PIR Alarm Settings interface:
Configuration > Advanced Configuration> Basic Event> Other Alarm
2. Check the checkbox of **Enable PIR Alarm** to activate the PIR alarm function.
3. Input the alarm name in the text field as desired.
4. Check the checkbox to select the linkage methods taken for the PIR alarm.
5. Click the **Edit** button to set the arming schedule.
6. Click **Save** to save the settings.
7. Go to **Configuration > Advanced Configuration> System> Remote Control** to arm the camera.

PIR Alarm

☒ Enable PIR Alarm

Alarm Name

Normal Linkage	Other Linkage
☒ Audible Warning	Trigger Alarm Output ☐ Select All
☒ Notify Surveillance Center	☐ A->1
☐ Send Email	Trigger Wireless Alarm
☐ Upload to FTP	☐ Wireless audible and visual alarm
☒ Trigger Channel	

Arming Schedule

Edit

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

Save

Figure 6-52 Configuring PIR Alarm Settings

● Emergency Alarm

Purpose:

You can press the Emergency button on the remote control to trigger the Emergency Alarm in case of an emergency.

Note: The remote control is required for the Emergency Alarm. Go to

Configuration > Advanced Configuration> System> Remote Control to study the remote control first.

Steps:

1. Enter the Emergency Alarm Settings interface:

Configuration > Advanced Configuration> Basic Event> Other Alarm

2. Check the checkbox to select the linkage methods taken for the Emergency alarm.
3. Click **Save** to save the settings.

Emergency Alarm	
Normal Linkage ☒ Audible Warning ☒ Notify Surveillance Center ☒ Send Email ☒ Upload to FTP ☒ Trigger Channel	Other Linkage Trigger Alarm Output ☐ Select All ☐ A->1 Trigger Wireless Alarm ☐ Wireless audible and visual alarm

Figure 6-53 Configuring Emergency Alarm Settings

6.6.7 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> Advanced Configuration> Smart Event> 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 the **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.
- 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.
- 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.
 - Click the **Edit** button to set the arming schedule.
 - Select the linkage methods for line crossing detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
 - Click **Save** to save the settings.

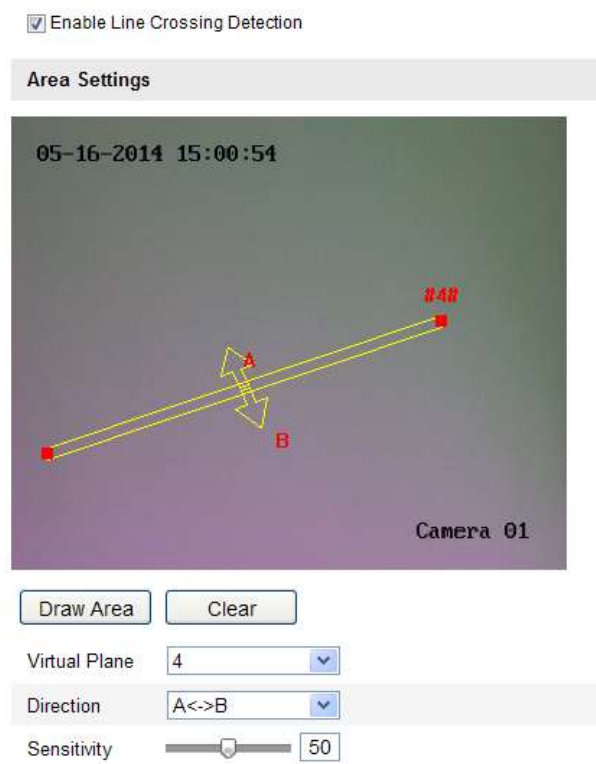


Figure 6-54 Draw Crossing Line

6.6.8 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> Advanced Configuration> Smart Event> 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 the **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 the **Edit** button to set the arming schedule.
9. 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.



Figure 6-55 Configuring Intrusion Area

Chapter 7 Storage Settings

Before you start:

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

7.1 Configuring NAS Settings

Before you start:

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

Steps:

1. Add the network disk

(1) Enter the NAS (Network-Attached Storage) Settings interface:

Configuration > Advanced Configuration > Storage > NAS

HDD No.	Type	Server Address	File Path
1	NAS	172.6.21.99	/dvr/test01
2	NAS		
3	NAS		
4	NAS		
5	NAS		
6	NAS		
7	NAS		
8	NAS		

Mounting Type: NFS SMB/CIFS User Name: Password:

Save

Figure 7-1 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 *User Manual of NAS* 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 (**Advanced Configuration > Storage > Storage Management**), in which you can view the capacity, free space, status, type and property of the disk.

HDD No.	Capacity	Free space	Status	Type	Property	Progress
g	20.00GB	0.00GB	Uninitialized	NAS	R/W	

Quota

Max. Picture Capacity	0.00GB
Free Size for Picture	0GB
Max. Record Capacity	0.00GB
Free Size for Record	0GB
Percentage of Picture	25%
Percentage of Record	75%

Figure 7-2 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**.

HDD Device List							Format
☐	HDD No.	Capacity	Free space	Status	Type	Property	Progress
☐	9	20.00GB	19.75GB	Normal	NAS	R/W	

Figure 7-3 View Disk Status

3. Define the quota for record and pictures.
 - (1) Input the quota percentage for picture and for record.
 - (2) Click **Save** and refresh the browser page to activate the settings.

Quota	
Max. Picture Capacity	4.94GB
Free Size for Picture	4.94GB
Max. Record Capacity	14.81GB
Free Size for Record	14.81GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 7-4 Quota Settings

Notes:

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

7.2 Configuring Recording Schedule

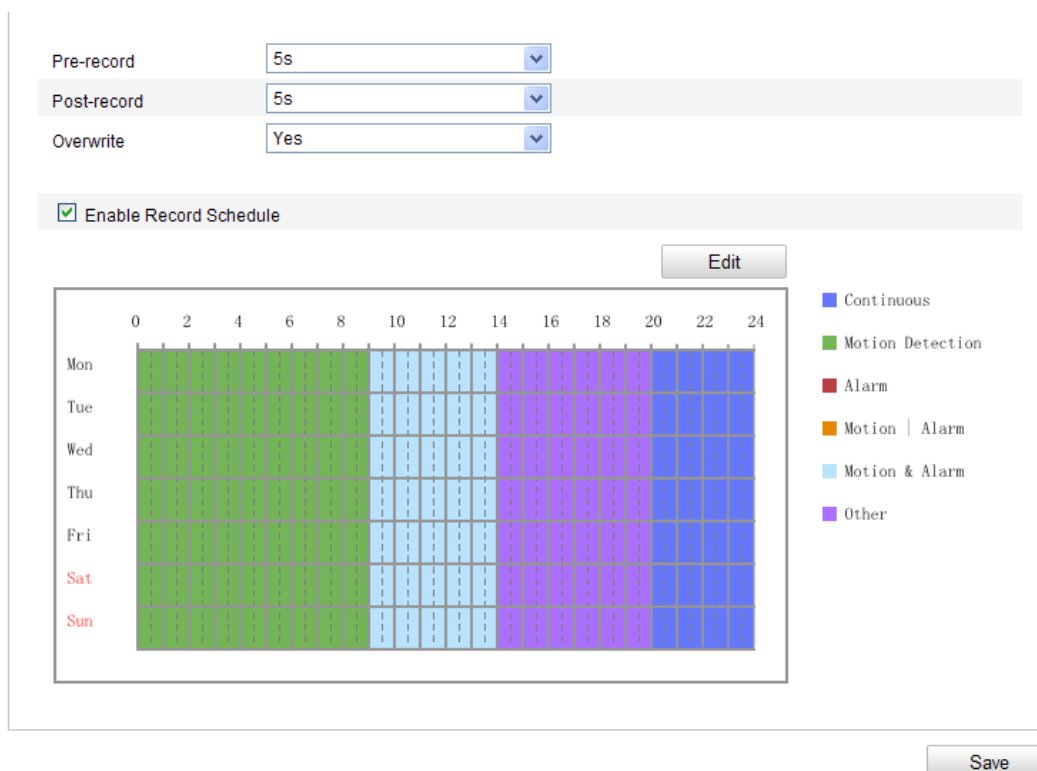
Purpose:

There are two kinds of recording for the cameras: manual recording and scheduled recording. For the manual recording, refer to *Section 5.3 Recording and Capturing Pictures Manually*. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the SD card (if supported) or in the network disk.

Steps:

1. Enter the Record Schedule Settings interface:

Configuration > Advanced Configuration> Storage > Record Schedule

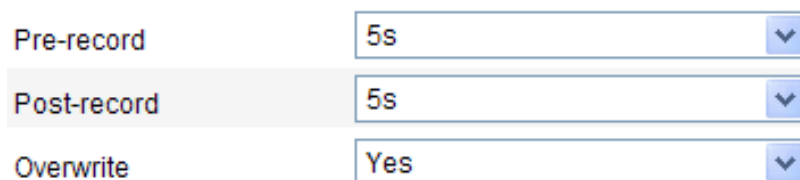


The interface shows recording schedule settings. At the top, there are three dropdown menus: 'Pre-record' set to '5s', 'Post-record' set to '5s', and 'Overwrite' set to 'Yes'. Below these is a checkbox labeled 'Enable Record Schedule' which is checked. To the right of the checkbox is an 'Edit' button. The main part of the interface is a grid representing a 24-hour cycle for each day of the week (Mon-Sun). The grid is divided into 2-hour segments. A legend on the right indicates the recording modes: Continuous (blue), Motion Detection (green), Alarm (red), Motion | Alarm (orange), Motion & Alarm (light blue), and Other (purple). The grid shows that from 0 to 8 hours, Motion Detection is active. From 8 to 10 hours, Motion & Alarm is active. From 10 to 12 hours, Motion Detection is active. From 12 to 14 hours, Motion & Alarm is active. From 14 to 16 hours, Other is active. From 16 to 18 hours, Other is active. From 18 to 20 hours, Other is active. From 20 to 22 hours, Continuous is active. From 22 to 24 hours, Continuous is active.

Save

Figure 7-5 Recording Schedule Interface

2. Check the checkbox of **Enable Record Schedule** to enable scheduled recording.
3. Set the record parameters of the camera.



The interface shows record parameters settings. There are three dropdown menus: 'Pre-record' set to '5s', 'Post-record' set to '5s', and 'Overwrite' set to 'Yes'.

Figure 7-6 Record Parameters

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

The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.

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

4. Click **Edit** to edit the record schedule.

Edit Schedule

Mon Tue Wed Thu Fri Sat Sun

☐ All Day

☒ Customize

Period	Start Time	End Time	Record Type
1	00:00	00:00	Continuous
2	00:00	00:00	Continuous
3	00:00	00:00	Continuous
4	00:00	00:00	Continuous
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Copy to Week ☐ Select All

☒ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

Figure 7-7 Record Schedule

5. Choose the day to set the record schedule.

- (1) Set all-day record or segment record:

- ◆ If you want to configure the all-day recording, please check the **All Day** checkbox.
- ◆ If you want to record in different time sections, check the **Customize** checkbox. Set the **Start Time** and **End Time**.

Note: The time of each segment can't be overlapped. Up to 4 segments can be configured.

- (2) Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, PIR Alarm, Wireless Alarm, Emergency Alarm, or Motion | Alarm Input | PIR | Wireless | Emergency.

- ◆ **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 *Step 1 Set the Motion Detection Area in the Section 6.6.1*.

◆ **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 6.6.3*.

◆ **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 6.6.1* and *Section 6.6.3* for detailed information.

◆ **Record Triggered by Motion | Alarm**

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

Besides configuring the recording schedule, you have to configure the settings on the **Motion Detection** and **Alarm Input Settings** interfaces. Please refer to *Section 6.6.1* and *Section 6.6.3* for detailed information.

Edit Schedule

Mon Tue Wed Thu Fri Sat Sun

☐ All Day

☒ Customize

Period	Start Time	End Time	Record Type
1	00:00	09:00	Motion Detection
2	09:00	14:00	Motion & Alarm
3	14:00	20:00	Scene Change I
4	20:00	24:00	Continuous
5	00:00	00:00	Continuous
6	00:00	00:00	Continuous
7	00:00	00:00	Continuous
8	00:00	00:00	Continuous

Copy to Week ☒ Select All

☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Figure 7-8 Edit Record Schedule

- (3) Check the checkbox of **Select All** and click **Copy** to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click **Copy**.
- (4) Click **OK** to save the settings and exit the **Edit Record Schedule** interface.
6. Click **Save** to save the settings.

7.3 Configuring Snapshot Settings

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. The captured picture can be stored in the SD card (if supported) or the netHDD (For detailed information about netHDD, please refer to *Section 7.1 Configuring NAS Settings*). You can also upload the captured pictures to a FTP server.

Basic Settings

Steps:

1. Enter the Snapshot Settings interface:

Configuration > Advanced Configuration > Storage > Snapshot

2. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot.

Check the **Enable Event-triggered Snapshot** checkbox to check event-triggered snapshot.

3. Select the quality of the snapshot.
4. Set the time interval between two snapshots.
5. Click **Save** to save the settings.

Uploading to FTP

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

- Upload continuous snapshots to FTP

Steps:

- 1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Please refer to *Section 6.3.12 Configuring FTP Settings* for more details to configure FTP parameters.
- 2) Check the **Enable Timing Snapshot** checkbox.

- Upload event-triggered snapshots to FTP

Steps:

- 1) Configure the FTP settings and check **Upload Picture** checkbox in FTP Settings interface. Please refer to *Section 6.3.12 Configuring FTP Settings* for more details to configure FTP parameters.
- 2) Check **Upload Picture** checkbox in Motion Detection Settings or Alarm Input interface. Please refer to *Step 3 Set the Alarm Actions Taken for Motion Detection* in *Section 6.6.1*, or *Step 4 Configuring External Alarm Input* in *Section 6.6.4*.
- 3) Check the **Enable Event-triggered Snapshot** checkbox.

The screenshot displays the 'Snapshot Settings' interface, which is divided into two main sections: 'Timing' and 'Event-Triggered'. Both sections have a 'Save' button at the bottom right.

Timing Section:

- ☒ Enable Timing Snapshot
- Format: JPEG (dropdown)
- Resolution: 1920*1080 (dropdown)
- Quality: High (dropdown)
- Interval: 0 (input field) and millisecond (dropdown)

Event-Triggered Section:

- ☒ Enable Event-Triggered Snapshot
- Format: JPEG (dropdown)
- Resolution: 1920*1080 (dropdown)
- Quality: High (dropdown)
- Interval: 0 (input field) and millisecond (dropdown)
- Capture Number: 4 (input field)

Figure 7-9 Snapshot Settings

7.4 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.

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 > Advanced Configuration > Storage > Lite Storage.**

Figure 7-10 Lite Storage Settings

2. Check the Checkbox of **Enable** to enable the lite storage function.
3. Select the level of lite storage. The level refers to the sensitivity of the linked motion detection. Low, medium, and high are selectable. The higher level asks for more bitrate and higher frames, which leads to higher storage pressure and less storage days.
4. Input the storage time in the text field. You can refer to the recommend storage time from the page. It is calculated by the available SD card space and the motion detection level.
5. Click **Save** to save the settings.

Chapter 8 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.

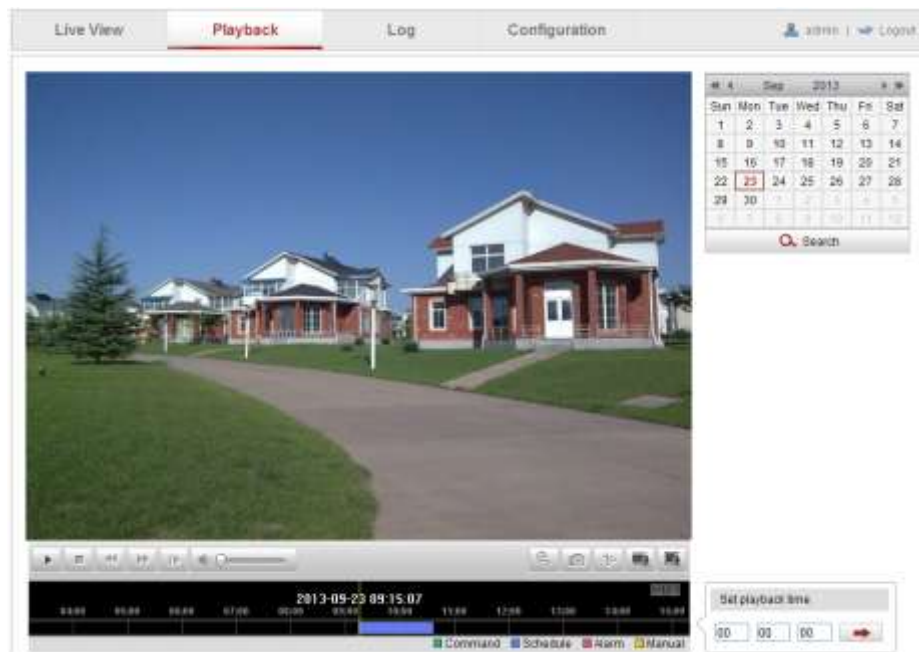


Figure 8-1 Playback Interface

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

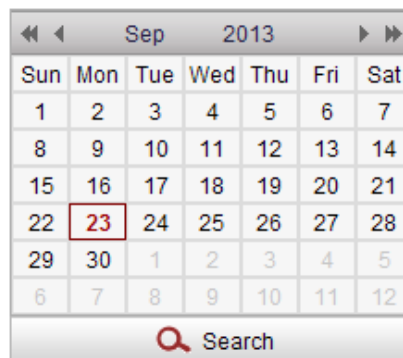


Figure 8-2 Search Video

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 8-3 Playback Toolbar

Table 8-1 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 video files
	Speed up		Download captured pictures
	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. Please refer to *Section 6.1* for details.

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

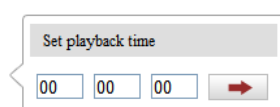


Figure 8-4 Set Playback Time

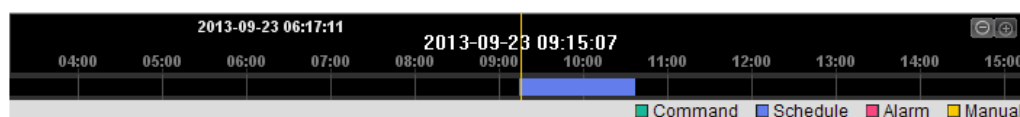


Figure 8-5 Progress Bar

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

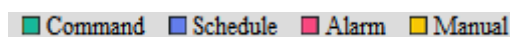


Figure 8-6 Video Types

Chapter 9 Log Searching

Purpose:

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

Before you start:

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

Steps:

1. Click **Log** on the menu bar to enter log searching interface.

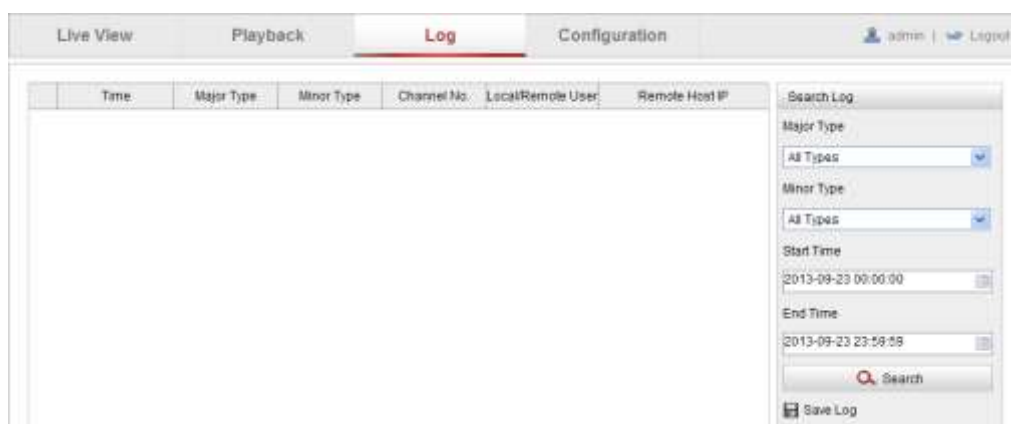


Figure 9-1 Log Searching Interface

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** interface.

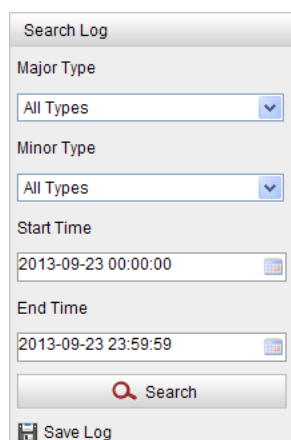


Figure 9-2 Log Searching

4. To export the log files, click **Save log** to save the log files in your computer.

Chapter 10 Others

10.1 Managing User Accounts

Enter the User Management interface:

Configuration > Basic Configuration > Security > User

Or **Configuration > Advanced Configuration > Security > User**



The screenshot shows a web interface for user management. At the top, there are tabs: 'User' (selected), 'Authentication', 'Anonymous Visit', 'IP Address Filter', and 'Security Service'. Below the tabs are three buttons: 'Add', 'Modify', and 'Delete'. A table displays the following user information:

No.	User Name	Level
1	admin	Administrator
2	Test	Operator

Figure 10-1 User Information

- **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.
- Different level user owns different permissions. Operator and user are selectable.



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

Add user

User Name: user1

Level: Operator

Password: ✓

Confirm:

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

Basic Permission	Camera Configuration
☐ Remote: Parameters Settings	☒ Remote: Live View
☒ Remote: Log Search / Interrogate Working Status	☒ Remote: PTZ Control
☐ Remote: Upgrade / Format	☒ Remote: Manual Record
☒ Remote: Two-way Audio	☒ Remote: Playback
☐ Remote: Shutdown / Reboot	
☐ Remote: Notify Surveillance Center / Trigger Alarm Output	
☐ Remote: Video Output Control	
☐ Remote: Serial Port Control	

OK Cancel

Figure 10-2 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** or **Password**.
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions.
4. Click **OK** to finish the user modification.

Modify user

User Name: test1

Level: Operator

Password: •••••

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

Confirm: •••••

Basic Permission	Camera Configuration
☐ Remote: Parameters Settings	☒ Remote: Live View
☒ Remote: Log Search / Interrogate Working Status	☒ Remote: PTZ Control
☐ Remote: Upgrade / Format	☒ Remote: Manual Record
☒ Remote: Two-way Audio	☒ Remote: Playback
☐ Remote: Shutdown / Reboot	
☐ Remote: Notify Surveillance Center / Trigger Alarm Output	
☐ Remote: Video Output Control	
☐ Remote: Serial Port Control	

OK Cancel

Figure 10-3 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 delete the user.

10.2 Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the Authentication interface: Configuration> Advanced Configuration> Security > Authentication

User Authentication Anonymous Visit IP Address Filter Security Service

RTSP Authentication basic

Save

Figure 10-4 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.

10.3 Anonymous Visit

Enabling this function allows visit for whom doesn't have the user name and password of the device.

Note: Only live view is available for the anonymous user.

Steps:

1. Enter the Anonymous Visit interface:

Configuration > Advanced Configuration > Security > Anonymous Visit

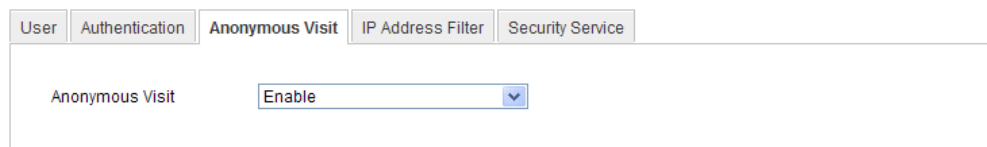


Figure 10-5 Anonymous Visit

2. Set the **Anonymous Visit** permission **Enable** or **Disable** in the drop-down list to enable or disable the anonymous visit.
3. Click **Save** to save the settings.

There will be a checkbox of Anonymous by the next time you logging in.

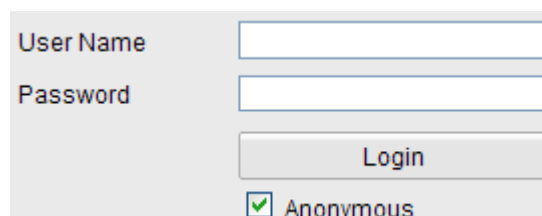


Figure 10-6 Login Interface with an Anonymous Checkbox

4. Check the checkbox of **Anonymous** and click **Login**.

By permitting the Anonymous “Live View” function, you may enable others to access your camera and view live images without providing login credentials. It therefore is

critical when permitting the Anonymous "Live View" function to ensure that your camera's field of view does not impact the privacy of individuals whose images might be captured without authorization.

Given its inherent intrusiveness, video surveillance is inappropriate in areas where people have a higher expectation of privacy.

10.4 IP Address Filter

Purpose:

This function makes it possible for access control.

Steps:

1. Enter the IP Address Filter interface:

Configuration > Advanced Configuration > Security > IP Address Filter

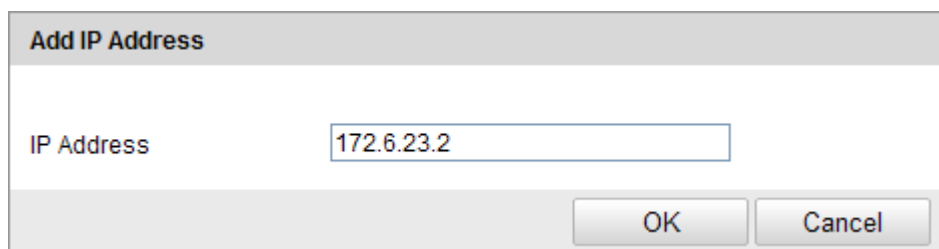
No.	IP
1	172.6.23.2

Figure 10-7 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 Address.



The dialog box has a title bar 'Add IP Address'. Below it is a label 'IP Address' followed by a text input field containing '172.6.23.2'. At the bottom right are two buttons: 'OK' and 'Cancel'.

Figure 10-8 Add an IP

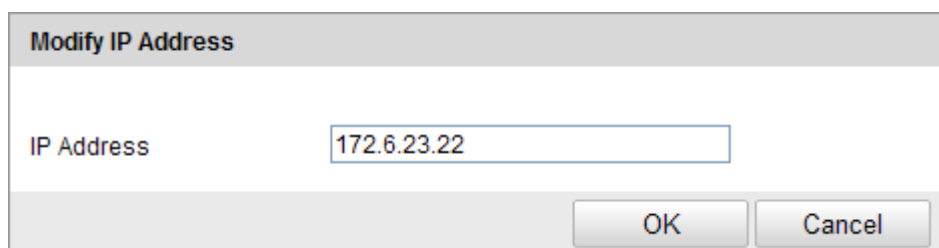
(3) Click the **OK** to finish adding.

- 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.



The dialog box has a title bar 'Modify IP Address'. Below it is a label 'IP Address' followed by a text input field containing '172.6.23.22'. At the bottom right are two buttons: 'OK' and 'Cancel'.

Figure 10-9 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.

10.5 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. Go to **Configuration > Advanced configuration > Security > Security Service** to enter the security service configuration interface.

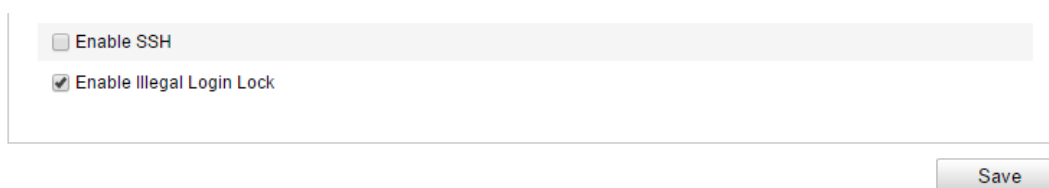


Figure 10-10 Security Service

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.

10.6 Viewing Device Information

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

In the **Device Information** interface, you can edit the Device Name.

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.

Device Information	Time Settings	Maintenance	RS232	RS485	DST	Service
Basic Information						
Device Name	IP CAMERA					
Device No.	88					
Model	XX-XXXXXXXX					
Serial No.	XXXXXXXXXXXXXXXXXXXX					
Firmware Version	XXXXXXXXXX					
Encoding Version	XXXXXXXXXX					
Number of Channels	1					
Number of HDDs	1					
Number of Alarm Input	1					
Number of Alarm Output	1					

Figure 10-11 Device Information

10.7 Maintenance

10.7.1 Rebooting the Camera

Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration > System > Maintenance

Or **Configuration > Advanced Configuration > System > Maintenance:**

2. Click **Reboot** to reboot the network camera.

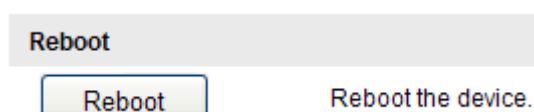


Figure 10-12 Reboot the Device

10.7.2 Restoring Default Settings

Steps:

1. Enter the Maintenance interface:

Configuration > Basic Configuration > System > Maintenance

Or **Configuration > Advanced Configuration > System > Maintenance**

- Click **Restore** or **Default** to restore the default settings.

Default	
Restore	Reset all the parameters, except the IP parameters and user information, to the default settings.
Default	Restore all parameters to default settings.

Figure 10-13 Restore Default Settings

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

10.7.3 Exporting / Importing Configuration File

Purpose:

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:

- Enter the Maintenance interface: Configuration > Basic Configuration> System > Maintenance, or Configuration>Advanced Configuration> System > Maintenance
- Click **Export** to export the current configuration file, and save it to the certain place.
- 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.

- Click **Export** and set the saving path to save the configuration file in local storage.

Import Config. File	
Config File	F:\12
Status	
Browse Import	

Export Config. File	
Export	

Figure 10-14 Import/Export Configuration File

10.7.4 Upgrading the System

Steps:

1. Enter the Maintenance interface: Configuration > Basic Configuration> System > Maintenance , or Configuration > Advanced Configuration> System > Maintenance
2. 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.
3. Click **Browse** to select the local upgrade file and then click **Upgrade** to start remote upgrade.



Figure 10-15 Remote Upgrade

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

10.8 RS-232 Settings

The RS-232 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 RS-232 Port Setting interface:

Configuration> Advanced Configuration> System > RS232

Device Information	Time Settings	Maintenance	RS232	RS485	DST	Service
Baud Rate	115200 bps					
Data Bit	8					
Stop Bit	1					
Parity	None					
Flow Ctrl	None					
Usage	Console					

Figure 10-16 RS-232 Settings

Note: If you want to connect the camera by the RS-232 port, the parameters of the RS-232 should be exactly the same with the parameters you configured here.

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

10.9 RS-485 Settings

Purpose:

The RS-485 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:

- Enter RS-485 Port Setting interface:

Configuration> Advanced Configuration> System > RS485

Device Information	Time Settings	Maintenance	RS232	RS485	DST	Service
Baud Rate	9600 bps					
Data Bit	8					
Stop Bit	1					
Parity	None					
Flow Ctrl	None					
PTZ Protocol	PELCO-D					
PTZ Address	0					

Figure 10-17 RS-485 Settings

- Set the RS-485 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.

10.10 Service Settings

Go to **Configuration> Advanced Configuration> System > Service** to enter the service settings interface.

Service settings refer to the hardware service the camera supports, and it varies according to the different cameras.

For the cameras support IR LED, ABF (Auto Back Focus), Auto Defog, or Status LED, you can go to the hardware service, and select to enable or disable the corresponding service according to the actual demands.

Appendix

Appendix 1 SADP Software Introduction

● Description of SADP

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

● Search active devices online

◆ Search online devices automatically

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

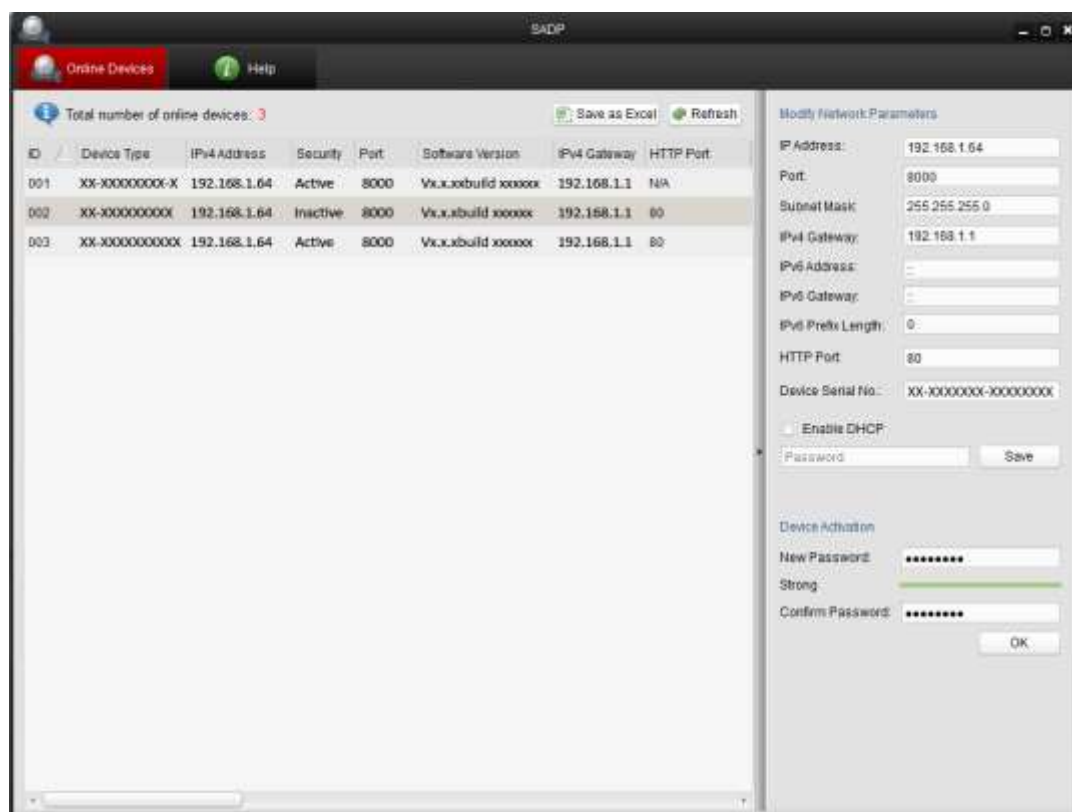
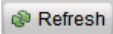


Figure A.1.1 Searching Online Devices

Note:

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

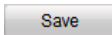
◆ Search online devices manually

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



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

● Modify network parameters**Steps:**

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



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

Modify Network Parameters

IP Address:	192.168.1.64
Port:	8000
Subnet Mask:	255.255.255.0
IPv4 Gateway:	192.168.1.1
IPv6 Address:	::
IPv6 Gateway:	::
IPv6 Prefix Length:	0
HTTP Port:	80
Device Serial No.:	XX-XXXXXXX-XXXXXXX

☐ Enable DHCP

Password

Figure A.1.2 Modify Network Parameters

Appendix 2 Port Mapping

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

Steps:

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

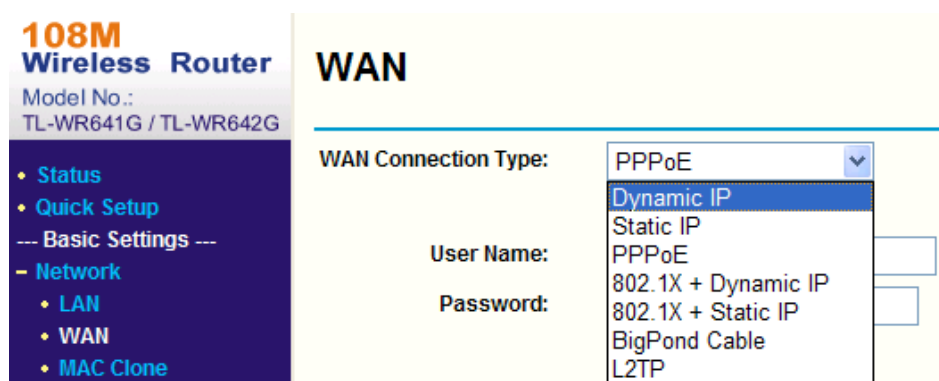


Figure A.2.1 Select the WAN Connection Type

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

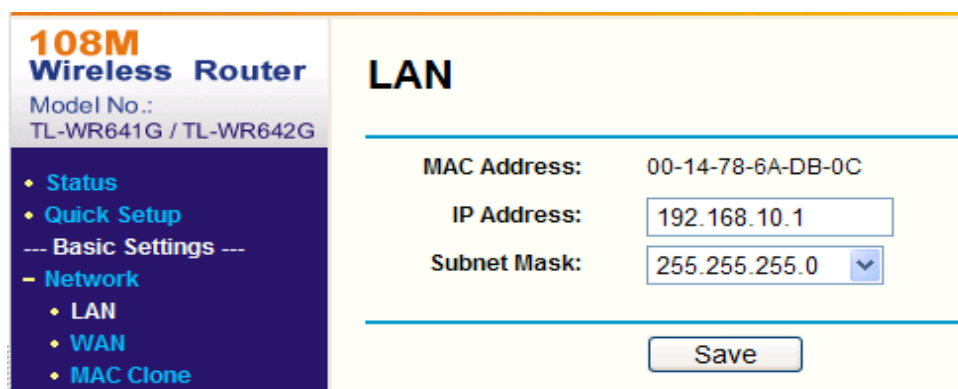


Figure A.2.2 Set the LAN parameters

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

Example:

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

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

Steps:

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

108M Wireless Router
Model No.:
TL-WR641G / TL-WR642G

- Status
- Quick Setup
- Basic Settings ---
- + Network
- Wireless
- Advanced Settings ---
- + DHCP
- Forwarding
 - Virtual Servers
 - Port Triggering
 - DMZ
 - UPnP
- + Security
 - Static Routing
 - Dynamic DNS
- Maintenance ---
- + System Tools

Virtual Servers

ID	Service Port	IP Address	Protocol	Enable
1	80	192.168.10.23	ALL	☒
2	8000	192.168.10.23	ALL	☒
3	554	192.168.10.23	ALL	☒
4	8200	192.168.10.23	ALL	☒
5	81	192.168.10.24	ALL	☒
6	8001	192.168.10.24	ALL	☒
7	555	192.168.10.24	ALL	☒
8	8201	192.168.10.24	ALL	☒

Common Service Port: DNS(53) Copy to ID 1

Previous Next Clear All Save

Figure A.2.3 Port Mapping

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