



ALL-CAM2372-WP

**2 Megapixel Indoor Full HD PTZ
Mini-Dome IP Camera**



User Manual

Default-IP
via DHCP
Username & Password:
admin

User Manual

About this Manual

This Manual is applicable to Network Mini PTZ Camera.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website.

Please use this user manual under the guidance of professionals.

Legal Disclaimer

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. The power consumption cannot be less than the required value.
- Do not connect several devices to one power adapter as an adapter overload may cause over-heating and can be a fire hazard.
- When the product is installed on a wall or ceiling, the device should be firmly fixed.
- To reduce the risk of fire or electrical shock, do not expose the indoor used 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.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the product yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)



Cautions:

- Make sure the power supply voltage is correct before using the product.
- Do not drop the product or subject it to physical shock. Do not install the product on vibratory surface or places.
- Do not expose it to high electromagnetic radiating environment.
- Do not aim the lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the product.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- For working temperature, please refer to the specification manual for details.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- While shipping, the product should be packed in its original packing.
- Please use the provided glove when open up the product cover. Do not touch the product cover with fingers directly, because the acidic sweat of the fingers may erode the surface coating of the product cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the product cover. Do not use alkaline detergents.
- Improper use or replacement of the battery may result in hazard of explosion. Please use the manufacturer recommended battery type.
- **Please use only the power supply unit that is delivered with the device!**

Table of Contents

Chapter 1 Overview	9
1.1 System Requirement	9
1.2 Functions.....	9
Chapter 2 Network Connection.....	12
2.1 Setting the Network PTZ Camera over the LAN	12
2.1.1 Wiring over the LAN	12
2.1.2 Activating the Speed Dome.....	13
2.2 Setting the Network PTZ Camera over the WAN	15
2.2.1 Static IP Connection	15
2.2.2 Dynamic IP Connection	16
Chapter 3 Access to the Network PTZ Camera.....	19
3.1 Accessing by Web Browsers.....	19
3.2 Accessing by Client Software	21
Chapter 4 Wi-Fi Settings	24
4.1 Configuring Wi-Fi Connection in Manage and Ad-hoc Modes	24
4.2 Easy Wi-Fi Connection with WPS function	28
4.3 IP Property Settings for Wireless Network Connection.....	30
Chapter 5 Live View	31
5.1 Power-up Action	31
5.2 Live View Page	31
5.3 Starting Live View	32
5.4 Recording and Capturing Pictures Manually	33
5.5 Operating PTZ Control.....	34
5.5.1 PTZ Control Panel.....	34
5.5.2 Setting / Calling a Preset.....	34
5.6 Configuring Live View Parameters	36
Chapter 6 PTZ Configuration.....	37
6.1 Configuring Initial Position	37
6.2 Configuring Basic PTZ Parameters	38
6.3 Configuring PTZ Limit Stops.....	39
6.4 Configuring Scheduled Tasks	40
6.5 Configuring Park Actions	42
6.6 Configuring Privacy Mask.....	43
6.7 Configuring PTZ Control Priority	44
6.8 Clearing PTZ Configurations	44

Chapter 7 PTZ Camera Configuration	45
7.1 Configuring Local Parameters.....	45
7.2 Configuring Time Settings.....	46
7.3 Configuring Network Settings	49
7.3.1 Configuring TCP/IP Settings.....	49
7.3.2 Configuring Port Settings	51
7.3.3 Configuring PPPoE Settings.....	51
7.3.4 Configuring DDNS Settings	52
7.3.5 Configuring SNMP Settings	54
7.3.6 Configuring QoS Settings	56
7.3.7 Configuring FTP Settings	56
7.3.8 Configuring UPnP™ Settings.....	58
7.3.9 Configuring NAT (Network Address Translation) Settings.....	59
7.3.10 Configuring Email Settings.....	59
7.3.11 Configuring HTTPS Settings.....	61
7.3.12 Configuring Platform Access Settings.....	63
7.4 Configuring Video and Audio Settings	64
7.4.1 Configuring Video Settings	64
7.4.2 Configuring Audio Settings.....	65
7.4.3 Configuring ROI Settings.....	66
7.5 Configuring Image Settings	67
7.5.1 Configuring Display Settings.....	67
7.5.2 Configuring OSD Settings.....	72
7.5.3 Configuring Text Overlay Settings	74
7.6 Configuring and Handling Alarms.....	74
7.6.1 Configuring Motion Detection.....	75
7.6.2 Configuring Video Tampering Alarm	79
7.6.3 Configuring External Alarm Input	80
7.6.4 Configuring Alarm Output.....	81
7.6.5 Handling Exception	82
7.6.6 Detecting Audio Exception.....	83
7.6.7 Configuring Dual-VCA	84
7.6.8 Configuring Intrusion Detection.....	84
7.6.9 Configuring Line Crossing Detection.....	86
Chapter 8 Record Settings	89
8.1 Configuring NAS Settings.....	89
8.2 Initializing and Configuring Storage.....	90
8.3 Configuring Recording Schedule	91
8.4 Configuring Snapshot Settings	95
Chapter 9 Playback.....	98

Chapter 10 Log Searching.....	102
Chapter 11 Others	103
11.1 Managing User Accounts.....	103
11.1.1 Add a User.....	103
11.1.2 Modify a User.....	104
11.1.3 Delete a User.....	105
11.2 Configuring RTSP Authentication.....	105
11.3 Configuring Anonymous Visit	106
11.4 Configuring IP Address Filter	107
11.5 Configuring Security Service Settings.....	107
11.6 Viewing Device Information	107
11.7 Maintenance.....	108
11.7.4 Rebooting the PTZ camera	108
11.7.5 Restoring Default Settings.....	109
11.7.6 Importing/Exporting Configuration File	109
11.7.7 Upgrading the System.....	110
11.8 Configuring RS-485	111
11.9 Configuring Remote Connection	111
Appendix.....	112
Appendix 1 SADP Software Introduction	112
Appendix 2 Port Mapping	115
Appendix 3 Bubble Maintenance.....	117
Appendix 4 12VDC Wire Gauge & Transmission Distance	118
Appendix 5 Table of Wire Gauge Standards	118
Appendix 6 Alarm In/Out Connections	120

Chapter 1 Overview

1.1 System Requirement

System requirement of web browser accessing is as follows:

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

CPU: Intel Pentium IV 3.0 GHz or higher

RAM: 1G or higher

Display: 1024×768 resolution or higher

Web Browser: Internet Explorer 8.0 and above version, Apple Safari 5.02 and above version, Mozilla Firefox 5 and above version and Google Chrome 18 and above versions.

1.2 Functions



The functions vary depending on the models of PTZ camera.

- **Limit Stops**

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

- **Preset Freezing**

This feature freezes the scene on the monitor when the PTZ camera is moving to a preset. This allows for smooth transition from one preset scene to another. It also guarantees that masked area will not be revealed when the PTZ camera is moving to a preset.

- **Presets**

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

- **Label Display**

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

- **Privacy Mask**

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

- **3D Positioning**

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

- **Proportional Pan/Tilt**

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

- **Auto Focus**

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

- **Day/Night Auto Switch**

The PTZ camera delivers color images during the day. And as light diminishes at night, the PTZ camera switches to night mode and deliver black and white images with high quality.

- **Slow Shutter**

In slow shutter mode, the shutter speed will automatically slow down in low illumination conditions to maintain clear video images by extending the exposure time. The feature can be enabled or disabled.

- **Backlight Compensation (BLC)**

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

- **Wide Dynamic Range (WDR)**

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



This feature varies depending on PTZ camera models.

- **White Balance (WB)**

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

- **Power Off Memory**

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

- **Time Task**

A time task is a preconfigured action that can be performed automatically at a specific date and time. The programmable actions include: preset 1-8, day, night, reboot, PT adjust, Alarm output, etc.

- **Park Action**

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

- **User Management**

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

- **3D Digital Noise Reduction**

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

- **Dual-VCA**

Combine the detected moving objects into the video stream, which can be used for the second-time analysis on the back-end device.

Chapter 2 Network Connection



- You shall acknowledge that the use of the product with Internet access might be under network security risks. For avoidance of any network attacks and information leakage, 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 speed dome, we recommend you to have the speed dome assessed and maintained termly. You can contact us if you need such service.

Before you start:

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

2.1 Setting the Network PTZ Camera over the LAN

Purpose:

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



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 PTZ camera and a computer:

Purpose:

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

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

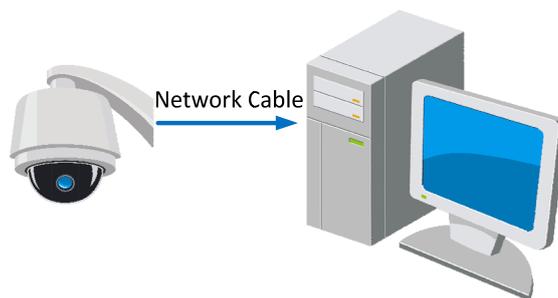


Figure 2-1 Connecting Directly

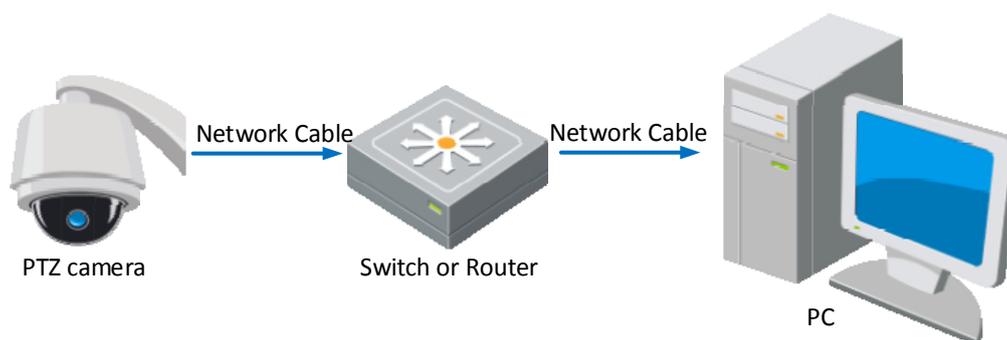


Figure 2-2 Connecting via a Switch or a Router

2.1.2 Activating the Speed Dome

Purpose:

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

Activation via Web Browser, Activation via SADP, and Activation via client software are supported. In the following sections, activation via web browser and SADP will be taken as examples. You may refer to the user manual of the speed dome for the details of activation via client software.

◆ **Activation via Web Browser**

Steps:

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



The default IP address will be assigned by DHCP. If no DHCP-Server is active you have to use the "SADP"-Tool to find out the ip address of the camera.



Figure 2-3 Activation Interface(Web)

3. Log in with the default username and password (admin/admin).



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

4. Click **LOGIN** to access the WEBUI.

2.2 Setting the Network PTZ Camera over the WAN

Purpose:

This section explains how to connect the network PTZ 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 PTZ camera via a router or connect it to the WAN directly.

• **Connecting the network PTZ camera via a router**

Steps:

1. Connect the network PTZ 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 PTZ camera.
3. Save the static IP in the router.
4. Set port mapping, E.g., 80, 8000 and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.



Refer to Appendix 2 for detailed information about port mapping.

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

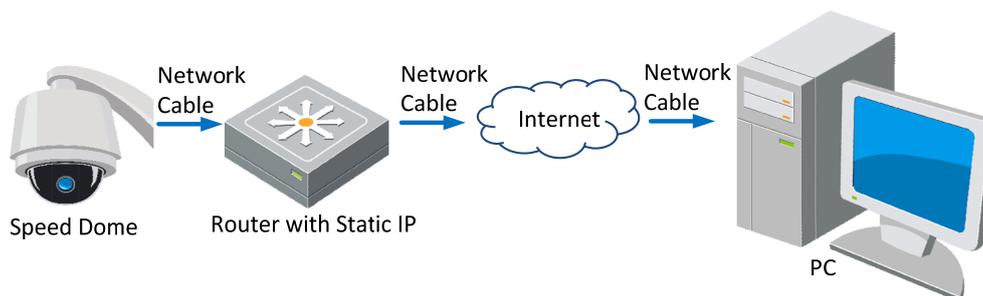


Figure 2-4 Accessing the PTZ Camera through Router with Static IP



• **Connecting the network PTZ camera with static IP directly**

You can also save the static IP in the PTZ 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 PTZ camera.

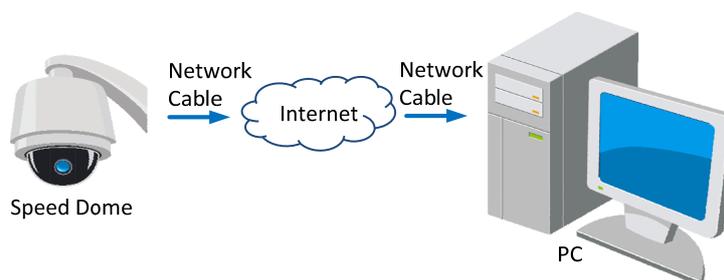


Figure 2-5 Accessing the PTZ Camera with Static IP Directly

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 PTZ camera to a modem or a router.

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

Steps:

1. Connect the network PTZ camera to the router.
2. In the PTZ camera, assign a LAN IP address, the subnet mask and the gateway. Refer to **Section 2.1.2** for detailed LAN configuration.
3. In the router, set the PPPoE user name, password and confirm the password.



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

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.



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 PTZ camera via the applied domain name.



• Connecting the network PTZ camera via a modem

Purpose:

This PTZ camera supports the PPPoE auto dial-up function. The PTZ camera gets a public IP address by ADSL dial-up after the PTZ camera is connected to a modem. You need to configure the PPPoE parameters of the network PTZ camera. Refer to **Section 7.3.3 Configuring PPPoE Settings** for detailed configuration.

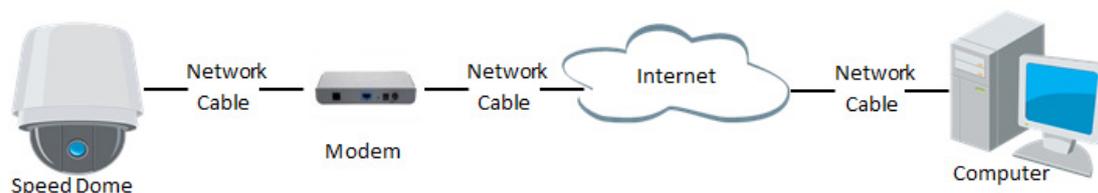


Figure 2-6 Accessing the PTZ Camera with Dynamic IP



The obtained IP address is dynamically assigned via PPPoE, so the IP address always changes after rebooting the PTZ 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 below steps for normal domain name resolution and private domain name resolution to solve the problem.

◆ Normal Domain Name Resolution

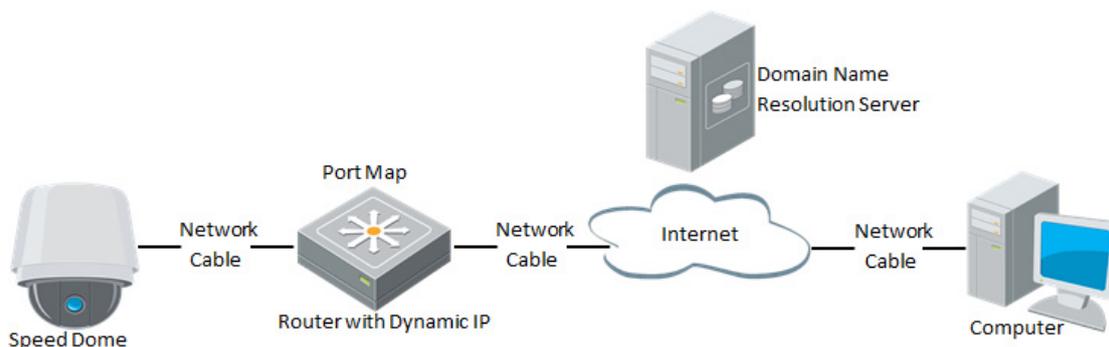


Figure 2-7 Normal Domain Name Resolution

Steps:

1. Apply a domain name from a domain name provider.
2. Configure the DDNS settings in the **DDNS Settings** interface of the network PTZ camera. Refer to **Section 7.3.4 Configuring DDNS Settings** for detailed configuration.
3. Visit the PTZ camera via the applied domain name.



◆ Private Domain Name Resolution

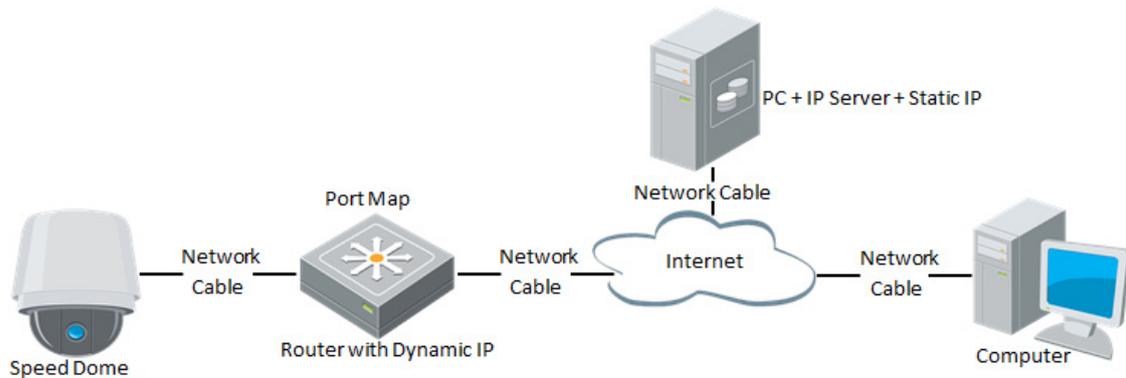


Figure 2-8 Private Domain Name Resolution

Steps:

1. Install and run the IP Server software in a computer with a static IP.
2. Access the network PTZ 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 7.3.4 Configuring DDNS Settings** for detailed configuration.



Chapter 3 Access to the Network PTZ Camera

3.1 Accessing by Web Browsers

Steps:

1. Open the web browser.
2. In the address field, input the IP address of the network PTZ camera and press the **Enter** key to enter the login interface.
3. Activate the speed dome for the first time using, refer to the section **2.1.2 Activating the Speed Dome**.
4. Select English as the interface language on the top-right of login interface.
5. Input the user name and password and click .

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



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



Figure 3-1 Login Interface

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

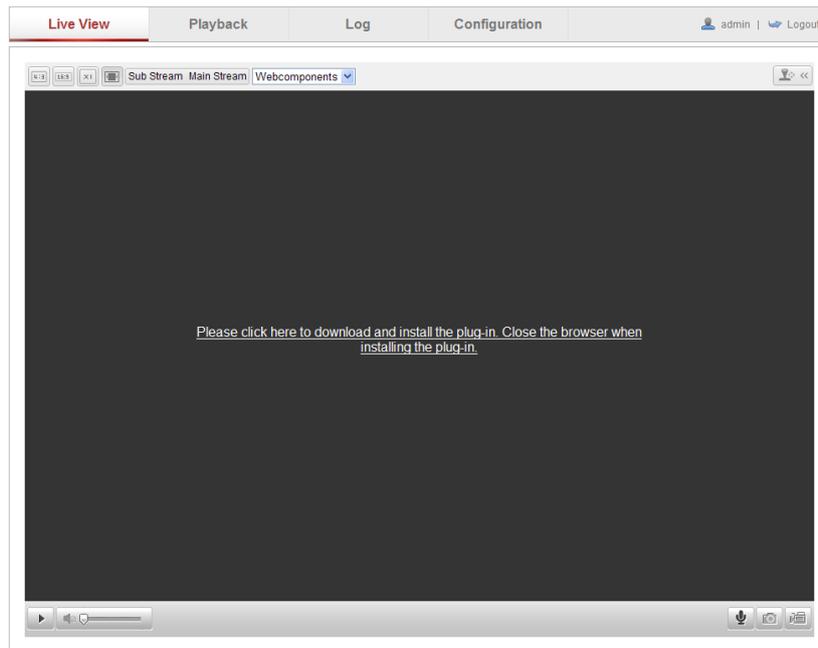


Figure 3-2 Download and Install Plug-in

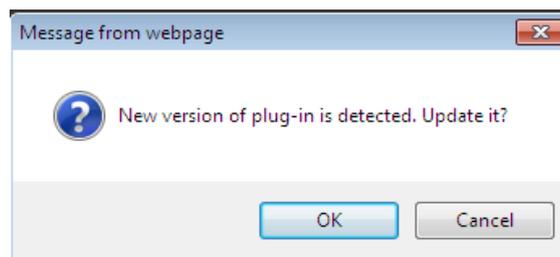


Figure 3-3 Install Plug-in (1)

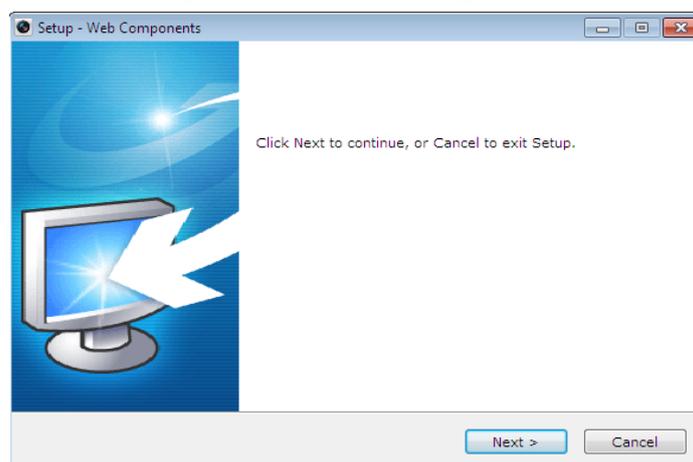


Figure 3-4 Install Plug-in (2)

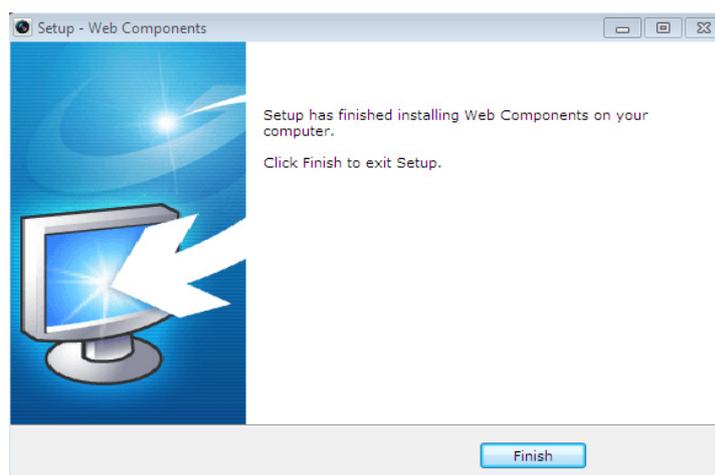


Figure 3-5 Install Plug-in (3)



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 client software. You can view the live video and manage the PTZ camera with the client software. Follow the installation prompts to install the client software and WinPcap. The configuration interface and live view interface of client software are shown below.

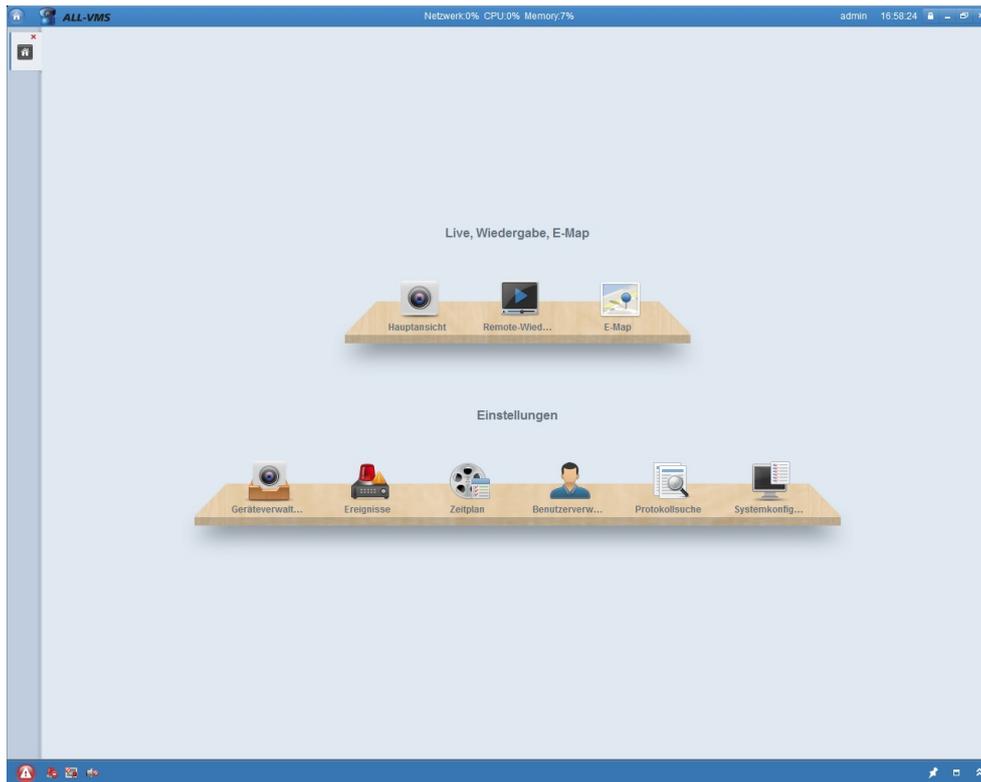


Figure 3-6 ALL-VMS Control Panel

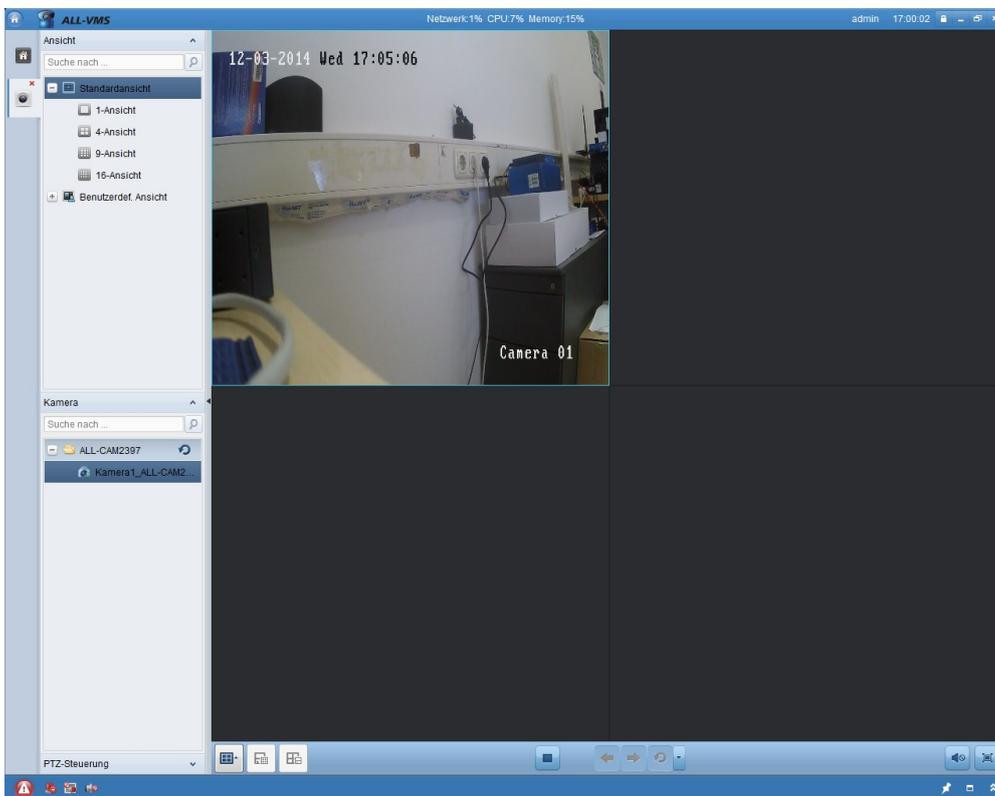


Figure 3-7 ALL-VMS Live View Interface



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

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.



This chapter is only applicable for the PTZ camera 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:

Network Mode: Manage Ad-Hoc

Security Mode:

Encryption Type:

Key 1

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 do not change it manually.



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 as the Network Mode.

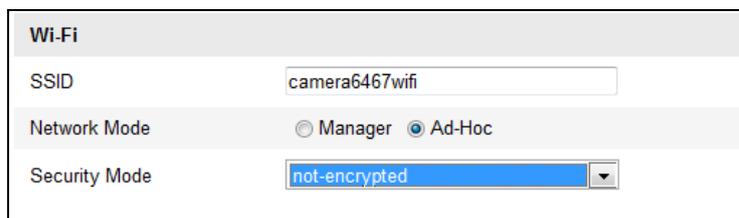


Figure 4-3 Wi-Fi Setting- Ad-hoc

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



Figure 4-4 Ad-hoc Connection Point

6. Choose the SSID and connect.

● **Security Mode Description:**



Figure 4-5 Security Mode

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

◆ WEP Mode:

Wi-Fi	
SSID	<input type="text" value="belkin54g"/>
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	<input type="text" value="WEP"/>
Authentication	<input checked="" type="radio"/> Open <input type="radio"/> Shared
Key Length	<input checked="" type="radio"/> 64bit <input type="radio"/> 128bit
Key Type	<input type="radio"/> HEX <input type="radio"/> ASCII
Key 1 <input checked="" type="radio"/>	<input type="text"/>
Key 2 <input type="radio"/>	<input type="text"/>
Key 3 <input type="radio"/>	<input type="text"/>
Key 4 <input type="radio"/>	<input type="text"/>

Figure 4-6 WEP Mode

- **Authentication:** Select Open or Shared Key System Authentication, depending on the method used by your access point. Not all access points have this option, in which case they probably use Open System, which is sometimes known as SSID Authentication.
- **Key length** - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key length can sometimes be shown as 40/64 and 104/128.
- **Key type** - The key types available depend on the access point being used. The following options are available:
HEX - Allows you to manually enter the hex key.
ASCII - In this method the string must be exactly 5 characters for 64-bit WEP and 13 characters for 128-bit WEP.

◆ WPA-personal and WPA2-personal Mode:

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

Wi-Fi	
SSID	<input type="text" value="belkin54g"/>
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	<input type="text" value="WPA-personal"/>
Encryption Type	<input type="text" value="TKIP"/>
Key 1 <input checked="" type="radio"/>	<input type="text"/>

Figure 4-7 Security Mode- WPA-personal

◆ WPA- enterprise and WPA2-enterprise Mode:

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

EAP-TLS:

Wi-Fi	
SSID	test
Network Mode	<input checked="" type="radio"/> Manager <input type="radio"/> Ad-Hoc
Security Mode	WPA-enterprise
Authentication	EAP-TLS
Identify	
Private key password	
EAPOL version	1
CA certificate	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>
User certificate	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>
Private key	<input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/>

Figure 4-8 EAP-TLS

- **Identity / User Name** - Enter the user ID to present to the network.
- **Private key password / 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

EAP-TTLS:

- **User Name** - Enter the user ID to present to the network.
- **Password** – Enter the password for your user ID.
- **Inner authentication** – Select the authentication mode as **PAP** or **MSCHAPv2**.
- **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 upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

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.



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

Steps:

Figure 4-9 Wi-Fi Settings - WPS

PBC Mode:

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

Steps:

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



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

3. Check on the Wi-Fi router to see if there is a WPS button. If yes push the button and you can see the indicator near the button start flashing, which means the WPS function of the router is enabled. For detailed operation, please see the user guide of the router.
4. Push the WPS button to enable the function on the camera. If there is not a WPS button on the camera, you can also click the virtual button to enable the PBC function on the web interface.
5. Click **Connect** button.



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

PIN Mode:

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

Steps:

1. Choose a wireless connection on the list and the SSID is shown.

 A screenshot of a web interface for WPS PIN Mode settings. It shows a 'WPS' section with a checked 'Enable WPS' checkbox. Below it is a 'PIN Code' field containing '70137231' and a 'Generate' button. There are two radio buttons: 'PBC connection' (unselected) and 'Use router PIN code' (selected). Each radio button has a 'Connect' button next to it. Below the radio buttons is an 'SSID' field containing 'AP' and a 'Router PIN code' field which is currently empty.

Figure 4-10 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	70137231	Generate
----------	----------	----------

2. Enter the code to the router, in the example, enter 70137231 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**

NIC Settings	
Select NIC	wlan
IPv4 Address	172.6.21.124
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	172.6.21.1
<input type="checkbox"/> DHCP	
Multicast Address	

Figure 4-11 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

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

5.1 Power-up Action

After the power is applied, the PTZ camera will perform self-test actions. It begins with lens actions and then pan and tilt movement.

5.2 Live View Page

Purpose:

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

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

Descriptions of the live view page:



Figure 5-1 Live View Page

Menu Bar:

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

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, focusing and zooming actions of the PTZ camera. The lighter, wiper, one-touch focus and lens initialization control.

Preset:

Set and call the preset for the PTZ camera.

Live View Parameters:

Configure the image size and stream type of the live video.

5.3 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 PTZ camera.



Figure 5-2 Start Live View

Table 5-1 Descriptions of the Toolbar

Icon	Description	Icon	Description
	Start/Stop Live view		Manually capture the pictures
	Manual recording off/on		Mute / Audio on and adjust volume
	Two-way audio off/on		3D positioning



- Not all the PTZ camera models support the above functions. Please take the browser interface of the actual product as standard.
- Before enabling the two-way audio or recording with audio functions, please set the **Stream Type** to **Video & Audio** referring

to Section **6.4.1 Configuring Video Settings**.

Full-screen Mode:

You can double-click on the live video to switch the current live view into full-screen or return to normal mode from the full-screen.

3D Positioning:

Steps:

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



Please refer to the following sections for more information:

- Configuring remote recording in **Section 8.3 Configuring Recording Schedule**.
- Setting the image quality of the live video in **Section 7.1 Configuring Local Parameters** and **Section 7.4.1 Configuring Video Settings**.
- Setting the OSD text on live video in **Section 7.5.2 Configuring OSD Settings**.

5.4 Recording and Capturing Pictures Manually

In the live view interface, click  on the toolbar to capture the live pictures and the The captured image will be saved as a JPEG file in your computer by default.

You can click  to record the live video.

The local saving paths of the captured pictures and clips can be set in the **Configuration > Local Configuration** interface, and the image format can also be edited in that interface.

To configure remote automatic recording, please refer to **Section 8.3**

Configuring Recording Schedule.

5.5 Operating PTZ Control

Purpose:

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

5.5.1 PTZ Control Panel

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

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

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



Figure 5-3 PTZ Control Panel

Table 5-2 Descriptions of PTZ Control Panel

Button	Description
	Zoom in/out
	Focus near/far
	Iris +/-
	Adjust speed of pan/tilt movements

5.5.2 Setting / Calling a Preset

Purpose:

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

● **Setting a Preset:**

Steps:

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

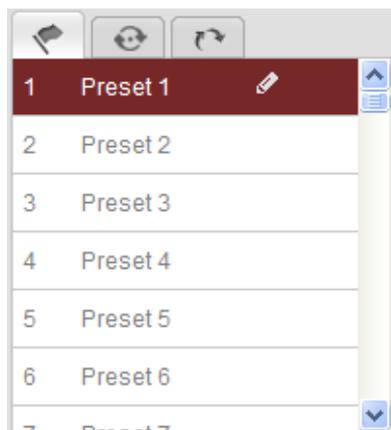


Figure 5-4 Setting a Preset

2. Use the PTZ control buttons to move the lens to the desired position.
 - Pan the PTZ camera to the right or left.
 - Tilt the PTZ 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.



You can configure up to 300 presets.



● Calling a Preset:

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

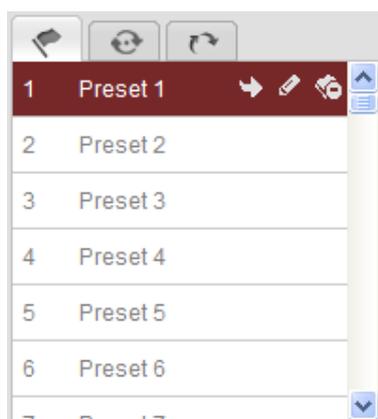


Figure 5-5 Calling a Preset

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

Steps:

1. Select any preset from the list.

2. Click the preset number you need on the keyboard.



The following presets are predefined with special commands. You can only call them but not configure them. For instance, preset 94 is the "Remote reboot". If you call the preset 94, the PTZ camera will reboot remotely.

Table 5-3 Special Presets

Special Preset	Function	Special Preset	Function
34	Back to initial position	92	Start to set limit stops
39	IR cut filter in	93	Set limit stops manually
40	IR cut filter out	94	Remote reboot

5.6 Configuring Live View Parameters

● Main stream/Sub-stream:

You can select or as the stream type of live viewing. The main stream is with a relatively high resolution and needs much bandwidth. The sub-stream is with a low resolution and needs less bandwidth. The default setting of stream type is .



Please refer to **Section 7.4.1 Configuring Video Settings** for more detailed parameter settings of the main stream and sub-stream respectively.

● Image Size:

You can scale up/down the live view image by clicking , , , . The image size can be 4:3, 16:9, original or auto.

Chapter 6 PTZ Configuration

6.1 Configuring Initial Position

Purpose:

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

● **Customize an Initial Position:**

Steps:

1. Enter the Initial Position Configuration interface:
Configuration > Advanced Configuration > PTZ > Initial Position

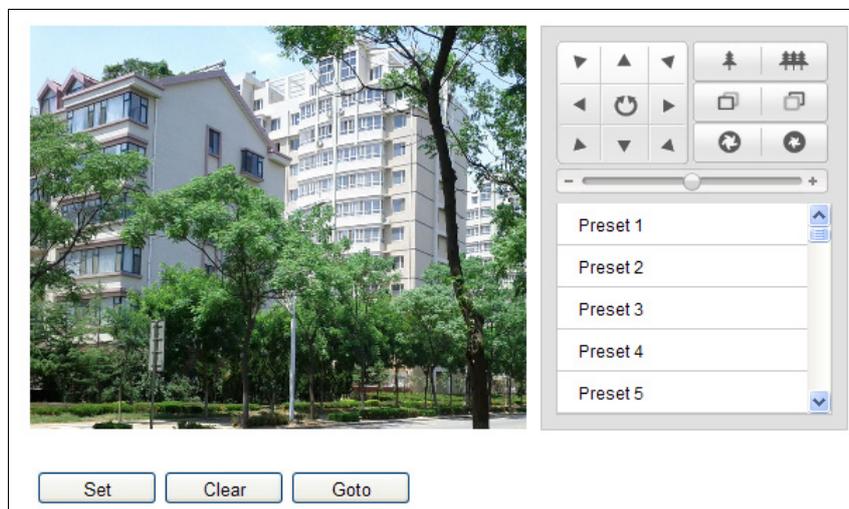


Figure 6-1 PTZ Configuration

2. Click the PTZ control buttons to find a position as the initial position of the PTZ camera; you can also call a defined preset and set it as the initial position of the PTZ camera.
3. Click **Set** to save the position.



● **Call/delete an Initial Position:**

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

6.2 Configuring Basic PTZ Parameters

Purpose:

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

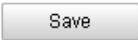
1. Enter the Basic PTZ Parameter Configuration interface:

Configuration > Advanced Configuration > PTZ > Basic

Basic Parameter	
<input checked="" type="checkbox"/> Enable Proportional Pan	
Preset Speed	4
Keyboard Control Speed	Normal
Manual Control Speed	Compatible
PTZ OSD	
Zoom Status	Always Close
PT Status	Always Close
Preset Status	Always Close
Power Off Memory	
Set Resume Time Point	30s

Figure 6-2 Basic PTZ Configuration Interface

2. Configure the following settings:
 - **Basic Parameters:** Enable/disable proportional pan and preset freezing, set the preset speed, and keyboard control speed.
 - ◆ **Proportional Pan:** If you enable this function, the pan/tilt speeds change according to the amount of zoom. When there is a large amount of zoom, the pan/tilt speed will be slower for keeping the image from moving too fast on the live view image.
 - ◆ **Preset Speed:** You can set the speed of a defined preset from 1 to 8.
 - ◆ **Keyboard Control Speed:** Define the speed of PTZ control by a keyboard as Low, Normal or High.
 - ◆ **Manual Control Speed:** The manual control speed can be set as Compatible, Pedestrian, Non-motor Vehicle, Motor Vehicle or Self-adaptive.
 - Compatible: The control speed is same as the Keyboard Control Speed.
 - Pedestrian: Choose the **Pedestrian** when you monitor the pedestrians.

- **Non-motor Vehicle:** Choose the **Non-motor Vehicle** when you monitor the non-motor vehicles.
 - **Motor Vehicle:** Choose the **Motor Vehicle** when you monitor the motor vehicles.
 - **Self-adaptive:** You are recommended to set the Self-adaptive when the application scene of the speed dome is complicated.
 - **PTZ OSD:** Set the on-screen display duration of the PTZ status.
 - ◆ **Zoom Status:** Set the OSD duration of zooming status as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - ◆ **PT Status:** Set the azimuth angle display duration while panning and tilting as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - ◆ **Preset Status:** Set the preset name display duration while calling the preset as 2 seconds, 5 seconds, 10 seconds, Always Close or Always Open.
 - **Power-off Memory:** The PTZ camera can resume its previous PTZ status or actions after it restarted from a power-off. You can set the time point of which the PTZ camera resumes its PTZ status. You can set it to resume the status of 30 seconds, 60 seconds, 300 seconds or 600 seconds before power-off.
3. Click  to save the settings.



6.3 Configuring PTZ Limit Stops

Purpose:

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

Steps:

1. Enter the Limit Configuration interface:
Configuration > Advanced Configuration > PTZ > Limit

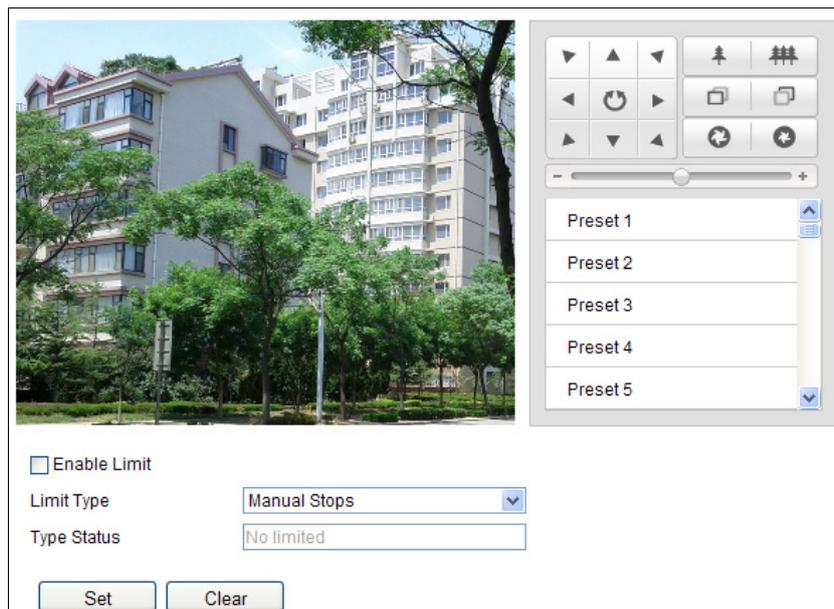


Figure 6-3 Configure the PTZ Limit

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



6.4 Configuring Scheduled Tasks

Purpose:

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

Steps:

1. Enter the Scheduled Task Settings interface:
Configuration > Advanced Configuration > PTZ > Scheduled Tasks

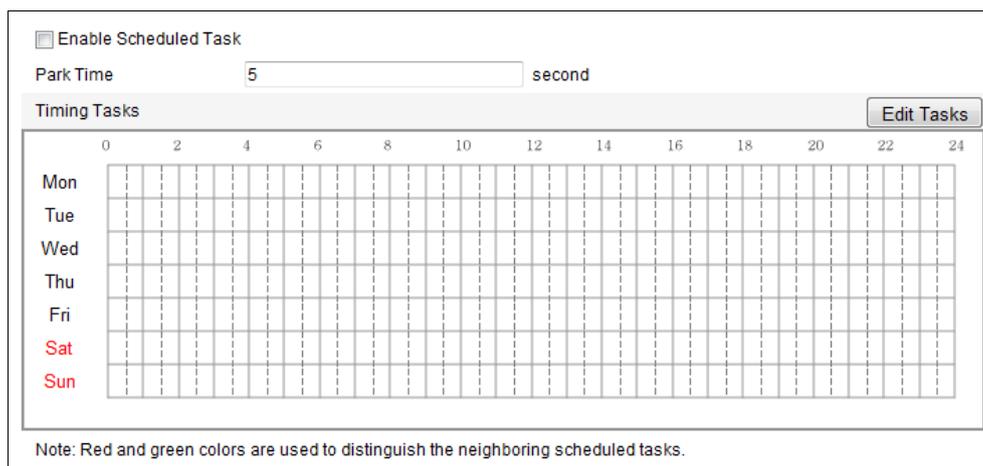


Figure 6-4 Configure Scheduled Tasks

2. Check the checkbox of **Enable Scheduled Task**.
3. Set the **Park Time**. You can set the park time (a period of inactivity) before the PTZ camera starts the scheduled tasks.
4. Set the schedule and task details.

Steps:

- (1) Click to edit the task schedule.

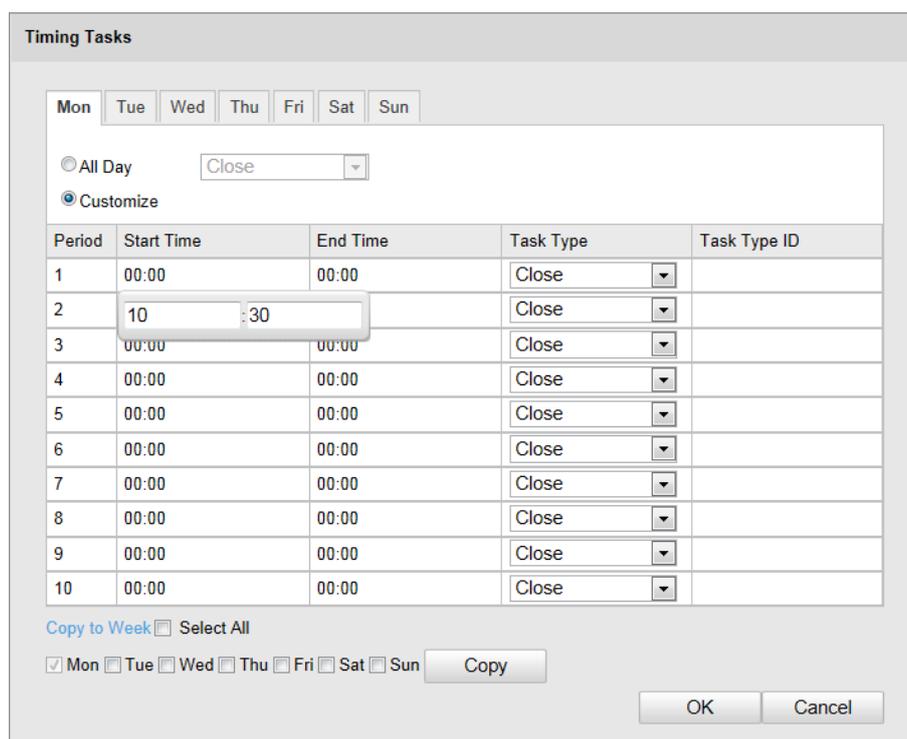


Figure 6-5 Edit the Schedule and Task Type

- (2) Choose the day you want to set the task schedule.
- (3) Click **All Day** to set the schedule as all day; or click **Customize** and input the **Start Time** and **End Time** for each task, and click **Enter** on your keyboard to enter the time.
- (4) Choose the task type from the drop-down list. You can choose

preset, etc..



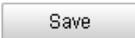
The valid task types may vary according to different camera models.

(5) After you set the scheduled task, you can copy the task to other days (Optional).

(6) Click  to save the settings.



The time of each task cannot be overlapped. Up to 10 tasks can be configured for each day.

5. Click  to save the settings.



6.5 Configuring Park Actions

Purpose:

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



Scheduled Tasks function is prior to **Park Action** function. When these two functions are set at the same time, only the **Scheduled Tasks** function takes effect.

Steps:

1. Enter the Park Action Settings interface:
Configuration > Advanced Configuration > PTZ > Park Action

<input checked="" type="checkbox"/>	Enable Park Action	
Park Time	<input type="text" value="5"/>	second
Action Type	<input type="text" value="Preset"/>	▼
Action Type ID	<input type="text" value="1"/>	▼

Figure 6-6 Set the Park Action

2. Check the checkbox of **Enable Park Action**.
3. Set the **Park Time** as the inactivity time of the PTZ camera before it starts the park actions.
4. Choose **Action Type** the from the drop-down list.

- Click to save the settings.



6.6 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:

- Enter the Privacy Mask Settings interface:

Configuration > Advanced Configuration > PTZ > Privacy Mask

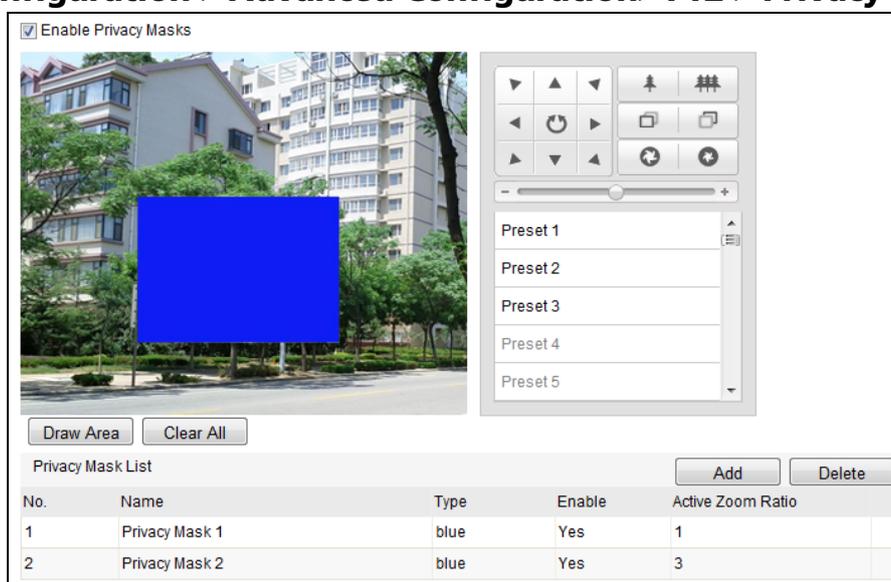


Figure 6-7 Draw the Privacy Mask

- Click the PTZ control buttons to find the area you want to set the privacy mask.
- Click ; click and drag the mouse in the live video window to draw the area.
- Click to save the privacy mask, and it will be listed in the **Privacy Mask List** area; you can select a mask and click to delete it from the list.

The color of the mask is set as blue by default, cannot be configured.

Privacy Mask List					<input type="button" value="Add"/>	<input type="button" value="Delete"/>
No.	Name	Type	Enable	Active Zoom Ratio		
1	Privacy Mask 1	blue	Yes	1		
2	Privacy Mask 2	blue	Yes	3		

Figure 6-8 Privacy Mask List

- Click to finish drawing or click to clear all of the areas you set without saving them.
- Check the checkbox of **Enable Privacy Mask** to enable this function.



You are allowed to draw up to 8 areas on the same image.



6.7 Configuring PTZ Control Priority

Steps:

- Get to the configuration interface:

Configuration > Advanced Configuration > PTZ > Prioritize PTZ.

- The PTZ camera can be controlled by network and RS-485 signals. You can set the control priority of these two signals.
- The operation of **Operator** is prior to that of **User**. When the **Operator** is controlling the PTZ camera, the **User** cannot control it. When the **Operator** finishes, the **User** can control the PTZ camera after the **Delay** time. The **Delay** time can be set in Priority PTZ interface as shown follows.

Prioritize PTZ	Network	▼
Delay	10	second

Figure 6-9 PTZ Priority

- Click to activate the settings.



6.8 Clearing PTZ Configurations

Purpose:

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

Steps:

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

- Click to clear the settings.

Chapter 7 PTZ Camera Configuration

7.1 Configuring Local Parameters



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

Steps:

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

Live View Parameters			
Protocol	<input checked="" type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> MULTICAST <input type="radio"/> HTTP
Live View Performance	<input type="radio"/> Shortest Delay	<input checked="" type="radio"/> Auto	
Rules	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Image Format	<input checked="" type="radio"/> JPEG	<input type="radio"/> BMP	
Record File Settings			
Record File Size	<input type="radio"/> 256M	<input checked="" type="radio"/> 512M	<input type="radio"/> 1G
Save record files to	<input type="text" value="C:\Users\Web\RecordFiles"/>	<input type="button" value="Browse"/>	
Save downloaded files to	<input type="text" value="C:\Users\Web\DownloadFiles"/>	<input type="button" value="Browse"/>	
Picture and Clip Settings			
Save snapshots in live view to	<input type="text" value="C:\Users\Web\CaptureFiles"/>	<input type="button" value="Browse"/>	
Save snapshots when playback to	<input type="text" value="C:\Users\Web\PlaybackPics"/>	<input type="button" value="Browse"/>	
Save clips to	<input type="text" value="C:\Users\Web\PlaybackFiles"/>	<input type="button" value="Browse"/>	

Figure 7-1 Local Configuration Interface

2. Configure the following settings:
 - **Live View Parameters:** Set the protocol type, stream type, image size 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 the protocol type to

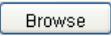


when using the Multicast function. For other

information about Multicast, refer to **Section 7.3.1 Configuring TCPIP Settings**.

- ◆ **Live View Performance:** Set the live view performance to Shortest Delay, or Auto.
- ◆ **Rules:** You can enable or disable the rules of dynamic analysis for motion here.
- ◆ **Image Format:** The captured pictures can be saved as different format. JPEG and BMP are available.
- **Record File Settings:** Set the saving path of the video files.
 - ◆ **Record File Size:** Select the packed size of manually recorded and downloaded video files. The size can be set to 256M, 512M or 1G.
 - ◆ **Save record files to:** Set the saving path for the manually recorded video files.
 - ◆ **Save downloaded files to:** Set the saving path for the downloaded video files in  interface.
- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files.
 - ◆ **Save snapshots in live view to:** Set the saving path of the manually captured pictures in  interface.
 - ◆ **Save snapshots when playback to:** Set the saving path of the captured pictures in  interface.
 - ◆ **Save clips to:** Set the saving path of the clipped video files in  interface.



You can click  to change the directory for saving video files, clips and pictures.

3. Click  to save the settings.



7.2 Configuring Time Settings

Purpose:

You can follow the instructions in this section to configure the time which

can be displayed on the video. There are Time Zone, Time Synchronization, Daylight Saving Time (DST) functions for setting the time. Time Synchronization consists of auto mode by Network Time Protocol (NTP) server and manual mode.

To enter the Time Settings interface:

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

The screenshot shows the 'Time Settings' interface. At the top, the 'Time Zone' is set to '(GMT+08:00) Beijing, Urumqi, Singapore'. Below this, the 'Time Sync.' section has two radio buttons: 'NTP' (selected) and 'Manual Time Sync.'. Under 'NTP', there are three input fields: 'Server Address' with 'time.windows.com', 'NTP Port' with '123', and 'Interval' with '1440' and 'min.' next to it. A 'Test' button is located below the interval field. Under 'Manual Time Sync.', there are two input fields: 'Device Time' with '2014-05-15T17:07:01' and 'Set Time' with '2014-05-16T17:07:25'. A checkbox labeled 'Sync. with computer time' is checked next to the 'Set Time' field.

Figure 7-2 Time Settings

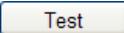
● Configuring Time Synchronization by NTP Server

Steps:

- (1) Check the radio button to enable the **NTP** function.
- (2) Configure the following settings:
 - Server Address:** IP address of NTP server.
 - NTP Port:** Port of NTP server.
 - Interval:** The time interval between the two synchronizing actions by NTP server. It can be set from 1 to 10080 minutes.

This is a close-up of the 'Time Sync.' section from Figure 7-2. It shows the 'NTP' radio button selected. The 'Server Address' field contains 'time.windows.com', the 'NTP Port' field contains '123', and the 'Interval' field contains '1440' with 'min.' to its right. A 'Test' button is positioned below the interval field.

Figure 7-3 Time Sync by NTP Server

- (3) You can click the  button to check whether the configuration is succeeded.

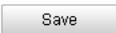


If the PTZ camera is connected to a public network, you should use a NTP server that has a time synchronization function, such as the server at the National Time Center (IP Address: 210.72.145.44). If the PTZ camera is set in a customized network, NTP software can be used to establish a NTP server for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



● Configuring Time Synchronization Manually

Steps:

- (1) Check the **Manual Time Sync** radio button.
- (2) Click  to set the system time from the pop-up calendar.
- (3) Click  to save the settings.



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

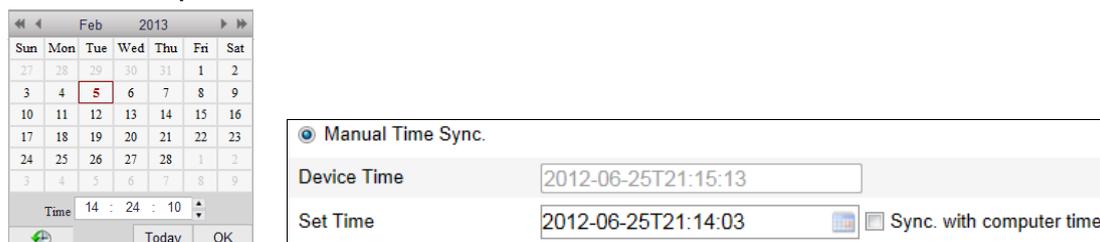


Figure 7-4 Time Sync Manually



● Select the Time Zone

Purpose:

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

From the **Time Zone** drop-down menu as shown in Figure 7-5, select the Time Zone in which the PTZ camera locates.

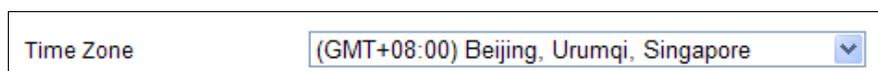


Figure 7-5 Time Zone Settings

● Configuring Daylight Saving Time (summer time)

Purpose:

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

Steps:

- (1) Enter the **DST** interface by **Configuration > Advanced Configuration > System > DST**
- (2) Check Enable DST to enable the DST function.
- (3) Set the date of the DST period.
- (4) Click  to save the settings.

DST						
<input checked="" type="checkbox"/>	Enable DST					
Start Time	Apr	First	Sun	02	o'clock	
End Time	Oct	Last	Sun	02	o'clock	
DST Bias	30min					

Figure 7-6 DST Settings



7.3 Configuring Network Settings

7.3.1 Configuring TCP/IP Settings

Purpose:

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

Steps:

1. Enter TCP/IP Settings interface:
Configuration > Basic Configuration > Network > TCP/IP
 Or **Configuration > Advanced Configuration > Network > TCP/IP**
2. Select the NIC you want to configure, LAN and WLAN are selectable.

NIC Settings	
Select NIC	lan
NIC Type	Auto
<input type="checkbox"/> DHCP	
IPv4 Address	10.16.1.243 <input type="button" value="Test"/>
IPv4 Subnet Mask	255.255.255.0
IPv4 Default Gateway	10.16.1.254
IPv6 Mode	Route Advertisement <input type="button" value="View Route Advertisement"/>
IPv6 Address	::
IPv6 Subnet Mask	0
IPv6 Default Gateway	
Mac Address	44:19:b6:59:f2:1c
MTU	1500
Multicast Address	
DNS Server	
Preferred DNS Server	8.8.8.8
Alternate DNS Server	

Figure 7-7 TCP/IP Settings

- Configure the NIC settings, including the **IPv4(IPv6) Address**, **IPv4(IPv6) Subnet Mask** and **IPv4(IPv6) Default Gateway**.
- Click to save the above settings.



- If the DHCP server is available, you can check DHCP to automatically obtain an IP address and other network settings from that server.
- If the IP address is set manually, you can click to check whether the IP address is already used to prevent the IP address conflict.
- The valid value range of Maximum Transmission Unit (MTU) is 500 ~ 9676. The default value is 1500.
- The Multicast sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, you have to enable the Multicast function of your router and configure the gateway of the network PTZ camera.
- If the DNS server settings are required for some applications (e.g., sending email), you should properly configure the **Preferred DNS Server** and **Alternate DNS server**.

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

Figure 7-8 DNS Server Settings



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



7.3.2 Configuring Port Settings

Purpose:

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

Steps:

1. Enter the Port Settings interface:

Configuration > Basic Configuration > Network > Port

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

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

Figure 7-9 Port Settings

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

HTTP Port: The default port number is 80.

RTSP Port: The default port number is 554.

HTTPS Port: The default port number is 443.

Server Port: The default port number is 8000.

3. Click to save the settings.



7.3.3 Configuring PPPoE Settings

Purpose:

If you have no router but only a modem, you can use Point-to-Point

Protocol over Ethernet (PPPoE) function.

Steps:

1. Enter the PPPoE Settings interface:

Configuration > Advanced Configuration > Network > PPPoE

<input checked="" type="checkbox"/> Enable PPPoE	
Dynamic IP	<input type="text" value="0.0.0.0"/>
User Name	<input type="text"/>
Password	<input type="text"/>
Confirm	<input type="text"/>

Figure 7-10 PPPoE Settings

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



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



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

4. Click to save and exit the interface.



7.3.4 Configuring DDNS Settings

Purpose:

If your PTZ 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 PTZ camera.



For your privacy and to better protect your system against security risks, we strongly recommend the use of strong passwords for all functions and

network devices. The password should be something of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers and special characters) in order to increase the security of your product.

Steps:

1. Enter the DDNS Settings interface:

Configuration > Advanced Configuration > Network > DDNS

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	DynDNS
Server Address	
Domain	
Port	0
User Name	
Password	
Confirm	

Figure 7-11 DDNS Settings

2. Check the **Enable DDNS** checkbox to enable this feature.
3. Select **DDNS Type**. Three DDNS types are selectable: IP Server, HiDDNS, NO-IP and DynDNS.

● **DynDNS:**

Steps:

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

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	DynDNS
Server Address	members.dyndns.org
Domain	123.dyndns.org
Port	0
User Name	test
Password	••••••
Confirm	••••••

Figure 7-12 DynDNS Settings

● **IP Server:**

Steps:

- (1) Enter the Server Address of the IP Server.
- (2) Click to save the settings.



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

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	IPServer
Server Address	202.23.10.117

Figure 7-13 IPServer Settings

● HiDDNS:

Steps:

- (1) Enter the Server Address: www.hiddns.com.
- (2) Enter the Domain name of the camera. The domain is the same with the device alias in the HiDDNS server.
- (3) Click to save the settings.

<input checked="" type="checkbox"/> Enable DDNS	
DDNS Type	HiDDNS
Server Address	www.hiddns.com
Domain	476721583
Port	0
User Name	
Password	
Confirm	

Figure 7-14 HiDDNS Settings

● NO-IP:

Steps:

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



7.3.5 Configuring SNMP Settings

Purpose:

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

Before you start:

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



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

Steps:

1. Enter the SNMP Settings interface:

Configuration > Advanced Configuration > Network > SNMP

SNMP v1/v2	
Enable SNMPv1	<input checked="" type="checkbox"/>
Enable SNMP v2c	<input checked="" type="checkbox"/>
Write SNMP Community	<input type="text" value="private"/>
Read SNMP Community	<input type="text" value="public"/>
Trap Address	<input type="text"/>
Trap Port	<input type="text" value="162"/>
Trap Community	<input type="text" value="public"/>
SNMP v3	
Enable SNMPv3	<input type="checkbox"/>
Read UserName	<input type="text"/>
Security Level	<input type="text" value="no auth, no priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key password	<input type="text"/>
Write UserName	<input type="text"/>
Security Level	<input type="text" value="no auth, no priv"/>
Authentication Algorithm	<input checked="" type="radio"/> MD5 <input type="radio"/> SHA
Authentication Password	<input type="text"/>
Private-key Algorithm	<input checked="" type="radio"/> DES <input type="radio"/> AES
Private-key password	<input type="text"/>
SNMP Other Settings	
SNMP Port	<input type="text" value="161"/>

Figure 7-15 SNMP Settings

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



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

4. Click  to save and finish the settings.



7.3.6 Configuring QoS Settings

Purpose:

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

Steps:

1. Enter the QoS Settings interface:

Configuration > Advanced Configuration > Network > QoS

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

Figure 7-16 QoS Settings

2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP and Management DSCP.
The valid DSCP value ranges from 0 to 63. The DSCP value is bigger, the priority is higher.
3. Click  to save the settings.



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



7.3.7 Configuring FTP Settings

Purpose:

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

Steps:

1. Enter the FTP Settings interface:

Configuration > Advanced Configuration > Network > FTP

Server Address	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="21"/>
User Name	<input type="text"/> <input type="checkbox"/> Anonymous
Password	<input type="password"/>
Confirm	<input type="password"/>
Directory Structure	<input type="text" value="Save in the root directory."/> ▼
Parent Directory	<input type="text" value="Use Device Name"/> ▼
Child Directory	<input type="text" value="Use Camera Name"/> ▼
Upload Type	<input type="checkbox"/> Upload Picture
<input type="button" value="Test"/>	

Figure 7-17 FTP Settings

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



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

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

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

- ◆ **Root directory:** The files will be saved in the root of FTP server.
- ◆ **Parent directory:** The files will be saved in a folder in FTP server. The name of folder can be defined as shown in following Figure 7-18.

Use Device Name	▼
Use Device Name	
Use Device Number	
Use Device IP address	

Figure 7-18 Parent Directory

- ◆ **Child directory:** It is a sub-folder which can be created in the parent directory. The files will be saved in a sub-folder in FTP server. The name of folder can be defined as shown in following Figure 7-19.

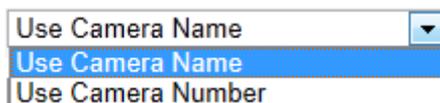


Figure 7-19 Child Directory

- **Upload type:** To enable uploading the captured picture to the FTP server.
3. Click  to save the settings.



If you want to upload the captured pictures to FTP server, you also have to enable the continuous snapshot or event-triggered snapshot in **Snapshot** interface. For detailed information, please refer to the Section **8.4 Configuring Snapshot Settings**.



7.3.8 Configuring UPnP™ Settings

Purpose:

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

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

Steps:

1. Enter the UPnP™ settings interface.
Configuration > Advanced Configuration > Network > UPnP™
2. Check the checkbox to enable the UPnP™ function.
You can edit the Friendly Name of the PTZ camera. This name can be detected by corresponding device, such as a router.

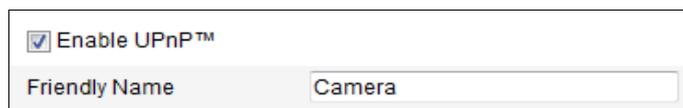


Figure 7-20 Configure UPnP Settings



7.3.9 Configuring NAT (Network Address Translation)

Settings

Steps:

1. Set the port mapping mode:

To port mapping with the default port numbers:

Choose

To port mapping with the customized port numbers:

Choose

And you can customize the value of the port No. by yourself.

<input checked="" type="checkbox"/> Enable Port Mapping				
Port Mapping Mode <input type="text" value="Manual"/>				
	Port Type	External Port	External IP Address	Status
<input checked="" type="checkbox"/>	HTTP	80	0.0.0.0	Not Valid
<input checked="" type="checkbox"/>	RTSP	554	0.0.0.0	Not Valid
<input checked="" type="checkbox"/>	Server Port	<input type="text" value="8002"/>	0.0.0.0	Not Valid

Figure 7-21 Configure the Port No.

2. Click to save the settings.



7.3.10 Configuring Email Settings

Purpose:

The system can be configured to send an Email notification to all designated receivers if an alarm event is detected, e.g., motion detection event, video loss, tamper-proof, 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 Email Settings interface:
Configuration > Advanced Configuration > Network > Email

Sender	
Sender	<input type="text"/>
Sender's Address	<input type="text"/>
SMTP Server	<input type="text"/>
SMTP Port	<input type="text" value="25"/>
<input type="checkbox"/> Enable SSL	
Interval	<input type="text" value="2s"/> <input type="checkbox"/> Attached Image
<input type="checkbox"/> Authentication	
User Name	<input type="text"/>
Password	<input type="text"/>
Confirm	<input type="text"/>
Receiver	
Receiver1	<input type="text"/>
Receiver1's Address	<input type="text"/> <input type="button" value="Test"/>
Receiver2	<input type="text"/>
Receiver2's Address	<input type="text"/>
Receiver3	<input type="text"/>
Receiver3's Address	<input type="text"/>

Figure 7-22 Email Settings

2. Configure the following settings:

Sender: The name of the email sender.

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

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

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

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.

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.



You can click to check whether the setting is invalid after the required parameters are configured.



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

3. Click  to save the settings.



7.3.11 Configuring 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.

Example:

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. Create the self-signed certificate or authorized certificate.

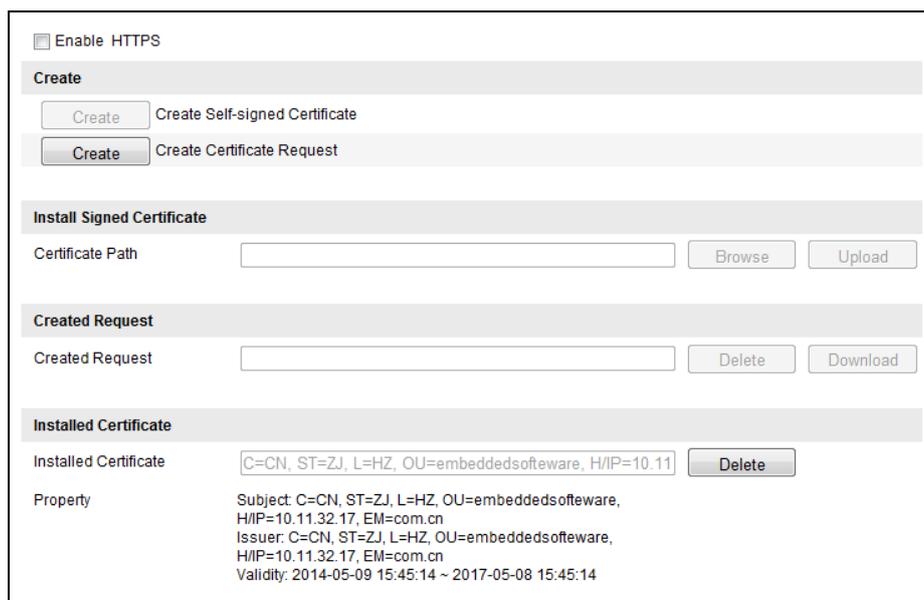


Figure 7-23 HTTPS Settings

OPTION 1: Create the self-signed certificate

- 1) Click the **Create** button to create the following dialog box.

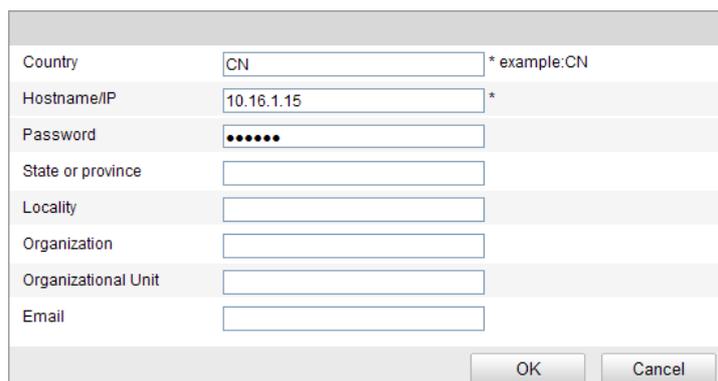


Figure 7-24 Create Self-signed Certificate

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

OPTION 2: Create the authorized certificate

- 1) Click the **Create** button to create the certificate request, and fulfill the required information.
 - 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.
3. There will be the certificate information after you successfully create and install the certificate.

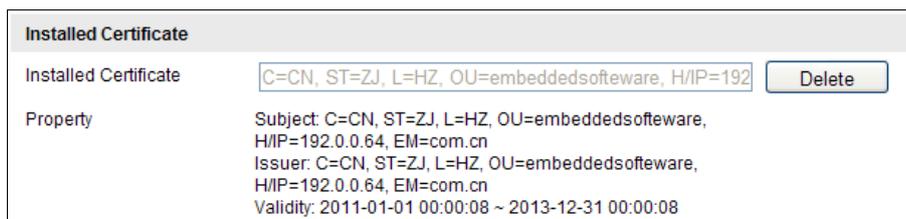


Figure 7-25 Installed Certificate Property



You can click configure the HTTPS port No. on your demand; refer to **Section 7.3.2 Configuring Port Settings** for details.

4. Check the checkbox of Enable HTTPS and click the **Save** button.



7.3.12 Configuring Platform Access Settings

Purpose:

Cloud P2P provides the mobile phone application and as well the service platform page to access and manage your connected NVR, which enables you to get a convenient remote access to the surveillance system.

Steps:

1. Enter the Platform Access configuration interface.
Configuration > Advanced Configuration > Network > Platform Access
2. Check the checkbox of the Enable.
3. Select the Platform Type as the **Cloud P2P** in the dropdown list.
4. Click the Save button to activate the settings.
You can view the register status of the device in the corresponding text.



You can only enable either Cloud P2P or DDNS.

7.4 Configuring Video and Audio Settings

7.4.1 Configuring Video Settings

Steps:

1. Enter the Video Settings interface:

Configuration > Basic Configuration > Video / Audio > Video

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

Stream Type	Main Stream(Normal)	▼
Video Type	Video&Audio	▼
Resolution	1280*720P	▼
Bitrate Type	Variable	▼
Video Quality	Medium	▼
Frame Rate	25	▼ fps
Max. Bitrate	2048	Kbps
Video Encoding	H.264	▼
I Frame Interval	50	
SVC	OFF	▼

Figure 7-26 Configure Video Settings

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

The main stream is usually for recording and live viewing with good bandwidth, and the sub-stream can be used for live viewing when the bandwidth is limited. Refer to the **Section 7.1 Configuring Local Parameters** for switching the main stream and sub-stream for live viewing.

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

Video Type:

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

Resolution:

Select the resolution of the video output.

Bitrate Type:

Select the bitrate type to constant or variable.

Video Quality:

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

selectable.

Frame Rate:

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, and the higher bandwidth is required as well.

Video Encoding:

The **Video Encoding** standard can be set to H.264 or MJPEG.

I Frame Interval:

Set the I-Frame interval from 1 to 400.

SVC:

SVC is a video encoding technology. It extracts frames from the original video and sends these frames to a video recorder which also supports SVC function when the network bandwidth is insufficient.

4. Click  to save the settings.



7.4.2 Configuring Audio Settings

Steps:

1. Enter the Audio Settings interface
Configuration > Basic Configuration > Video / Audio > Audio
 Or **Configuration > Advanced Configuration > Video / Audio > Audio**

Audio Encoding	MP2L2	▼
Sampling Rate	16kHz	▼
Audio Stream Bitrate	64kbps	▼
Audio Input	MicIn	▼
Input Volume	 50	
Environmental Noise Filter	OFF	▼

Figure 7-27 Audio Settings

2. Configure the following settings.
Audio Encoding: G.722.1, G.711ulaw, G.711alaw, MP2L2 and G.726.
Sampling Rate: When the Audio Encoding is selected as MP2L2, you can configure the Sampling Rate in the dropdown list. The greater the

value is, the better the audio quality will be.

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

Audio Input: When an intercom is connected to the PTZ camera, you need to set this option to **Lineln**. When a microphone is connected to the PTZ camera, you need to set this option to **MicIn**.

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

Environmental Noise Filter: When the monitoring environment is very noisy, you can enable this function to reduce part of the noise.

3. Click to save the settings.



7.4.3 Configuring ROI Settings

Before you start:

ROI (Region of Interest) encoding is used to enhance the quality of images which are specified in advance.

Enter the RIO Settings interface:

Configuration > Advanced Configuration > Video / Audio > RIO

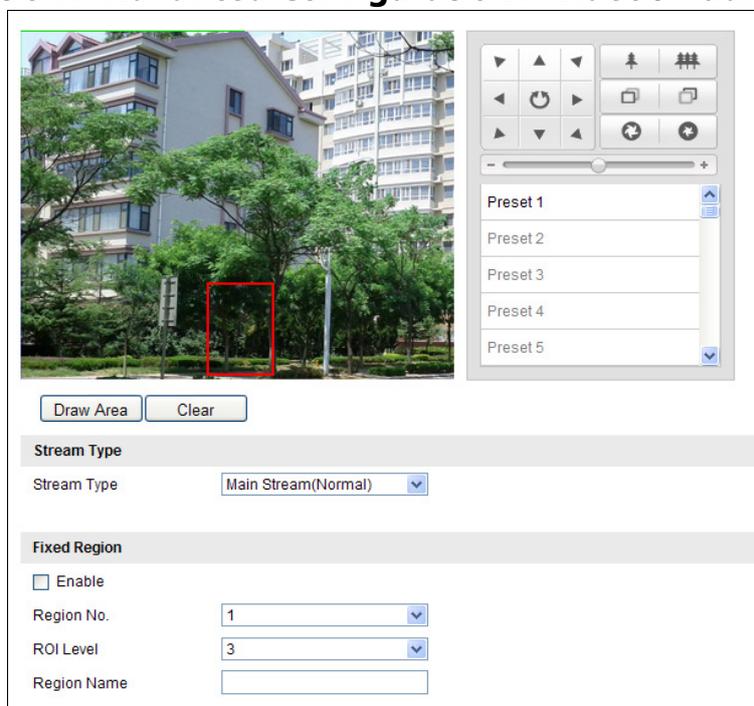


Figure 7-28 Region of Interest

Stream Type:

You can set the ROI function for main stream or sub stream. Select a

stream type and then configure the ROI settings.

Fixed Region:

The fixed region encoding is the ROI encoding for the manually configured area. And you can choose the Image Quality Enhancing level for ROI encoding, and you can also name the ROI area.

Steps:

1. Select a **Region No.**.
2. Check the check box of **Enable** under **Fixed Region**.
3. Click  and draw a red frame in the live view image.
4. Adjust the **ROI level** from 1 to 6. The higher the value, the better image quality in the red frame.
5. Enter a **Region Name** and click **Save** to save the settings.



7.5 Configuring Image Settings

7.5.1 Configuring Display Settings

Purpose:

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



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

Steps:

1. Enter the Display Settings interface:
Configuration > Basic Configuration> Image> Display Settings
Or **Configuration > Advanced Configuration> Image> Display Settings**
2. You can select the **Mounting Scenario** in the dropdown list with different predefined image parameters.
3. Set the image parameters of the PTZ camera.



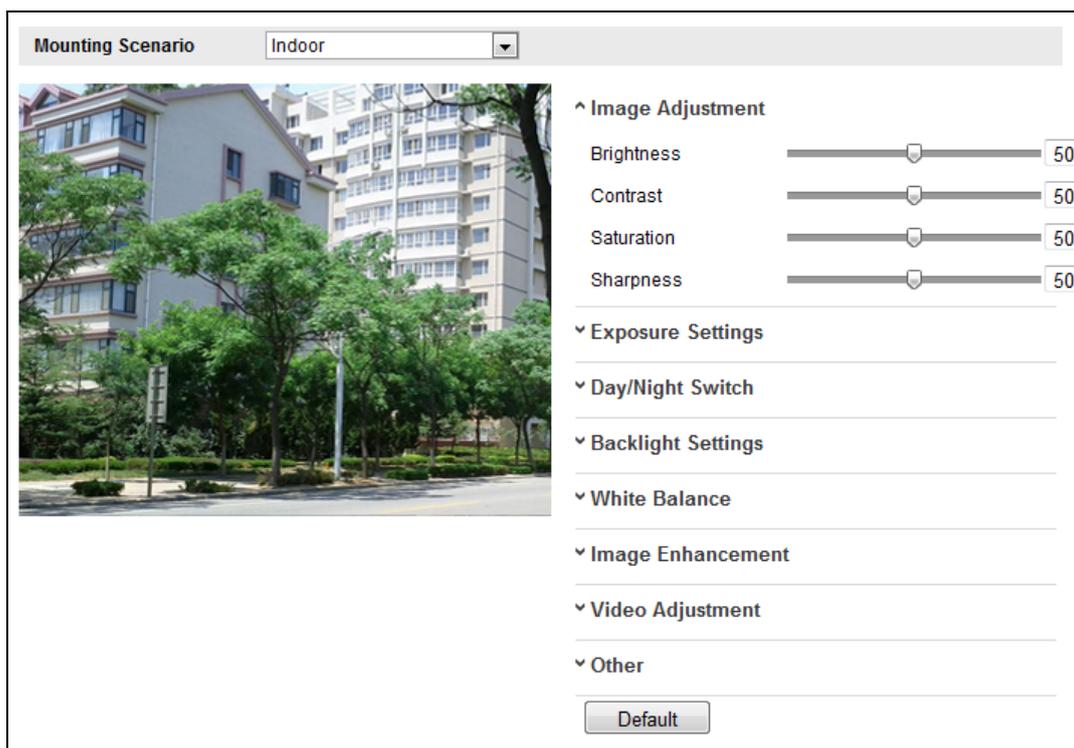


Figure 7-29 Display Settings

Image Adjustment

- **Brightness**

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

- **Contrast**

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

- **Saturation**

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

- **Sharpness**

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



This function varies depending on the models of PTZ camera.

Exposure Settings

- **Exposure Mode**

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

- ◆ Auto:

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

◆ **Manual:**

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



This function varies depending on the models of PTZ camera.

● **Limit Gain**

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

● **Slow Shutter**

This function can be used in underexposure condition. It lengthens the shutter time to ensure full exposure. The slow shutter value can be set to **Slow Shutter*2, *4, *6, *12, *16, *24** and ***32**.

Slow Shutter	ON
Slow Shutter Level	Slow Shutter*12

Figure 7-30 Slow Shutter

Day/Night Switch



The IR related functions are supported by the IR PTZ camera only.

● **Day/Night Switch**

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

◆ **Auto:**

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

◆ **Day:**

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

◆ **Night:**

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

◆ **Schedule**

In **Schedule** mode, you can set the time schedule for day mode as shown in Figure 7-31. The rest time out of the schedule is for night mode.

Day/Night Switch	Schedule
Start Time	07:00:00
End Time	18:00:00

Figure 7-31 Day Night Schedule

- **IR Light Mode**

The IR mode is set as Auto by default, and is read-only, which means the IR light is turned on/off according to the illumination.

- **Brightness Limit**

The image brightness is adjusted automatically, you can specify the brightness limit on your demand.

Backlight Settings

- **BLC**

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

- **WDR (Wide Dynamic Range)**

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

You can enable or disable the WDR function as shown in Figure 7-32. The wide dynamic level ranges from 0 to 100.

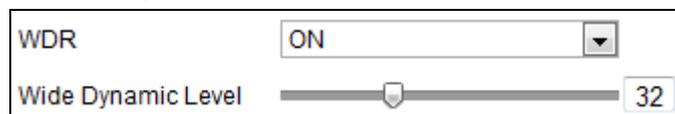


Figure 7-32 WDR



This function varies depending on the models of PTZ camera.

- **HLC**

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

White Balance

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

- ◆ **Auto:**

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

◆ **MWB:**

In **MWB** (Manual White Balance) mode, you can adjust the color temperature manually to meet your own demand as shown in Figure 7-33.



Figure 7-33 Manual White Balance

◆ **Outdoor**

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

◆ **Indoor**

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

◆ **Fluorescent Lamp**

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

◆ **Sodium Lamp**

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

◆ **Auto-Track**

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



This function varies depending on the models of PTZ camera.

Image Enhancement

● **Digital Noise Reduction**

The digital noise reduce function processes the noise in the video signal. You can set **Digital Noise Reduction** function to **ON** and adjust the **Noise Reduction Level** as shown in Figure 7-34. The level ranges from 0 to 100.

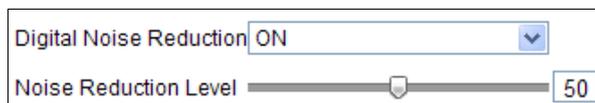


Figure 7-34 Digital Noise Reduction



This function varies depending on the models of PTZ camera.

Video Adjustment

● **Mirror**

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



This function varies depending on the models of PTZ camera.

● **Video Standard**

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



This function varies depending on the models of PTZ camera.

Other

● **Zoom Limit**

You can set **Zoom Limit** value to limit the maximum value of zooming. The value can be set to 3, 6, 12, 24 and 48.



This function varies depending on the models of PTZ camera.

7.5.2 Configuring OSD Settings

Purpose:

The PTZ camera supports following on screen displays:

Zoom: Identifies the amount of magnification.

Direction: Displays panning and tilting direction, with the format of PXXX TXXX. The XXX following P indicates the degrees in pan direction, while the XXX following T indicates the degrees in tilt position.

Time: Supports for time display.

Preset Title: Identifies preset being called.

Camera Name: Identifies the name of PTZ camera.

Steps:

1. Enter the OSD Settings interface:

Configuration > Advanced Configuration > Image > OSD Settings

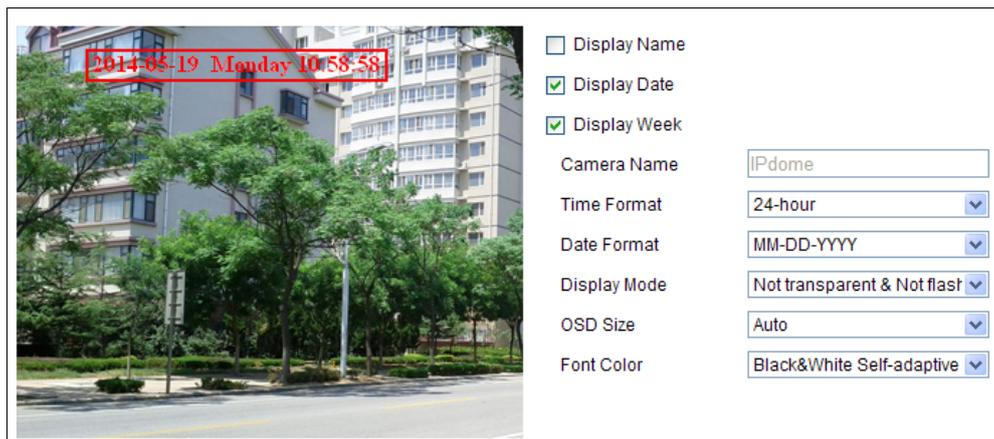


Figure 7-35 OSD Settings

2. Check the corresponding checkbox to select the display of PTZ camera name, date or week if required.
3. (Optional) If you choose to enable the Display name, and then edit the PTZ camera name in the text field of **Camera Name**.
4. Select from the drop-down list to set the time format, date format and display mode.
5. You can use the mouse to click and drag the text frame **IPdome2** in the live view window to adjust the OSD position.



Figure 7-36 Adjust OSD Location

6. The font color can also be customized, select the Custom in the drop down list and select the font color on your demand.
7. Click to activate above settings.

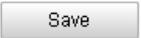


7.5.3 Configuring Text Overlay Settings

Purpose:

You can customize the text overlay.

Steps:

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



There are up to 4 text overlays configurable.

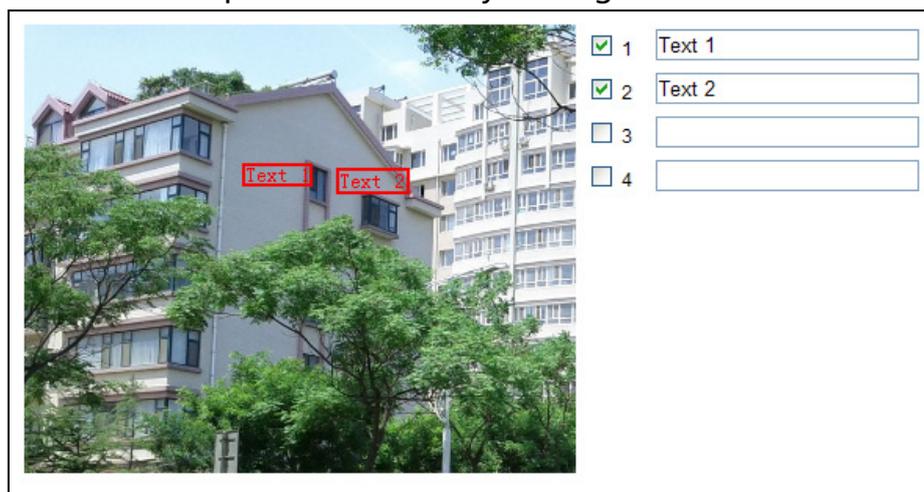


Figure 7-37 Text Overlay Settings



7.6 Configuring and Handling Alarms

Purpose:

This section explains how to configure the network PTZ camera to respond to alarm events, including motion detection, external alarm input, video loss, tamper-proof and exception. These events can trigger the alarm actions, such as Notify Surveillance Center, Send Email, Trigger Alarm Output, etc.

For example, when an external alarm is triggered, the network PTZ camera sends a notification to an e-mail address.

7.6.1 Configuring Motion Detection

Purpose:

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

Steps:

1. Enter the motion detection setting interface:
Configuration > Advanced Configuration > Events > Motion Detection
2. Check the checkbox of the **Enable Motion Detection** to enable this function.
You can check the **Enable Dynamic Analysis for Motion** checkbox if you want the detected object get marked with rectangle in the live view.
3. Select the configuration mode as Normal or Expert and set the corresponding motion detection parameters.
 - **Normal**

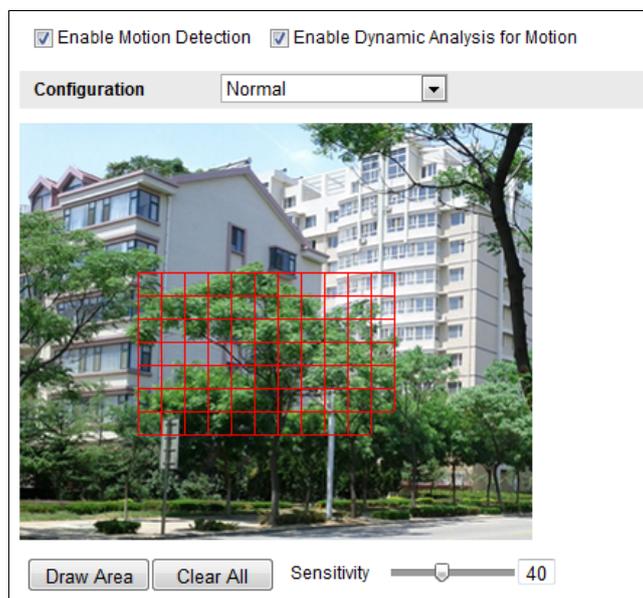


Figure 7-38 Motion Detection Settings-Normal

Steps:

- (1) Click **Draw Area**. Click and drag the mouse on the live video image to draw a motion detection area.
- (2) Click **Stop Drawing** to finish drawing.



- You can draw up to 8 motion detection areas on the same image.
 - You can click to clear all of the areas.
- (3) Move the slider to set the sensitivity of the detection.
- **Expert**

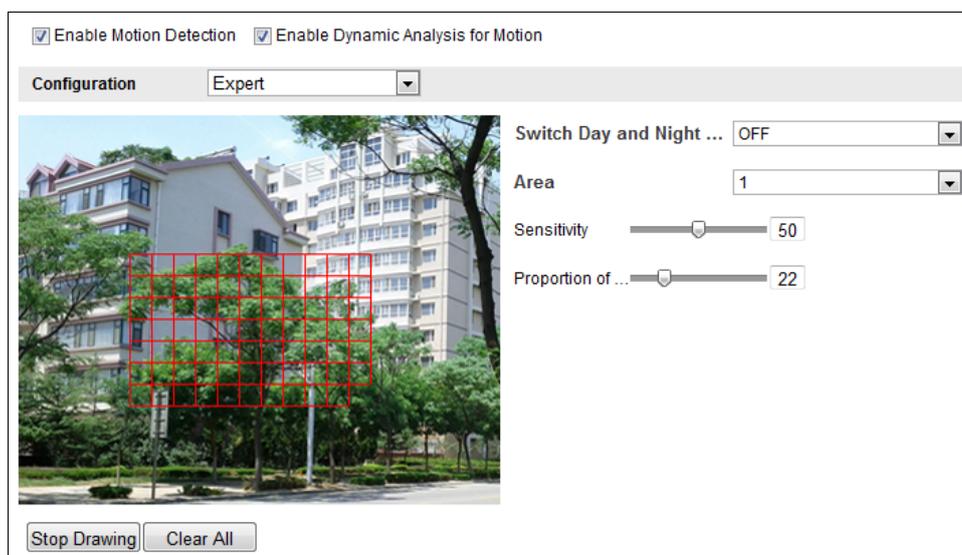


Figure 7-39 Motion Detection Settings-Expert

Steps:

- (1) Set the Day&Night switch mode, there are OFF, Auto-Switch and Scheduled-Switch selectable. If the Day&Night switch mode is enabled, you can configure the detection rule for the day and night separately.
 - OFF:** Disable the day and night switch.
 - Auto-Switch:** Switch the day and night mode according to the illumination automatically.
 - Scheduled-Switch:** Switch to the day mode at 6:00 a.m., and switch to the night mode at 18:00 p.m..
- (2) Select Area No. to configure in the dropdown list.
- (3) Set the values of sensitivity and proportion of object on area.
 - Sensitivity:** The greater the value is, the easier the alarm will be triggered.
 - Proportion of Object on Area:** When the size proportion of the moving object exceeds the predefined value, the alarm will be triggered. The less the value is, the easier the alarm will be triggered.
4. Set the Arming Schedule for Motion Detection.

(1) Click  in Figure 7-40.

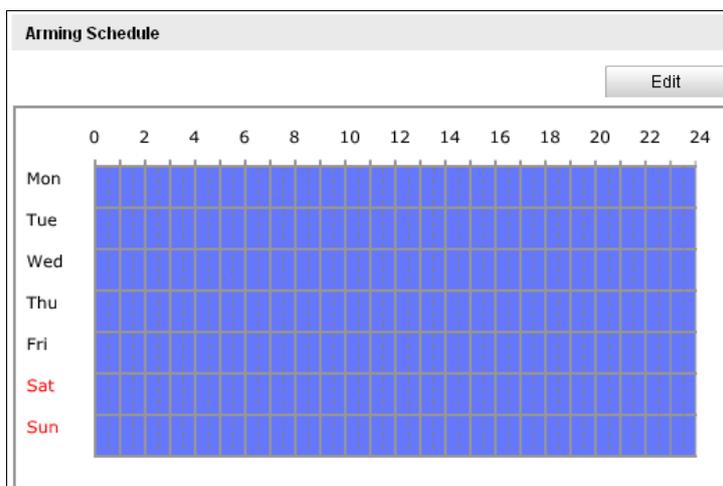


Figure 7-40 Arming Schedule

(2) Choose the day you want to set the arming schedule as shown in Figure 7-41.

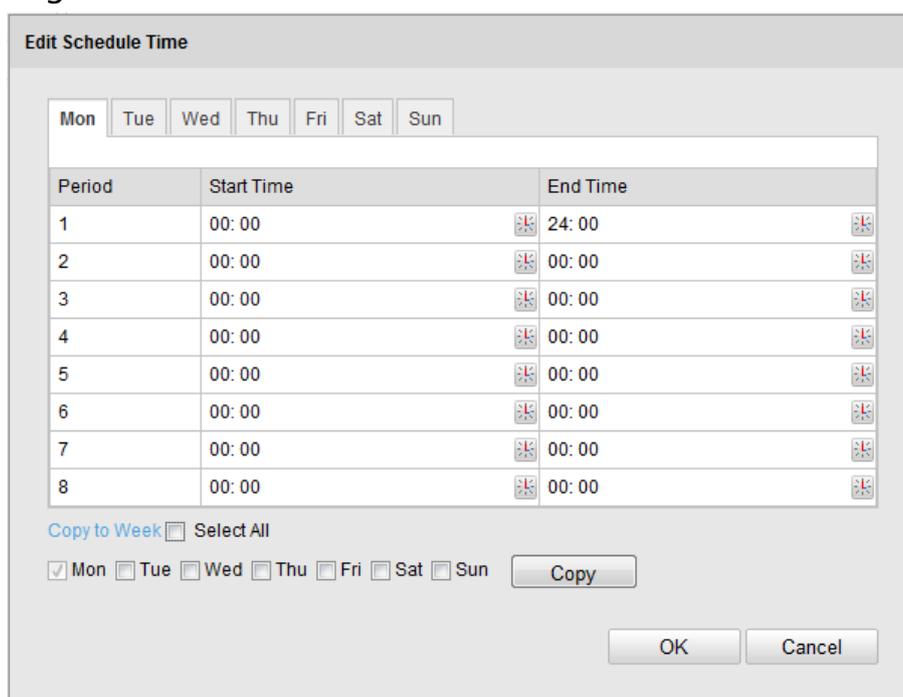


Figure 7-41 Arming Time Schedule

(3) Click  to set the time period for the arming schedule.

(4) (Optional) After you set the arming schedule, you can click  to copy the schedule to other days.

(5) Click  to save the settings.



The time of each period cannot be overlapped. Up to 8 periods can be configured for each day.

5. Set the Alarm Actions for Motion Detection.

You can specify the linkage method when an event occurs. The following contents are about how to configure the different types of linkage method.

Linkage Method	
Normal Linkage	Other Linkage
<input type="checkbox"/> Notify Surveillance Center <input type="checkbox"/> Send Email <input type="checkbox"/> Upload to FTP <input type="checkbox"/> Trigger Channel	Trigger Alarm Output <input type="checkbox"/> Select All <input type="checkbox"/> A->1 <input type="checkbox"/> A->2

Figure 7-42 Linkage Method

Check the checkbox to select the linkage method. Notify surveillance center, send email, upload to FTP, trigger channel and trigger alarm output are selectable.

- **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.



To send the Email when an event occurs, you need to refer to **Section 7.3.10 Configuring Email Settings** to set the Email parameters.

- **Upload to FTP**

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



You need a FTP server and set FTP parameters first. Refer to **Section 7.3.7 Configuring FTP Settings** for setting FTP parameters.

- **Trigger Channel**

Record a video when an event occurs.



You have to set the recording schedule to realize this function. Please refer to **Section 8.3 Configuring Recording Schedule** for settings the recording schedule.

- **Trigger Alarm Output**

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



To trigger an alarm output when an event occurs, please refer to **Section 7.6.4 Configuring Alarm Output** to set the alarm output parameters.



7.6.2 Configuring Video Tampering Alarm

Purpose:

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

Steps:

1. Enter the video tampering Settings interface:
Configuration > Advanced Configuration > Events > Video Tampering

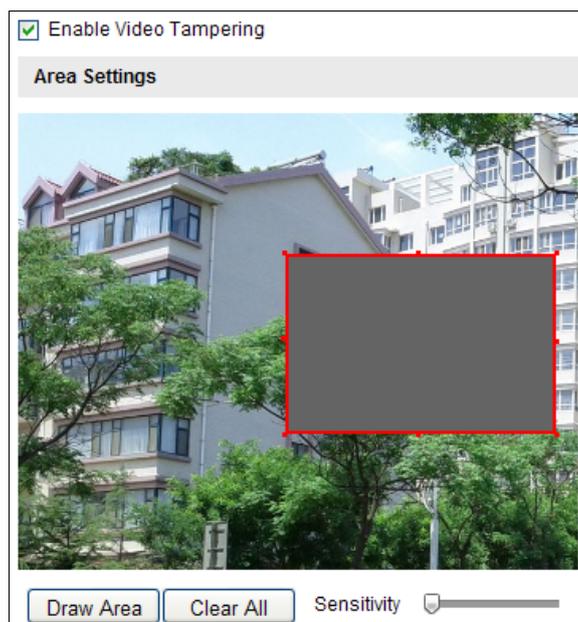


Figure 7-43 Tampering Alarm

2. Check **Enable Video Tampering** checkbox to enable the tampering detection.
3. Set the tampering area. Refer to *Step 1* in **Section 7.6.1 Configuring Motion Detection**.
4. Click to edit the arming schedule for tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Step 2* in **Section 7.6.1 Configuring Motion Detection**.
5. Check the checkbox to select the linkage method taken for the

tampering. Notify surveillance center, send email, trigger channel and trigger alarm output are selectable. Please refer to *Step 3* in **Section 7.6.1 Configuring Motion Detection**.

6. Click to save the settings.



7.6.3 Configuring External Alarm Input

Steps:

1. Enter the Alarm Input Settings interface:
Configuration > Advanced Configuration > Events > Alarm Input:
2. Choose the alarm input No. and the Alarm Type. The alarm type can be NO (Normally Open) and NC (Normally Closed).
3. Edit the name in to set a name for the alarm input (optional).

The screenshot shows the 'Alarm Input Settings' interface. At the top, there are three fields: 'Alarm Input No.' with a dropdown menu showing 'A<-1', 'Alarm Name' with a text input field containing 'alarm1' and a '(cannot copy)' label, and 'Alarm Type' with a dropdown menu showing 'NO'. Below these fields is a section titled 'Arming Schedule' which contains a grid for scheduling. The grid has columns for hours from 0 to 24 in increments of 2, and rows for days of the week: Mon, Tue, Wed, Thu, Fri, Sat, and Sun. An 'Edit' button is located to the right of the grid.

Figure 7-44 Alarm Input Settings

4. Click to set the arming schedule for the alarm input. Refer to *Step 2* in **Section 7.6.1 Configuring Motion Detection**.
5. Check the checkbox to select the linkage method taken for the alarm input. Refer to *Step 3* in **Section 7.6.1 Configuring Motion**

Detection.

6. You can also choose the PTZ linking for the alarm input. Check the relative checkbox and select the No. to enable Preset Calling.
7. You can copy your settings to other alarm inputs.
8. Click  to save the settings.

Linkage Method	
Normal Linkage	Other Linkage
<input type="checkbox"/> Notify Surveillance Center <input type="checkbox"/> Send Email <input type="checkbox"/> Upload to FTP <input type="checkbox"/> Trigger Channel	Trigger Alarm Output <input type="checkbox"/> Select All <input type="checkbox"/> A->1 <input type="checkbox"/> A->2 PTZ Linking <input type="checkbox"/> Preset No. <input type="text" value="1"/> <input type="button" value="v"/> <input type="checkbox"/> Patrol No. <input type="text" value="1"/> <input type="button" value="v"/> <input type="checkbox"/> Pattern <input type="text" value="1"/> <input type="button" value="v"/>
Copy to Alarm	
<input type="checkbox"/> Select All <input checked="" type="checkbox"/> A<-1 <input type="checkbox"/> A<-2 <input type="checkbox"/> A<-3 <input type="checkbox"/> A<-4 <input type="checkbox"/> A<-5 <input type="checkbox"/> A<-6 <input type="checkbox"/> A<-7	

Figure 7-45 Linkage Method



7.6.4 Configuring Alarm Output

Steps:

1. Enter the Alarm Output Settings interface:
Configuration>Advanced Configuration>Events > Alarm Output
2. Select one alarm output channel in the **Alarm Output** drop-down list.
3. Set a name in for the alarm output (optional).
4. The **Delay** time can be set to **5sec, 10sec, 30sec, 1min, 2min, 5min, 10min** or **Manual**. The delay time refers to the time duration that the alarm output remains in effect after alarm occurs.
5. Click  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 *Step 2* in **Section 7.6.1 Configuring Motion Detection**.

The screenshot shows the 'Alarm Output Settings' interface. At the top, there are three fields: 'Alarm Output' with a dropdown menu showing 'A->1', 'Alarm Name' with a text input field and '(cannot copy)' to its right, and 'Delay' with a dropdown menu showing '5s'. Below these is a section titled 'Arming Schedule' with an 'Edit' button. The schedule is represented by a grid with days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun) on the vertical axis and a 24-hour time scale (0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24) on the horizontal axis. Each cell in the grid contains a vertical line, indicating that the alarm is armed throughout the entire 24-hour period for every day of the week.

Figure 7-46 Alarm Output Settings

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



7.6.5 Handling Exception

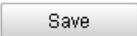
The exception type can be HDD full, HDD error, network disconnected, IP address conflicted and illegal login to the PTZ camera.

Steps:

1. Enter the Exception Settings interface:
Configuration > Advanced Configuration > Events > Exception
2. Check the checkbox to set the actions taken for the Exception alarm.
Refer to Step 3 in **Section 7.6.1 Configuring Motion Detection**.

The screenshot shows the 'Exception Settings' interface. At the top, there is a dropdown menu for 'Exception Type' set to 'HDD Full'. Below this are two sections: 'Normal Linkage' and 'Other Linkage'. The 'Normal Linkage' section has two checkboxes: 'Notify Surveillance Center' and 'Send Email', both of which are currently unchecked. The 'Other Linkage' section has a 'Trigger Alarm Output' checkbox which is checked, followed by a 'Select All' checkbox which is unchecked. Below these are two more checkboxes: 'A->1' and 'A->2', both of which are currently unchecked.

Figure 7-47 Exception Settings

3. Click  to save the settings.



7.6.6 Detecting Audio Exception

Purpose:

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

Steps:

1. Enter the video audio exception detection interface:

Configuration > Advanced Configuration > Events > Audio Exception Detection

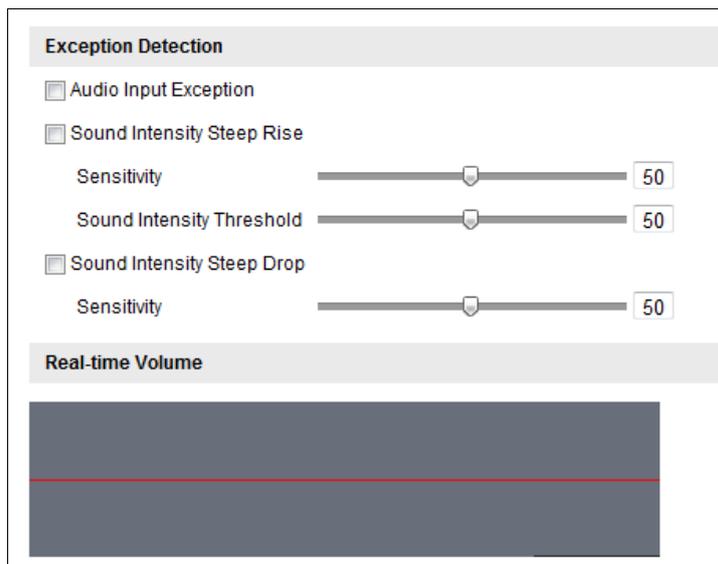
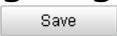


Figure 7-48 Audio Exception Detection

2. Check the checkbox of **Audio Input Exception** to enable the audio input exception detection.
3. Check the checkbox of **Sudden Intensity Steep Rise** checkbox to enable the sudden rise detection.
 - **Sensitivity:** Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
 - **Sound Intensity Threshold:** Range [1-100], it can filter the sound in the environment, the louder the environment sound, the higher the value should be. You can adjust it according to the actual environment.
4. Check the checkbox of **Sudden Intensity Steep Drop** checkbox to enable the sudden drop detection.

Sensitivity: Range [1-100], the smaller the value the more severe the sound change will trigger the detection.
5. Click to edit the arming schedule. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Step 2* in **Section 7.6.1 Configuring Motion Detection**.

6. Check the checkbox to select the linkage method taken for audio exception. Notify surveillance center, send email, trigger alarm output, etc. are selectable. Please refer to *Step 3* in **Section 7.6.1 Configuring Motion Detection**.
7. Click  to save the settings.



7.6.7 Configuring Dual-VCA

Purpose:

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

Steps:

1. Enter the Dual-VCA function configuration interface.
Configuration > Advanced Configuration > Video/Audio > Display Info. on Stream
2. Check the **Enable Dual-VCA** checkbox.
3. Click  to save the settings.

7.6.8 Configuring Intrusion Detection

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

Steps:

1. Enter the intrusion detection interface:
Configuration > Advanced Configuration > Events > Intrusion Detection
2. Check the **Enable Intrusion Detection** checkbox.

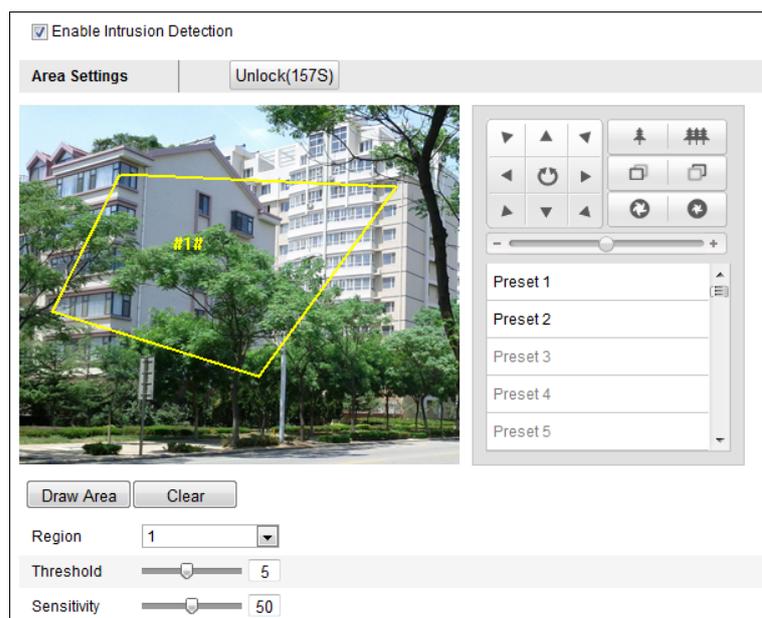


Figure 7-49 Configuring Intrusion Area

3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the intrusion detection interface. Optionally, you can click the **Unlock(170S)** button to manually activate the movement, or lock the movement when the button turns to **Lock** by clicking it.
4. Draw area.
 - (1) Select the Region No.in dropdown list.
 - (2) Click **Draw Area** to draw a rectangle on the image as a defense region.
 - (3) Click on the image to specify a corner of the rectangle, and right-click the mouse after four corners are configured.



Up to four areas are supported.

You can click **Clear** to clear the areas you drawn.

5. Configure the parameters for each defense region separately.
 - **Threshold:** Range [0-10s], the threshold for the time of the object loitering in the region. If you set the value as 0, alarm is triggered immediately after the object entering the region.
 - **Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm, when the sensitivity is high, a very small object can trigger the alarm.

6. Click to edit the arming schedule for tampering. The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Step 2* in **Section 7.6.1 Configuring Motion Detection**.
7. Check the checkbox to select the linkage method taken for the intrusion detection. Notify surveillance center, send email, trigger channel, smart tracking and trigger alarm output are selectable. Please refer to *Step 3* in **Section 7.6.1 Configuring Motion Detection**.
8. Click to save the settings.



7.6.9 Configuring Line Crossing Detection

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

Steps:

1. Enter the Line Crossing Detection interface:
Configuration > Advanced Configuration > Events > Line Crossing Detection
2. Check the **Line Crossing Detection** checkbox.
3. The event triggered and park action related PTZ movement will be locked for 180 seconds after you enter the line crossing detection interface. Optionally, you can click the button to manually activate the movement, or lock the movement when the button turns to by clicking it.

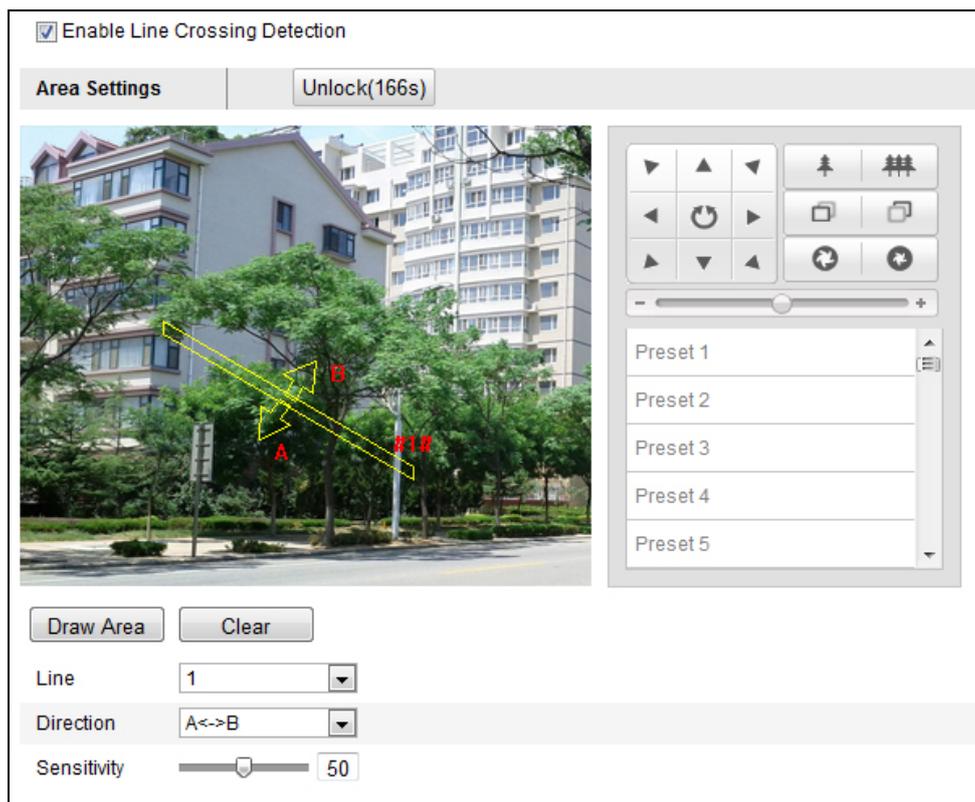


Figure 7-50 Configuring Line

4. Draw area.

- (1) Select the Line No.in dropdown list.
- (2) Click to draw a plane on the image.
- (3) Click the line to switch to the editing mode.

Click and drag an end to the desired place to adjust the length and angle of the plane. And click and on the line to adjust the location.



Up to 4 lines are supported.

5. Configure the parameters for each defense region separately.

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

6. Click to edit the arming schedule for line crossing detection.

The arming schedule configuration is the same as the setting of the arming schedule for motion detection. Refer to *Step 2* in **Section 7.6.1**

Configuring Motion Detection.

7. Check the checkbox to select the linkage method taken for the line crossing detection. Notify surveillance center, send email, upload to FTP, trigger channel, and trigger alarm output are selectable. Please refer to *Step 3* in **Section 7.6.1 Configuring Motion Detection**.
8. Click  to save the settings.



Chapter 8 Record Settings

Before you start:

To configure record settings, please make sure that you have the network storage device within the network or the storage card has been inserted in the corresponding card slot. Refer to the installation guide for the location of the storage card slot.

8.1 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. Enter the NAS (Network-Attached Storage) Settings interface:
Configuration > Advanced Configuration > Storage > NAS
2. Select the NAS type as NFS or SMB/CIFS. If you select SMB/CIFS, you need to enter the User Name and Password.

HDD No.	Type	Server Address	File Path
1	NAS		
	Mounting Type	NFS	User Name <input type="text"/> Password <input type="text"/>
		NFS	
2	NAS		

Figure 8-1 Select NAS Type

3. Enter the IP address of the network disk. The default NFS storage format of file path is `/dvr/test` as shown in Figure 8-2. And the default SMB/CIFS storage format of file path is `/test`.

HDD No.	Type	Server Address	File Path
1	NAS	10.99.105.249	/dvr/test
2	NAS		
3	NAS		
4	NAS		

Figure 8-2 Add Network Disk

4. Click to add the network disk.



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



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

8.2 Initializing and Configuring Storage

Steps:

1. Initialize the local disk or 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.
 - (2) If the status of the disk is **Uninitialized** as shown in Figure 8-3, check the corresponding checkbox to select the disk and click to start initializing the disk.

HDD Device List							<input type="button" value="Format"/>
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input checked="" type="checkbox"/>	9	0.96GB	0.00GB	Uninitialized	NAS	R/W	

Figure 8-3 Initialize Disk

HDD Device List							<input type="button" value="Format"/>
<input checked="" type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input checked="" type="checkbox"/>	9	39.06GB	0.00GB	Uninitialized	NAS	R/W	7%

Figure 8-4 Initializing

When the initialization completed, the status of disk will become **Normal** as shown in Figure 8-5.

HDD Device List							<input type="button" value="Format"/>
<input type="checkbox"/>	HDD No.	Capacity	Free space	Status	Type	Property	Progress
<input type="checkbox"/>	9	39.06GB	38.75GB	Normal	NAS	R/W	

Figure 8-5 View Disk Status

2. Configure the quota for saving the video and picture. Enter the percentage for picture and record in the text filed, and the total percentage must be 100%.

Quota	
Max. Picture Capacity	49.50GB
Free Size for Picture	49.50GB
Max. Record Capacity	149.25GB
Free Size for Record	149.25GB
Percentage of Picture	25 %
Percentage of Record	75 %

Figure 8-6 Setting Quota



8.3 Configuring Recording Schedule

Before you start:

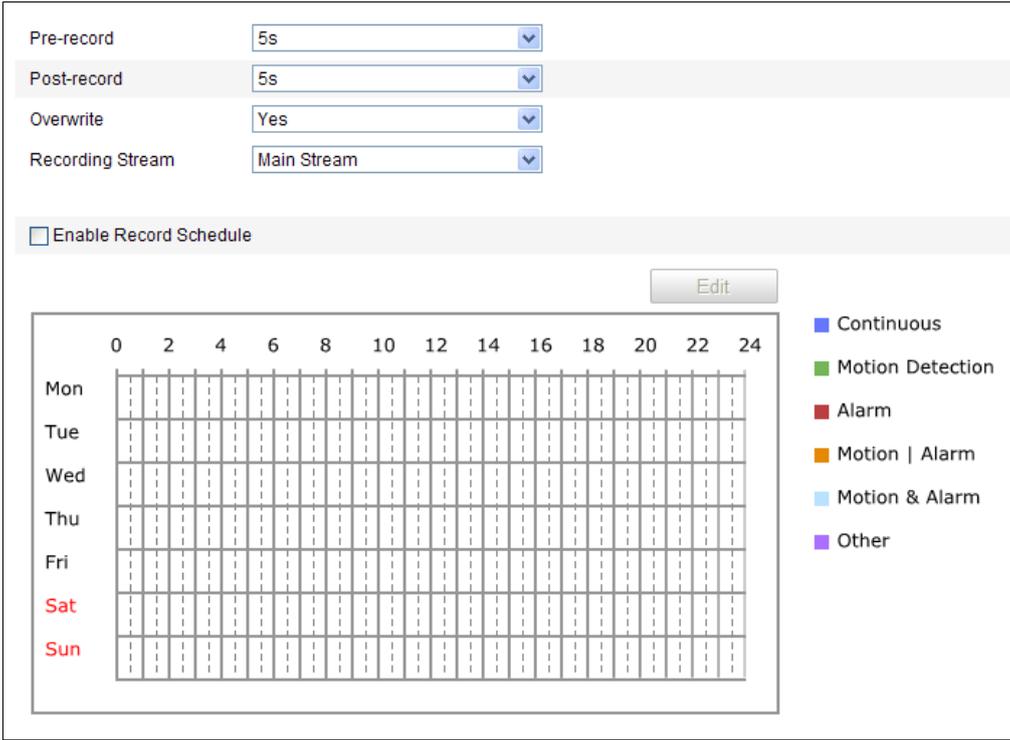
Please make sure a local storage card is inserted in the PTZ camera or the network storage is added to the PTZ camera, and is initialized.

Purpose:

There are two kinds of recording for the PTZ camera: manual recording and scheduled recording. For the manual recording, refer to **Section 5.4 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:

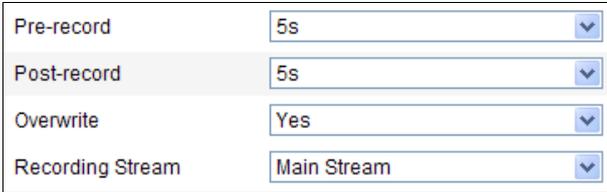
1. Enter the Record Schedule Settings interface:
Configuration > Advanced Configuration > Storage > Record Schedule



The interface shows recording parameters and a schedule grid. The parameters are: Pre-record (5s), Post-record (5s), Overwrite (Yes), and Recording Stream (Main Stream). Below these is a checkbox for 'Enable Record Schedule' which is currently unchecked. To the right of the grid is an 'Edit' button. The grid shows days of the week (Mon-Sun) and hours (0-24). A legend on the right indicates recording modes: Continuous (blue), Motion Detection (green), Alarm (red), Motion | Alarm (orange), Motion & Alarm (light blue), and Other (purple).

Figure 8-7 Recording Schedule Interface

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



The parameters are: Pre-record (5s), Post-record (5s), Overwrite (Yes), and Recording Stream (Main Stream).

Figure 8-8 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 PTZ camera starts to record at 9:59:55.
The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.



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

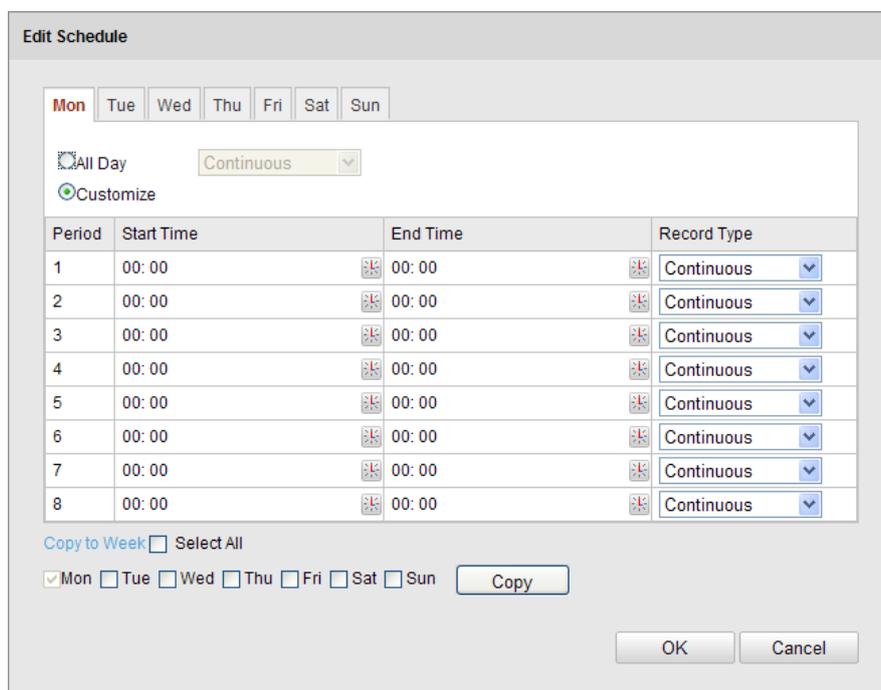
- **Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the PTZ camera records until 11:00:05.
The Post-record time can be configured as 5 s, 10 s, 30 s, 1 min, 2 min, 5 min or 10 min.



The Pre-record and Post-record parameters vary depending on the PTZ camera model.

- **Overwrite:** If you enable this function and the HDD is full, the new record files overwrite the oldest record files automatically.
- **Recording Stream:** You can select the stream type for recording; Main stream and Sub Stream are selectable. If you select the sub stream, you can record for a longer time with the same storage capacity.

4. Click  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 8-9 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**.



The time of each segment cannot be overlapped. Up to 8 segments can be configured for each day.

- (2) Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, Face Detection, Intrusion Detection, Line Crossing Detection, Audio Exception

Detection and All events.

◆ **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 in the **Section 7.6.1 Configuring Motion Detection***.

◆ **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 7.6.3 Configuring External Alarm Input**.

◆ **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 7.6.1** and **Section 7.6.3** 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 7.6.1** and **Section 7.6.3** for detailed information.

◆ **Record Triggered by Line Crossing Detection**

If you select **Line Crossing Detection**, the video will be recorded when the line crossing detection is triggered.

Besides configuring the recording schedule, you have to configure the settings on the **Line Crossing Detection** interface. Please refer to **Section 7.6.9** for detailed information.

◆ **Record Triggered by Intrusion Detection**

If you select **Intrusion Detection**, the video will be recorded when an intrusion is detected.

Besides configuring the recording schedule, you have to configure

the settings on the **Intrusion Detection** interface. Please refer to **Section 7.6.8** for detailed information.

◆ **Record Triggered by Audio Exception Detection**

If you select **Audio Exception Detection**, the video will be recorded when the audio exception is detected.

Besides configuring the recording schedule, you have to configure the settings on the **Audio Exception Detection** interface. Please refer to **Section 7.6.6** for detailed information.

◆ **Record Triggered by All Events**

If you select **All Events**, the video will be recorded when any event is detected.

(3) Check the checkbox **Select All** and click to copy settings of this day to the whole week. You can also check any of the checkboxes before the date and click .

(4) Click to save the settings and exit the Edit Record Schedule interface.

6. Click to save the settings.



8.4 Configuring Snapshot Settings

Purpose:

You can configure the scheduled snapshot and event-triggered snapshot. You can upload the captured pictures to a FTP server.

● **Basic Settings**

Steps:

1. Enter the Snapshot Settings interface:

Configuration > Advanced Configuration > Storage > Snapshot

Timing																																																																																																																	
<input checked="" type="checkbox"/> Enable Timing Snapshot																																																																																																																	
Format	JPEG																																																																																																																
Resolution	1920*1080																																																																																																																
Quality	High																																																																																																																
Interval	0 millisecond																																																																																																																
<input type="button" value="Edit"/>																																																																																																																	
<table border="1"> <thead> <tr> <th></th> <th>0</th><th>2</th><th>4</th><th>6</th><th>8</th><th>10</th><th>12</th><th>14</th><th>16</th><th>18</th><th>20</th><th>22</th><th>24</th> </tr> </thead> <tbody> <tr><td>Mon</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Tue</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Wed</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Thu</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Fri</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Sat</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>Sun</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>			0	2	4	6	8	10	12	14	16	18	20	22	24	Mon														Tue														Wed														Thu														Fri														Sat														Sun													
	0	2	4	6	8	10	12	14	16	18	20	22	24																																																																																																				
Mon																																																																																																																	
Tue																																																																																																																	
Wed																																																																																																																	
Thu																																																																																																																	
Fri																																																																																																																	
Sat																																																																																																																	
Sun																																																																																																																	
Event-Triggered																																																																																																																	
<input checked="" type="checkbox"/> Enable Event-Triggered Snapshot																																																																																																																	
Format	JPEG																																																																																																																
Resolution	1920*1080																																																																																																																
Quality	High																																																																																																																
Interval	0 millisecond																																																																																																																
Capture Number	4																																																																																																																

Figure 8-10 Snapshot Settings

2. Check the **Enable Timing Snapshot** checkbox to enable continuous snapshot, and configure the schedule of timing snapshot. Check the **Enable Event-triggered Snapshot** checkbox to enable event-triggered snapshot.
3. Select the quality of the snapshot.
4. Set the time interval between two snapshots.
5. Click to save the settings.



● Uploading to FTP



Please make sure that the FTP server is online.
You can follow below configuration instructions to upload the snapshots to FTP.

◆ Upload continuous snapshots to FTP

Steps:

- 1) Check the **Enable Timing Snapshot** checkbox.
- 2) Configure the FTP settings and check Upload Picture checkbox in FTP Settings interface. Please refer to **Section 7.3.7 Configuring FTP Settings** for more details to configure FTP parameters.



- ◆ Upload event-triggered snapshots to FTP

Steps:

- 1) Check the **Enable Event-triggered Snapshot** checkbox.
- 2) Configure the FTP settings and check Upload Picture checkbox in FTP Settings interface. Please refer to **Section 7.3.7 Configuring FTP Settings** for more details to configure FTP parameters.
- 3) Check Upload to FTP checkbox in Motion Detection Settings or Alarm Input interface. Please refer to *Step 3* in **Section 7.6.1 Configuring Motion Detection**.



Chapter 9 Playback

Purpose:

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

Task 1: To play back the video files

Steps:

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

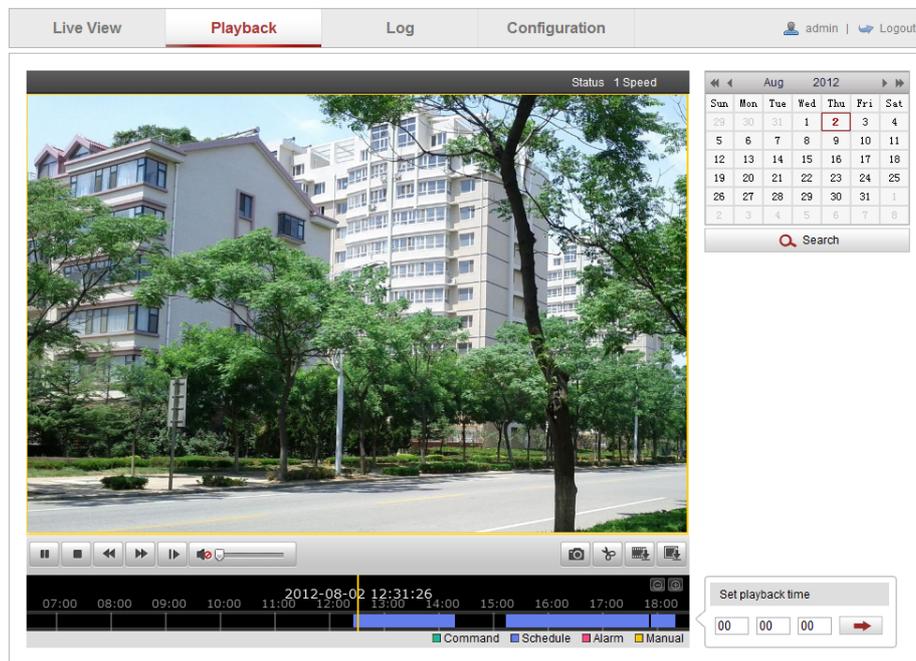


Figure 9-1 Playback Interface

2. Select the date and click .

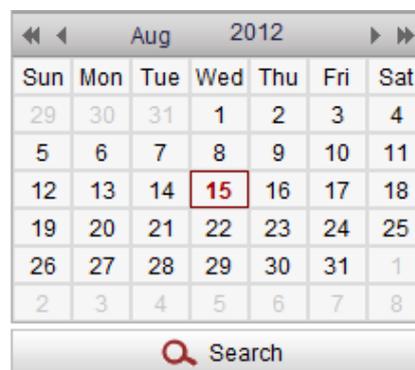


Figure 9-2 Search Video

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 9-3 Playback Toolbar

Table 9-1 Description of the buttons

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



You can choose the file paths locally for downloaded playback video files and pictures in Local Configuration interface. Please refer to **Section 7.1 Configuring Local Parameters** for details.

Drag the progress bar with the mouse to locate the exact playback point.

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

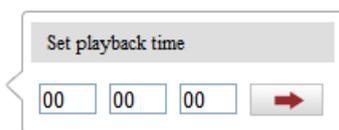


Figure 9-4 Set Playback Time



Figure 9-5 Progress Bar

The different colors of the video on the progress bar stand for the different video types as shown in Figure 9-6.

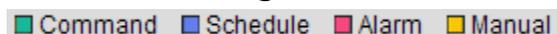


Figure 9-6 Video Types

Task 2: To download the video files

Steps:

1. Click  on the playback interface. The pop-up menu is shown in Figure 9-7.
2. Set the start time and end time. Click **Search**. The corresponding video files are listed on the left.

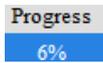
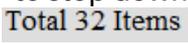


Total 23 Items [First Page](#) [Prev Page 1/1](#) [Next Page](#) [Last Page](#)

Figure 9-7 Video Downloading interface

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



- The progress ratio  displays the downloading ratio of the video file.
- You can click  to stop downloading.
- The total number  displays the amount of the video files.

Task 3: To download the captured pictures

Steps:

1. Click  on the playback interface. The pop-up menu is shown in Figure 9-8.

2. Set the linkage type of capturing the pictures as timing, alarm, motion, etc..
3. Set the start time and end time. Click **Search**. The corresponding picture files are listed on the left.
4. Check the checkbox in front of the files that you need to download.
5. Click  **Download** to download the files.

<input type="checkbox"/>	No.	File Name	File Date	File Size	Progress

Timing ▼

Start Time
2013-07-8 00:00:00 📅

End Time
2013-07-8 23:59:59 📅

 Search

 Download

Figure 9-8 Picture Downloading interface



Chapter 10 Log Searching

Purpose:

The operation, alarm, exception and information of the PTZ 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 PTZ camera or insert a SD card in the PTZ camera.

Steps:

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

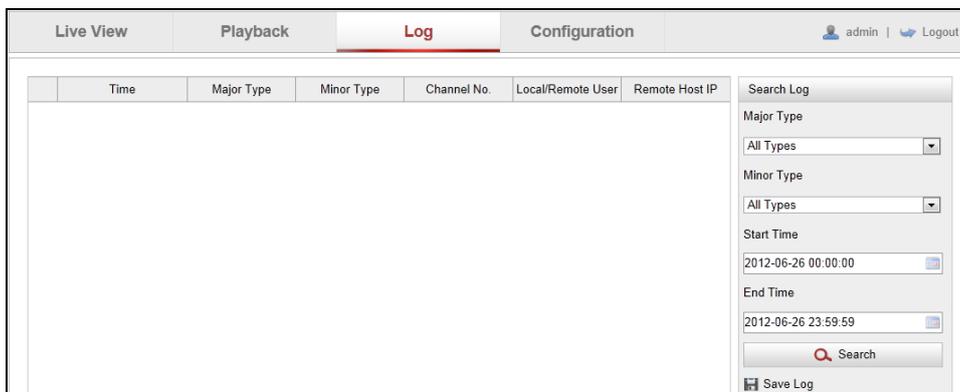


Figure 10-1 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time as shown in Figure 10-2.
3. Click  to search log files. The matched log files will be displayed on the **Log** interface.

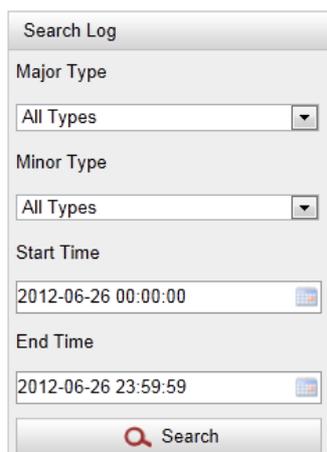


Figure 10-2 Log Searching

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



Chapter 11 Others

11.1 Managing User Accounts

Enter the User Management interface:

Configuration > Basic Configuration > Security > User

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

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

<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>		
No.	User Name	Level
1	admin	Administrator

Figure 11-1 User Information

11.1.1 Add a User

Steps:

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



The level indicates the permissions you give to the user. You can define the user as **Operator** or **User**.



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

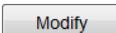
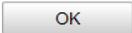
3. In the **Basic Permission** field and **Camera Configuration** field, you can check or uncheck the permissions for the new user.
4. Click to finish the user addition.

Figure 11-2 Add a User



11.1.2 Modify a User

Steps:

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



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

Figure 11-3 Modify a User



11.1.3 Delete a User

Steps:

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



11.2 Configuring RTSP Authentication

Purpose:

You can specifically secure the stream data of live view.

Steps:

1. Enter the RTSP Authentication interface:
Configuration > Advanced Configuration > Security > Authentication
2. Set the authentication mode for each authentication type.
RTSP Authentication: Select the authentication mode as basic or disable in the dropdown list to enable or disable the RTSP authentication.
3. Click to save the settings.



11.3 Configuring Anonymous Visit

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



Only live view is available for the anonymous user.

Steps:

1. Enter the Anonymous Visit interface:

Configuration > Advanced Configuration > Security > Anonymous Visit

The screenshot shows a configuration box with the label 'Anonymous Visit' on the left and a dropdown menu on the right. The dropdown menu is currently set to 'Enable'.

Figure 11-4 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.

The screenshot shows a login interface with two input fields: 'User Name' and 'Password'. Below the fields is a 'Login' button. At the bottom, there is a checkbox labeled 'Anonymous' which is checked.

Figure 11-5 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 speed dome 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.

11.4 Configuring IP Address Filter

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

Filter Type	Description
Forbidden	Forbid the IP addresses added in the IP Address Filter interface to log in.
Filter Type	Description
Allowed	Allow only the IP addresses added in the IP Address Filter interface to log in.

Enable IP Address Filter
 IP Address Filter Type: Forbidden

IP Address Filter

No.	IP
1	172.6.21.119

Figure 11-6 IP Address Filter

11.5 Configuring Security Service Settings

Steps:

1. Enter the Security Service interface:
Configuration > Advanced Configuration > Security > Security Service
2. Check the checkbox to enable the SSH function.
Enable SSH: Enabling SSH (Secure Shell) function is to encrypt and compress the data and to reduce the transmission time.
3. Click to save the settings.



11.6 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 PTZ camera, such as Model, Device No., 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.

Basic Information	
Device Name	<input type="text" value="IP DOME"/>
Device No.	<input type="text" value="88"/>
Model	XX-XXXXXXXXXX
Serial No.	XX-XXXXXXXXXXXXXXXXXXXXXXXXXX
Firmware Version	Vx.x.x build xxxxxx
Encoding Version	Vx.x build xxxxxx
Number of Channels	1
Number of HDDs	0
Number of Alarm Input	1
Number of Alarm Output	1

Figure 11-7 Device Information

11.7 Maintenance

11.7.4 Rebooting the PTZ camera

Steps:

1. Enter the Maintenance interface:
Configuration > Basic Configuration > System > Maintenance
 Or **Configuration > Advanced Configuration > System > Maintenance:**

2. Click to reboot the network PTZ camera.



Figure 11-8 Reboot the Device



11.7.5 Restoring Default Settings

Steps:

1. Enter the Maintenance interface:
Configuration > Basic Configuration > System > Maintenance
 Or **Configuration > Advanced Configuration > System > Maintenance**
2. Click or to restore the default settings.



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

Default	
<input type="button" value="Restore"/>	Reset all the parameters, except the IP parameters and user information, to the default settings.
<input type="button" value="Default"/>	Restore all parameters to default settings.

Figure 11-9 Restore Default Settings



11.7.6 Importing/Exporting Configuration File

Steps:

1. Enter the Maintenance interface:
Configuration > Basic Configuration > System > Maintenance
 Or **Configuration > Advanced Configuration > System > Maintenance**
2. Click to select the local configuration file and then click to start importing configuration file.



You need to reboot the PTZ camera after importing configuration file.

3. Click and set the saving path to save the configuration file in local storage.

Figure 11-10 Import/Export Configuration File



11.7.7 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.
 - **Firmware:** when you select **Firmware**, you need to find the firmware in your computer to upgrade the device.
 - **Firmware Directory:** You need to find the directory where the firmware locates. The device can find the firmware in the directory automatically.
3. Click to select the local upgrade file and then click to start remote upgrade.



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

Figure 11-11 Remote Upgrade



11.8 Configuring RS-485

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:

1. Enter RS-485 Port Setting interface:

Configuration > Advanced Configuration > System > RS485

Baud Rate	9600 bps
Data Bit	8
Stop Bit	1
Parity	None
Flow Ctrl	None
PTZ Protocol	PELCO_P
PTZ Address	1

Figure 11-12 RS-485 Settings

2. Set the RS-485 parameters and click to save the settings.



The Baud Rate, PTZ Protocol and PTZ Address parameters of the PTZ camera should be exactly the same as those of the control device.



11.9 Configuring Remote Connection

Steps:

1. Enter the interface of configuring the remote connection:
Configuration > Advanced Configuration > System > Service
2. Input a number in text field as the upper limit of the remote connection number. E.g. when you specify the remote connection number as 10, then the 11th remote connection cannot be established.

Software	
Live View Connection	10

3. Click the button to activate the settings.

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.

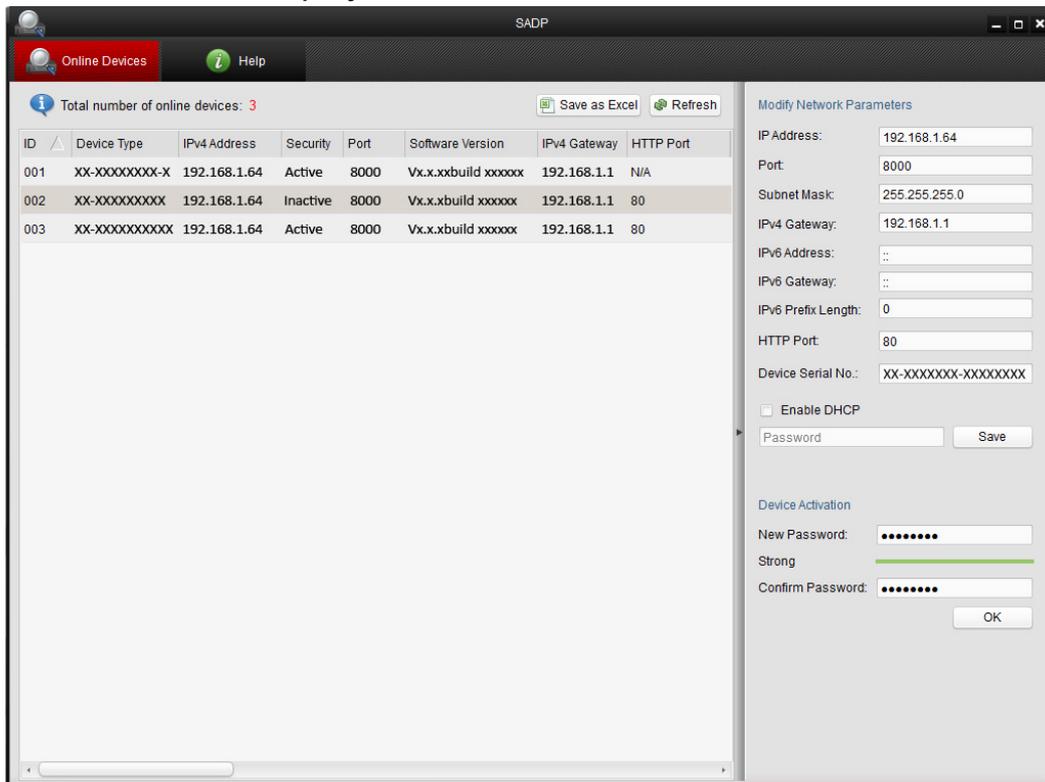


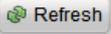
Figure A.1.1 Searching Online Devices



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

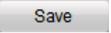
You can also click  to refresh the online device list manually. The newly searched devices will be added to the list.



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 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:

Port:

Subnet Mask:

IPv4 Gateway:

IPv6 Address:

IPv6 Gateway:

IPv6 Prefix Length:

Serial No.:

 Note: Enter the admin password of the device before you save the network parameters.

Figure A.1.2 Modify Network Parameters



Appendix 2 Port Mapping

The following settings are for TP-LINK router (TL-R410). The settings vary depending on different models of routers.

Steps:

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

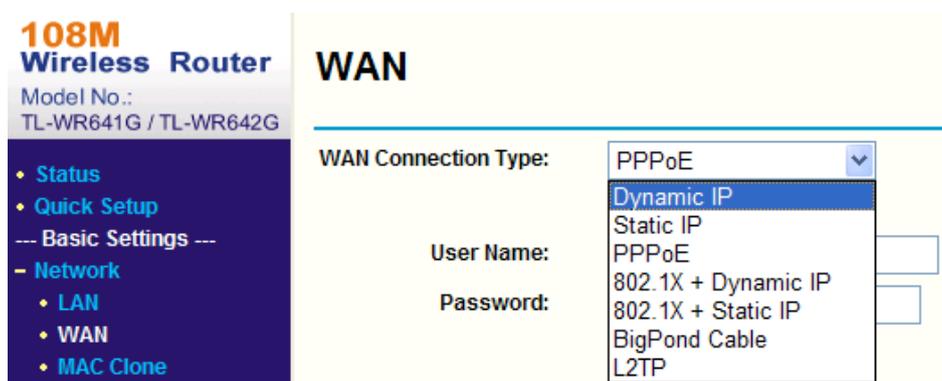


Figure A-3 Select the WAN Connection Type

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

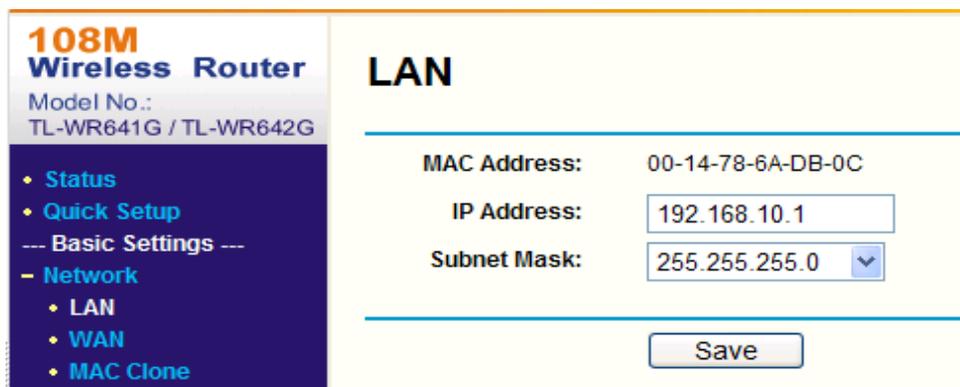


Figure A-4 Set the LAN parameters

3. Set the port mapping in the virtual servers of **Forwarding**. You need to forward ports 80, 8000, 8200~8210 and 554 for a PTZ camera.



- You can change 80, 8000 and 554 ports value in the PTZ camera with web browser or client software.
- In the PTZ camera, the 8200~8210 ports change with the 8000 port with a constant value of 200. E.g. if the 8000 port is changed to 8005, then the 8200~8210 ports should be changed to 8205~8215.

Example:

When the PTZ cameras are connected to the same router, you can forward the ports of a PTZ camera as 80, 8000, 8200~8210 and 554 with IP address 192.168.1.23, and the ports of another PTZ camera as 81, 8001, 8201~8211 and 555 with IP 192.168.1.24. Refer to the steps below:

Steps:

1. As the settings mentioned above, forward the port 80, 8000, 8200~8210 and 554 for the network PTZ camera at 192.168.1.23
2. Forward the port 81, 8001, 8201~8211 and 555 for the network PTZ camera at 192.168.1.24.
3. Enable ALL or TCP protocols.
4. Check the Enable checkbox and click .

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	<input checked="" type="checkbox"/>
2	8000	192.168.10.23	ALL	<input checked="" type="checkbox"/>
3	554	192.168.10.23	ALL	<input checked="" type="checkbox"/>
4	8200	192.168.10.23	ALL	<input checked="" type="checkbox"/>
5	81	192.168.10.24	ALL	<input checked="" type="checkbox"/>
6	8001	192.168.10.24	ALL	<input checked="" type="checkbox"/>
7	555	192.168.10.24	ALL	<input checked="" type="checkbox"/>
8	8201	192.168.10.24	ALL	<input checked="" type="checkbox"/>

Common Service Port: ID

Figure A-5 Port Mapping



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

Appendix 3 Bubble Maintenance

The bubble is a transparent plastic. The dust, oil and finger print, etc. will cause scratch or image blur. Please refer to the following method to clean the bubble.

- Handling dust

Use oil free soft brush or blowing dust ball to clean the dust.

- Handling oil

Steps:

1. Wipe off the water-drop or oil by soft cloth and dry the bubble.
2. Use oil free cotton cloth to wipe the bubble with alcohol or detergent.
3. Change the cloth to wipe the bubble until the bubble is clean.

Appendix 4 12VDC Wire Gauge & Transmission Distance

The following table describes the recommended max. distance adopted for the certain wire gauge when the loss rate of 12VDC voltage is less than 15%. For the DC driven device, the maximum voltage loss rate is 15% allowable.

Distance (feet) \ Wire Gauge (mm)	0.800(20)	1.000(18)	1.250 (16)	2.000(12)
10	97(28)	153(44)	234(67)	617(176)
20	49(14)	77(22)	117(33)	308(88)
24	41(12)	64(18)	98(28)	257(73)
30	32(9)	51(15)	78(22)	206(59)
40	24(7)	38(11)	59(17)	154(44)
48	20(6)	32(9)	49(14)	128(37)
50	19(6)	31(9)	47(13)	123(35)
60	16(5)	26(7)	39(11)	103(29)
70	14(4)	22(6)	33(10)	88(25)
80	12(3)	19(5)	29(8)	77(22)
90	10.8(3.1)	17(5)	26(7)	69(20)
100	9.7(2.8)	15(4)	23(7)	62(18)
110	8.9(2.5)	14(4)	21(6)	56(16)
120	8.1(2.3)	13(4)	20(6)	51(15)
130	7.5(2.1)	11.8(3.4)	18(5)	47(14)
140	7(2)	11(3.1)	17(5)	44(13)
150	6.5(1.9)	10.2(2.9)	16(4)	41(12)
160	6.1(1.7)	9.6(2.7)	15(4)	39(11)
170	5.7(1.6)	9(2.6)	14(4)	36(10)
180	5.4(1.5)	8.5(2.4)	13(4)	34(10)

Appendix 5 Table of Wire Gauge Standards

Bare Wire Gauge(mm)	American Wire Gauge AWG	British Wire Gauge SWG	Cross-sectional Area of Bare Wire(mm ²)
0.750	21		0.4417
0.800	20	21	0.5027
0.900	19	20	0.6362
1.000	18	19	0.7854
1.250	16	18	1.2266
1.500	15	17	1.7663
2.000	12	14	3.1420

2.500			4.9080
3.000			7.0683

Appendix 6 Alarm In/Out Connections



This section is only for the PTZ cameras with alarm in/out functions. The PTZ camera can be connected with alarm inputs (0~5VDC) and alarm outputs. Refer to the following diagrams for alarm output:

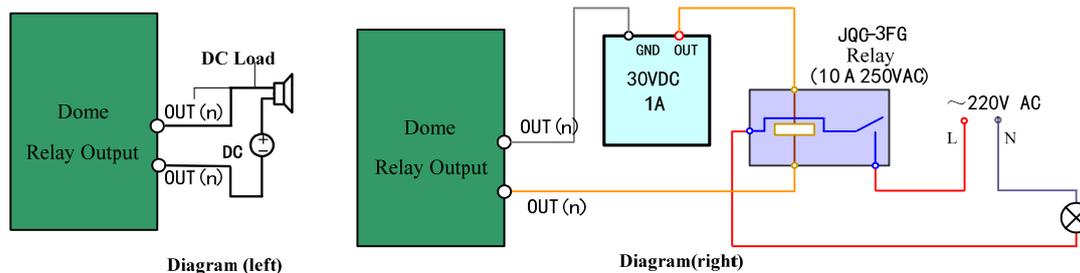


Figure A-6 Alarm Out Connections

The alarm provides the relay output (no voltage), and the external power supply is required when it connects to the alarm device.

- For DC power supply (left diagram), the input voltage must be no more than 30VDC, 1A.
- For AC power supply, the external relay must be used (right diagram) to prevent damages to the PTZ camera and avoid risk of electric shock.

ALLNET GmbH Computersysteme declares that the device **ALL-CAM2372-WP** is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. The Declaration of conformity can be found under this link:
www.allnet.de/downloads.html.

GPL Declaration for ALLNET products

DISCLAIMER_OF_WARRANTY

This Program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; version 2 of the License.

This Program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this Program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

The full text of the GNU General Public License version 2 is included with the software distribution in the file LICENSE.GPLv2

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Written Offer for Source Code

For binaries that you receive from ALLNET GmbH Computersysteme on physical media or within the download of the offered firmware that are licensed under any version of the GNU General Public License (GPL) or the GNU LGPL, you can receive a complete machine-readable copy of the source code by sending a written request to:

ALLNET GmbH Computersysteme
Maistrasse 2
82110 Germering

Your request should include: (i) the name of the covered binary, (ii) the version number of the ALLNET product containing the covered binary, (iii) your name, (iv) your company name (if applicable) and (v) your return mailing and email address (if available). We may charge you a nominal fee to cover the cost of the media and distribution. Your request must be sent within three (3) years of the date you received the GPL or LGPL covered code. For your convenience, some or all of the source code may also be found at:

<http://www.allnet.de/gpl.html>

LICENSE.GPLv2
GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or

a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
 - b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
 - c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
 - a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
 - c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this

License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Also add information on how to contact you by electronic and paper mail. If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

LICENSE.LGPLv2.1

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be

consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms.

A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
 - a) The modified work must itself be a software library.
 - b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
 - c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
 - d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a

newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions

files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.
- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.
- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.
- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:
 - a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.
 - b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.
8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.
10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients'

exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK

- AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library 'Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!