Network Fisheye Camera

User Manual
UD.6L0201D1996A01
User Manual

COPYRIGHT ©2015 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

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

About this Manual

This Manual is applicable to Network Fisheye Camera (V5.3.3).

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

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

Hikvision® and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY,
FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

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

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

**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.

<table>
<thead>
<tr>
<th>Warnings</th>
<th>Cautions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Follow these safeguards to prevent serious injury or death.</td>
<td>Follow these precautions to prevent potential injury or material damage.</td>
</tr>
</tbody>
</table>

**Warnings:**

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

- Make sure the power supply voltage is correct before using the camera.
- Do not drop the camera or subject it to physical shock.
- Do not touch sensor modules with fingers. If cleaning is necessary, use a clean cloth with a bit of ethanol and wipe it gently. If the camera will not be used for an extended period of time, put on the lens cap to protect the sensor from dirt.
- Do not aim the camera lens at the strong light such as sun or incandescent lamp. The strong light can cause fatal damage to the camera.
- The sensor may be burned out by a laser beam, so when any laser equipment is being used, make sure that the surface of the sensor not be exposed to the laser beam.
- Do not place the camera in extremely hot, cold temperatures (the operating temperature should be between -30°C ~ 60°C, or -40°C ~ 60°C if the camera model has an “H” in its suffix), dusty or damp environment, and do not expose it to high electromagnetic radiation.
- To avoid heat accumulation, good ventilation is required for a proper operating environment.
- Keep the camera away from water and any liquid.
- While shipping, the camera should be packed in its original packing.
- Improper use or replacement of the battery may result in hazard of explosion.
  Please use the manufacturer recommended battery type.

Notes:

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

- Dust or grease on the dome cover will cause IR reflection. Please do not remove the dome cover film until the installation is finished. If there is dust or grease on the dome cover, clean the dome cover with clean soft cloth and isopropyl alcohol.
- Make certain the installation location does not have reflective surfaces of objects
too close to the camera. The IR light from the camera may reflect back into the lens causing reflection.

- The foam ring around the lens must be seated flush against the inner surface of the bubble to isolate the lens from the IR LEDs. Fasten the dome cover to camera body so that the foam ring and the dome cover are attached seamlessly.

0503031050521
# Table of Contents

**Chapter 1** System Requirement .................................................................................. 10

**Chapter 2** Network Connection .................................................................................. 11

2.1 Setting the Network Camera over the LAN ............................................................... 11

   2.1.1 Wiring over the LAN ......................................................................................... 11

   2.1.2 Creating a Password ......................................................................................... 12

2.2 Setting the Network Camera over the WAN ............................................................. 18

   2.2.1 Static IP Connection .......................................................................................... 18

   2.2.2 Dynamic IP Connection .................................................................................... 19

**Chapter 3** Access to the Network Camera .................................................................. 22

3.1 Accessing by Web Browsers ...................................................................................... 22

3.2 Accessing by Client Software .................................................................................... 24

**Chapter 4** Live View .................................................................................................. 25

4.1 Live View Page .......................................................................................................... 25

4.2 Starting Live View ...................................................................................................... 26

4.3 Recording and Capturing Pictures Manually ............................................................. 27

4.4 Operating e-PTZ Control ............................................................................................ 28

   4.4.1 e-PTZ Control Panel ......................................................................................... 28

   4.4.2 Setting / Calling / Deleting a Preset ................................................................. 29

   4.4.3 Setting / Calling / Deleting a Patrol ................................................................. 31

**Chapter 5** Network Camera Configuration ................................................................. 34

5.1 Configuring Local Parameters .................................................................................... 34

5.2 Configuring Time Settings ........................................................................................ 36

5.3 Configuring Network Settings .................................................................................. 38

   5.3.1 Configuring TCP/IP Settings ............................................................................. 38

   5.3.2 Configuring Port Settings ............................................................................... 39

   5.3.3 Configuring PPPoE Settings ............................................................................ 40

   5.3.4 Configuring DDNS Settings ............................................................................ 40

   5.3.5 Configuring SNMP Settings ........................................................................... 43

   5.3.6 Configuring 802.1X Settings ........................................................................... 44

   5.3.7 Configuring QoS Settings ................................................................................. 45

   5.3.8 Configuring UPnP™ Settings ........................................................................... 46

   5.3.9 Email Sending Triggered by Alarm ................................................................. 47

   5.3.10 Configuring NAT Settings ............................................................................. 49

   5.3.11 Configuring FTP Settings ............................................................................... 49

   5.3.12 Configuring Wi-Fi Settings ............................................................................ 51

   5.3.13 Configuring HTTPS Settings ......................................................................... 56
Chapter 9
5.4 Configuring Video and Audio Settings .................................................. 58
  5.4.1 Configuring Video Settings ........................................... 58
  5.4.2 Configuring Audio Settings ........................................ 59
  5.4.3 Configuring ROI Encoding ........................................... 60
  5.4.4 Displaying Info on Stream ............................................ 61
5.5 Configuring Image Parameters ........................................................... 62
  5.5.1 Configuring Display Settings .......................................... 62
  5.5.2 Configuring OSD Settings ........................................... 65
  5.5.3 Configuring Text Overlay ............................................. 66
  5.5.4 Configuring Privacy Mask ............................................ 66
5.6 Configuring and Handling Alarms ......................................................... 67
  5.6.1 Configuring Motion Detection ....................................... 68
  5.6.2 Configuring Video Tampering Alarm ............................... 72
  5.6.3 Configuring Alarm Input ............................................. 73
  5.6.4 Configuring Alarm Output .......................................... 74
  5.6.5 Handling Exception ................................................... 75
  5.6.6 Configuring Line Crossing Detection ............................... 76
  5.6.7 Configuring Intrusion Detection ................................... 77
Chapter 6 Storage Settings ........................................................................ 79
  6.1 Configuring NAS Settings .................................................. 79
  6.2 Configuring Recording Schedule ........................................... 81
  6.3 Configuring Snapshot Settings ............................................ 84
Chapter 7 Playback ..................................................................................... 87
Chapter 8 Log Searching ........................................................................... 90
Chapter 9 Others ......................................................................................... 91
  9.1 Managing User Accounts .................................................... 91
  9.2 Authentication ............................................................................ 93
  9.3 Anonymous Visit .......................................................................... 94
  9.4 IP Address Filter ........................................................................ 94
  9.5 Security Service ........................................................................... 96
  9.6 Viewing Device Information ..................................................... 97
  9.7 Maintenance ................................................................................ 97
    9.7.1 Rebooting the Camera ................................................... 97
    9.7.2 Restoring Default Settings ............................................. 98
    9.7.3 Exporting / Importing Configuration File ......................... 98
    9.7.4 Upgrading the System .................................................. 99
  9.8 RS-232 Settings ............................................................................. 99

8
9.9  DST Settings ............................................................... 100
9.10 RS-485 Settings............................................................ 101
9.11 Service Settings............................................................ 102
9.12 Fisheye Parameters....................................................... 102

Appendix ............................................................................. 104

Appendix 1 SADP Software Introduction............................... 104
Appendix 2 Port Mapping....................................................... 106
Chapter 1 System Requirement

**Operating System:** Microsoft Windows XP SP1 and above version

**CPU:** 2.0 GHz or higher

**RAM:** 1G or higher

**Display:** 1024×768 resolution or higher

**Web Browser:** Internet Explorer 8.0 and above version, Apple Safari 5.0.2 and above version, Mozilla Firefox 5.0 and above version and Google Chrome 18 and above version
Chapter 2  Network Connection

Note:

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

Before you start:

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

2.1  Setting the Network Camera over the LAN

Purpose:

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

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

2.1.1  Wiring over the LAN

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

Purpose:

- To test the network camera, you can directly connect the network camera to the computer with a network cable as shown in Figure 2-1.
- Refer to the Figure 2-2 to set network camera over the LAN via a switch or a router.

![Connecting Directly](image1)

**Figure 2-1 Connecting Directly**

![Connecting via a Switch or a Router](image2)

**Figure 2-2 Connecting via a Switch or a Router**

### 2.1.2 Creating a Password

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

Creating a Password via Web Browser, Creating a Password via SADP, and Creating a Password via Client Software are all supported.

- **Creating a Password via Web Browser**

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

  **Notes:**
  - The default IP address of the camera is 192.168.1.64.
  - For the camera enables the DHCP by default, the IP address is allocated automatically. And you need to activate the camera via SADP software. Please refer to the following chapter for Activation via SADP.
3. Create a password and input the password into the password field.

![Figure 2-3 Creating a Password via Web Browser](image)

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

4. Confirm the password.

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

❖ **Creating a Password via SADP Software**

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

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

**Steps:**

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

2. Check the device status from the device list, and select the inactive device.
3. Create a password and input the password in the password field, and confirm the password.

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

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

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

5. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.
6. Input the password and click the **Save** button to activate your IP address modification.

- **Creating a Password via Client Software**

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

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

  **Steps:**

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

![Figure 2-5 Modify the IP Address](image-url)
2. Click the **Device Management** icon to enter the Device Management interface, as shown in the figure below.
3. Check the device status from the device list, and select an inactive device.

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

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

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

   ![Activation Interface (Client Software)](image)

   Figure 2-8 Activation Interface (Client Software)

6. Click **OK** button to start activation.

7. Click the Modify Netinfo button to pop up the Network Parameter Modification interface, as shown in the figure below.
8. Change the device IP address to the same subnet with your computer by either modifying the IP address manually or checking the checkbox of Enable DHCP.

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

## 2.2 Setting the Network Camera over the WAN

**Purpose:**

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

### 2.2.1 Static IP Connection

**Before you start:**

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

- Connecting the network camera via a router

**Steps:**

1. Connect the network camera to the router.
2. Assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.

3. Save the static IP in the router.

4. Set port mapping, e.g., 80, 8000, and 554 ports. The steps for port mapping vary according to the different routers. Please call the router manufacturer for assistance with port mapping.

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

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

![Figure 2-10 Accessing the Camera through Router with Static IP](image)

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

![Figure 2-11 Accessing the Camera with Static IP Directly](image)

### 2.2.2 Dynamic IP Connection

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

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

*Steps:*
1. Connect the network camera to the router.

2. In the camera, assign a LAN IP address, the subnet mask and the gateway. Refer to Section 2.1.2 for detailed IP address configuration of the network camera.

3. In the router, set the PPPoE user name, password and confirm the password.

4. Set port mapping. E.g. 80, 8000, and 554 ports. The steps for port mapping vary depending on different routers. Please call the router manufacturer for assistance with port mapping.

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

5. Apply a domain name from a domain name provider.

6. Configure the DDNS settings in the setting interface of the router.

7. Visit the camera via the applied domain name.

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

  **Purpose:**

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

  ![Diagram](image)

  **Figure 2-12 Accessing the Camera with Dynamic IP**

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

  ◆ **Normal Domain Name Resolution**
Figure 2-13 Normal Domain Name Resolution

**Steps:**

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

Private Domain Name Resolution

**Steps:**

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

3.1  Accessing by Web Browsers

Steps:

1. Open the web browser.

2. Input the IP address of the network camera in the address bar, e.g., 192.168.1.64 and press the Enter key to enter the login interface.

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

![Login Interface]

Figure 3-1 Login Interface

Notes:

Switch the display language from the upper-right corner between Chinese and English.

4. Install the plug-in before viewing the live video and operating the camera. Please follow the installation prompts to install the plug-in.
Figure 3-2 Download and Install Plug-in

Figure 3-3 Install Plug-in (1)

Figure 3-4 Install Plug-in (2)

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

3.2 Accessing by Client Software

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

Follow the installation prompts to install the software. The control panel interface of iVMS-4200 client software is shown as bello.

![Figure 3-5 iVMS-4200 Client Software](image)

**Note:** For detailed information about the software, please refer to the user manual of the iVMS-4200 Client Software.
Chapter 4  Live View

4.1 Live View Page

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

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

**Descriptions of the live view page:**

![Live View Page](image)

**Figure 4-1 Live View Page**

**Menu Bar:**  
Click the tab to enter Live View, Playback, Log and Configuration page respectively.

**Aspect Ratio:**  
Click the icon to adjust the length-to-width ratio of each display window. 4:3, 16:9, original and auto are selectable.

**Stream Type:**  
Select main stream or sub stream for live view.

**Live View Mode:**
Display the live video in Fisheye View, Panorama View, or PTZ View.

- **Fisheye View:** In the Fisheye View mode, the whole wide-angle view of the fisheye camera is displayed. This view mode is called Fisheye View because it approximates the vision of a fish’s convex eye. The lens produces curvilinear images of a large area, while distorting the perspective and angles of objects in the image.

- **Panorama View:** In the Panorama View mode, the distorted fisheye image is transformed to normal perspective image by some calibration methods.

- **PTZ View:** The PTZ View is the close-up view of some defined area in the Fisheye View or Panorama View, and it supports the electronic PTZ function, which is also called e-PTZ.
  
  *Note:* Each PTZ View is marked on the Fisheye View and Panorama View with a specific navigation box.

**Live View Window:**
Display the live video on the display window of live view.

**Live View Toolbar:**
Start / Stop the live view, enable / disable the two-way audio, adjust the audio volume, capture pictures and record the video files.

**e-PTZ Control:**
Realize the pan / tilt / zoom function of PTZ view via the navigation box, and set the PTZ moving speed.

**Preset/Patrol Settings:**
Set and call the preset/patrol for the camera.

### 4.2 Starting Live View

Click the **Live View** tab to open the Live View Page.

You can click the icon ▶ / ■ on the toolbar to start / stop the live view of the camera.
Table 4-1 Descriptions of Live View Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>The length-to-width ratio of image display window is 4:3.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>The length-to-width ratio of image display window is 16:9.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Window size for original video stream.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Self-adaptive window size.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Click to show / hide the e-PTZ Control panel.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Start/Stop live view.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Display the live video in full screen.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Enable / Disable the two-way audio.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Adjust the audio volume.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Manually capture the picture during live view.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Manually start/stop recording.</td>
</tr>
</tbody>
</table>

*Note:* The two-way audio function varies according to the camera model.

### 4.3 Recording and Capturing Pictures Manually

In the live view interface, click ![Icon] on the toolbar to capture the live pictures or click ![Icon] to record the live video. The saving paths of the captured pictures and
record files can be set on the Configuration > Local Configuration page. To configure remote scheduled recording, please refer to Section 6.2.

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

4.4 Operating e-PTZ Control

Purpose:
The PTZ View is the close-up view of some defined area on the panoramic / fisheye view, and it supports digital PTZ control, also called e-PTZ control function.

When PTZ View is selected for live view, you can use the e-PTZ control buttons to realize pan / tilt / zoom control of the PTZ View.

![Live View](image)

Figure 4-3 e-PTZ Control

Note: If Fisheye View or Panorama View is selected for live view together with the PTZ View, a navigation box related to the PTZ View is displayed on the Fisheye View or Panorama View.

4.4.1 e-PTZ Control Panel

On the live view page, you can click to show the e-PTZ control panel or click
Figure 4-4 e-PTZ Control Panel

Table 4-2 Descriptions of e-PTZ Control Panel

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direction Arrows</td>
<td>Direction Arrows</td>
</tr>
<tr>
<td>Auto Scan</td>
<td>Auto Scan</td>
</tr>
<tr>
<td>Zoom in/out</td>
<td>Zoom in/out</td>
</tr>
<tr>
<td></td>
<td>Adjust speed of pan/tilt movements</td>
</tr>
</tbody>
</table>

**Steps:**

1. Click to select a PTZ View on the display window, and then the navigation box appears on the Fisheye View and Panorama View.
2. Click the direction arrows on the e-PTZ control panel, and the navigation box will move in the corresponding pan/tilt direction.
3. Click the icon / to zoom in/zoom out.
4. Click-and-drag the slider on the speed bar to adjust the moving speed of PTZ View in the corresponding pan/tilt direction.

**4.4.2 Setting / Calling / Deleting a Preset**

- **Setting a Preset:**

  **Purpose:**
  A preset for the Fisheye camera is a predefined PTZ View which contains information of pan, tilt, focus and other parameters.

  **Steps:**
1. Click to select a PTZ View on the display window.
2. Click the direction / zoom buttons on the e-PTZ Control panel to adjust the PTZ View as desired.
3. Select a preset number from the preset list.
4. Click the icon 🏷️ to save the current PTZ View as the preset.
   The preset name turns from grey to black.

![Figure 4-5 Setting a Preset](image)

*Note:* Up to 256 presets are supported.

- **Calling a Preset:**

  **Purpose:**
  The PTZ View of the Fisheye camera can directly and quickly move to the area of interest, which is defined as a preset.

  **Before you start:**
  Set the preset, and the icon ➡️ and 🏷️ will appear on the preset list.

  **Steps:**
  1. Click to select a PTZ View on the display window.
  2. Select the preset number from the list.
  3. Click the icon ➡️ to call the selected preset.
     The selected PTZ View will move to the pre-defined preset scene.
Deleting a Preset

Steps:
1. Select the preset number from the list.
2. Click the icon to delete the selected preset.

   The preset name turns from black to grey.

4.4.3 Setting / Calling / Deleting a Patrol

Purpose:
A patrol is a scanning track specified by a group of defined presets, with the duration
time at each preset separately programmable.

**Before you start:**

At least 2 presets are required to set a patrol.

- **Setting a Patrol**

  **Steps:**

  1. Click the icon 🔄 to enter the patrol configuration interface.

  ![Figure 4-8 Patrol Configuration](image)

  2. Select a path No. from the drop-down list, and click the icon 📞 in the lower-left corner to add the presets as the key points.

  ![Figure 4-9 Setting Key Point of Patrol](image)

  3. Select the defined preset from the drop-down list, input the duration time at each preset, and click **OK** to save the preset as the key point of patrol.

  4. Repeat Step 3 to set other key points of the patrol.
5. Click the icon 📦 to save the current patrol path.

**Note:** Up to 32 patrol paths can be set, and each path supporting 16 key points at most.

- **Calling a Patrol**

  **Steps:**
  1. Click to select a PTZ View on the display window.
  2. Select the patrol path number from the drop-down list.
  3. Click the icon 📦 to call the selected patrol path.

- **Deleting a Patrol**

  1. Select the patrol path number from the drop-down list.
  2. Click the icon 🗑 to delete the key point of the patrol path one by one.

    You can also click the icon 🗑 to directly delete the patrol path.
Chapter 5  Network Camera Configuration

5.1 Configuring Local Parameters

Purpose:
Local configuration provides live view parameters settings, record file settings and picture and clip settings. The recorded videos and captured pictures can be saved on the local PC running the web browser.

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

![Local Configuration Interface]

Figure 5-1 Local Configuration Interface

2. Configure the following settings:
   - **Live View Parameters**: Set the protocol type and live view performance.
     - **Protocol Type**: TCP, UDP, MULTICAST and HTTP are selectable.
     - **TCP**: Ensures complete delivery of streaming data and better video quality, yet the real-time transmission will be affected.
UDP: Provides real-time audio and video streams.

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

MULTICAST: It’s recommended to select MCAST type when using the Multicast function. For detailed information about Multicast, refer to Section 5.3.1 Configuring TCP/IP Settings.

- **Live View Performance:** Set the live view performance to Shortest Delay or Auto.

- **Rules:** It refers to the rules on your local browser, select enable or disable to display or not display the colored marks when the motion detection, or intrusion detection is triggered. E.g.: If motion detection and rules are both enabled, when a moving object is detected, it will be marked with a green rectangle on the live video.

- **Image Format:** The captured picture can be saved in format of *.jpeg or *.bmp.

- **Record File Settings:** Set the saving path of the recorded video files. Valid for the record files you recorded with the web browser.

  - **Record File Size:** Select the packed size of the manually recorded and downloaded video files to 256M, 512M or 1G. After the selection, the maximum record file size is the value you selected.

  - **Save record files to:** Set the saving path for the manually recorded video files.

  - **Save downloaded files to:** Set the saving path for the downloaded video files in playback mode.

- **Picture and Clip Settings:** Set the saving paths of the captured pictures and clipped video files. Valid for the pictures you captured with the web browser.

  - **Save snapshots in live view to:** Set the saving path of the manually captured pictures in live view mode.

  - **Save snapshots when playback to:** Set the saving path of the captured pictures in playback mode.
Save clips to: Set the saving path of the clipped video files in playback mode.

*Note:* You can click **Browse** to change the directory for saving the clips and pictures.

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

## 5.2 Configuring Time Settings

**Purpose:**

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

**Steps:**

1. Enter the Time Settings interface:

   Configuration > Basic Configuration > System > Time Settings

   Or Configuration > Advanced Configuration > System > Time Settings

   ![Time Settings](image)

   **Figure 5-2 Time Settings**

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

   ✦ Synchronizing Time by NTP Server.

   (1) Check the **NTP** item to enable the NTP function.

   (2) Configure the following settings:

   - **Server Address:** IP address of NTP server.
   - **NTP Port:** Port of NTP server.
   - **Interval:** The time interval between the two synchronizing actions with NTP
server.

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

![Time Sync by NTP Server](image)

Figure 5-3 Time Sync by NTP Server

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

♦ Synchronizing Time Manually

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

(2) Click the icon ![icon] to open the calendar page.

(3) Click on the calendar to select the date, set the time, and click **OK** to save.

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

![Time Sync Manually](image)

Figure 5-4 Time Sync Manually

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

**Note:** For region using the summer time, DST settings are required to be configured. Please refer to *Section 9.9 DST Settings* for detailed information.
5.3 Configuring Network Settings

5.3.1 Configuring TCP/IP Settings

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

Steps:
1. Enter TCP/IP Settings interface:
   Configuration > Basic Configuration > Network > TCP/IP
   
Or Configuration > Advanced Configuration > Network > TCP/IP

2. Configure the basic network settings, including the NIC Type, IPv4 or IPv6 Address, IPv4 or IPv6 Subnet Mask, IPv4 or IPv6 Default Gateway, MTU settings and Multicast Address.

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

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

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

### 5.3.2 Configuring Port Settings

**Purpose:**

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

**Steps:**

1. Enter the Port Settings interface:
   
   **Configuration > Basic Configuration > Network > Port**  
   
   Or **Configuration > Advanced Configuration > Network > Port**

   ![Port Settings Table](image)

   Figure 5-6 Port Settings

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

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

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

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

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

3. Click **Save** to save the settings.
5.3.3 Configuring PPPoE Settings

Steps:
1. Enter the PPPoE Settings interface:

   Configuration > Advanced Configuration > Network > PPPoE

   Figure 5-7 PPPoE Settings

2. Check the Enable PPPoE checkbox to enable this feature.
3. Enter User Name, Password, and Confirm password for PPPoE access.
   Note: The User Name and Password should be assigned by your ISP.
4. Click Save to save and exit the interface.
   Note: A reboot is required for the settings to take effect.

5.3.4 Configuring DDNS Settings

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

Before you start:
Registration on the DDNS server is required before configuring the DDNS settings of the camera.

Steps:
1. Enter the DDNS Settings interface:

   Configuration > Advanced Configuration > Network > DDNS
2. Check the **Enable DDNS** checkbox to enable this feature.

3. Select **DDNS Type**. Four DDNS types are selectable: HiDDNS, IPServer, DynDNS and NO-IP.
   - **DynDNS**:
     
     **Steps:**
     
     1. Enter **Server Address** of DynDNS (e.g. members.dyndns.org).
     2. In the **Domain** text field, enter the domain name obtained from the DynDNS website.
     3. Enter the **Port** of DynDNS server.
     4. Enter the **User Name** and **Password** registered on the DynDNS website.
     5. Click **Save** to save the settings.

   **Figure 5-9 DynDNS Settings**

   - **IP Server**:
     
     **Steps:**
     
     1. Enter the Server Address of the IP Server.
     2. Click **Save** to save the settings.
**Note:** For the IP Server, you have to apply a static IP, subnet mask, and gateway and preferred DNS from the ISP. The **Server Address** should be entered with the static IP address of the computer that runs the IP Server software.

![IPServer Settings](image)

**Figure 5-10** IPServer Settings

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

- **NO-IP:**

  **Steps:**

  1. Choose the DDNS Type as NO-IP.

    ![NO-IP DNS Settings](image)

    **Figure 5-11** NO-IP DNS Settings

    2. Enter the Server Address as [www.noip.com](http://www.noip.com)

    3. Enter the Domain name you registered.

    4. Enter the Port number, if needed.

    5. Enter the User Name and Password.

    6. Click **Save** and then you can view the camera with the domain name.

- **HiDDNS**

  **Steps:**

  1. Choose the DDNS Type as HiDDNS.
(2) Enter the Server Address `www.hik-online.com`.

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

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

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

### 5.3.5 Configuring SNMP Settings

*Purpose:*

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

*Before you start:*

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

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

*Steps:*

1. Enter the SNMP Settings interface:

   **Configuration > Advanced Configuration > Network > SNMP**
2. Check the corresponding version checkbox (Enable SNMP SNMPv1, Enable SNMPv2c, Enable SNMPv3) to enable the feature.

3. Configure the SNMP settings.

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

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

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

### 5.3.6 Configuring 802.1X Settings

**Purpose:**

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

*Note:* 802.1X settings vary according to the camera model.

*Before you start:*

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

*Steps:*

1. Enter the 802.1X Settings interface:

   **Configuration > Advanced Configuration > Network > 802.1X**

   ![Figure 5-14 802.1X Settings](image)

2. Check the **Enable IEEE 802.1X** checkbox to enable the feature.

3. Configure the 802.1X settings, including EAPOL version, user name and password.

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

4. Enter the user name and password to access the server.

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

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

### 5.3.7 Configuring QoS Settings

*Purpose:*

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

*Steps:*

1. Enter the QoS Settings interface:

   **Configuration > Advanced Configuration > Network > QoS**
2. Configure the QoS settings, including video / audio DSCP, event / alarm DSCP and Management DSCP.

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

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

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

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

### 5.3.8 Configuring UPnP™ Settings

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

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

**Steps:**

1. Enter the UPnP™ settings interface.

   **Configuration > Advanced Configuration > Network > UPnP**

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

   The name of the device when detected online can be edited.
5.3.9 Email Sending Triggered by Alarm

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

**Before you start:**
Please configure the DNS Server settings under **Basic Configuration > Network > TCP/IP** or **Advanced Configuration > Network > TCP/IP** before using the Email function.

**Steps:**
1. Enter the TCP/IP Settings (**Configuration > Basic Configuration > Network > TCP/IP** or **Configuration > Advanced Configuration > Network > TCP/IP**) to set the IPv4 Address, IPv4 Subnet Mask, IPv4 Default Gateway and the Preferred DNS Server.
   
   **Note:** Please refer to **Section 5.3.1 Configuring TCP/IP Settings** for detailed information.

2. Enter the Email Settings interface:
   
   **Configuration > Advanced Configuration > Network > Email**
3. Configure the following settings:

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

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

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

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

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

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

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

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

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

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

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

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

### 5.3.10 Configuring NAT Settings

**Purpose:**

1. Enter the NAT settings interface.

   ![Configuration > Advanced Configuration > Network > NAT](image)

2. Choose the port mapping mode.

   **To port mapping with the default port numbers:**

   Choose **Auto** as the port mapping mode

   **To port mapping with the customized port numbers:**

   Choose **Manual** as the port mapping mode

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

   ![Enable Port Mapping](image)

   ![Configure NAT Settings](image)

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

### 5.3.11 Configuring FTP Settings

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

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

2. Configure the FTP settings; and the user name and password are required for login the FTP server.

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

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

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

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

3. (Optional) You can click the **Test** button to test the settings.

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

   **Note:** If you want to upload the captured pictures to FTP server, you have to
enable the continuous snapshot or event-triggered snapshot on **Snapshot** page. For detailed information, please refer to the Section 6.3.

5.3.12 Configuring Wi-Fi Settings

*Purpose:*

By connecting to the wireless network, you don’t need to use cable of any kind for network connection, which is very convenient for the actual surveillance application. *Note:* This chapter is only applicable for the cameras with the built-in Wi-Fi module.

**Configuring Wi-Fi Connection in Manage and Ad-hoc Modes**

- **Wireless Connection in Manage Mode**

1. Enter the Wi-Fi Settings interface:
   - **Configuration > Advanced Configuration > Network > Wi-Fi**

   ![Wireless Network List](5-20)

   Figure 5-20 Wireless Network List

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

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

4. Check the checkbox to select the **Network mode as Manager**, and the **Security mode** of the network is automatically shown when you select the wireless network, please don’t change it manually.

   ![Wi-Fi Settings - Manage Mode](5-21)

   Figure 5-21 Wi-Fi Settings-Manage Mode
Note: These parameters are exactly identical with those of the router.

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

6. Click Save to save the settings

➢ Wireless Connection in Manager 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.

1. Check the checkbox to select the Network mode as Ad-Hoc.

![Figure 5-22 Wi-Fi Setting- Ad-hoc]

2. Customize a SSID for the camera.


![Figure 5-23 Security Mode- Ad-hoc Mode]

4. Enable the wireless connection function for your PC.

5. On the PC side, search the network and you can see the SSID of the camera listed.

![Figure 5-24 Ad-hoc Connection Point]
6. Choose the SSID and connect.

**Easy Wi-Fi Connection with WPS function**

*Purpose:*
The setting of the wireless network connection is never easy. To avoid the complex setting of the wireless connection you can enable the WPS function. WPS (Wi-Fi Protected Setup) refers to the easy configuration of the encrypted connection between the device and the wireless router. The WPS makes it easy to add new devices to an existing network without entering long passphrases. There are two modes of the WPS connection, the PBC mode and the PIN mode. *Note:* If you enable the WPS function, you do not need to configure the parameters such as the encryption type and you don’t need to know the key of the wireless connection.

*Steps:*

![Wi-Fi Settings - WPS](image)

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

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

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

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

4. Push the WPS button to enable the function on the camera.

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

5. Click **Connect** button.

   ![PBC connection](image)

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.

   ![Wi-Fi Settings](image)

   **Figure 5-26 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.

4. **Click Generate.**

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

**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> Basic Configuration> Network> TCP/IP**
   - **Or Configuration> Advanced Configuration> Network> TCP/IP**

   ![Figure 5-27 TCP/IP Settings](image)

2. Select the NIC as wlan.

3. (Optional) You can check the checkbox of **DHCP** to automatically get the assigned IP address.

4. Customize the IPv4 address, the IPv4 Subnet Mask and the Default Gateway.
   The setting procedure is the same with that of LAN. For details, see Section 5.3.1 **Configuring TCP/IP Settings**.
5.3.13 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.

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

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

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

![Figure 5-28 HTTPS Settings](image)

- Create the self-signed certificate
  
  (1) Click **Create** button to enter the creation interface.
(2) Enter the country, host name/IP, validity and other information.

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

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

♦ Create the authorized certificate

(1) Click **Create** button to create the certificate request.

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

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

3. There will be the certificate information after you successfully create and install the certificate.

4. Click the **Save** button to save the settings.
5.4 Configuring Video and Audio Settings

5.4.1 Configuring Video Settings

Steps:
1. Enter the Video Settings interface:

   Configuration > Basic Configuration > Video / Audio > Video

   Or Configuration > Advanced Configuration > Video / Audio > Video

2. Select the Stream Type of the camera to main stream (normal), sub-stream.
   The main stream is usually for recording and live view with good bandwidth, and
   the sub-stream can be used for live viewing when the bandwidth is limited.

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

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

   **Resolution:**
   Select the resolution of the video output.

   **Bitrate Type:**
   Select the bitrate type to constant or variable.
Video Quality:
When bitrate type is selected as Variable, 6 levels of video quality are selectable.

Frame Rate:
Set the frame rate to 1/16~25 fps. The frame rate is to describe the frequency at which the video stream is updated and it is measured by frames per second (fps). A higher frame rate is advantageous when there is movement in the video stream, as it maintains image quality throughout.

Max. Bitrate:
Set the max. bitrate to 32~16384 Kbps. The higher value corresponds to the higher video quality, but the higher bandwidth is required.

Video Encoding:
If the Stream Type is set to main stream, H.264 is selectable, and if the stream type is set to sub stream, H.264 and MJPEG are selectable.

Note: The supported video encoding may differ according to the different platform.

Profile:
Main Profile for H.264 coding is selectable.

I Frame Interval:
Set the I-Frame interval to 1~400.

SVC:
Scalable Video Coding is an extension of the H.264/AVC standard. Set it OFF or ON according to your actual needs.

4. Click Save to save the settings.

5.4.2 Configuring Audio Settings

Steps:
1. Enter the Audio Settings interface
   Configuration > Basic Configuration > Video / Audio > Audio
   Or Configuration > Advanced Configuration > Video / Audio > Audio
2. Configure the following settings.

   **Audio Encoding**: G.711 ulaw, G.711alaw, G.726, G.722.1 and MP2L2 are selectable. And 32kbps, 64kbps, and 128kbps are supported if MP2L2 is selected.

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

   **Input Volume**: 0-100

   **Environmental Noise Filter**: Set it as OFF or ON. When you set the function on the noise detected can be filtered.

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

   **Note**: The audio settings vary according to the camera model.

### 5.4.3 Configuring ROI Encoding

ROI stands for the region of interest. And the ROI encoding enables you to discriminate the ROI and background information in compression, that is to say, the technology assigns more encoding resource to the region of interest to increase the quality of the ROI whereas the background information is less focused.

**Steps**:

1. Enter the ROI settings interface

   **Configuration > Advanced Configuration > Video / Audio >ROI**
2. Check the checkbox of **Enable** under Fixed Region item.
3. Select the stream type for ROI encoding.
4. Select the region No. from the drop-down list for ROI settings. There are four fixed regions selectable.
5. Click the **Draw Area** button, and then click-and-drag the mouse to draw the region of interest on the live video.
6. Select the ROI level to set the image quality enhancing level. The larger the value is, the better the image quality is.
7. Input the region name for ROI as desired.
8. Click **Save** to save the settings.

### 5.4.4 Displaying Info on Stream

Check the checkbox to enable the function of Dual-VCA which can be used cooperatively with NVR to implement dual-VCA retrieval during playback.
5.5 Configuring Image Parameters

5.5.1 Configuring Display Settings

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

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

**Steps:**
1. Enter the Display Settings interface:
   Configuration > Basic Configuration > Image > Display Settings
   Or Configuration > Advanced Configuration > Image > Display Settings
2. Set the image parameters of the camera.
   **Note:** In order to guarantee the image quality in the different illumination, it provides two sets of parameters for user to configure.

**Day/Night Auto-switch**
Figure 5-35  Display Settings of Day/night Auto-switch

♦ Image Adjustment

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

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

**Hue** adjusts color of the image.

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

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

♦ Exposure Settings

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

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

♦ Day/Night Switch

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

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

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

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

**Schedule:** The camera switches between the day mode and the night mode according to the configured time period.

**Triggered by Alarm Input:** The camera switches to the day mode or the night mode after the alarm is triggered.
**Smart IR**: Smart IR function gives user an option to adjust the power of the IR LED, thus avoiding image over-exposure.

Set the smart IR to **ON**, and Auto and Manual are selectable for IR mode. Select AUTO, and the IR LED changes according to the actual luminance. E.g.: if the current scene is bright enough, then the IR LED adjusts itself to lower power; and if the scene is not bright enough, the IR LED adjusts itself to higher power.

Select Manual, and you can adjust the IR LED by adjusting the distance. E.g.: If the object is near the camera, the device adjusts the IR LED to lower power, and the IR LED is in higher power if the object is far.

◊ **Backlight Settings**

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

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

◊ **White Balance**

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

◊ **Image Enhancement**

**Digital Noise Reduction**: DNR reduces the noise in the video stream. Select **ON**/**OFF** to enable / disable the digital noise reduction function. If the function is enabled, set the DNR level from 0 to 100, and the default value is 50.

◊ **Video Adjustment**

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

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

**Capture Mode**: It’s the selectable video input mode to meet the different demands of field of view and resolution.
5.5.2 Configuring OSD Settings

**Purpose:**
You can customize the camera name and time on the screen.

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

   ![Figure 5-36 OSD Settings](image)

   **Figure 5-36 OSD Settings**

2. Check the corresponding checkbox to select the display of camera name, date or week if required.
3. Edit the camera name in the text field of Camera Name.
4. Select from the drop-down list to set the time format, date format, display mode and the OSD font size.
5. You can use the mouse to click-and-drag the Time and Camera Name text frames in the live view window to adjust the OSD position.
6. Set the font color for the OSD text. You can select Black&White Self-adaptive and can also customize the color as desired.
7. Click **Save** to save the settings.
5.5.3 Configuring Text Overlay

*Purpose:*
You can set the content of the text overlay and display some customized information on the live video.

*Steps:*
1. Enter the Text Overlay Settings interface:

   **Configuration > Advanced Configuration > Image > Text Overlay**

   ![Text Overlay Settings](image)

   Figure 5-37 Text Overlay Settings

2. Check the checkbox in front of text field to enable the on-screen display.

3. Input the characters in the text field.

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

5. Click *Save* to save the settings.

   *Note:*
   Up to 4 text overlays are configurable.

5.5.4 Configuring Privacy Mask

*Purpose:*
Privacy mask enables you to cover certain areas on the live video to prevent certain spots in the surveillance area from being live viewed and recorded.
Steps:
1. Enter the Privacy Mask Settings interface:
   \textbf{Configuration > Advanced Configuration > Image > Privacy Mask}

2. Check the checkbox of \textbf{Enable Privacy Mask} to enable this function.

3. Click the \textbf{Draw Area} button to start drawing.

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

5. Click \textbf{Stop Drawing} to finish drawing.

6. You can click \textbf{Clear All} to clear all the configured privacy masks.

7. Click \textbf{Save} to save the settings.

\textit{Note:} Up to 4 privacy masks are configurable.

5.6 Configuring and Handling Alarms

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

\textit{Note:} Check the checkbox of \textbf{Notify Surveillance Center} if you want to push the alarm information to the surveillance client such as the mobile phone, computer, etc.,
as soon as the alarm is triggered.

### 5.6.1 Configuring Motion Detection

**Purpose:**

Motion detection is a feature which can take alarm response actions and record the video for the motion occurred in the surveillance scene.

**Steps:**

1. Enter the Motion Detection Settings interface
   
   **Configuration > Advanced Configuration > Events > Motion Detection**
   
   ![Motion Detection Settings](image)
   
   Figure 5-39 Motion Detection Settings

2. Check the checkbox of **Enable Motion Detection**.

3. (Optional) Check the checkbox of **Enable Dynamic Analysis for Motion** if you want to mark the detected objects with green rectangles on the live view window.

   **Note:** You can go to **Configuration > Local Configuration > Live View Parameters > Rules**, and then select Disable for rules if you don’t want the detected objects displayed with the rectangles.

4. Configure the motion detection area settings.

   Two types of configuration modes are selectable: Normal mode and Expert mode.
   
   - **Normal Mode**

     If Normal is selected as the configuration mode, one set of parameters are adopted
for motion detection without considering the day / night switch.

![Motion Detection Settings](image)

**Figure 5-40 Motion Detection Settings-Normal Mode**

1. Click the **Draw Area** button to start drawing.
2. Click-and-drag the mouse on the live video to draw a motion detection area.
3. Click **Stop Drawing** to finish drawing.
4. Repeat above steps to draw other detection areas.
5. Click-and-drag the slider to set the sensitivity of the detection.
   - The sensitivity value ranges from 0 to 100. And the higher the value is, the easier the motion can be detected.
6. You can click **Clear All** to clear all of the configured areas.

- **Expert Mode**

  If Expert is selected as the configuration mode, different sets of parameters are adopted for motion detection at day and night.
Figure 5-41 Motion Detection Settings-Expert Mode

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 from the drop-down list.

3. Set the values of sensitivity and proportion of object on area for each 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.
Steps:

(1) Click **Edit** to edit the arming schedule.

(2) Choose the day you want to set the arming schedule.

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

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

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

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

6. Check the checkbox to set the alarm actions for Motion Detection.
Figure 5-44 Linkage Method

- **Notify Surveillance Center**
  Send an exception or alarm signal to remote management software when an event occurs.

- **Send Email**
  Send an email with alarm information to a user or users when an event occurs.
  **Note:** To send the Email when an event occurs, you need to refer to *Section 5.3.9* to set the related parameters.

- **Upload to FTP**
  Capture the image when an alarm is triggered and upload the picture to a FTP server.
  **Note:** Set the FTP address and the remote FTP server first. Refer to *Section 5.3.11* for detailed information.

- **Trigger Channel**
  The video will be recorded when the motion is detected. You have to set the recording schedule to realize this function. Please refer to *Section 6.2* for detailed information.

- **Trigger Alarm Output**
  Trigger one or more external alarm outputs when an event occurs.
  **Note:** To trigger an alarm output when an event occurs, please refer to *Section 5.6.4* to set the related parameters.

### 5.6.2 Configuring Video Tampering Alarm

**Purpose:**
You can configure the camera to trigger the alarm when the lens is covered and take
alarm response action.

Steps:

1. Enter the Tamper-proof Settings interface:
   - Configuration > Advanced Configuration > Events > Video Tampering

2. Check the checkbox of Enable Video Tampering to enable video tampering detection function.

![Figure 5-45 Video Tampering Detection Settings](image)

3. Set the detection area for video tampering. For details, refer to Step 4 in Section 5.6.1.

4. Click Edit to edit the arming schedule for video tampering detection. For details, refer to Step 5 in Section 5.6.1.

5. Check the checkbox to set the alarm actions for video tampering.
   Notify surveillance center, send email and trigger alarm output are selectable. For details, refer to Step 6 in Section 5.6.1.

6. Click Save to save the settings.

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

<table>
<thead>
<tr>
<th>Alarm Input No.</th>
<th>Alarm Name</th>
<th>Alarm Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Camera 01</td>
<td>NO</td>
</tr>
</tbody>
</table>

Alarm Input Settings

<table>
<thead>
<tr>
<th>Arming Schedule</th>
<th>Edit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 5-46 Alarm Input Settings

3. Click **Edit** to set the arming schedule for the alarm input. For details, refer to Step 5 in *Section 5.6.1*.

4. Check the checkbox to select the linkage method taken for the alarm input. For details, refer to Step 6 in *Section 5.6.1*.

5. (Optional) You can copy your settings to other alarm inputs.

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

*Note:* Alarm input settings vary according to the camera model.

### 5.6.4 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. (Optional) Input the alarm output name in the text field.

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 **Edit** to set the arming schedule for the alarm output. For details, refer to Step 5 in **Section 5.6.1**.

6. (Optional) You can copy the settings to other alarm outputs.

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

![Alarm Output Settings](image)

**Figure 5-47 Alarm Output Settings**

*Note*: Alarm output settings vary according to the camera model.

### 5.6.5 Handling Exception

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

**Steps:**

1. Enter the Exception Settings interface:
   
   **Configuration > Advanced Configuration> Events > Exception**

2. Check the checkbox to select the linkage method taken for exception. For details, refer to Step 6 in **Section 5.6.1**.

![Exception Settings](image)

**Figure 5-48 Exception Settings**
3. Click **Save** to save the settings.

### 5.6.6 Configuring Line Crossing Detection

**Purpose:**

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

**Steps:**

1. Enter the Line Crossing Detection settings interface:
   
   **Configuration > Advanced Configuration > Events > Line Crossing Detection**

2. Check the checkbox of **Enable Line Crossing Detection** to enable the function.

3. Click the **Draw Area** button, and a virtual line is displayed on the live video.

4. Click-and-drag the line, and you can locate it on the live video as desired.
   
   Click on the line, two red squares are displayed on each end, and you can click-and-drag one of the red squares to define the shape and length of the line.

5. Select the direction for line crossing detection. And you can select the directions as A<->B, A->B, and B->A.
   
   **A<->B:** Only the arrow on the B side shows; when an object going across the plane with both direction can be detected and alarms are triggered.
   
   **A->B:** Only the object crossing the configured line from the A side to the B side can be detected.
   
   **B->A:** Only the object crossing the configured line from the B side to the A side can be detected.

6. Click-and-drag the slider to set the detection sensitivity.
   
   Sensitivity: Range [1-100]. The higher the value is, the more easily the line crossing action can be detected.

7. You can click the **Clear** button to clear the pre-defined line.

9. Click the **Edit** button to set the arming schedule.

10. Select the linkage methods for line crossing detection, including Notify
Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.

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

![Line Crossing Detection Settings](image)

**Figure 5-49 Line Crossing Detection Settings**

### 5.6.7 Configuring Intrusion Detection

**Purpose:**

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

**Steps:**

1. Enter the Intrusion Detection settings interface:
   
   **Configuration > Advanced Configuration > Events > Intrusion Detection**

2. Check the checkbox of **Enable Intrusion Detection** to enable the function.

3. Click the **Draw Area** button to start the region drawing.

4. Click on the live video to specify the four vertexes of the detection region, and right click to complete drawing.

5. Set the time threshold, detection sensitivity and object percentage for intrusion
detection.

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

**Sensitivity:** Range [1-100]. The value of the sensitivity defines the size of the object which can trigger the alarm. When the sensitivity is high, a very small object can trigger the alarm.

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

6. You can click the **Clear** button to clear the pre-defined region.
7. Click the **Edit** button to set the arming schedule.
8. Select the linkage methods for intrusion detection, including Notify Surveillance Center, Send Email, Upload to FTP, Trigger Channel and Trigger Alarm Output.
9. Click **Save** to save the settings.

![Intrusion Detection Settings](image)

---

**Figure 5-50 Intrusion Detection Settings**
Chapter 6  Storage Settings

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

6.1 Configuring NAS Settings

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

Steps:
1. Add the network disk
   (1) Enter the NAS (Network-Attached Storage) Settings interface:

   
   ![Configuration > Advanced Configuration > Storage > NAS]

   
   Figure 6-1 Add Network Disk

   (2) Enter the IP address of the network disk, and enter the default file.

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

   (3) Click Save to add the network disk.

   Note: Reboot the camera to activate the settings.

2. Initialize the added network disk.
   (1) Enter the HDD Settings interface:

   
   Configuration > Advanced Configuration > Storage > Storage Management

   You can view the capacity, free space, status, type and property of the disk.
Figure 6-2 Storage Management Interface

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

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

Figure 6-3 View Disk Status

3. Define the quota for record and pictures.

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

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

Figure 6-4 Quota Settings

Notes:

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

Purpose:
There are two kinds of recording for the cameras: manual recording and scheduled recording. For the manual recording, refer to Section 4.3 Recording and Capturing Pictures Manually. In this section, you can follow the instructions to configure the scheduled recording. By default, the record files of scheduled recording are stored in the SD card (if supported) or in the network disk.

Steps:
1. Enter the Record Schedule Settings interface:

Configuration > Advanced Configuration > Storage > Record Schedule

![Recording Schedule Interface](image)

Figure 6-5 Recording Schedule Interface

2. Check the checkbox of Enable Record Schedule to enable scheduled recording.

3. Set the record parameters of the camera.

![Record Parameters](image)

Figure 6-6 Record Parameters
**Pre-record:** The time you set to start recording before the scheduled time or the event. For example, if an alarm triggers recording at 10:00, and the pre-record time is set as 5 seconds, the camera starts to record at 9:59:55.

The Pre-record time can be configured as No Pre-record, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s or not limited.

**Post-record:** The time you set to stop recording after the scheduled time or the event. For example, if an alarm triggered recording ends at 11:00, and the post-record time is set as 5 seconds, the camera records until 11:00:05.

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

**Overwrite:** Select Yes, and then the record files will be overwritten when the SD card or network disk becomes full; Select No, and then the recording will stop when the SD card or network disk becomes full.

**Recording Stream:** Set the stream type for recording. Main Stream and Sub Stream are selectable.

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

5. Choose the day to set the record schedule.

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

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

**Note:** The time of each segment can’t be overlapped. Up to 8 segments can be configured.

(2) Select a **Record Type**. The record type can be Continuous, Motion Detection, Alarm, Motion | Alarm, Motion & Alarm, etc.

- **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 **Section 5.6.1 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 5.6.3 Configuring 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 5.6.1** and **Section 5.6.3** 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 5.6.1* and *Section 5.6.3* for detailed information.

♦ **Record Triggered by Line Crossing Detection**

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

Besides configuring the recording schedule, you have to set the detection line and check the checkbox of **Trigger Channel** in the **Linkage Method** of Line Crossing Detection Settings interface. For detailed information, please refer to *Section 5.6.6 Configuring Line Crossing Detection*.

♦ **Record Triggered by Intrusion Detection**

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

Besides configuring the recording schedule, you have to set the intrusion detection area and check the checkbox of **Trigger Channel** in the **Linkage Method** of Intrusion Detection Settings interface. For detailed information, please refer to *Section 5.6.7 Configuring Intrusion Detection*.

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

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

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

### 6.3 Configuring Snapshot Settings

*Purpose:*

You can configure the scheduled snapshot and event-triggered snapshot. The captured
picture can be stored in the SD card (if supported) or in the network disk (For details, please refer to Section 6.1 Configuring NAS Settings). The captured pictures can also be uploaded to a FTP server.

**Timing Snapshot**

**Steps:**

1. Enter the Snapshot Settings interface:
   
   Configuration > Advanced Configuration > Storage > Snapshot

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

3. Select picture format, resolution, and quality for the snapshots.

4. Set the time interval between two snapshots.

5. Click **Edit** to set the arming schedule for timing snapshot. For details, refer to Step 5 in Section 5.6.1.

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

7. (Optional) To upload the captured pictures to the FTP server, configure the FTP parameters and check **Upload Picture** checkbox in FTP Settings interface. For details, please refer to Section 5.3.11 Configuring FTP Settings.

![Timing Snapshot](image)

Figure 6-8 Timing Snapshot
Event-triggered Snapshot

**Before you start:**

Select **Upload to FTP** as the linkage method for the events, including motion detection, alarm input, line crossing detection and intrusion detection. For details, please refer to **Section 5.6**.

**Steps:**

1. Enter the Snapshot Settings interface:
   
   **Configuration > Advanced Configuration > Storage > Snapshot**

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

3. Select picture format, resolution, and quality for the snapshots.

4. Set the time interval between two continuous snapshots.

5. Set the capture number for each event-triggered snapshot time.

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

7. (Optional) To upload the captured pictures to the FTP server, configure the FTP parameters and check **Upload Picture** checkbox in FTP Settings interface. For details, please refer to **Section 5.3.11 Configuring FTP Settings**.

![Event-triggered Snapshot Settings](image)

**Figure 6-9** Event-triggered Snapshot Settings
Chapter 7  Playback

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

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

![Playback Interface](image1)

**Figure 7-1 Playback Interface**

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

![Search Video](image2)

**Figure 7-2 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 7-3 Playback Toolbar

Table 7-1 Description of Playback Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🎥_lowercase / 🎥_uppercase</td>
<td>Start / Pause the video playback.</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Stop the video playback.</td>
</tr>
<tr>
<td>🎥_lowercase / 🎥_uppercase</td>
<td>Decrease / Increase the speed of video playback.</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Play the video back frame by frame.</td>
</tr>
<tr>
<td>🎥_lowercase</td>
<td>Manually capture the picture during playback.</td>
</tr>
<tr>
<td>🎥_lowercase / 🎥_uppercase</td>
<td>Start/Stop clipping video files.</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Adjust the audio volume.</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Download video files</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Download captured pictures</td>
</tr>
<tr>
<td>🎥_uppercase</td>
<td>Select the playback mode.</td>
</tr>
</tbody>
</table>

Notes:

- You can set the local file saving path for the downloaded video files and pictures in Local Configuration interface. For details, please refer to Section 5.1.
- Click the icon 🎥_lowercase, and you can select the playback mode, including Fisheye View, Panorama View, Fisheye+3PTZ, Panorama View +3 PTZ, 4PTZ Views, Fisheye + 8 PTZ, Panorama + 8 PTZ.

Figure 7-4 Playback Mode

- e-PTZ function is also supported in playback.

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 7-5 Set Playback Time

Different video types are marked in different colors on the progress bar.

Figure 7-6 Progress Bar

Figure 7-7 Video Types
Chapter 8  Log Searching

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

Before you start:
Please configure network disk for the camera or insert a SD card in the camera.

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

![Log Searching Interface](image1)

Figure 8-1 Log Searching Interface

2. Set the log search conditions to specify the search, including the Major Type, Minor Type, Start Time and End Time.

3. Click Search to search log files. The matched log files will be displayed on the Log interface.

![Log Searching](image2)

Figure 8-2 Log Searching

4. To export the log files, click Save log to save the log files in your computer.
Chapter 9  Others

9.1 Managing User Accounts

Enter the User Management interface:

**Configuration > Basic Configuration > Security > User**

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

![User Information](image)

**Figure 9-1 User Information**

- **Adding a User**

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

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

**Steps:**

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

**Notes:**

- Up to 31 user accounts can be created.
- Different level user owns different permissions. Operator and user are selectable.

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

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

![Add User interface](image)

**Figure 9-2 Add a User**

- **Modifying a User**

*Steps:*

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

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

9.2 Authentication

Purpose:
You can specifically secure the stream data of live view.

Steps:
1. Enter the RTSP Authentication interface:

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

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

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

### 9.3 Anonymous Visit

**Purpose:**
You can specifically secure the stream data of live view.

**Steps:**

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

![Figure 9-5 RTSP Authentication](image)

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

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

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

### 9.4 IP Address Filter

**Purpose:**
This function makes it possible for access control.

**Steps:**

1. Enter the IP Address Filter interface:

   **Configuration > Advanced Configuration > Security > IP Address Filter**
2. Check the checkbox of Enable IP Address Filter.

3. Select the type of IP Address Filter in the drop-down list, Forbidden and Allowed are selectable.

4. Set the IP Address Filter list.
   - Add an IP Address
     
     **Steps:**
     
     (1) Click the Add to add an IP.
     
     (2) Input the IP Address.
     
     (3) Click the OK to finish adding.
   
   - Modify an IP Address
     
     **Steps:**
     
     (1) Click the IP address from filter list and click Modify.
     
     (2) Modify the IP address in the text field.
(3) Click the **OK** to finish modifying.

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

- **Delete all IP Addresses**
  
  Click **Clear** to delete all the IP addresses.

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

### 9.5 Security Service

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

**Steps:**

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

   ![Security Service](image)

   Figure 9-9 Security Service

2. Check the checkbox of **Enable SSH** to enable the data communication security, and uncheck the checkbox to disable the SSH.

3. Check the checkbox of **Enable Illegal Login Lock**, and then the IP address will be locked if the admin user performs 7 failed user name/ password attempts (5 times for the operator/user).

   **Note:** If the IP address is locked, you can try to login the device after 30 minutes.
9.6 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 or Device No..

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

![Device Information Table]

Figure 9-10 Device Information

9.7 Maintenance

9.7.1 Rebooting the Camera

*Steps:*

1. Enter the Maintenance interface:

**Configuration > Basic Configuration> System > Maintenance**

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

2. Click **Reboot** to reboot the network camera.
9.7.2 Restoring Default Settings

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

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

9.7.3 Exporting / Importing Configuration File

Purpose:
Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

Steps:
Enter the Maintenance interface:
Configuration > Basic Configuration> System > Maintenance
Or Configuration > Advanced Configuration> System > Maintenance
1. Click Export to export the current configuration file, and save it to the certain place.
2. Click Browse to select the saved configuration file and then click Import to start importing configuration file.

Note: You need to reboot the camera after importing configuration file.
3. Click **Export** and set the saving path to save the configuration file in local storage.

![Import/Export Configuration File](image)

Figure 9-13 Import/Export Configuration File

### 9.7.4 Upgrading the System

**Steps:**

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

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

![Remote Upgrade](image)

Figure 9-14 Remote Upgrade

### 9.8 RS-232 Settings

**Purpose:**

The RS-232 port can be used in two ways:

- Parameters Configuration: Connect a computer to the camera through the serial port. Device parameters can be configured by using software such as HyperTerminal. The serial port parameters must be the same as the serial port
parameters of the camera.

- **Transparent Channel:** Connect a serial device directly to the camera. The serial device will be controlled remotely by the computer through the network.

**Steps:**

1. Enter RS-232 Port Setting interface:

   **Configuration> Advanced Configuration> System > RS232**

   ![RS-232 Settings](image)

   **Figure 9-15 RS-232 Settings**

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

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

### 9.9 DST Settings

**Purpose:**

For region using the summer time, DST (daylight saving time) settings can be configured according to the actual needs.

**Steps:**

1. Enter DST Settings interface:

   **Configuration> Advanced Configuration> System > DST**

2. Check the checkbox of **Enable DST** to enable daylight saving time.

3. Set the start time and end time for the DST period.

4. Select the DST bias from the drop-down list.

5. Click **Save** to save the settings.
9.10 RS-485 Settings

**Purpose:**
The RS-485 serial port is used to control the PTZ of the camera. The configuring of the PTZ parameters should be done before you control the PTZ unit.

**Note:** RS-485 settings vary according to the camera model.

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

2. Set the RS-485 parameters.

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

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

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

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

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

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

![Service Settings Interface](image)

Figure 9-18 Service

9.12 Fisheye Parameters

Steps:

1. Enter Fisheye Parameters interface:
   
   Configuration> Advanced Configuration> System > Fisheye Parameters

2. Select the mounting type of the fisheye camera according to your actual environment and demand. Ceiling mounting, table mounting, and wall mounting are selectable for the mounting type.

   For example, if the fisheye camera is mounted on the ceiling, here you should select Ceiling as the mounting type.

3. Click Save to save the settings.
Figure 9-19 Fisheye Parameters
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](image)

Figure A.1.1 Searching Online Devices
Note:

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

♦ Search online devices manually

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

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

● Modify network parameters

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

![Modify Network Parameters](image)

Figure A.1.2 Modify Network Parameters
Appendix 2 Port Mapping

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

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

![Select the WAN Connection Type](image1)

Figure A.2.1 Select the WAN Connection Type

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

![Set the LAN parameters](image2)

Figure A.2.2 Set the LAN parameters

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

**Example:**

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

**Steps:**
1. As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23
3. Enable **ALL** or **TCP** protocols.
4. Check the **Enable** checkbox and click **Save**.

![Virtual Servers](image)

Figure A.2.3 Port Mapping

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