Disclaimer statement

“Underwriters Laboratories Inc. ("UL") has not tested the performance or reliability of the security or signaling aspects of this product. UL has only tested for fire, shock or casualty hazards as outlined in UL’s Standard(s) for Safety, UL60950-1. UL Certification does not cover the performance or reliability of the security or signaling aspects of this product. UL MAKES NO REPRESENTATIONS, WARRANTIES OR CERTIFICATIONS WHATSOEVER REGARDING THE PERFORMANCE OR RELIABILITY OF ANY SECURITY OR SIGNALING RELATED FUNCTIONS OF THIS PRODUCT.”
# Content

- Important information .................................................................................................................. 6
- Limitation of liability .................................................................................................................. 6
- Safety warnings and cautions ...................................................................................................... 7
- Advisory messages ......................................................................................................................... 9
- Warranty information ................................................................................................................... 10
- System requirement ...................................................................................................................... 11
- Camera default login information ............................................................................................... 11
- Network connection .................................................................................................................... 12
  - Setting the network camera over LAN ..................................................................................... 12
  - Wiring over LAN .......................................................................................................................... 12
  - Setting the Clare Vision Plus camera over WAN ................................................................. 15
    - Static IP connection .................................................................................................................. 15
    - Connecting the network camera with static IP directly ........................................................ 15
    - Dynamic IP connection .......................................................................................................... 16
- Access to the network camera ..................................................................................................... 18
  - Accessing through a web browser ............................................................................................ 18
- Wi-Fi settings .............................................................................................................................. 20
  - Configuring Wi-Fi connection in manage and ad-hoc modes ............................................... 20
    - Wireless connection in ad-hoc mode ..................................................................................... 21
- Security mode ............................................................................................................................ 22
  - WPA-personal and WPA2-personal mode ............................................................................. 22
  - WPA- enterprise and WPA2-enterprise mode ......................................................................... 23
  - Easy Wi-Fi connection with WPS function ............................................................................ 24
- IP property settings for wireless network connection ................................................................. 26
- Live View .................................................................................................................................. 27
  - Live View page ........................................................................................................................ 27
  - Starting live view ....................................................................................................................... 28
  - Recording and capturing pictures manually .......................................................................... 29
  - Configuring PTZ .................................................................................................................... 29
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating PTZ control</td>
<td>29</td>
</tr>
<tr>
<td>Setting/calling a preset and patrol</td>
<td>31</td>
</tr>
<tr>
<td>Configuring the PTZ limit settings</td>
<td>33</td>
</tr>
<tr>
<td>Configuring the initial PTZ position</td>
<td>33</td>
</tr>
<tr>
<td>Configuring the PTZ park action</td>
<td>33</td>
</tr>
<tr>
<td>Configuring the PTZ privacy mask</td>
<td>34</td>
</tr>
<tr>
<td>Configuring a PTZ scheduled task</td>
<td>35</td>
</tr>
<tr>
<td>Clearing a PTZ configuration</td>
<td>35</td>
</tr>
<tr>
<td>Configuring the prioritize PTZ</td>
<td>35</td>
</tr>
<tr>
<td>Network camera configuration</td>
<td>36</td>
</tr>
<tr>
<td>Configuring local parameters</td>
<td>36</td>
</tr>
<tr>
<td>Configuring basic settings</td>
<td>38</td>
</tr>
<tr>
<td>Online upgrades</td>
<td>38</td>
</tr>
<tr>
<td>Configuring time settings</td>
<td>39</td>
</tr>
<tr>
<td>RS-232 settings</td>
<td>40</td>
</tr>
<tr>
<td>RS-485 settings</td>
<td>42</td>
</tr>
<tr>
<td>DST settings</td>
<td>43</td>
</tr>
<tr>
<td>External devices</td>
<td>43</td>
</tr>
<tr>
<td>VCA resource</td>
<td>44</td>
</tr>
<tr>
<td>Maintaining the camera’s settings</td>
<td>45</td>
</tr>
<tr>
<td>Upgrade and maintenance</td>
<td>45</td>
</tr>
<tr>
<td>Log</td>
<td>45</td>
</tr>
<tr>
<td>System service</td>
<td>46</td>
</tr>
<tr>
<td>Configuring security settings</td>
<td>47</td>
</tr>
<tr>
<td>Anonymous visit</td>
<td>47</td>
</tr>
<tr>
<td>IP address filter</td>
<td>48</td>
</tr>
<tr>
<td>Security service</td>
<td>49</td>
</tr>
<tr>
<td>Managing user accounts</td>
<td>49</td>
</tr>
<tr>
<td>Online users</td>
<td>51</td>
</tr>
<tr>
<td>Network settings</td>
<td>52</td>
</tr>
<tr>
<td>Configuring basic settings</td>
<td>52</td>
</tr>
<tr>
<td>Configuring TCP/IP settings</td>
<td>52</td>
</tr>
<tr>
<td>Configuring DDNS settings</td>
<td>53</td>
</tr>
</tbody>
</table>
Configuring PPPoE settings.................................................................55
Configuring port settings ...................................................................56
Configuring NAT settings ...................................................................56
Configuring UPnP settings .................................................................57
Configuring advanced settings ...........................................................58
Configuring SNMP settings ...............................................................58
Configuring FTP settings ...................................................................60
Configuring Platform Access – Cloud P2P........................................62
Configuring HTTPS settings ...............................................................64
Configuring QoS settings ...................................................................65
Configuring video and audio settings ..................................................67
Configuring video settings ..................................................................67
Configuring audio settings ..................................................................69
Configuring ROI encoding .................................................................70
Configuring displayed on-stream information ......................................71
Configuring target cropping ...............................................................72
Image settings....................................................................................73
Configuring display settings .............................................................73
Configuring OSD Settings .................................................................76
Configuring privacy mask ...................................................................76
Configuring picture overlay ...............................................................78
Event settings ....................................................................................79
Configuring basic events ....................................................................79
Configuring alarm input .................................................................84
Configuring alarm output ...............................................................84
Handling exception ..........................................................................86
Configuring other alarms ..................................................................86
Configuring Smart Events .................................................................89
Configuring audio exception detection ..............................................89
Configuring defocus detection ........................................................90
Configuring scene change detection ................................................91
Configuring face detection .............................................................91
Configuring line crossing detection ..................................................92
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Intrusion detection</td>
<td>94</td>
</tr>
<tr>
<td>Configuring region entrance detection</td>
<td>95</td>
</tr>
<tr>
<td>Configuring region exiting detection</td>
<td>96</td>
</tr>
<tr>
<td>Configuring unattended baggage detection</td>
<td>97</td>
</tr>
<tr>
<td>Configuring object removal detection</td>
<td>98</td>
</tr>
<tr>
<td>VCA configuration</td>
<td>100</td>
</tr>
<tr>
<td>Face capture</td>
<td>106</td>
</tr>
<tr>
<td>Heat map</td>
<td>110</td>
</tr>
<tr>
<td>People counting</td>
<td>111</td>
</tr>
<tr>
<td>Counting</td>
<td>113</td>
</tr>
<tr>
<td>Road traffic</td>
<td>115</td>
</tr>
<tr>
<td>Storage settings</td>
<td>117</td>
</tr>
<tr>
<td>Configuring recording schedule</td>
<td>117</td>
</tr>
<tr>
<td>Configuring Net HDD</td>
<td>119</td>
</tr>
<tr>
<td>Configuring memory card detection</td>
<td>120</td>
</tr>
<tr>
<td>Configuring lite storage</td>
<td>121</td>
</tr>
<tr>
<td>Playback</td>
<td>122</td>
</tr>
<tr>
<td>Picture</td>
<td>124</td>
</tr>
<tr>
<td>Application</td>
<td>125</td>
</tr>
<tr>
<td>Face capture statistics</td>
<td>125</td>
</tr>
<tr>
<td>People counting statistics</td>
<td>125</td>
</tr>
<tr>
<td>Heat map statistics</td>
<td>126</td>
</tr>
<tr>
<td>Counting statistics</td>
<td>126</td>
</tr>
<tr>
<td>Understanding camera capacity in an NVR</td>
<td>128</td>
</tr>
<tr>
<td>NVR model Capacity</td>
<td>128</td>
</tr>
<tr>
<td>Streaming video types</td>
<td>128</td>
</tr>
<tr>
<td>Adjusting settings</td>
<td>129</td>
</tr>
<tr>
<td>Camera installation</td>
<td>130</td>
</tr>
<tr>
<td>Before you start</td>
<td>130</td>
</tr>
<tr>
<td>Cube camera installation</td>
<td>130</td>
</tr>
<tr>
<td>Dome camera installation</td>
<td>133</td>
</tr>
<tr>
<td>Conduit installation on the side</td>
<td>135</td>
</tr>
<tr>
<td>Ceiling mounting with gang box</td>
<td>136</td>
</tr>
</tbody>
</table>
Wall mounting ........................................................................................................... 137
Image and focus adjusting ...................................................................................... 139
Bullet camera installation ...................................................................................... 141
Appendix 1 ........................................................................................................... 143
SADP software introduction ............................................................................... 143
Description of SADP ......................................................................................... 143
Search online devices manually ..................................................................... 144
Appendix 2 ........................................................................................................... 145
Port mapping ....................................................................................................... 145
Important information

Limitation of liability
To the maximum extent permitted by applicable law, in no event will Clare Controls, LLC. be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Clare Controls, LLC. shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Clare Controls, LLC. has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Clare Controls, LLC. assumes no responsibility for errors or omissions.
Safety warnings and cautions

Follow the warnings and cautions below to avoid danger and property damage.

**Hazardous voltage may be present:** Special measures and precautions must be taken when using this device. Some voltages on the device may present a hazard to the user. This device should only be used by certified electricians.

**Power supply hazardous voltage:** AC mains voltages are present within the power supply assembly. This device must be connected to a UL approved, completely enclosed power supply with the proper voltage and current. There are no user serviceable parts inside the power supply.

**System grounding:** To avoid shock, ensure that no AC wiring is exposed and that grounding is maintained. Ensure that any equipment to which this device will be attached is also connected properly to wired, grounded receptacles.

**Power connect and disconnect:** The AC power supply cord is the main disconnect device to mains (AC power). The socket outlet should to be installed near the equipment and be easily accessible.

**Installation and Maintenance:** Do not connect/disconnect any cables or perform installation/maintenance on this device during an electrical storm.

**Power cord requirements:** The connector that plugs into the wall outlet must be a grounding-type male plug designed for use in your region. It must have certification by an agency in your region. The connector that plugs into the AC receptacle on the power supply must be an IEC 320, sheet C13, female connector. See the following website for more information [http://kropla.com/electric2.htm](http://kropla.com/electric2.htm).

**Lithium battery:** This device contains a lithium battery. There is an explosion risk if the battery replacement is incorrect. Dispose of used batteries according to the vendor’s instructions and in accordance with local environmental regulations.
**Perchlorate material:** Special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate. This notice is required by California Code of Regulations, Title 22, Division 4.5, and Chapter 33: Best Management Practices for Perchlorate Materials. This device includes a battery which contains perchlorate material.

⚠️ **Thermal and mechanical injury:** Some components such as heat sinks, power regulators, and processors may be hot. Care should be taken to avoid contact with these components.

**Electromagnetic interference:** This equipment has not been tested for compliance with emission limits of the FCC and similar international regulations. This device is not, and may not be, offered for sale or lease without authorization from the United States FCC or its equivalent in other countries. It is prohibited to use this equipment in a residential location. This equipment generates, uses, and can radiate radio frequency energy. This can result in harmful interference to radio communications.

**Lead content:** Recycle this device in a responsible manner. Refer to local environmental regulations for proper recycling; do not dispose of device in unsorted municipal waste.
Advisory messages

Warnings

• Input voltage should meet both the SELV (Safety Extra Low Voltage) and the Limited Power Source with 24 VAC or 12 VDC according to the IEC60950-1 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 professional and should conform to all the local codes.

• Install blackout equipment in the power supply circuit for convenient supply interruption.

• If mounting the camera to the ceiling, make sure that the ceiling can support more than 50 (N) Newton gravities.

• Never attempt to disassemble the camera yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

Cautions

• Before using the camera, ensure that the power supply voltage is correct.

• Do not drop or subject the camera to physical shock.

• Do not touch the sensor modules with your fingers. When cleaning, use a clean cloth with a drop of ethanol and wipe it gently. If the camera will not be used for an extended period, put the lens cap on to protect the sensor from dirt.

• Do not aim the camera lens at strong light such as the sun or an incandescent lamp. This can cause severe damage to the camera.

• The sensor may be burned out by a laser beam. Make sure that the surface of the sensor is not exposed to laser equipment.

• Do not place the camera in areas that are extremely hot, cold, dust, or damp. The operating temperature should be between 14 to 140˚F (-10 to 60°C).

• Good ventilation is required for a proper operating environment avoiding heat accumulation.

• Keep away from water or any liquid.

• When returning, the camera should be in its original packing.

• Improper use or replacement of the battery may result in explosion. Always use the manufacturer recommended battery type.

IR Reflection

If your camera supports IR, note the following to prevent IR reflection:
• Do not remove the dome cover until the camera is fully installed. Removing the cover exposes the camera to dust and grease which causes IR reflections.
• Ensure that the camera is not near shiny/reflective surfaces or objects.
• Ensure that the foam lens ring is flush against the dome to isolate the lenses from IR LEDs.

Warranty information
Clare Controls offers a three (3) year limited warranty on original Clare Controls components, from the date of shipment from Clare Controls. To view complete limited warranty details, including limitations and exclusions, www.clarecontrols.com/warranty.
System requirement

Operating system: Microsoft Windows XP SP1 and above versions
CPU: 2.0 GHz, or higher
RAM: 1 G or higher
Display: 1024 × 768 resolution, or higher
Web browser: Internet Explorer 8.0 and above; Apple Safari 5.02 and above; and Mozilla Firefox 5.0 and above.

Camera default login information

The information below is the Clare Controls Camera default login information. We recommend changing the login information for security purposes.

IP Address: DHCP
Port number: 8000
User name: clareadmin
Password: secure7

Note: Features in this manual vary based on Clare Vision Plus camera.
Network connection
The network connection can use LAN (Local Area Network) or WAN.

If you want to set the network camera via a LAN (Local Area Network), refer to “Setting the network camera over LAN” on page 12.

**Note:** The camera must be activated before use.

If you want to set the network camera via a WAN (Wide Area Network), refer to “Setting the Clare Vision Plus camera over WAN” on page 15.

**Note:** The camera must be activated before use.

Setting the network camera over LAN
To view and configure the camera via LAN, you must connect the camera to the same subnet as your computer. Install the SADP software to search for and change the IP of the network camera.

**Note:** For information on SADP, see “SADP software introduction” on page 143.

Wiring over LAN
The following figures show the two ways for establishing the cable connection of a network camera and a computer.

To test the network camera, connect it directly to the computer with a network cable, as shown in Figure 1.

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

**Figure** Direct connection
Activating the camera

The camera must be activated before use. Select an activation method below.

Activating the camera using a web browser:

1. Turn the camera on, and then connect it to the network.
2. Enter the IP address into the web browser’s address bar, and then press Enter to access the activation interface.
   
   **Note:** The default IP address of the camera is 192.168.1.64.

3. Enter a password, confirm the password, and click **OK**.

Activating the camera using SADP software:

1. Turn the camera on, and then connect it to the network.
2. Run the SADP software, and then select the device from the displayed list.

![Device selection screen](image)

3. Enter a password, confirm the password, and then click **OK**.

4. Modify the IP address to match your computer.
   
   – or –

   Select the **Enable DHCP** checkbox.

![Modify Network Parameters](image)

5. Enter the password, and then click **Save**.
Setting the Clare Vision Plus camera over WAN
This section explains how to connect the camera to a WAN with a static IP or a dynamic IP.

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

To connect the network camera via a router:
1. Connect the camera to the router.
2. Assign the LAN IP address, subnet mask, and gateway.
3. Save the static IP in the router.
4. Set port mapping – for example, 80, 8000, 8200, and the 554 ports. Port mapping varies based on router. Call the router manufacturer for assistance with port mapping.
   Note: For information regarding port mapping, see “Port mapping” on page 145.
5. Visit the camera through a web browser or the client software.

Connecting the network camera with static IP directly
You can save the static IP in the camera and connect it directly to the internet without using a router.
Dynamic IP connection
Apply a dynamic IP from an ISP. With the dynamic IP address, you can connect the network camera to a modem or a router.

To connect the network camera via a router:
1. Connect the network camera to the router.
2. Accessing the camera, assign a LAN IP address, subnet mask, and gateway.
3. Accessing the router, set the PPPoE user name and password.
4. Set port mapping, e.g., 80, 8000, 8200 and the 554 ports. Port mapping varies based on the router. Call the router manufacturer for assistance with port mapping.
   
   **Note:** For information regarding port mapping, see “Port mapping” on page 145.
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
If the camera supports the PPPoE auto dial-up function, the camera receives a public IP address through ADSL dial-up after the camera is connected to a modem. Configure the PPPoE parameters of the network camera.

**Figure 5:** Accessing the camera with dynamic IP

**Note:** The new IP address is dynamically assigned via PPPoE, so the IP address will change after every reboot. To stop the IP address from changing, obtain a domain name from a DDNS provider – for example, [www.myclarevision.com](http://www.myclarevision.com). Follow the below steps for normal and private domain name resolution.
To obtain a normal domain name:
1. Obtain and apply a domain name from a domain name provider.
2. Configure the DDNS settings in the DDNS settings interface of the network camera, and then click **Save**.
3. When prompted, reboot for the settings to take effect.
4. Configure the DDNS settings of the camera via the applied domain name.

To obtain a private domain name:
1. Install and run the IP server software on a computer with a static IP.
2. Access the network camera through a LAN with a web browser or the client software.
3. Enable DDNS and select the IP Server as the protocol type, and then click **Save**.
4. When prompted, reboot for the settings to take effect.
Access to the network camera

Accessing through a web browser

Accessing the network camera through a web browser lets you view the camera feed and configure the cameras settings.

To access the camera using a web browser:
1. Open the web browser.
   Note: We recommend not using Google Chrome. Not all camera features/access are available in Chrome.
2. In the address field, enter the IP address of the network camera (e.g., 192.168.1.64), and then press Enter. This brings you to the login interface.
3. Enter the user name and password, and then click Login.

   Notes
   • The default user name is clareadmin and the password is secure7.
   • The device IP address locks after 5 failed login attempts.

4. Install the plug-in, if prompted, and follow the installation prompts before viewing the live video and operating the camera.
   Note: You may need to close the web browser to install the plug-in. After installing the plug-in, reopen the web browser and log in.
5. Click **OK**.

![Message from webpage](image)

**New version of plug-in is detected. Update it?**

- **OK**
- **Cancel**

6. Click **Next**.

![Setup - Web Components](image)

**Click Next to continue, or Cancel to exit Setup.**

7. Click **Finish**.

![Setup - Web Components](image)

**Setup has finished installing Web Components on your computer.**

- **Click Finish to exit Setup.**
Wi-Fi settings
You do not need to use cables when connecting to the wireless network.

Note: This chapter is only applicable for Clare Vision Plus cameras with a built-in Wi-Fi module.

Configuring Wi-Fi connection in manage and ad-hoc modes
A wireless network must be configured.

To configure a wireless connection in Manage Mode:

1. Enter the Wi-Fi configuration interface.

   Configuration > Advanced Configuration > Network > Wi-Fi

2. Click Search to search for online wireless connections.

3. Click to select a wireless connection in the list.

4. Set the Network Mode to Manager.
5. The Security Mode and the network Encryption Type are automatically selected when you choose the wireless network, do not change it manually.

   **Note:** These parameters must match the router.

6. Enter the password to connect the wireless network. This password is the same one set above for the router.

**Wireless connection in ad-hoc mode**

If you choose Ad-Hoc mode, you do not need to connect the wireless camera using a router. The camera broadcast its own wireless signal.

**To configure a wireless connection in ad-hoc mode:**

1. Select Ad-Hoc mode.

2. Customize the camera’s SSID.

3. Select the wireless connection’s Security Mode.

4. Enable the wireless connection function on your PC.

5. On the PC, search the network to see the SSIDs of the cameras available.

6. Choose the SSID and connect.
Security mode

Select the Security Mode; not-encrypted, WEP, WPA-personal, WPA-enterprise, WPA2-personal, and WPA2-enterprise.

---

Wi-Fi security mode options

- **Authentication** - Select Open or Shared Key System Authentication, depending on the method used by the access point. Not all access points have this option.

- **Key Length** - This sets the length of the key used for the wireless encryption, 64 or 128 bit. The encryption key displays as 40/64 or 104/128.

- **Key Type** - The key types depend on the access point being used. The following options are available:
  - **HEX**: Allows you to manually enter the hex key.
  - **ASCII**: In this method the string must be exactly 5 characters for 64 bit WEP and 13 characters for 128 bit WEP.

---

**WPA-personal and WPA2-personal mode**

Enter the required pre-shared key for the access point, a hexadecimal number or a passphrase.
WPA- enterprise and WPA2-enterprise mode

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

EAP-TLS

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

EAP-PEAP:

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

WPS (Wi-Fi Protected Setup) refers to the 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 WPS connection; PBC mode and PIN mode.

Note: If you enable the WPS function, you do not need to configure the parameters or know the key of the wireless connection.

Figure 12: WPS PBC configuration

<table>
<thead>
<tr>
<th>WPS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable WPS</td>
<td>✔</td>
</tr>
<tr>
<td>PIN Code</td>
<td>12345678</td>
</tr>
<tr>
<td>PBC connection</td>
<td>Connect</td>
</tr>
<tr>
<td>Use router PIN code</td>
<td>Connect</td>
</tr>
<tr>
<td>SSID</td>
<td>C:WPA2-Parsonal</td>
</tr>
<tr>
<td>Router PIN code</td>
<td></td>
</tr>
</tbody>
</table>

PBC mode:

PBC (Push-Button-Configuration) allows the user to push a button on both the Access Point and the new wireless client device for configuration.

To enable the PBC function:

1. Select the **Enable WPS** checkbox.
2. Set the connection mode to PBC.
   
   **Note**: Each access point must support PBC mode.

3. Check the Wi-Fi router for a WPS button. Push the button, and the indicator near the button starts flashing.
   
   This means the WPS function is enabled. For detailed operation, see the user guide of the router.

4. Push the WPS button on the camera.
If there is no WPS button on the camera, click the virtual button on the web interface to enable PBC.

5. Click Connect.

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

**PIN mode:**
The PIN (Personal Identification Number) mode requires the pin from either a sticker or the display on the new wireless device. This PIN must then be entered to connect to the network.

**To enter PIN mode:**
1. Select a wireless connection on the list and the SSID displays.
2. Select Use router Pin code.
   - If the PIN is generated from the router, enter the PIN in the **Router PIN code** field, and then click Connect.
   - or -
   You can generate a PIN code using the camera, and then click Generate.

**Note:** The expiration time for the PIN code is 120 seconds.

<table>
<thead>
<tr>
<th>WPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable WPS</td>
</tr>
<tr>
<td>PIN Code</td>
</tr>
<tr>
<td>PBC connection</td>
</tr>
<tr>
<td>Use router PIN code</td>
</tr>
<tr>
<td>SSID</td>
</tr>
<tr>
<td>Router PIN code</td>
</tr>
</tbody>
</table>

3. Enter the PIN in the **PIN Code** field.
IP property settings for wireless network connection

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

To change the default IP:

1. Enter the TCP/IP configuration interface.
   - Configuration > Basic Configuration > Network > TCP/IP
2. Click the WLAN tab.

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

The settings use the same process as the LAN.

If you do not want to assign the IP address, select the checkbox to enable the DHCP.
Live View

Live View page
The live video page lets you view live video, capture images, utilize PTZ control, set/call presets, and configure the video parameters.

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

Figure 13: Live View page with descriptions

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

**Live View window**: Displays the live video.

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

**PTZ control**: Panning, tilting, and zooming actions of the camera. This also includes the lighter and wiper control (only available if the camera has a PTZ function or an external pan/tilt unit has been installed).

**Preset/Patrol settings**: Set and call the presets for the camera (only compatible with PTZ functioning cameras).
Starting live view

Click on the toolbar to start the live view of the camera.

Figure 14: Live View toolbar

Table 1: Description of the Live View toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Play/Pause</td>
<td>This starts/stops the live view.</td>
</tr>
<tr>
<td>4:3</td>
<td>Sets the window size to 4:3.</td>
</tr>
<tr>
<td>16:9</td>
<td>Sets the window size to 16:9.</td>
</tr>
<tr>
<td>Original</td>
<td>Sets the window to its original size.</td>
</tr>
<tr>
<td>Self-adaptive</td>
<td>Sets the window to be self-adaptive.</td>
</tr>
<tr>
<td>Live main stream</td>
<td>Live view of the main stream.</td>
</tr>
<tr>
<td>Live sub stream</td>
<td>Live view of the sub stream.</td>
</tr>
<tr>
<td>Live third stream</td>
<td>Live view of the third stream.</td>
</tr>
<tr>
<td>Plugin</td>
<td>Select a third party plugin.</td>
</tr>
<tr>
<td>Capture</td>
<td>Manually captures the picture.</td>
</tr>
<tr>
<td>Recording</td>
<td>Manually starts/stops the recording.</td>
</tr>
<tr>
<td>Volume</td>
<td>Adjusts the volume or mutes the recording.</td>
</tr>
<tr>
<td>Microphone</td>
<td>Turns the microphone on/off.</td>
</tr>
<tr>
<td>Zoom</td>
<td>Starts/stops the digital zoom function.</td>
</tr>
</tbody>
</table>

Notes

- Icons vary depending on camera model in use.
- Before using the two-way audio function or recording with audio, set the **Stream Type** to **Video & Audio** referring to the “Operating PTZ control” on page 29.
- Not all cameras support third-stream and 3D positioning.

Full-screen mode

You can double-click on the live video to switch between full-screen and normal mode.
Recording and capturing pictures manually

In the live view interface, click 📸 to capture live images. Click 📹 to record live video. The saving paths of the captured pictures and video can be set on the Local Configuration tab (Configuration > Local Configuration).

Note: The captured image defaults to saving as a JPEG or BMP file in your computer. This can be customized on the Configuration tab.

Configuring PTZ

This section explains the PTZ functions of the network camera. This enables the pan/tilt/zoom control of the camera.
To realize PTZ control, the camera connected to the network must support the PTZ function, or a pan/tilt unit must be installed on the camera. Properly set the PTZ parameters in the Network camera configuration section.

Operating PTZ control

In the live view interface, use the PTZ control buttons to realize pan/tilt/zoom control of the camera.
To realize PTZ control, the camera connected to the network must support the PTZ function or a pan/tilt unit must be installed on the camera. Properly set the PTZ parameters on RS-485 settings on page 42.
PTZ control panel

To control PTZ:

1. On the live view page, click to show the PTZ control panel and to hide it.
2. Click the direction buttons to control the pan/tilt movements.
3. Click the zoom/iris/focus buttons to realize lens control.

   Note: There are 8 arrows ( , , , , , , ) in the live view window.

Table 2: Description of the PTZ control panel

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>α^-</td>
<td>Zoom in/out</td>
</tr>
<tr>
<td>α^+</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Focus near/far</td>
</tr>
<tr>
<td></td>
<td>Iris +/-</td>
</tr>
<tr>
<td></td>
<td>Light on/off</td>
</tr>
<tr>
<td></td>
<td>Wiper on/off</td>
</tr>
<tr>
<td></td>
<td>Auxiliary focus</td>
</tr>
<tr>
<td></td>
<td>Initialize lens</td>
</tr>
<tr>
<td></td>
<td>Adjust speed of pan/tilt movements</td>
</tr>
<tr>
<td></td>
<td>Smart manual tracking</td>
</tr>
<tr>
<td></td>
<td>Start 3D zoom</td>
</tr>
</tbody>
</table>
Setting/calling a preset and patrol
Setting a preset allows you to switch the camera to a preset position, without having to readjust manually. The preset can be selected at any time or be set for certain events. A patrol is a pattern of presets.

To set and call a preset:

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

![Preset list]

2. Use the PTZ control buttons to move the lens to the desired position.
   - Pan the camera to the right or left.
   - Tilt the camera up or down.
   - Zoom in or out.
   - Refocus the lens.
3. Click 🔄 to finish the setting of the current preset.
4. Click × to delete the preset.

Calling a preset allows the camera to point to a specified preset scene manually or when an event takes place.

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

To set and call a patrol:

Note: You must have 2 presets configured before setting a patrol.

1. Click 🔄 to access the patrol configuration interface.
2. Set a path No., and click 📘.
3. Select the preset, enter the patrol duration, and then enter the patrol speed.
4. Click OK to save the preset.
5. Repeat the above steps to add additional presets.

6. Click OK.

7. Click to start the patrol, to stop it, and to delete the patrol. Configuring the basic PTZ settings

The Basic settings lets you change basic parameters, speeds, and OSD.

To configure the basic settings interface:
1. Enter the Basic settings interface.
   
   Configuration > Camera Configuration > PTZ > Basic

2. Select the Enable Proportional Pan checkbox. This will enable customization of the following parameters.
   
   Preset Speed: Select an option 1 to 8.
   
   Keyboard Control Speed: Select an option; Low, Normal, or High.
   
   Auto Scene Speed: Select an option 1 through 40.
   
   Max. Tilt-angle: Select either -5 to 90, -4 to 90, -3 to 90, -2 to 90, -1 to 90, and 0 to 90.
   
   Auto Flip: Select either On or Off.
   
   Zooming Speed: Select 1, 2, or 3.

3. In the PTZ OSD fields, customize the following.
   
   Zoom Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.
   
   PT Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.
   
   Preset Status: Select Always Open, Always Closed, 2 seconds, 5 seconds, and 10 seconds.

4. In the Power Off Memory field select one of the following, Disable, 30 seconds, 60 seconds, 300 seconds, 600 seconds.

5. Click Save.
Configuring the PTZ limit settings
The Limit settings let you set a limit for camera movement.

To configure the limit settings:
1. Enter the Limit settings interface.
   
   Configuration > Camera Configuration > PTZ > Limit

2. Select the Enable Limit checkbox.

3. Select from the Limit Type drop-down.
   
   Manual Stops, movement being controlled by user.
   
   - or -
   
   Scan Stops, is automatic movement.

4. Customize the position and movement on the left. You also have the option to select a preset.

5. Click Save.

Configuring the initial PTZ position
The Initial Position lets you set an initial starting position for the camera.

To configure the initial position:
1. Enter the Initial Position settings interface.
   
   Configuration > Camera Configuration > PTZ > Initial Position

2. Use the arrow, zoom, focus, iris, and touring (same controls for Live View) to set the initial position of the camera.

3. Click the Set button to keep the configured position settings.
   
   - or -
   
   Click the Clear button to clear the position settings.
   
   - or -
   
   Click Goto to go to the set Initial Position.

Configuring the PTZ park action
The Park Actions lets you stop the camera.

To configure the park action:
1. Enter the Park Action settings interface.
   
   Configuration > Camera Configuration > PTZ > Park Action

2. Select the Enable Park Action checkbox to enable this function.

3. In the Park Time field, enter a time in seconds for the park time.
4. Customize the **Action Type** drop-down from the following options.
   
   **Auto Scan**: This scans automatically.
   
   **Frame Scan**: This scans by image frame.
   
   **Random Scan**: This scans at random, stopping at random points, depending on the park action.
   
   **Patrol**: This scans in a path of presets.
   
   **Pattern**: This scans in a recorded motion sequence.
   
   **Preset**: This scans to a recorded location.
   
   **Panorama Scan**: This scans in panoramic view.
   
   **Tilt Scan**: This scans at a tilted angle, moving up and down on the Y axis.

5. Click **Save**.

**Configuring the PTZ privacy mask**

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

**To configure privacy mask:**

1. Enter the Privacy Mask settings interface.
   
   **Configuration > Camera Configuration > PTZ > Privacy Mask**

2. Select the **Enable Privacy Mask** checkbox to enable this function.

3. Click **Draw Area**.

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

5. The Privacy Mask List lets you customize the name, type, if enable, and add or delete an area.
   
   **Note**: You can set two areas on the same image.

6. Click **Stop Drawing** to finish drawing, or click **Clear All** to clear all of the areas you set without saving them.

7. Click **Save**.

**Note**: Privacy masks are set to a location on the view screen and are not relative to the location of the camera. The mask will stay in the same spot regardless of where the camera moves.
Configuring a PTZ scheduled task
Scheduled task lets you set a schedule for the PTZ tasks.

To configure a scheduled task:
1. Enter the Scheduled Task settings interface.
   Configuration > Camera Configuration > PTZ > Scheduled Task
2. Set a second amount in the Park Time field.
3. Click Edit Tasks to change the day, task type, start time, and end time.
   Note: You can copy the tasks to other days of the week.
4. Click Save.

Clearing a PTZ configuration
The Clear Configuration interface lets you clear other settings individually, by selection of more than one, or all at the same time.

To clear the configuration:
1. Enter the Clear Configuration settings interface.
   Configuration > Camera Configuration > PTZ > Clear Configuration
2. Select the checkboxes of the desired areas.
3. Click Save.

Configuring the prioritize PTZ
Prioritizing the PTZ lets you prioritize where PTZ control comes from.

To configure the prioritize PTZ:
1. Enter the Prioritize PTZ settings interface.
   Configuration > Camera Configuration > PTZ > Prioritize PTZ
2. In the Prioritize PTZ field, select Network or RS485 from the drop-down.
3. In the Delay field, set the time in seconds for the delay to occur.
4. Click Save.
Network camera configuration

Configuring local parameters

The local configuration refers to the parameters of the live view, recorded files, and captured pictures on the browser.

To configure local parameters:

1. Enter the Local Configuration interface.

   **Configuration > Local Configuration**

<table>
<thead>
<tr>
<th>Live View Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol: TCP</td>
</tr>
<tr>
<td>Play Performance: Shortest Delay</td>
</tr>
<tr>
<td>Rules: Enable</td>
</tr>
<tr>
<td>Image Format: JPG</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Record File Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record File Size: 256M</td>
</tr>
<tr>
<td>Save recorded files to: C:/Users/test/RecordFiles</td>
</tr>
<tr>
<td>Save downloaded files to: C:/Users/test/DownloadFiles</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Picture and Clip Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save snapshots in live view to: C:/Users/test/CaptureFiles</td>
</tr>
<tr>
<td>Save snapshots when playback to: C:/Users/test/PlaybackFiles</td>
</tr>
<tr>
<td>Save clips to: C:/Users/test/PlaybackFiles</td>
</tr>
</tbody>
</table>

   2. Configure the following settings:

   **Live View parameters**: Set the protocol type and live view performance.

   - **Protocol Type**: Select TCP, UDP, MULTICAST, or HTTP.
     - **TCP**: Ensures the complete delivery of streaming data and better video quality, the real-time transmission will be affected.
     - **UDP**: Provides real-time audio and video streams.
     - **MULTICAST**: It is recommended when using the Multicast function.
     - **HTTP**: Allows the same quality as TCP without setting specific ports for streaming under some network environments.

   - **Live View performance**: Set the live view performance to Least Delay, Balanced, or Best Fluency.

   - **Rule**: The rules set on the local browser. Enable, disable, or do not display the colored markings for motion detection, face detection, or intrusion detection.

   - **Image format**: Choose the image format for capturing pictures.
**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:** Set the packed size of the manually recorded and downloaded video files to 256 M, 512 M or 1 G.
- **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. This is only valid on the pictures captured with the web browser.

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

**Note:** Click **Browse** to change the directory for saving clips and pictures.

3. Click **Save**.
Configuring basic settings
Follow the instructions in this section to configure the camera’s basic settings: system settings, maintenance, security, user management, etc.

To configure basic settings:
1. Enter the Basic Settings interface.

   Configuration > System > System Settings > Basic Information

2. Configure each field as desired.

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Time Settings</th>
<th>RS232</th>
<th>RS485</th>
<th>DST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>IP CAMERA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device No.</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model</td>
<td>XX-XXXXXXXXXX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial No.</td>
<td>XX-XXXXXXXXXXXXX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware Version</td>
<td>Vx.x.xbuild xxxx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encoding Version</td>
<td>Vx.xbuild xxxx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Version</td>
<td>Vx.x.xbuild xxxx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plugin Version</td>
<td>Vx.x.xbuild xxxx</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Channels</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of HDDs</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Alarm Input</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of Alarm Output</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Online upgrades
Some camera models support online upgrades. Click Update on the right of the firmware version to see if a new version is available. If a new version is available, the version number is displayed in the new version field. Click Upgrade.

Notes
The camera must have a memory card to upgrade.
It will take 1 to 2 minutes for the upgrade, do not turn the power off during the upgrade.
Configuring time settings

Follow the instructions in this section to configure the time synchronization and DST settings.

To configure time settings:

1. Enter the Time Settings interface.

   Configuration > System > System Settings > Time Settings

   ![Time Settings interface]

   - **Time Zone**: (GMT+08:00) Beijing, Urumqi, Singapore
   - **NTP**
     - **Server Address**: time.windows.com
     - **NTP Port**: 123
     - **Interval**: 1440 min
     - **Test** button
   - **Manual Time Sync.**
     - **Device Time**: 2015-06-25T13:45:50
     - **Set Time**: 2015-06-25T13:46:46

2. Select the Time Zone.

3. Select the checkbox to enable synchronization using the NTP function.
4. Configure the following settings.

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

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

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

![NTP Settings Table]

**Note**: If the camera is connected to a public network, use an NTP server that has a time synchronization function. If the camera is set in a customized network, the NTP software can be used to establish an NTP server for time synchronization.

**To change Time Synchronization manually**:

1. Enable the **Manual Time Sync** function, and then click ![Set System Time] to set the system time.

![Set System Time]

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

2. Click **Save**.

**RS-232 settings**

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

**Parameters configuration**: Connect a computer to the camera through the serial port. Configure the device parameters 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.
To configure RS-232 settings:

1. Enter RS-232 Port Setting interface.

   Configuration > Advanced Configuration > System > RS232

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Time Settings</th>
<th>RS232</th>
<th>RS485</th>
<th>DST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>115200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Bit</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stop Bit</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flow Ctrl</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usage</td>
<td>Console</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** If you want to connect the camera by the RS-232 port, the parameters of the RS-232 must match the parameters configured here.

2. Click **Save**.
RS-485 settings
The RS-485 serial port is used to control the PTZ of the camera. Configure the PTZ parameters before you control the PTZ unit.

To configure RS-485 settings:
1. Enter RS-485 Port Setting interface.

   Configuration > Advanced Configuration > System > RS485

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

   By default, the Baud Rate is set as 9600 bps, the Data Bit is set to 8, the stop bit is set 1, and the Parity and Flow Control is set to None.
DST settings
Daylight savings time (DST) settings use natural daylight by adjusting the clock forward in the summer, and back in fall.

To configure DST settings:
1. Enter the DST configuration interface.

   Configuration > System > System Settings > DST

   - Enable DST
   - Start Time: Jan 1st Sun 00
   - End Time: Jan 1st Sun 00
   - DST Bias: 30min

2. Select the start and end times.
3. Set the DST Bias.
4. Click Save.

External devices
External devices, wiper or LED light, are controlled via the web browser. External devices vary by camera model.

To configure external devices:
1. Enter the External Device configuration interface.

   Configuration > System > System Settings > External Device

   - Enable Supplement Light
   - Low Beam Brightness: 10
   - High Beam Brightness: 10
   - LED Light On: Timing

2. Select the Enable Supplement Light checkbox.
3. Move the slider to adjust the low beam and high beam brightness.
4. Select the LED Light mode.

Timing: The LED is turned on by a schedule.

Auto: The LED is turned on according to the environment settings.

5. Click Save.

**VCA resource**

VCA resource presents options for VCA functions. These options become available when according to need.

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Time Settings</th>
<th>DST</th>
<th>RS232</th>
<th>RS485</th>
<th>VCA Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SMART Event + Face Detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SMART Event + Heat Map</td>
</tr>
</tbody>
</table>

To configure VCA resources:

1. Enter the VCA Resources configuration interface.
2. Select the desired VCA combinations.
3. Click Save.

Note: Face detection and heat map are mutually exclusive, only one can be used at a time.
Maintaining the camera’s settings
Follow the below information for basic maintenance settings.

Upgrade and maintenance
This interface allows you to process operations.

Enter the Maintenance interface.

Configuration > System > Maintenance > Upgrade & Maintenance
• Reboot: Restart the device.
• Restore: Reset all parameters, except the IP parameters and user information, to the default settings.
• Default: Restore all parameters to the factory default.
  Note: After restoring the default settings, the IP address is also restored to the default IP address, please be careful for this action.
• Export/Import Config. File: Configuration file is used for the batch configuration of the camera, which can simplify the configuration steps when there are a lot of cameras needing configuring.

  To export/import files:
  1. Click Device Parameters, and then save the file.
  2. Click Browse to select the saved file, and then click Import. Note: The camera must reboot for changes to take effect.
• Upgrade: Upgrades the device version.
  To upgrade the version:
  1. Select the firmware or firmware directory to locate the files.
  Firmware: Select the exact path to browse to the firmware.
  Firmware directory: Select the directory the upgrade files resides in.
  2. Click Browse to select the local upgrade file, and then click Upgrade.
  Note: Upgrading takes from 1 to 10 minutes, do not disconnect power during this process.

Log
The log stores files for operation, alarm, exception, and camera information. These files can be exported.

Before starting, configure the camera’s network storage or insert an SD card in the camera.
To export log files:

1. Enter the Log searching interface.

   **Configuration > System > Maintenance > Log**

   ![Log interface]

   - Major Type: All Types
   - Minor Type: All Types
   - Start Time: 2015-06-04 00:00:00
   - Search

2. Set the log search conditions.

3. Click **Search**.

   ![Log list]

   - No.
   - Time
   - Major Type
   - Minor Type
   - Channel No.
   - Local/Remote User
   - Remote Host IP

4. Click **Export**.

**System service**

System service settings refer the hardware service supported by the camera.

**Configuration > Advanced Configuration > System > Service**

For the cameras support IR LED, ABF (Auto Back Focus), Auto Defog, or Status LED, you can go to the hardware service, and select to enable or disable the corresponding service per demands.
Configuring security settings
Configure the parameters, including Authentication, Anonymous Visit, IP Address Filter, and Security Service from security interface. **Configuring authentication**
You can specifically secure the stream data of live view.

**To configure RTSP authentication:**
1. Enter the Authentication interface.
   - **Configuration > System > Security > Authentication**

   ![Authentication interface]

     - RTSP Authentication:
       - basic
     - Save

2. Set the RTSP authentication type to basic or disable, to disable the RTSP authentication.
   **Note:** If you disable the RTSP authentication, anyone can access the video stream by the RTSP protocol using the IP address.

3. Click **Save**.

**Anonymous visit**
Enabling this function allows users that do not have the user name and password of the device to view it.

**To set anonymous visit:**
1. Enter the Anonymous Visit interface.
   - **Configuration > System > Security > Anonymous Visit**

2. Set the Anonymous Visit permission or disable the anonymous visit option.

3. Click **Save**.
   - The Anonymous checkbox displays the next time you log in.

4. Select the Anonymous checkbox, and then click **Login**.
   **Note:** By enabling anonymous access, you are enabling others access to your camera and live view images. It is imperative that you ensure your camera’s field of view does not infringe upon the privacy of others.
IP address filter
This function makes it possible for access control.

To configure the IP address filter:
1. Enter the IP Address Filter interface.

   **Configuration > System > Security > IP Address Filter**

2. Select the **Enable IP Address Filter** checkbox.
3. Set the IP Address Filter type.
4. Set the IP Address Filter list.
5. Click **Save**.

To add an IP address:
1. Click **Add** to add an IP.
2. Enter the IP Address.
3. Click **OK** to finish adding.

To modify an IP address:
1. Click an IP address from the filter list and click **Modify**.
2. Modify the IP address in the text filed.
3. Click **OK** to finish modifying.

To delete an IP address:
1. Click an IP address from the filter list and click **Delete**.

To delete all IP addresses:
1. Click **Clear** to delete all of the IP addresses. 2. Click **Save**.
Security service
This function provides a security service to enable remote login and improve data communication.

To configure security services:
1. Enter the security service configuration interface. **Configuration > System > Security > Security Services**

   ![Configuration Interface]

   - **Authentication**
   - **IP Address Filter**
   - **Security Service**

     - Enable SSH
     - Enable Illegal Login Lock

     ![Save Button]

2. Select the **Enable SSH** checkbox, and then clear the checkbox.
3. Select the **Enable Illegal Login Lock** checkbox.

   **Notes**
   - This checkbox allows the device to lock if the incorrect user name or password are entered 5 consecutive times.
   - If a device is locked, try to login after 30 minutes, or reboot the device and try again.

Managing user accounts
Enter the User Management interface.

**Configuration > System > Security > User Management**

**Note:** The admin user has access to create, modify, and delete other accounts. Up to 15 user accounts can be created.

**Figure 15: User interface**

<table>
<thead>
<tr>
<th>User Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User List</strong></td>
</tr>
<tr>
<td>No.</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>
To add a user:
1. Click Add.
2. Enter the new User Name, select the Level, and input a Password.
   Note: The level indicates the permissions given to the user. You can define the user as an Operator or User.
3. In the Basic Permission field and Camera Configuration field, select or clear the permissions for the new user.
4. Click OK.

To modify a user:
1. Left-click a user and click Modify.
2. Modify the User Name, Level, or Password as desired.
3. In the Basic Permission field and Camera Configuration field, select or clear the permissions.
4. Click **OK**.

![Modify user window](image)

**To delete a user:**

1. Click the user name you want to delete and click **Delete**.
2. Click **OK**.

**Online users**

You can see a list of users currently using the device. User information is displayed with their name.

![User Management and Online Users](image)
Network settings

Configuring basic settings
The below section explores network settings and configurations.

Configuring TCP/IP settings
Configure the TCP/IP settings to operate the camera over the network. The camera supports both the IPv4 and IPv6, both versions may be configured simultaneously without conflicting with each other. At least one IP must be configured.

To configure the TCP/IP settings:
1. Enter the TCP/IP Settings interface.

   Configuration > Network > Basic Settings > 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 500 to 1500.
• The Multicast sends a stream to the multicast group address. It allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Before utilizing this function, enable the Multicast function of your router.

3. Click Save.
4. When prompted, reboot for the settings to take effect.

Configuring DDNS settings
If your camera is set to use PPPoE as its default network connection, use the Dynamic DNS (DDNS) for network access.
Registration on the DDNS server is required before configuring the DDNS settings of the camera.

To configure DDNS settings:
1. Enter the DDNS Settings interface.

   **Configuration > Network > Basic Settings > DDNS**

<table>
<thead>
<tr>
<th>TCP/IP</th>
<th>DDNS</th>
<th>PPPoE</th>
<th>Port</th>
<th>NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Enable DDNS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DynDNS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>members.dyndns.org</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>123.dyndns.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Select the Enable DDNS checkbox.
3. Select DDNS Type.
To configure DDNS:
1. Enter the **Server Address** of DDNS (e.g. myclarevision.com).
2. In the **Domain** text field, enter the domain name obtained from the website.
3. Enter the **Port** of the DDNS server.
4. Enter the **User Name** and **Password** registered on the DDNS website.
5. Click **Save**.

To configure IP server:
1. Enter the Server Address of the IP Server.
2. Click **Save**. **Notes**
   - For the IP Server, you have to apply a static IP, subnet mask, gateway, and the preferred DNS from the ISP. The **Server Address** must match the static IP address of the computer that runs the IP Server software.
   - Enter 173.200.91.74 as the server address (US and Canada only).

To configure CVDDNS:
1. Set the DDNS type to CVDDNS.
2. Enter the Server Address www.myclarevision.com.
3. Enter the Domain name of the camera. The domain name matches the device alias in the CVDDNS server.
4. Click **Save**.
5. When prompted, reboot for the settings to take effect.

**Configuring PPPoE settings**

To configure PPPoE settings:

1. Enter the PPPoE Settings interface.

   **Configuration > Network > Basic Settings > PPPoE**

   ![PPPoE Settings Interface](image)

   2. Select the **Enable PPPoE** checkbox.
   3. Enter **User Name**, **Password**, and **Confirm** the password for PPPoE access.
      
      **Note**: The User Name and Password is assigned by your ISP.
   4. Click **Save**. 5. When prompted, reboot for the settings to take effect.
Configuring port settings
You can set the port numbers of the camera, e.g., HTTP port, RTSP port, and HTTPS port.

To configure port settings:
1. Enter the Port Settings interface.
   
   **Configuration > Network > Basic Settings > Port**

<table>
<thead>
<tr>
<th>TCP/IP</th>
<th>DDNS</th>
<th>PPPOE</th>
<th>Port</th>
<th>NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>80</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTSP Port</td>
<td>554</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HTTPS Port</td>
<td>443</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Port</td>
<td>8000</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Set the HTTP port, RTSP port and HTTPS port of the camera.
   - **HTTP Port**: The default port number is 80, it can be changed to a port range from 1024 to 65535.
   - **RTSP Port**: The default port number is 554, it can be changed to a port range from 1024 to 65535.
   - **HTTPS Port**: The default port number is 443, it can be changed to any nonoccupied port.
   - **Server Port**: The default SDK port number is 8000, it can be changed to a port range from 2000 to 65535.

3. Click **Save**.

4. When prompted, reboot for the settings to take effect.

Configuring NAT settings
Configure the NAT (Network Address Translation) settings.

To configure NAT settings:
1. Browse to NAT Settings.
   
   **Configuration > Network > Basic Settings > NAT**
2. Select the port mapping mode.
   **Auto:** This mode uses the default port numbers.
   **Manual:** This mode uses custom port numbers.

3. Click **Save**.

**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 simplifies the implementation of networks in the home and corporate environments.

With the function enabled, the camera is connected to the Wide Area Network via the router, you do not need to configure port mapping for each port.

**To configure UPnP settings:**

1. Enter the UPnP settings interface.

   **Configuration > Network > Basic Settings > UPnP**

2. Select the **Enable UPnP** checkbox, enabling the **Friendly Name** field.

3. In the **Friendly Name** field, enter the name of the device.

4. From the Port Mapping Mode drop-down, choose one of the following:

   - **Auto** for port mapping with the default port numbers.
   - **Manual** for port mapping with the customized port numbers.

5. Click **Save**.
Configuring advanced settings
The below section goes in-depth to explore network settings and configurations.

Configuring SNMP settings
You can set the SNMP function to get the camera status, parameters, alarm-related information, and manage the camera remotely when it is connected to the network. Before setting the SNMP, download the SNMP software and 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 match the SNMP software. Use the version that corresponds with the security level you required. SNMP v1 provides no security, SNMP v2 requires password for access, and SNMP v3 provides encryption. If you use the third version, HTTPS protocol must be enabled.

To configure SNMP settings:
1. Enter the SNMP Settings interface.
   
   Configuration > Network > Advanced Settings > SNMP
2. Select the corresponding version checkbox to enable the feature.
3. Configure the SNMP settings.
   
   **Note**: The settings of the SNMP software must match the settings configured here.

4. Click Save.
5. When prompted, reboot for the settings to take effect.
Configuring FTP settings
You can configure the FTP server related information to enable the uploading of the captured images to the FTP server. The captured pictures can be triggered by events or a timing snapshot task.

To configure FTP settings:
1. Enter the FTP Settings interface.

   Configuration > Network > Advanced Settings > FTP

<table>
<thead>
<tr>
<th>SNMP</th>
<th>FTP</th>
<th>Email</th>
<th>HTTPS</th>
<th>QoS</th>
<th>802.1x</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Server Address</td>
<td>0.0.0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Directory Structure</td>
<td>Save in the root directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Picture Filing Interval</td>
<td>7</td>
<td></td>
<td></td>
<td>Day(s)</td>
<td></td>
</tr>
<tr>
<td>Picture Name</td>
<td>Default</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upload Picture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Enter the user name and password required to log into the FTP server in the corresponding fields.

3. In the Directory Structure field, select the root directory, parent directory, or 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.

   When the Child Directory is selected, you can use the Camera Name or Camera No. as the name of the directory.

4. Select the Upload Type checkbox to enable uploading the captured image to the FTP server.
5. Select the **Anonymous** checkbox to enable anonymous access to the FTP server. When you select this checkbox, the user name and password will not be requested. **Note:** The anonymous access function must be supported by the FTP server.

6. Click **Save**.

**Note:** If you want to upload the captured images to the FTP server, you must enable the continuous snapshot or the event-triggered snapshot on the Snapshot page.

**Configuring email triggers for alarms**

Configure email notifications for alarm events. For example – motion detection, video loss, and video tampering.

**Note:** Before using email notifications, configure the DNS server settings. To access the settings, browse to TCP/IP.

**To configure DNS settings:**

1. Browse to TCP/IP Settings.

   **Configuration > Network > Basic Settings >TCP/IP**

2. Set the IPv4 Address, IPv4, Subnet Mask, IPv4 Default Gateway, and the preferred DNS server. For detailed TCP/IP configuration information, see "Configuring basic settings" on page 38.

3. The below section explores network settings and configurations.

**To configure email settings for alarms:**

1. Browse to Email Settings.

   **Configuration > Network > Advanced Settings >> Email**

2. Configure the settings as below.

   **Sender fields**

   The Sender fields are configured as the person sending the email. The email from the camera is sent via the designated email. For example, the email is sent from test@gmail.com.

   **Sender:** The sender's name. For example, if you use the name test, the email will appear as it comes from Test.

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

   **SMTP Server:** The SMTP Server IP address or host name, for example – smtp.263xmail.com.

   **SMTP Port:** The SMTP port in use. The default TCP/IP port for SMTP is 25 (not secured), and the SSL SMTP port 465.
Enable SSL: If SSL is required by the SMTP server, select the checkbox to enable SSL.

Attached Image: To send an image with the alarm, select the Attached Image checkbox.

Interval: The interval is the time between images sent. For example, at an interval of 5 seconds, a new image is taken every 5 seconds.

Authentication: (Optional) This is only required if your email server requires user authentication. Select the Authentication checkbox. Then enter the user name and password required for login.

Receiver fields

The receiver fields are configured for the people receiving the alarm emails.

Receiver 1: The name of the first receiver.

Receiver1’s Address: The email address of the first receiver.

<table>
<thead>
<tr>
<th>SMTP</th>
<th>FTP</th>
<th>Email</th>
<th>HTTPS</th>
<th>QoS</th>
<th>802.1x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>test</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sender’s Address</td>
<td><a href="mailto:test@gmail.com">test@gmail.com</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP Server</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP Port</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail Encryption</td>
<td>None</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attached Image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interval</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confirm</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Receiver</th>
<th>Receiver</th>
<th>Receiver’s Address</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>Test</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. Click Save.

Configuring Platform Access – Cloud P2P

Platform access provides you with an option to manage your Clare Vision Plus devices using the Cloud P2P platform.

Note: Cloud P2P access functions vary depending on Clare Vision Plus device.
To enable Cloud P2P:

1. Browse Platform Access

   **Configuration > Network > Advanced Settings > Platform Access**

2. Select the Enable checkbox to enable Cloud P2P.

   This allows the user the ability to manage the Clare Vision Plus device through the Cloud P2P website or through the Clare Vision Plus mobile App.

**Configuring wireless dial settings**

Audio, video, and image data are transferable using a 3G/4G wireless network.

**Note:** Not all Clare Vision Plus cameras support wireless dial functions.

To enable and configure wireless dial functions:

1. Click the **Wireless Dial** tab to enter the Wireless Dial configuration interface.

   **Configuration > Network > Advanced Settings > Wireless Dial**

2. Select the **Enable** checkbox to enable the wireless dial settings.

3. Configure the Dial Parameters.

   **Dial Mode:** The dial modes available are Auto and Manual. When Auto is selected, you can set the dialing arming schedule. When Manual is selected, you can set the offline time and manual dialing parameters.

   **Access Number:** (Optional) Set the access number, user name, password, APN, MTU and verification protocol. You can also leave these parameters blank, and the device will adopt the default settings for dialing after other parameters are configured.

   **Network Mode:** Select Auto, 3G, or 4G. When Auto is selected, the network selection priority is 4G, 3G, and then Wired Network.

   **Offline Time:** When using the manual dial mode, you must enter the offline time. This is represented in seconds.

   **UIM Number:** Input the UIM Number (Mobile Phone Number).

   **Edit:** When the dial mode is set to auto, the edit button allows you to set the arming schedule.

4. Click **Save**.

5. Click **Refresh** to view the dial status.

6. Set the white list.

   a. Select the checkbox of **Enable SMS Alarm**.

      The mobile phone numbers on the white list receive alarm messages from the camera and have the ability to reboot it through SMS.
**Note:** The white list services up to 8 phone numbers. You will need to configure the permissions for each mobile number.

b. Select the number on the white list, and then click the **Edit** button to view the SMS Alarm Settings interface.

c. Input a mobile phone number, and then select the permissions for that number.
   - Reboot via SMS
     **Note:** To reboot the camera via SMS, send the message "reboot" to the camera. After a successful reboot, the camera relays “reboot success.”
   - Alarm for SMS push
d. Click **OK**.
e. (Optional) You can click **Send Test SMS** to send a test message to the mobile device.
f. Click **Save**.

### Configuring HTTPS settings

HTTPS provides authentication for a website and the associated communicating web server. Configure the port number for HTTPS.

For example, if you set the port number to 443, and the IP address is 192.168.1.64, you can access the device by opening a web browser and entering `https://192.168.1.34:443`.

**To configure the HTTPS:**

1. Browse HTTPS.
   - **Configuration > Network > Advanced Settings > HTTPS**
2. Select the **Enable HTTPS** checkbox.
3. Create a certificate.
Self-signed certificate
  a. Click Create next to Create Self-signed Certificate.
  b. Enter the requested information (country, host name/IP, validity, etc.).
  c. Click OK.

  **Note:** If a certificate is already installed, the Create Self-signed Certificate is not available.

Authorized certificate.
  a. Click Create next to Create Certificate Request.
  b. Download the certificate request, and then submit it to the trusted certificate authority for signature.
  c. After receiving the signed valid certificate, import the certificate on the device.

4. Certificate information displays, click **Save**.

## Configuring QoS settings

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

**To configure QoS settings:**

1. Enter the QoS Settings interface.

   **Configuration > Network > Advanced Settings > QoS**

2. Configure the QoS settings, including video/audio DSCP, event/alarm DSCP, and Management DSCP.

   **Notes**
   - 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.
   - The valid value range of the DSCP is 0 to 63. The larger the DSCP value, the higher the priority is.

3. Click **Save**.
4. When prompted, reboot for the settings to take effect.

**Configuring 802.1X settings**

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

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

**To configure 802.1X settings:**

1. Enter the 802.1X Settings interface.

   ![Configuration > Network > Advanced Settings > 802.1X](image)

   2. Select the **Enable IEEE 802.1X** checkbox.

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

   **Note:** The EAPOL version must match the router or the switch.

   4. Click **Save** to finish the settings. 5. When prompted, reboot for the settings to take effect.
Configuring video and audio settings

Configuring video settings

Customizing the video settings allows for better quality images based on the needs of that video stream.

To configure video settings:

1. Enter the Video settings interface. **Configuration > Video/Audio > Video**

<table>
<thead>
<tr>
<th>Video</th>
<th>Audio</th>
<th>Display Info. on Stream</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stream Type</td>
<td>Main Stream (Normal)</td>
<td></td>
</tr>
<tr>
<td>Video Type</td>
<td>Video &amp; Audio</td>
<td></td>
</tr>
<tr>
<td>Resolution</td>
<td>1920x1080P</td>
<td></td>
</tr>
<tr>
<td>Bitrate Type</td>
<td>Variable</td>
<td></td>
</tr>
<tr>
<td>Video Quality</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Frame Rate</td>
<td>25</td>
<td>fps</td>
</tr>
<tr>
<td>Max Bitrate</td>
<td>4096</td>
<td>Kbps</td>
</tr>
<tr>
<td>Max Average Bitrate</td>
<td>2048</td>
<td>Kbps</td>
</tr>
<tr>
<td>Video Encoding</td>
<td>H.264</td>
<td></td>
</tr>
<tr>
<td>H.264+</td>
<td>ON</td>
<td></td>
</tr>
<tr>
<td>Profile</td>
<td>High Profile</td>
<td></td>
</tr>
<tr>
<td>I Frame Interval</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>SVC</td>
<td>OFF</td>
<td></td>
</tr>
<tr>
<td>Smoothing</td>
<td>50</td>
<td>Clear&lt;&gt;Smooth</td>
</tr>
</tbody>
</table>

2. In the **Stream Type** field, select **Main Stream** (normal), **Sub-Stream**, or **Third Stream**.

**Note:** Main Stream is optimal for recording and live viewing with good bandwidth. Sub Stream and Third Stream can be used for live viewing with limited bandwidth.
3. Configure the selected Stream.

**Video type:** Set the stream type to video stream (video only), or video and audio composite stream (both video and audio).

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

**Bitrate type:** Set the bitrate type to constant or variable.

**Video quality:** When the bitrate type is set to Variable, six levels of video quality are available.

**Frame rate:** Set the frame rate from 1/16 to 25 fps. The frame rate describes the frequency at which the video stream is updated. It is measured by frames per second (fps). A higher frame rate is beneficial when there is movement in the video stream, it maintains the image quality throughout.

**Max. bitrate:** Set the maximum bitrate from 32 to 16384 Kbps. The higher the value, the higher video quality. Bandwidth requirements go up with the video quality.

**Video encoding:** When the Stream Type of the camera is set to main stream, the Video encoding standard can be set to H.264 or MPEG4.

When the Stream type of the camera is sub-stream, the Video Encoding standard can be set to H.264, MJPEG, and MPEG4.

**Profile:** Basic Profile, Main Profile, and High Profile are options for coding.

**I Frame interval:** Set the I-Frame interval from 1 to 400.

**SVC:** Scalable video coding (SVC) is an extension of the H.264/AVC standard. The technology encodes the video signal with layers, a basic layer and several enhanced layers. It adapts to network conditions to transfer different video streams. For example, when bandwidth is limited, only the basic layer of data is encoded and transferred. Enable this function when you want to view the video with several terminals, for example - a smartphone, or a computer with an IP network.

**Smoothing:** It refers to the smoothness of the stream. The higher the smoothing value, the better fluency of the stream. A high value may lower video quality. A low value allows for good video quality, but will not be as fluent.

4. Click **Save.**
Configuring audio settings

Customizing the audio settings allows for better quality sounds based on the custom needs of that audio stream.

To configure audio settings:

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

2. Configure the Audio settings.
   - **Audio Encoding**: Select G722.1, G.711 ulaw, G.711 alaw, G.726, MP2L2, or PCM. When selecting MP2L2 the sampling rate and audio stream bitrate are configurable. When selecting PCM, the sampling rate is configurable.
   - **Audio Input**: Select either MicIn (microphone) or LineIn (pickup).
   - **Input Volume**: Set the volume from 0 to 100.
   - **Environmental Noise Filter**: Set the filter to on or off. When the filter is on, some background noise can be removed.

3. Click **Save**.
Configuring ROI encoding

ROI (region of interest) encoding lets you discriminate the ROI and background information in comparison. This means that the technology assigns more encoding resources to the region of interest to increase the quality of the ROI view.

**Note:** Not all cameras support this function.

**To configure ROI encoding:**
1. Enter the ROI settings interface. **Configuration > Video/Audio > ROI**

![ROI settings interface](image)

- **Stream Type**
  - Stream Type: Main Stream (Normal)

- **Fixed Region**
  - Enable
  - Region No.: 1
  - ROI Level: 3
  - Region Name:

- **Dynamic Region**
  - Enable Face Tracking
  - ROI Level: 3
2. Select the Stream Type, and decide if you want to use fixed regions or dynamic regions.

**Fixed region:** Fixed region ROI is encoding for a manually configured area. You can choose the Image Quality Enhancing level for ROI encoding, and name the ROI area.

**Dynamic tracking:** Dynamic tracking ROI is defined by intelligent analysis, such as human face detection. You can choose the Image Quality Enhancing level for the ROI encoding.

To configure Fixed Region ROI encoding:
1. Select the **Enable** checkbox.
2. Select the Region number, there are 4 regions.
3. Click **Draw Area**, and then click and drag the mouse over the live view to select the ROI.

**Note:** You can draw up to 4 ROI regions.
4. Select the ROI level to set the image enhancement level. The larger the number, the better the image quality.
5. In the **Region Name** field, enter the desired region name. For example, highway middle lane.
6. Click **Save**.

To configure Dynamic Region ROI encoding:
1. Select the **Enable Face Tracking** checkbox.
2. Select the **Enable License Plate Tracking** checkbox.
3. Select the ROI levels for each enabled feature to set the image enhancement level. The larger the number, the better the image quality.
4. In the **Region Name** field, enter the desired region name. For example, highway middle lane.
5. Click **Save**.

**Configuring displayed on-stream information**

Select the Enable Dual-VCA checkbox to enable object to be marked in the video stream. This allows you to set rules on the connected device detecting events including line crossing, intrusion, etc.
Configuring target cropping
You can specify an area on the live video to display using the third-stream, providing a more detailed view of the target area.

To crop:
1. Enter the Target Cropping settings interface.
   
   **Configuration > Advanced Configuration > Video/Audio > Target Cropping**

2. Select the **Enable Target Cropping** checkbox.

3. Select Third Stream for the stream type.

4. Select the cropping resolution for the video display of the target area.
   
   A red rectangle displays on the live video to mark the target area. Click and drag the rectangle to position the target area as desired.

5. Click **Save**.
Image settings
Follow the below instructions for configuring image settings.

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

Note: The Display parameters vary depending on the camera model.

To configure display settings:
1. Enter the Display Settings interface.
   Configuration > Image > Display Settings
2. Set the image parameters of the camera.

![Image Adjustment](image adjustment screenshot)

Image Adjustment

**Brightness**: The brightness of the image, this ranges from 1 to 100. The default value is 50.

**Contrast**: The contrast of the image, this ranges from 1 to 100. The default value is 50.

**Saturation**: The saturation of the image, this ranges from 1 to 100. The default value is 50.

**Sharpness**: The sharpness of the image, this ranges from 1 to 100. The default value is 50.
Exposure Settings

**Manual:** This is the only option for cameras with a fixed lens. This option also prohibits iris mode.

**Auto:** This option allows you to set the auto-iris level from 0 to 100. Different iris options are available based on the camera’s lens.

**Exposure Time:** This is the electronic shutter time, it ranges from 1 to 1/100,000s. Adjust this setting according to the lighting conditions.

**Gain:** Manually configure the gain of the images from 0 to 100. The larger the value, the brighter the image and amplified noise.

---

Focus Settings

**Auto:** When selecting auto, the focus is adjusted automatically based on the monitoring scenario.

**Manual:** When selecting manual, the focus is adjusted through manual lens adjustment of the zoom, focus, lens initialization, and auxiliary focus for the PTZ control interface.

**Semi-auto:** When selecting semi-auto, the camera focuses automatically when adjusting the zoon parameters.

Day/Night Switch

**Day:** The camera stays in day mode at all times.

**Night:** The camera stays in night mode at all times.

**Auto:** The camera switches between day and night mode according to lighting conditions.

**Sensitivity:** The sensitivity ranges from 0 to 7, the higher the value, the easier the mode switches.

**Filtering Time:** The time interval between the day/night switch. This ranges from 5 to 120s.

**Smart IR:** This allows adjustment of the IR LED’s power. Set it to ON, and then select Auto or Manual.
**Backlight Settings**

**BLC:** This setting compensates light sensitivity to make objects appear clear.

**WDR:** Wide dynamic range can be used when there is a high contrast of bright area and dark area in a scene.

**HLC:** High Light Compression is used with strong lights to affect image quality.

**White Balance**

The below figure shows the white balance options. Select the white balance based on the environment. For example, if there is a fluorescent lamp in the surveillance scene, select the white balance type as Fluorescent Lamp.

<table>
<thead>
<tr>
<th>AWB2</th>
<th>MWB</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWB1</td>
<td></td>
</tr>
<tr>
<td>AWB2</td>
<td></td>
</tr>
<tr>
<td>Locked WB</td>
<td></td>
</tr>
<tr>
<td>Fluorescent Lamp</td>
<td></td>
</tr>
<tr>
<td>Incandescent Lamp</td>
<td></td>
</tr>
<tr>
<td>Warm White Lamp</td>
<td></td>
</tr>
<tr>
<td>Natural Light</td>
<td></td>
</tr>
</tbody>
</table>

**Image Enhancement**

**Digital noise reduction:** Select Off, Normal, or Expert Mode.

Normal mode allows you to set the DNR level from 0 to 100. The default DNR level in normal mode is 50.

Expert mode allows you to set the DNR level from both the space DNR level and the time DNR level, each can be set from 0 to 100.

**Defog Mode:** This feature enhances subtle details to give a clean image in a foggy or misty environment.

**Electrical Image Stabilizer:** EIS (Electrical Image Stabilizer) reduces the effects of vibrations in a video.

**Grey Scale:** Select the gray scale range of the recording. Grey scale is set from 0 to 255 or 16 to 235.

**Video Adjustment**

**Mirror:** The mirror function enables you to view another aspect of the image. You can flip the image left or right and up or down.

**Rotate:** Enable the rotate function when using the camera in a narrow view scene. When installing, turn the camera to the 90 degrees or rotate the 3-axis lens to 90 degrees, and then set the corridor mode as on. You will get a normal view of the scene with 9:16 aspect ratio.

**Scene Mode:** Select indoor or outdoor depending on the location of the camera.
**Video Standard:** Select 50 Hz or 60 Hz. Choose based on video standards; 50 Hz for the PAL standard and 60 Hz for the NTSC standard.

**Capture Mode:** Select the video input mode to meet the varying demands of field of view and resolution.

**Lens Distortion Correction:** When set to on, a distorted image cause by a wide-angle lens is corrected.

---

### Configuring OSD Settings

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

**To configure OSD settings:**
1. Enter the OSD Settings interface. **Configuration > Image > OSD Settings**
2. Select the corresponding checkbox for display, name, date, or week.
3. In the **Camera Name** field, enter the name of the camera.
4. Using the drop-downs, set the time format, date format, display mode, and the OSD font size and color.
5. In the live view window, use the mouse to click and drag the text frame (e.g., IP Camera 01) to adjust the OSD position.
6. Click **Save**.

---

### Configuring privacy mask

Privacy masks let you cover certain areas on live video to prevent zones in the surveillance area from being viewed or recorded.

**To configure privacy mask**
1. Enter the Privacy Mask Settings interface. **Configuration > Image > Privacy Mask**
2. Select the box of **Enable Privacy Mask** check box.

3. Click **Draw Area**.

4. Click and drag the mouse in the live video window to draw the mask area.
   
   **Note:** You can configure 4 areas on the same image.

5. Click **Stop Drawing** to finish drawing.
   
   – or –
   
   Click **Clear All** to clear all areas without saving them.

6. Click **Save**.
Configuring picture overlay
Picture overlay lets you overlay a picture on the image. For example, you can have a logo display over the recording.

Note: The image must be in the RGB24 bmp format and no larger than 128 by 128.

To configure picture overlay:
1. Enter the Picture Overlay Settings interface.
   
   **Configuration > Image > Picture Overlay**

   ![Configuration Interface]

   2. Click **Browse** to select a picture from your PC.
   3. Click **Upload**.
   4. Select the **Enable Picture Overlay** checkbox.
   5. Set the **X** and **Y Coordinate** values for the location of the picture on the image.
   6. Set the **Picture Width** and **Height** to adjust the size of the picture.
Event settings
This section goes over configuring the network camera to respond to alarm events, including basic events and smart events.

Configuring basic events
Follow the instructions in this section to configure basic events. Basic events consist of motion detection, video tampering, alarm input, alarm output, and exception.

Configuring motion detection
Motion detection senses moving objects in the configured surveillance area, and can take alarm response actions when the alarm is triggered. To reduce the false alarm rate, select the desired configuration, normal or expert.

Normal configuration: Normal configuration shares 1 set of motion detection parameters for day and night.

Expert configuration: Expert configuration has a motion parameter set for day and another for night.

To set the motion detection area with a normal configuration:
1. Enter the Motion Detection settings interface.
   Configuration > Event > Basic Event > Motion Detection
2. Select the Enable Motion Detection checkbox.
3. Set the Enable Dynamic Analysis to Motion, enabling detected objects to be marked with green rectangles.
4. Click **Draw Area**, and then click and drag the mouse on the live video image to draw a motion detection area.

5. Click **Stop Drawing** to finish drawing.
   – or –
   Click **Clear All** to clear all areas without saving.

6. (Optional) Move the Sensitivity slider to set the detection sensitivity.

To set the arming schedule for motion detection with normal configuration:

1. Click **Arming Schedule**.

2. Click the time bar, and then drag the mouse to select the time period.

3. Click **Delete** to remove the current arming schedule, or click **Save**.

**Note:** 8 periods can be configured each day. No recording times can overlap.
To set the linkage method for motion detection with normal configuration:

1. Select the desired linkage method checkboxes.

   - **Audible Warning**: When triggered, an audible warning sounds. The device must have an audio output.
   - **Notify Surveillance Center**: When triggered, an alarm signal is sent to a remote management software.
   - **Send Email**: When triggered, an email containing alarm information is sent to the set users.
   - **Upload to FTP**: When triggered, captures an image and uploads it to the FTP server. See “Configuring FTP settings” on page 60.
   - **Trigger Channel**: When triggered, video is recorded. You must configure the recording schedule for feature functions.
   - **Trigger Alarm Output**: Triggers one or more external alarm outputs. See “Configuring alarm output” on page 84.

To set the motion detection area in expert configuration with the day/night switch set to off:

1. Click **Draw Area**, and then click and drag the mouse on the live video image to draw a motion detection area.
   
   **Note**: Up to 8 areas are supported.

2. Click **Stop Drawing** to finish drawing.
   
   – or –

   Click **Clear All** to clear all areas without saving.

3. Set the Switch Day and Night drop-down to Off.

4. Set the Area drop-down.

5. Set the arming schedule and linkage methods as above, and then click **Save**.
To set the motion detection area in expert configuration with enabled day/night switch:

1. Click **Draw Area**, and then click and drag the mouse on the live video image to draw a motion detection area.
   
   **Note:** Up to 8 areas are supported.

2. Click **Stop Drawing** to finish drawing.
   
   – or –
   
   Click **Clear All** to clear all of the areas without saving.

3. Set the Switch Day and Night drop-down to Auto-Switch.

4. Select the Area.

5. Slide the Day Sensitivity and Proportion sliders to the appropriate level.

6. Slide the Night Sensitivity and Proportion sliders to the appropriate level.

7. Set the arming schedule and linkage methods as above, and then click **Save**.

To set the motion detection are in expert configuration with a scheduled day/night switch:

1. Click **Draw Area**, and then click and drag the mouse on the live video image to draw a motion detection area.
   
   **Note:** Up to 8 areas are supported.

2. Click **Stop Drawing** to finish drawing.
   
   – or –
   
   Click **Clear All** to clear all of the areas without saving.

3. Set the Switch Day and Night drop-down to Scheduled-Switch.

   
   ![Switch Day and Night Set](image)

4. Select the start and end time for the switch.

5. Select the Area.

6. Slide the Day Sensitivity and Proportion sliders to the appropriate level.

7. Slide the Night Sensitivity and Proportion sliders to the appropriate level.

8. Set the arming schedule and linkage methods as above, and then click **Save**.
Configuring video tampering alarm

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

To configure the video tampering alarm:

1. Enter the Video Tampering settings interface.

   **Configuration > Event > Basic Event > Video Tampering**

2. Select the **Enable Video Tampering** checkbox to enable the tamper-proof detection.

3. Set the tamper-proof area.

4. Click **Edit**.

5. Set the linkage method for video tampering. Select the checkbox for Audible warning, notify surveillance center, or send email. 6. Click **Save**.
Configuring alarm input
You can configure the alarm input.

To configure the alarm inputs:
1. Enter the Alarm Input settings interface.
   - Configuration > Event > Basic Events > Alarm Input
2. Select the Alarm Input Number, and then enter an Alarm Name.
3. Select the Alarm Type, NO (Normally open) or NC (Normally closed).
4. Click Edit to set the arming schedule for the alarm input.
5. Select the checkbox for the desired linkage method.
6. If applicable, select the alarm’s PTZ actions.
7. Click Save.
   You can copy the settings to other alarm inputs.

Configuring alarm output
You can configure the alarm output.

To configure the alarm outputs:
1. Enter the Alarm Output settings interface.
   - Configuration > Advanced Configuration > Basic Events > Alarm Output
2. Select the one alarm output channel.
3. Set the Delay Time from 5 seconds to 10 minutes, or have the delay time set to manual.

**Note:** The delay time is the duration that the alarm output remains in effect after the alarm occurs.

4. Click **Edit** to set the arming schedule for the alarm input.

5. Click **Save**.

You can copy the settings to other alarm inputs.
Handling exception
There are several camera handling exceptions. The exception type can be HDD full, HDD error, network disconnected, IP address conflicted, or illegal login to the cameras.

To configure handling exceptions:
1. Enter the Exception Settings interface.
   - Configuration > Event > Basic Event > Exception
   Select the checkbox to set the actions taken for the Exception alarm.

2. Click Save.

Configuring other alarms
This section is for cameras that support external wireless alarms (access control alarm), PIR (passive infrared sensor) alarms, or Emergency alarms.

Wireless alarm
The wireless alarm signal is sent to the camera from a detector, for example – a wireless door contact. Once the alarm is triggered, a series of response actions can occur.

To configure a wireless alarm:
1. Enter the Wireless Alarm Settings interface.
   - Configuration > Advanced Configuration > Basic Event > Wireless Alarm
2. Select the wireless alarm number. 
   Up to 8 channel of external wireless alarm inputs are supported.

3. Select the **Enable Wireless Alarm** checkbox.

4. Enter a name in the **Alarm Name** field.

5. Select the checkbox for the desired linkage method.

6. Click **Save**.

7. Locate the external wireless device, and then enter the Remote Control settings interface to arm the camera and study the wireless alarm.

**Configuration > System > System Settings > Remote Control**

<table>
<thead>
<tr>
<th>Basic Information</th>
<th>Time Settings</th>
<th>RS232</th>
<th>Remote Control</th>
<th>DST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Alarm</td>
<td>1</td>
<td></td>
<td>Study</td>
<td></td>
</tr>
</tbody>
</table>

**Arm / Disarm**

<table>
<thead>
<tr>
<th>Arm</th>
<th>Disarm</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>0s</td>
<td>Set</td>
<td></td>
</tr>
</tbody>
</table>

**PIR alarm**

The PIR (passive infrared) alarm is triggered when an intruder moved within the detector’s field of vision.

**To configure a PIR alarm:**

1. Enter the PIR Alarms settings interface.

**Configuration > Advanced Configuration > Basic Event > PIR Alarm**

<table>
<thead>
<tr>
<th>Motion Detection</th>
<th>Video Tampering</th>
<th>Exception</th>
<th>PIR Alarm</th>
<th>Wireless Alarm</th>
<th>Emergency Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Arming Schedule</th>
<th>Linked Method</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Select the Enable PIR Alarm checkbox.
3. Enter a name in the **Alarm Name** field.

4. Select the checkbox for the desired linkage method. Click **Edit** to set the arming schedule.

5. Click **Save**.

6. Enter the Remote Control settings interface and arm the camera. **Configuration > Advanced Configuration > System > Remote Control**

   - **Study**
     - Remote Control: Study

   - **Arm / Disarm**
     - Arm: 0s

**Emergency alarm**

Pressing the emergency button on the camera’s remote triggers an Emergency Alarm.

**Note:** The remote control is required for an emergency alarm. The camera must study the remote control before it can connect. Access the Remote Control settings interface to study the remote control.

**Configuration > System > System > Remote Control**

To configure an emergency alarm:

1. Enter the Emergency Alarms settings interface.

   **Configuration > Event > Basic Event > Emergency Alarms**

2. Select the checkbox for the desired linkage method.

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

Configuring audio exception detection
Audio exception detects abnormal sounds in a surveillance scene. For example, the increase/decrease of sound intensity. Actions can be triggered when audio exception is detected.

To configure audio exception detection:
1. Enter the Audio Exception Detection settings interface.
   Configuration > Event > Smart Event > Audio Exception Detection

2. Select the Audio Loss Exception checkbox.
3. Select the Sudden Increase of Sound Intensity Detection and Sudden Decrease of Sound Intensity Detection checkboxes to detect when the sound rises/drops, you can set the detection sensitivity and threshold for sound intensity.

**Notes**
- The sensitivity ranges from 1 to 100. The smaller the entered value, the more severe the change must be to trigger the detection.
- The intensity threshold ranges from 1 to 100. This feature filters out environment sound. The louder the area, the higher the value should be.

4. Click **Edit** to set the arming schedule.
5. Select the linkage methods.
6. Click **Save**.

**Configuring defocus detection**

When the image is blurry due to the defocus of the lenses, an alarm can be triggered.

**To configure defocus detection:**
1. Enter the Defocus Detection settings interface.

   ![Configuration > Event > Smart Event > Defocus Detection](image)

   2. Select the **Enable Defocus Detection** checkbox.
3. Click and drag the slider to set the detection sensitivity.
   
   **Note:** The sensitivity ranges from 1 to 100. The higher the value, the easier the defocus image triggers the alarm.
4. Select the linkage method.
5. Click **Save**.
Configuring scene change detection
When the surveillance environment changes due to external factors, an alarm can be triggered. For example, when the camera is rotated or moved.

To configure scene change detection:
1. Enter the Configure Scene settings interface.
   
   Configuration > Event > Smart Event > Scene Change Detection

2. Select the Enable Scene Change Detection checkbox.

3. Click and drag the slider to set the detection sensitivity.
   
   Note: The sensitivity ranges from 1 to 100. The higher the value, the easier the scene change triggers the alarm.

4. Select the linkage method.

5. Click Save.

Configuring face detection
When a face appears in the surveillance scene, an alarm can be triggered.

To configure face detection:
1. Enter the Face Detection settings interface.
   
   Configuration > Event > Smart Event > Face Detection

2. Select the Enable Face Detection checkbox.

3. Select the Enable Dynamic Analysis for Face Detection, and then the detected face is marked with a green rectangle.
4. Click and drag the slider to set the detection sensitivity.  
   **Note:** The sensitivity ranges from 1 to 5. The higher the value, the easier faces are detected.

5. Click **Arming Schedule**.

6. Select the linkage method.

7. Click **Save**.

---

**Configuring line crossing detection**

When an object crosses a pre-defined virtual line, an alarm can be triggered.

**To configure line crossing detection:**

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

2. Select the **Enable Line Crossing Detection** checkbox.

3. Select the line in the Detection Settings drop-down.

4. Click **Draw Area**, and virtual line displays on the video feed.

5. Click and drag the line, placing it where desired. A red square appears on each end of the line, drag the red squares to define the shape and length of the line.
6. Select the line crossing direction.
   - **A<->B**: Objects crossing from side a or b to the other side are detected.
   - **A->B**: Only an object crossing from the A side of the line to the B side is detected.
   - **B->A**: Only an object crossing from the B side of the line to the A side is detected.

7. Click and drag the slider to set the detection sensitivity.
   - **Note**: The sensitivity ranges from 1 to 100. The higher the value, the easier the line crossing action triggers the alarm.

8. Repeat steps 2 through 7 for each line. Up to 4 lines can be configured.

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

10. Select the linkage method.

11. Click **Save**.
Configuring Intrusion detection
When an object enters and loiters in a pre-defined virtual region, an alarm can be triggered.

To configure intrusion detection:
1. Enter the Intrusion Detection settings interface.

   Configuration > Event > Smart Event > Intrusion Detection

2. Select the Enable Intrusion Detection checkbox.
3. Select the region from the detection drop-down.
4. Click Draw Area.
5. Click on the live video to specify the regions.
6. Configure the intrusion sliders.
   - **Threshold**: The time of the object loitering in a region. This ranges from 0s to 10s. If the slider is set to 0, the alarm is triggered immediately.
   - **Sensitivity**: The size of an object which can trigger the alarm. This ranges from 0 to 100. When the sensitivity is high, a very small object can trigger the alarm.
**Percentage:** The ratio of the in-region part of the object which triggers the alarm. For example, if the percentage is at 50, when the object enters the set region and occupies 50% of the region, an alarm is triggered. This ranges from 0 to 100.

7. Repeat steps 4 through 6 for each region, up to 4 can be set.
8. Click **Edit** to set the arming schedule.
9. Select the linkage method.
10. Click **Save**.

**Configuring region entrance detection**
When an object enters a pre-defined virtual region, an alarm can be triggered.

To configure region entrance detection:
1. Enter the Region Entrance Detection settings interface.

**Configuration > Event > Smart Event > Region Entrance Detection**
2. Select the **Enable Region Entrance Detection** checkbox.
3. Select the region from the detection drop-down.
4. Click **Draw Area**.
5. Click on the live video to specify the regions.
6. Click and drag the slider to set the detection sensitivity.
   
   **Note:** The sensitivity relates to the size of the object entering the region. The sensitivity ranges from 1 to 100. When the sensitivity is high, a very small object can trigger the alarm.
7. Repeat steps 3 through 6 for each region, up to 4 can be set.
8. Click **Edit** to set the arming schedule.
9. Select the linkage method.
10. Click **Save**.

**Configuring region exiting detection**

When an object exits a pre-defined virtual region, an alarm can be triggered.

**To configure region exit detection:**

1. Enter the Region Exit Detection settings interface.

   **Configuration > Event > Smart Event > Region Exit Detection**
2. Select the **Enable Region Exit Detection** checkbox.
3. Select the region from the detection drop-down.
4. Click **Draw Area**.
5. Click on the live video to specify the regions.
6. Click and drag the slider to set the detection sensitivity.
   
   **Note:** The sensitivity relates to the size of the object exiting the region. The sensitivity ranges from 1 to 100. When the sensitivity is high, a very small object can trigger the alarm.
7. Repeat steps 3 through 6 for each region, up to 4 can be set.
8. Click **Edit** to set the arming schedule.
9. Select the linkage method.
10. Click **Save**.

**Configuring unattended baggage detection**

When an object is left in a pre-defined region, an alarm can be triggered. For example, when baggage, a purse, or dangerous materials are left in a pre-defined region, an alarm is triggered.

To configure unattended baggage detection:

1. Enter the Unattended Baggage Detection settings interface.
   
   **Configuration > Event > Smart Event > Unattended Baggage Detection**
2. Select the **Enable Unattended Baggage Detection** checkbox.
3. Select the region from the detection drop-down.
4. Click **Draw Area**.
5. Click on the live video to specify the regions.
6. Set the threshold and sensitivity sliders.
   
   **Threshold:** The time the object is left in the region. This ranges from 5s to 20s. If the slider is set to 10, the alarm is triggered after the object has been in the same location for 10 seconds.
   
   **Sensitivity:** The size of an object which can trigger the alarm. This ranges from 0 to 100. When the sensitivity is high, a very small object can trigger the alarm.
7. Repeat steps 4 through 6 for each region, up to 4 can be set.
8. Click **Edit** to set the arming schedule.
9. Select the linkage method.
10. Click **Save**.
Configuring object removal detection
When an object is removed from a pre-defined region, an alarm can be triggered.

To configure an object removal detection:
1. Enter the Object Removal Detection settings interface.
   *Configuration > Event > Smart Event > Object Removal Detection*
2. Select the **Enable Object Removal Detection** checkbox.
3. Select the region from the detection drop-down.
4. Click **Draw Area**.
5. Click on the live video to specify the regions.
6. Set the threshold and sensitivity sliders.
**Threshold:** The time the object is missing from the region. This ranges from 5s to 20s. If the slider is set to 10, the alarm is triggered after the object has been missing from the region for 10 seconds.

**Sensitivity:** The size of an object which can trigger the alarm. This ranges from 0 to 100. When the sensitivity is high, a very small object can trigger the alarm.

7. Repeat steps 4 through 6 for each region, up to 4 can be set.
8. Click **Edit** to set the arming schedule.
9. Select the linkage method.
10. Click **Save**.
VCA configuration
Video content analysis (VCA) is available in most Clare Vision Plus cameras. VCA gives the camera the ability to analyze and detect information about the video recording.

Behavior analysis
When the analysis detects suspicious behavior, an alarm can be triggered.

Figure 16: Behavior Analysis

VCA information
There are several analysis algorithms.

Note: Verify that the desired rules are enabled. Browse to Rules.

Configuration > Local Configuration > Rules

Display Information: The settings below modify the display of the image/live video.

Display Target into on Alarm Picture: When an alarm image is taken and uploaded, a frame appears around the target.

Display Rules info. on Alarm Picture: The target and area have a frame in the alarm image.

Display VCA info. on Stream: Green frames appear on the target in live view and playback.
**Snapshot Setting:** This allows you to set the quality and resolution of the captured images.

- **Upload JPEG Image to Center:** When triggered, this option uploads the captured image to the surveillance center.
- **Picture Quality:** The quality of the image. Select high, medium, or low.
- **Picture Resolution:** The resolution of the image. Select CIF, 4CIF, 720P, or 1080P.

**Camera calibration**

Camera calibration measures and calculates the size of targets. When the camera is calibrated, VCA detection is more accurate.

**To calibrate the camera:**
1. Select the Camera Calibration checkbox.
2. Select the calibration mode.
   - **Input Basic Data:** Manually enter the camera’s mounting height, viewing angle, and horizon ratio.
   - **Draw on Live View:** Click Draw Verification Line (Horizontal)/(Vertical) to draw a line displaying on live view, and then enter the length in the **Real Length** field. When the line is drawn, the camera is able to assess the object in view.
3. (Optional) Select the Enable Verification of Camera Calibration, and then click **Horizontal Verify/Vertical Verify**. This allows you to draw a line on the live video. Clicking calibrate allows the camera to determine the line length to the actual length.
4. Click **×** to remove drawn lines
5. Click **Save**.

**Note:** If live view is not active while calibration is taking place, the camera will not calibrate accurately.
Shield region

The shield region allows you to designate an area that behavior analysis ignores. You can configure up to 4 shield regions. For example, you have a birdcage with lots of activity. You do not want the birds to trigger an alarm, so you create a shield for the region of the cage in live view.

To configure a shield region:

1. Click **Shield Region**.
2. Click the hexagon.
   
   Draw the area using the left and right buttons on your mouse. Left-click to add an end-point and right-click to finish.

**Notes**

- Shapes can have up to 10 sides.
- If live view is not active, you will not be able to create shield regions.

3. Click **Save**.
Rule

Behavior analysis supports many behaviors, including but not limited to line crossing detection, intrusion, region entrance, and region exiting. See each behaviors corresponding page for more information.

Figure 17: Rule configuration interface

To configure rule:
1. Click the Rule tab.
2. Select the Single Rule checkbox.
3. Configure the rule settings.

Note: When configure the rule settings, live video must be active.

Filter type: This selects the size of the object that triggers the alarm. The filter can be set to pixels or the actual size.
- **Pixels:** This allows you to draw an area of maximum and minimum size on the live view for each rule.
• **Actual Size:** This allows you to enter the length and width for the maximum and minimum sizes.

  **Note:** Verify that the camera calibration is configured for actual size.

**Detection Target:** This allows you to select detection for humans, vehicles, or both to detect all objects in the region.

**Draw line/area:** When using line crossing detection, you must draw a line and select the crossing direction. The line is bidirectional (A to B, or B to A). For other events, such as intrusions or region entrance, you must configure the line. Left-click the live video to set end points for the area, and then right click to finish the drawing.

4. Select the Combined Rule checkbox. This allows you to combine 2 single rules.

5. Select 2 configured rules (Rule A and Rule B) to form a combined rule, set the time intervals, and then select the trigger order.

**Notes**

• Setting the rule type to none prevents behavior analysis.

• Trigger order for single rules can be set to In Ascending Order or In Ascending/Descending Order.

• Configure up to 8 single rules and 2 combined rules.

6. Click **Save**.

7. Click **Arming Schedules**, and then click **Edit** to set the arming schedule

8. Click **Alarm Linkage**, and then select the linkage method for each rule.

9. Click **Save**.
Advanced configuration

Behavior analysis has advanced parameter configuration options.

Figure 18: Parameter tab

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Global Size Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavior Analysis Version</td>
<td>V3.5.0build20150513</td>
</tr>
</tbody>
</table>

**Detection Parameters**

- **Detection Sensitivity (0-4):** The sensitivity level at which the camera detects a target. The higher the value, the easier a target is recognized, but the higher the misinformation. The default value, 3, is recommended.

- **Background Update Rate (0-4):** The speed that the new scene replaces the previous scene. The default value, 3, is recommended.

- **Single Alarm:** When single alarm is selected an object will only trigger one alarm. If it is not selected an object could trigger an alarm multiple times.

- **Leave Interface Suppression:** Select this to interference cause by object leaving the configured region.

- **Output Type:** Select the frame position.

- **Restore Default:** Clicking this defaults the parameters.

- **Restart VCA:** This restarts the behavior analysis algorithms library.

**Detection Sensitivity (0-4):** The sensitivity level at which the camera detects a target. The higher the value, the easier a target is recognized, but the higher the misinformation. The default value, 3, is recommended.

**Background Update Rate (0-4):** The speed that the new scene replaces the previous scene. The default value, 3, is recommended.

**Single Alarm:** When single alarm is selected an object will only trigger one alarm. If it is not selected an object could trigger an alarm multiple times.

**Leave Interface Suppression:** Select this to interference cause by object leaving the configured region.

**Output Type:** Select the frame position.

**Restore Default:** Clicking this defaults the parameters.

**Restart VCA:** This restarts the behavior analysis algorithms library.

To configure the Global Size Filter:

1. Select the **Global Size Filter** checkbox.
2. Select the filter type.

**Pixels:** This allows you to draw an area of maximum and minimum size on the live view for each rule.

**Actual Size:** This allows you to enter the length and width for the maximum and minimum sizes.

**Notes**

- The drawn area is converted to pixels by the background algorithm.
- The global size filter can only be configured when live view is active.
- Maximum sizes must be set to larger than the minimum sizes.

3. Click **Save**.

**Face capture**

Face capture detects and captures faces appearing in the set region. Face characterization including the age, gender, and glasses appearance is uploaded with the captured image.

**Figure 19: Face capture interface**

---

**VCA Info**

When the analysis detects suspicious behavior, an alarm can be triggered.

**VCA information**

There are several analysis algorithms.

**Display Information:** The settings below modify the display of the image/live video.

**Display Target into. on Alarm Picture:** When an alarm image is taken and uploaded, a frame appears around the target.

**Display Rules info. on Alarm Picture:** The target and area have a frame in the alarm image.
**Display VCA info. on Stream:** Green frames appear on the target in live view and playback.

**Snapshot Setting:** This allows you to set the quality and resolution of the captured images.

**Shield region**

The shield region allows you to designate an area that face capture ignores. You can configure up to 4 shield regions.

**To configure a shield region:**

1. Click **Shield Region**.
2. Click **Draw Area**.
   
   Draw the area using the left and right buttons on your mouse. Left-click to add an end-point and right-click to finish.

   **Notes**
   
   - Shapes can have up to 10 sides.
   - If live view is not active, you will not be able to create shield regions.
3. Click **Save**.

**Rule**

Configure rules for face capture.

**To configure rule:**

1. Select the **Face Capture** rule checkbox.
2. Click Minimize Pupil Distance to set a minimum pupil distance. This helps the camera identify the target.
3. Click **Draw Area**.
   
   Draw the area using the left and right buttons on your mouse. Left-click to add an end-point and right-click to finish.

   **Notes**
   
   - Shapes can have up to 10 sides.
   - If live view is not active, you will not be able to create shield regions.
4. Click **Save**.
Advanced configuration

Face capture has advanced parameter configuration options.

**Generation Speed (1-5):** The speed at which the target is identified. The higher the speed, the faster the target is identified. Setting a low speed helps reduce misinformation. For example, posters on the wall or paintings are not detected with a low speed. We recommend leaving the speed at the default, 3.

**Capture Times (1-10):** The times at which a face is captured while in the configured region.

**Sensitivity (1-5):** The sensitivity in target identification. The higher the value, the easier a face is recognized. We recommend leaving the sensitivity at the default, 3.

**Capture Interval (1 to 255):** The frame interval at which pictures are captured. If the value is set to 1, the default, the camper captures the face in every frame.

**Capture Sensitivity (0-20):** The threshold at which the camera sees the target as a face. Only when the face score from the algorithm is equal or higher than the value, does the camera treat the target as a face. We recommend leaving the capture sensitivity at the default, 2.

**Face Capture Advanced Parameters**

**Face Exposure:** Select the face exposure checkbox.

**Reference Brightness (0-100):** The reference brightness of a face in exposure mode. When a face is detected, the camera adjusts the brightness to the set level. The higher the value, the brighter the face.

**Minimum Duration (1-60min):** The minimum duration of the camera exposure on faces.

**Note:** If face exposure is enabled, verify that the WDR function is disabled, and that the manual iris is selected.

**Enable Face ROI:** When the camera captures a face, that area is treated as the region of interest, the image quality of the region improves.

**Restore Default:** Click Restore to restore all advanced configuration settings.
### Detection Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation Speed</td>
<td>3</td>
</tr>
<tr>
<td>Capture Times</td>
<td>1</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>5</td>
</tr>
<tr>
<td>Capture Interval</td>
<td>2</td>
</tr>
<tr>
<td>Capture Sensitivity</td>
<td>10</td>
</tr>
</tbody>
</table>

- **Face Exposure**

- **Reference Brightness**
  - Value: 50

- **Min. Duration**
  - Value: 1

- **Enable Face ROI**

Setting the stream type as H.264 is required to make sure the ROI functioning.

### Restore Parameters

- **Restore defaults**
  - **Restore**
Heat map

The heat map is a graphical representation of data. This function analyzes visit and dwell time of customers or people in a configured area.

To configure a heat map:
2. Click the Heat Map Configuration tab.
3. Select the Enable Heat Map checkbox.
4. Click **Draw Area**, and define the areas for heat values.

   Draw the area by left-clicking 4 endpoints in the live view window, and then right-clicking to finish drawing.

**Notes**

- You can configure up to 8 areas.
- You can click Select All, and select the entire live view window.

5. Configure the drawn area parameters.

   - **Detection Sensitivity (0-100)**: The sensitivity level at which the camera identifies a target. The higher the value, the easier a target is recognized, but the higher the misinformation. The default value, 50, is recommended.
   - **Background Update Rate (0-100)**: The speed that the new scene replaces the previous scene. The default value, 50, is recommended.
   - **Scene Change Level (0-100)**: The level at which the camera responds to a dynamic environment. The default value, 50, is recommended.
   - **Minimum Target Size (0-100)**: The minimum size that the camera identifies a target. The default value, 50, is recommended.
   - **Target Track**: Select on or off to enable/disable target tracking.

6. Click **Edit** to set the arming schedule.

7. Select the linkage methods, and then click **Save**.

**Note:** For Heat Map statistics, access the application **People counting**

The people counting function helps calculate the number of people who entered or left the specified region.

**Notes**

- People counting is supported in some iDS camera models.
- We recommend installing the camera vertically with the ground.

To configure **people counting**:

1. Browse to People Counting.

   **Configuration > People Counting**
2. Click the **People Counting Configuration** tab.

3. Select the **Enable People Counting** checkbox.

4. (Optional) Select the **Enable OSD Overlay** checkbox to display the count on the live video.

5. Set the detection line.

   A line is set on the live video, and people crossing (entering or exiting) the line are counted.

**Notes**

- When drawing the detection line, ensure that it covers the entire entrance/exit.
- Click \( \times \) to delete the detection line.
- Click \( \Rightarrow \) to change the line direction.
- Click \( / \) to view the live image.
- Click \( 0 \) to reset the counter.
6. Select the Camera Calibration checkbox.

**Camera calibration**: Set the width of objects counted as people.

**Blue horizontal lines**: A single blue line indicates the detected width of a person. Up to 8 blue lines can be present on each side of the detection line.

**Calibration line (green vertical)**: The distance from the left endpoint to the calibration line indicates the width of a person. Drag the calibration line to adjust the distance according to the blue line distribution.

**Advanced**: Adjust the position and size of the detection line and calibration line.

a. Drag the cursor, or input the values in the text field, to set the detection line start and end points.

b. Click ☰ to refresh the calibration line.

c. Drag the cursor, or input the desired values, to set the calibration width. Set the value as suggested, or customize it according to need.

7. Click **Reset Counter** to clear the number of people to 0.

8. Click **Edit** to set the arming schedule.

9. Select the Notify Surveillance Center checkbox to set the linkage action.

10. Click **Save**.

**Note**: For People Counting statistics, access the application.

**Counting**

The counting function calculates the number of objects that entered or exited a set region. This feature is generally used for monitoring entrances/exits.

**Notes**

- This feature is only available on specific non-iDS cameras.
- This function is similar to people counting on iDS cameras, but counting does not require calibration settings.
- Install the camera vertically to get the most accurate results.
To configure counting:

1. Enter the Counting Configuration interface.

   **Configuration > Counting**

   - Enable Counting
   - Enable OSD Overlay

2. Click the **Counting Configuration** tab.

3. Select the **Enable Counting** checkbox.

4. (Optional) Select the **Enable OSD Overlay** checkbox.

   **Note:** This displays the real-time number of objects that enter/exit on the live video.
5. Set the detection line.

   **Note:** This is a reference line. Objects crossing this line (entering/exiting) are counted.
   
   a. Click /.
   
   b. Click and drag the line to adjust its position, and then click and drag the endpoints to adjust its length.

   **Note:** If the detection line is used on an entrance/exit, it must span the entire doorway/area to render an accurate count.

   o Click ✗ to delete the detection line.
   
   o Click ⇔ to change the line direction.
   
   o Click / to view the live image.
   
   o Click 0 to reset the counter.

6. Click **Edit** to set the arming schedule.

7. Select the **Notify Surveillance Center** checkbox or set the desired linkage method.

8. Click **Save**.

**Road traffic**

Detect and monitor traffic using vehicle detection or mixed-traffic detection. Use the road traffic features to send a signal notifying the surveillance center with the captured image.

**Vehicle detection:** A passing vehicle is detected, a picture of the license plate, the vehicle color, logo, and other visual information is captured.

**Mixed-traffic detection:** A pedestrian, vehicle, and non-motor vehicle is detected. A picture captures the visual information.

**To configure detection settings:**

1. Select the detection type.

   **Note:** When switching the traffic type, you must reboot the device for the new settings to take effect.

2. Select the **Enable** checkbox.

3. Select the lane number. Select up to 4 lanes.

4. Click and drag the lane line to the desired position, or click and drag the line endpoint to adjust the length and angle.

5. Adjust the zoom ratio.

   **Note:** Only 1 license plate is captured in each lane.
6. Select the province/state abbreviation.

7. Set the arming schedule for vehicle detection.
   a. Click **Edit**.
   b. Select the arming schedule day.
   c. Click **to edit the time**.
   d. (Optional) After setting the arming schedule, click Copy to copy the schedule to other days.
   e. Click **Ok**.

   **Note**: Time periods cannot overlap.

8. Select the linkage method.

   **Notify surveillance center**: This option sends an exception/alarm to a remote management software when the alarm is triggered.

   **Upload to FTP**: This captures the image, uploads it to the FTP server, and saves the picture on the local SD card/NAS when an alarm is triggered.

9. Click **Save**.
Storage settings
To configure record settings, make sure that you have a network storage device in the network, or have the SD card inserted in your camera.

Configuring recording schedule
There are two kinds of camera recordings: manual recordings and scheduled recordings. In this section, follow the instructions to configure the scheduled recording. By default, the record files of the scheduled recording are stored in the SD card (if supported) or in the network disk.

To configure a recording schedule:
1. Enter the Record Schedule Settings interface.
   
   Configuration > Storage > Storage Settings > Capture

2. Access the Capture Schedule tab.
3. Click Advanced, and then set the stream type.

4. Click Save.
To configure snapshot settings:

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

2. Select the desired snapshot type checkbox.

   **Enable Event Timing:** This enables a continuous snapshot based on a schedule.
   **Enable Event-triggered Snapshot:** This enables a snapshot based on a trigger event.

3. Select the snapshot quality.

   ![Snapshot Settings Interface](Image)

4. Set the time interval between snapshots. 5. Click **Save**.
Configuring Net HDD

The network disk must be added and available in the network and configured to store recorded files, log files, and pictures.

To add the Net HDD:

1. Enter the Net HDD interface.

   **Configuration > Storage > Storage Management > Net HDD**

   1. Enter the networks disk’s IP address and file path.
   2. Select the mounting type.
   3. Click **Save**.

To initialize the network disk:

1. Enter the HDD interface.

   **Configuration > Storage > Storage Management > HDD Management**

   2. If the disk’s status is uninitialized, select the corresponding checkbox to select the disk and click **Format**. After initialization, the status displays normal.
3. Define the quota for recordings and pictures.
   a. Enter the quota percentage for pictures and recordings.
   b. Click **Save**, and then refresh the browser.

<table>
<thead>
<tr>
<th>Quota</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Max. Picture Capacity</td>
<td>4.75GB</td>
</tr>
<tr>
<td>Free Size for Picture</td>
<td>4.75GB</td>
</tr>
<tr>
<td>Max. Record Capacity</td>
<td>14.50GB</td>
</tr>
<tr>
<td>Free Size for Record</td>
<td>14.50GB</td>
</tr>
<tr>
<td>Percentage of Picture</td>
<td>25%</td>
</tr>
<tr>
<td>Percentage of Record</td>
<td>75%</td>
</tr>
</tbody>
</table>

   **Note:** Connect up to 8 NAS disks to the camera.

---

### Configuring memory card detection

Memory card detection allows you to view the memory card status, lock the memory card, and receive notifications when the memory card is detected as abnormal.

**Note:** Memory card detection function is only supported for specific memory cards and camera models.

**To configure the memory card detection:**

1. Enter the Memory Card Detection configuration interface.
   
   **Configuration > Storage > Storage Management > Memory Card Detection**

<table>
<thead>
<tr>
<th>HDD Management</th>
<th>Net HDD</th>
<th>Memory Card Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Detection</td>
<td>RW Lock</td>
<td>Arming Schedule</td>
</tr>
</tbody>
</table>

   - Remaining Lifespan: 99%
   - Health Status: Normal

   **Save**

2. Click the **Status Detection** tab to view the memory card status.
**Remaining Lifespan:** Displays the percentage of the remaining lifespan. Memory card lifespan is influenced by capacity and bitrate.

**Health Status:** Displays the condition of the memory card; good, bad, or damaged. When the arming schedule and linkage methods are set and the status is anything other than good.

3. Click the R/W tab to add and lock the memory card.

   **Add a lock**
   a. Set the lock switch to ON.
   b. Enter the password.
   c. Click Save.

   **Unlock**
   a. If a camera locks the memory card, it is automatically unlocked.
   b. If the memory card has a lock, access the HDD Management interface to unlock the memory card.
      1. Select memory card, and then click Unlock.
      2. Enter the password as prompted.

   **Remove the lock**
   c. Set the Lock Switch to OFF.
   d. Enter the password.
   e. Click Save.

4. Set the arming schedule and linkage method.
5. Click Save.

**Configuring lite storage**
Reduce the frame rate and bitrate of the video stream when there is no motion. The reduction lengthens the SD card’s storage time.

**Note:** Files recorded in storage are played back at the full frame rate (25 to 30 fps).

**To configure lite storage:**
1. Enter the Lite Storage interface.
   
   Configuration > Storage > Storage Management > Lite Storage

2. Select the Enable checkbox, and then enter the storage time.
   
   **Note:** The available SD space is displayed in the field above.

3. Click Save.
Playback
View the recorded video files stored in the network disks or SD cards.

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

![Playback interface]

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

![Calendar and search interface]

3. Click to play the video files found on this date.
Use the toolbar on the bottom of Playback interface to control play.

![Playback toolbar]

Table 3: Description of the Playback toolbar

<table>
<thead>
<tr>
<th>Icon</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>➤</td>
<td>Play</td>
</tr>
<tr>
<td>❌</td>
<td>Pause</td>
</tr>
<tr>
<td>❌</td>
<td>Stop</td>
</tr>
<tr>
<td>🔄</td>
<td>Slow down</td>
</tr>
<tr>
<td>➤</td>
<td>Speed up</td>
</tr>
<tr>
<td>➤</td>
<td>Playback by frame</td>
</tr>
<tr>
<td>📸</td>
<td>Capture a picture</td>
</tr>
<tr>
<td>✂️</td>
<td>Start/stop clipping video files</td>
</tr>
<tr>
<td>🜶/🔍</td>
<td>Enable/disable digital zoom</td>
</tr>
<tr>
<td>📺</td>
<td>Audio on and adjust volume/Mute</td>
</tr>
<tr>
<td>📠</td>
<td>Download video files</td>
</tr>
</tbody>
</table>

**Note:** You can choose the file path locally for downloaded playback video files and pictures in Local Configuration interface.

To locate an exact playback point, you can drag the progress bar with the mouse, input the time and click 🔽, or click 🔽 to zoom out/in the progress bar.

**Figure 20:** Set time

![Set playback time]

**Figure 21:** Progress bar

![Progress bar]
Picture
Click the **Picture** tab to enter the picture searching interface. Search, view, and download the pictures stored in the local storage/network storage.

**Notes**
- Verify that the HDD, NAS, or memory card are configured before searching.
- Verify that the capture schedule is configured.

**Configuration > Storage > Schedule Settings > Capture**

To search for pictures:
1. Select the file type.
2. Select the start/end time.
3. Click **Search**.
4. Select the checkboxes for the desired pictures, and then click **Download**.

**Note:** Up to 4,000 pictures are displayed at one time.
Application
Click Application to enter the statistics counting interface. Search, view, and download the statistical information stored in the local/network storage.

Face capture statistics
After enabling the face capture function, view and download the face data from the Application tab. Use different charts to view the data.

To access face capture statistics:
1. Select the report type.
2. Select the statistics type.
3. Select the start/end time, and then click Counting.

   The results are displayed. Click Table or Pie Chart to view the results in different ways.

   Note: If you list the counting results in a table, you can export the data to an Excel file.

People counting statistics
After enabling the people counting function, view and download the face data from the application tab. Use different charts to view the data.

To access people counting statistics:
1. Select the report type.
2. Select the statistics type.
3. Select the start/end time, and then click Counting.

   The results are displayed. Click Table, Bar Chart, or Line Chart to view the results in different ways.

   Note: If you list the counting results to list statistics, you can export the data to an Excel file.
Heat map statistics
After enabling the heat map function, view and download the face data from the application tab. Use different charts to view the data.

To access heat map statistics:
1. Select the report type.
2. Select the start/end time, and then click Counting.
3. The results are displayed. Click Space Heat Map or Time Heat Map to view the results in different ways.

Note: If you list the map results to list statistics, you can export the data to an Excel file.

Counting statistics
After enabling the counting function, view and download the face data from the application tab. Use different charts to view the data.

To access counting statistics:
1. Select the report type.
2. Select the statistics type.

3. Select the start time, and then click **Counting**.

4. Select **Table**, **Bar Chart**, or **Line Chart** to view the results.

   **Note:** If you select a table to list statistics, you can export the data to an Excel file.
Understanding camera capacity in an NVR

When setting up your NVR and cameras, you may notice that some of the camera images may not display in Live View. This most often occurs when you are displaying images in 1×5 mode, or 1×7 mode because the total bit rate for all cameras is exceeding the NVR’s capacity. The actual capacity depends on the total bit rate from all the cameras. However, it is good practice to allow some headroom for machine operations, such as remote streaming.

<table>
<thead>
<tr>
<th>NVR model</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-channel</td>
<td>20 Mb</td>
</tr>
<tr>
<td>8-channel</td>
<td>40 Mb</td>
</tr>
<tr>
<td>16-channel</td>
<td>80 Mb</td>
</tr>
<tr>
<td>32-channel</td>
<td>160 Mb</td>
</tr>
<tr>
<td>64-channel</td>
<td>160 Mb</td>
</tr>
</tbody>
</table>

To fully understand NVR capacity, it is necessary to understand the concepts of streaming video, resolution, quality, and bit rate. Streaming video is content sent in compressed form over a network and processed in real time, that is, as it is received.

**Streaming video types**

**Main Stream:** the high quality video that is being recorded and may be streamed.

**Sub Stream:** never recorded; intended for streaming only. Default is 704 × 480, 584 Kbps at 8 fps.

Can be video alone, or video and audio compressed together. Audio requires very little bandwidth.

The combination of the main stream and sub streams make up the total bit rate of each camera. This is expressed in Kbps (kilobits per second) or Mbps (megabits per second).

Bit rate is determined by the selected resolution (1280 × 720, 1920 × 1080, 2560 × 1920, etc.), frame rate (frames per second), and video quality (the amount of compression being applied to each camera).

**Example**

32 channels of 720P cameras at 15 fps with good image quality will have 32 x (1536 + 512) = 65536 Kbps (about 66Mbps), so the 32-channel NVR can support them.

Each channel can support a different camera, as long as they do not exceed the total bit rate limit. It is entirely possible to mix 5 MP cameras with 4CIF IP cameras, etc. Generally, 5 MP at 30 fps requires around 20 Mbps for best quality. A 4-channel NVR is currently limited to 16 Mbps.
Adjusting settings

Be aware of your NVR’s capacity and make adjustments if necessary. Adjust the bit rate by lowering the resolution, frame rate, or video quality setting.

To adjust the setting:

1. Enter the Live View settings interface.
2. Adjust the Resolution, Frame Rate, and Video Quality settings.
Camera installation
The below camera installations are subject to change based on model. For specifications, see each camera's corresponding data sheet.

Before you start
• Make sure that the device in the package is in good condition and all the assembly parts are included.
• Make sure that all the related equipment is powered off during the installation.
• Make sure the power supply matches the required voltage to avoid damage.
• If the product does not function properly, contact your dealer or the nearest service center. Do not disassemble the camera for repair or maintenance by yourself.
• Make sure that the wall is strong enough to withstand three times the weight of the camera.

Cube camera installation
To ensure the camera operates properly, install the camera according to the instructions below.

Note: The cube camera instructions use the ClareVision CV-B13C10-IDIW.

To mount the camera on the stand:
1. Assemble the 3-axis bracket.
2. Align the camera body on the bracket, and then rotate the camera to tighten and secure the bracket.

3. Attach cables.

To mount the camera on the stand:
1. Drill the cable hole and the screw holes in the ceiling according to the supplied drilling template.

2. Fix the mounting base to the ceiling with screws.
3. Attach the camera to the bracket.

4. Adjust the surveillance angle.
   a. Loosen the knob to adjust the pan and tilt positions.
   b. After adjusting the angle of the camera to the desired position, fasten the knob.
Dome camera installation
To ensure the camera operates properly, install the camera according to the instructions below.

Note: The dome camera instructions use the ClareVision CV-M13D10-ODI.

Disassembling
To disassemble the camera:
1. Loosen the three screws on the edge of the lower dome with screwdriver.
2. Open the lower dome and remove the inner black liner, as shown below.

Mounting
To mount on a ceiling:
1. Disassemble the camera as described in the previous section.
2. Attach the drill template to the place where you want to fix the camera.
3. As shown in the drill template below, drill three screw holes in the ceiling.
4. If you want to route the cables inside the ceiling, drill a cable hole in the ceiling according to the drill template. Skip this step, if you want to route the cables on the surface of the ceiling.

5. Attach the camera to the ceiling by aligning the holes of the back box with the holes on the ceiling.

6. Secure the camera with the supplied screws, as shown below.

7. Route the cables through the cable hole.

8. Connect the video output connector to the monitor. Connect the power connector to the power supply.

9. Adjust the image and focus.

10. Install the inner black liner back to the camera.

11. Install the lower dome back to the camera and secure it with screws, as shown below.
Conduit installation on the side
If you want to route the cables from side of the camera, you need to follow the steps below to install a conduit for cable routing.

To route the cables from the side:
1. Rotate the waterproof plug counterclockwise to remove it from the camera.
2. Remove the waterproof plug.
3. Route the power cable and network cable through the side outlet to the conduit.
4. Align the conduit to the side outlet and rotate clockwise until it is tight.

Note: For wall mounting, position the side outlet directly downward for waterproofing.
Ceiling mounting with gang box

To mount the camera on the ceiling with a gang box:

1. Disassemble the camera.
2. Install the gang box in the ceiling.
3. Attach the mounting base to the gang box with two screws.
4. Route the cables through the hole in the center of the mounting base.
5. Align the camera with the mounting base.
6. Tighten the screws to secure the camera with the mounting base.
7. Connect the video output connector to the monitor. Connect the power connector to the power supply.
8. Adjust the image and focus.
9. Install the inner black liner back to the camera.
10. Align the lower dome with the camera.
11. Tighten the screws to secure the lower dome with the camera, as shown below.

Wall mounting
For the wall mounting, you have to purchase a wall mount.

To mount the camera on the wall:
1. Disassemble the camera.
2. Install the wall mount and mounting adapter, as shown below.
3. Align the screw holes of the mounting base with the corresponding screw holes of the mounting adapter.
4. Secure the mounting base to the mounting adapter with four screws.

5. Route the cables through the hole in the center of the wall mount.

6. Align the camera with the mounting base.

7. Tighten the set screws to secure the camera with the mounting base.

8. Connect the video output connector to the monitor. Connect the power connector to the power supply.

9. Adjust the image and focus.
10. Install the inner black liner back to the camera.
11. Align the lower dome with the camera.
12. Tighten the screws to secure the lower dome with the camera.

Image and focus adjusting

To adjust image and focus:
1. Make the three-axis adjustment.
2. View the camera image using the monitor.
3. Rotate the panning table to adjust the panning position of the camera.
4. Rotate the tilting axes to adjust the tilting position of the camera.
5. Rotate the lens table to adjust the azimuth angle of the image.

To adjust zoom and focus:
1. View the camera image using the monitor.
2. Loosen the zoom lever and move the lever between T (Tele) and W (Wide) to obtain the appropriate angle of view.
3. Tighten the zoom lever.
4. Loosen the focus lever and move the lever between F (Far) and N (Near) to obtain the optimum focus.

5. Tighten the focus lever.
Bullet camera installation
To ensure the camera operates properly, install the camera according to the instructions below.

Note: The bullet camera instructions use the ClareVision CV-B13B10-ODI.

To mount the camera to a wall:
1. Attach the drill template on the wall.
2. Secure the camera to the wall with the supplied expansion screws.
3. Adjust the lens.
4. Loosen the adjustable nut on the bracket.
5. Adjust the panning angle [0 to 360°] of the camera.
6. Adjust the tilting angle [0 to 90°] of the camera.
7. Rotate 0 to 360° to adjust azimuth angle of the image.
8. Tighten the adjustable nut to complete the installation.
Appendix 1

SADP software introduction

Description of SADP

SADP (Search Active Devices Protocol) is a user-friendly, installation-free online device search tool. It searches for the active online devices in your subnet and displays their information. Using this software, you can modify the basic network information of the devices.

Note: SADP is a Windows only product.

Search active devices online

After launching the SADP software, it automatically searches for online devices, every 15 seconds, on your computers subnet. The online interface displays information on the found devices. This information includes the device type, IP address, port number, and gateway.

Figure 22: Searching online devices

Note: Once a device is online for 15 seconds, it can be found using the SAPD tool. After 45 seconds of a device being offline, it is removed from the devices list.
Search online devices manually
Click **Refresh** to view a current device list. All new devices are displayed on the list.

**Note:** Click ▲ or ▼ on each column heading to change the order of the information.
Click ➡ to expand the device table and hide the network parameter panel on the right side, or click ◀ to show the network parameter panel.

Modify network parameters

To modify network parameters:
1. Select a device in the list and the network parameters display.
2. Only certain parameters can be modified. Edit the modifiable network parameters – for example, the IP address and port number.
3. Enter the password of the device’s admin account, and then click **Save**.

![Modify Network Parameters.png](https://via.placeholder.com/150)

**To restore the default password:**
Enter the code in the **Serial code** field, and then click **Confirm** to restore the default password.

**Note:** The serial code is a series of characters combining the start time and serial number of the device.
Appendix 2

Port mapping
The following settings are for a TP-LINK router (TL-R410). The settings vary depending on the router model.

To set port mapping:
1. Select the WAN **Connection Type**, as shown below.

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

3. Set the port mapping in the virtual servers of Forwarding. By default, the camera uses port 80, 8000, 554 and 8200. Change the port values using a web browser or client software.

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

**Note:** The 8200 port changes with the 8000 port with a constant value of 200. E.g. if the 8000 port is changed to 8005, then the 8200 port should be changed to 8205.
As the settings mentioned above, map the port 80, 8000, 554 and 8200 for the network camera at 192.168.1.23

**To map the ports:**

1. Map the port 81, 8001, 555 and 8201 for the network camera at 192.168.1.24.
2. Enable **ALL** or **TCP** protocols.
3. Select the **Enable** checkbox and click **Save**.

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