Vicon Industries Inc. does not warrant that the functions contained in this equipment will meet your requirements or that the operation will be entirely error free or perform precisely as described in the documentation. This system has not been designed to be used in life-critical situations and must not be used for this purpose.
Trademark Acknowledgement

Vicon and its logo are the property of Vicon Industries Inc. Other trademarks, company names and product names contained in this manual are the property of their respective owners.

Disclaimer

**CAUTION!**

The default password is used for your first login. To ensure account security, please change the password after your first login. You are recommended to set a strong password (no less than eight characters).

- To the maximum extent permitted by applicable law, the product described, with its hardware, software, firmware and documents, is provided on an “as is” basis.
- Best effort has been made to verify the integrity and correctness of the contents in this manual, but no statement, information, or recommendation in this manual shall constitute formal guarantee of any kind, expressed or implied. We shall not be held responsible for any technical or typographical errors in this manual. The contents of this manual are subject to change without prior notice. Update will be added to the new version of this manual.
- Use of this manual and the subsequent result shall be entirely on the user’s own responsibility. In no event shall we be reliable to you for any special, consequential, incidental, or indirect damages, including, among others, damages for loss of business profits, business interruption, or loss of data or documentation in connection with the use of this product.
- Video and audio surveillance can be regulated by laws that vary from country to country. Check the law in your local region before using this product for surveillance purposes. We shall not be held responsible for any consequences resulting from illegal operations of the device.
- The illustrations in this manual are for reference only. The screenshots in this manual may have been customized to meet specific requirements and user preferences. As a result, some of the examples and functions featured may differ from those displayed on your monitor.
- Due to uncertainties such as physical environment, discrepancy may exist between the actual values and reference values provided in this manual. The ultimate right to interpretation resides in our company.
Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Symbols

The symbols in the following table may be found in this manual. Carefully follow the instructions indicated by the symbols to avoid hazardous situations and use the product properly.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![WARNING!]</td>
<td>Contains important safety instructions and indicates situations that could cause bodily injury.</td>
</tr>
<tr>
<td>![CAUTION!]</td>
<td>Means reader be careful and improper operations may cause damage or malfunction to product.</td>
</tr>
<tr>
<td>![NOTE!]</td>
<td>Means useful or supplemental information about the use of product.</td>
</tr>
</tbody>
</table>
## Contents

1 Network Connection........................................................................................................................................1

2 Login..........................................................................................................................................................1
   Preparation.................................................................................................................................................1
   Logging In to the Web Interface................................................................................................................3
   Introduction to the Web Interface..............................................................................................................4
   Initial Configuration..................................................................................................................................5

3 Configuring Parameters............................................................................................................................5
   Local Parameters.......................................................................................................................................5
   Network Configuration.................................................................................................................................7
      Ethernet..................................................................................................................................................7
      Port.........................................................................................................................................................9
      FTP.........................................................................................................................................................10
      E-Mail.....................................................................................................................................................12
      Port Mapping.........................................................................................................................................13
      DNS.......................................................................................................................................................13
      DDNS......................................................................................................................................................13
      SNMP...................................................................................................................................................13
      802.1x...................................................................................................................................................14
   Image Configuration....................................................................................................................................15
      Image Adjustment....................................................................................................................................15
      OSD Setting...........................................................................................................................................22
      Privacy Mask.........................................................................................................................................23
   Audio and Video Configuration..................................................................................................................24
      Video Configuration................................................................................................................................24
      Snapshot.................................................................................................................................................25
      ROI..........................................................................................................................................................25
      Media Stream Configuration....................................................................................................................26
   Intelligent Alarm Configuration..................................................................................................................27
      Smart Settings.......................................................................................................................................27
      Perimeter Protection: Cross Line Detection...........................................................................................27
      Perimeter Protection: Intrusion Detection...............................................................................................28
      Exception Protection and Statistics: Object Moving..............................................................................29
      Exception Protection and Statistics: Object Left.....................................................................................30
      Exception Protection and Statistics: Defocus Detection..........................................................................31
      Exception Protection and Statistics: Scene Change Detection...............................................................32
      Face Detection.......................................................................................................................................32
      People Counting.....................................................................................................................................34
      Advanced Settings..................................................................................................................................34
   Common Alarm Configuration.......................................................................................................................35
      Configuring Motion Detection Alarm.....................................................................................................35
      Configuring Tampering Alarm....................................................................................................................40
   System Maintenance....................................................................................................................................41
      Security....................................................................................................................................................42
Setting the System Time........................................................................................................45
Upgrading the Device ............................................................................................................46
Restarting the System .........................................................................................................46
Importing and Exporting System Configuration File ..........................................................47
Collecting Diagnosis Information .......................................................................................47

4 Live View ................................................................................................................................................. 48
Live View Toolbar .........................................................................................................................48
Viewing Certain Area of Images .................................................................................................49
Using Digital Zoom .....................................................................................................................49

Appendix FAQ .......................................................................................................................................... 50
1 Network Connection

Before accessing a network camera (also known as IP Camera or IPC) from a PC, you need to connect the network camera to the PC directly with a network cable or via a switch or router.

Use a Shielded Twisted Pair (STP) cable to connect the network interfaces of the network camera and the PC.

Use Shielded Twisted Pair (STP) cables to connect the network interfaces of the camera and the switch or router.

2 Login

Preparation

After you have completed the installation in accordance with the quick guide, connect the camera to power to start it. After the camera is started, you can access the camera from a PC client installed with a web browser. Internet Explorer (IE) is a recommended web browser.

The following takes IE on a Microsoft Windows 7 operating system as an example.

Check before login

- The camera is operating correctly.
- The network connection between the PC and the camera is normal.
- The PC is installed with Internet Explorer 10.0 or higher.
- (Optional) The resolution is set to 1440 x 900.
Add the IP address as a trusted site

1. Click on "Tools" in the top menu.
2. Select "Internet Options".
3. Click on "Trusted sites".
4. Add the IP address (e.g., http://192.168.1.13) to the trusted sites list.
5. Clear the check box for "Require server verification (https) for all sites in this zone".
6. Click "Close".
7. Click "OK" to apply changes.

You can now access the site without SSL validation issues.
NOTE!
The IP address 192.168.1.13 is an example. Please replace it with the actual address of your camera if it has been changed.

(Optional) Modify user access control settings
Before you access the camera, follow the steps to set User Account Control Settings to Never notify.

Logging In to the Web Interface

DHCP is turned on by default. If a DHCP server is used in the network, the IP address of your camera may be assigned dynamically, and you need to use the correct IP address to log in. If your network does not have a DHCP server, the camera will use a link local IP, i.e., 169.254.x.x.

The device management software tool can be used to discover the camera on your network. This tool can be found on Vicon’s website under Software Downloads < Vicon Cameras/Encoders.

The following uses IE as an example to describe the login procedure.

1. Browse to the login page by entering the correct IP address of your camera in the address bar.

2. When you log in for the first time, follow system prompts and install the ActiveX. You need to close your browser to complete the installation.
NOTE!

- To manually load the ActiveX, type http://IP address/ActiveX/Setup.exe in the address bar and press Enter.
- The default password is used for your first login. To ensure account security, please change the password after your first login. You are recommended to set a strong password (no less than eight characters).
- The camera protects itself from illegal access by limiting the number of failed login attempts. If login fails six times consecutively, the camera locks automatically for ten minutes.

3. Enter the username and password, and then click Login. For the first login, use the default username “ADMIN” and password “1234”.
   - If you log in with Live View selected, live video will be displayed when you are logged in. Otherwise, you need to start live video manually in the live view window.
   - If you log in with Save Password selected, you do not need to enter the password each time when you log in. To ensure security, you are not advised to select Save Password.
   - To clear the Username and Password text boxes and the Save Password check box, click Reset.

Introduction to the Web Interface

By default the Live view window is displayed when you are logged in to the Web interface. The following shows an example.

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Menu</td>
</tr>
<tr>
<td>2</td>
<td>Live view window</td>
</tr>
<tr>
<td>3</td>
<td>Live view toolbar</td>
</tr>
</tbody>
</table>

NOTE!

- The look of the menus screens on your unit may be different but functionality will be the same or similar.
**Initial Configuration**

After you log in to the device, perform the following initial configuration.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Ethernet</strong>.</td>
<td>Reconfigure the device IP and network parameters based on the actual networking.</td>
</tr>
<tr>
<td>2. Log out and log in again to the Web using the new IP address.</td>
<td>-</td>
</tr>
<tr>
<td>3. <strong>Set the system time</strong>.</td>
<td>Set the system time based on the actual situation.</td>
</tr>
<tr>
<td>4. <em>(Optional)</em> <strong>Set the management server</strong>.</td>
<td>Set the management server based on the actual networking.</td>
</tr>
<tr>
<td>5. <em>(Optional)</em> Set the server for storing photos.</td>
<td>Set the server for storing photos based on the actual networking.</td>
</tr>
<tr>
<td>6. <strong>Set OSD</strong>.</td>
<td>Set the information displayed on the screen as needed, for example, time.</td>
</tr>
<tr>
<td>7. <em>(Optional)</em> <strong>Manage users</strong>.</td>
<td>Change the default password and add common users as needed.</td>
</tr>
</tbody>
</table>

You can view the live video after finishing the initial configuration. Configure other parameters as needed; details follow.

**NOTE!**
- The parameters that are grayed out cannot be modified. For the actual settings, see the Web interface.
- It is recommended that you change the password after you log in the first time. For details about how to change a password, see Security.

### 3 Configuring Parameters

#### Local Parameters

Set local parameters for your PC.

1. Select **Setup > Common > Local Settings**.
2. Modify the settings as required. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intelligent Mark</strong></td>
<td><strong>Untriggered Target</strong>  When enabled, the camera will display an on-screen mark on the target (e.g., face when face detection is enabled) and track it.</td>
</tr>
</tbody>
</table>
| **Video**                   | **Processing Mode**  
- Real-Time Priority: Recommended if the network is in good condition.  
- Fluency Priority: Recommended if you want short time lag for live video.  
- Ultra-low Latency: Recommended if you want the minimum time lag for live video.  
**Protocol**  
Set the protocol used to transmit media streams to be decoded by the PC. |
| **Recording and Snapshot**  | **Recording**  
- Subsection By Time: Duration of recorded video for each recording file on the computer. For example, 2 minutes.  
- Subsection By Size: Size of each recording file stored on the computer. For example, 5M.  
**Record Overwrite**  
- Overwrite: When the assigned storage space on the computer is used up, the camera deletes the existing recording files to make room for the new recording file.  
- Full Stop: When the assigned storage space on the computer is full, recording stops automatically. |

3. Click **Save**.
Network Configuration

Ethernet

Modify communication settings such as the IP address for the camera so that the camera can communicate with other devices.

NOTE!

- After you have changed the IP address, you need to use the new IP address to log in.
- The configurations of DNS (Domain Name System) server are applicable when the device is accessed by domain name.

Static Address

1. Click Setup > Network > Network.

2. Select Static from the Obtain IP Address drop-down list.

3. Enter the IP address, subnet mask, and default gateway address. Make sure that the IP address of the camera is unique in the network.

4. Click Save.

PPPoE

If the camera is connected to the network through Point to Point over Ethernet (PPPoE), you need to select PPPoE as the IP obtainment mode.

1. Click Setup > Network > Network.
2. Select **PPPoE** from the **Obtain IP Address** drop-down list.
3. Enter the username and password provided by your Internet Service Provider (ISP).
4. Click **Save**.
**DHCP**

The Dynamic Host Configuration Protocol (DHCP) is enabled by default when the camera is delivered. If a DHCP server is deployed in the network, the camera can automatically obtain an IP address from the DHCP server.

To manually configure DHCP, follow the steps below:

1. Click **Setup > Network > Network**.

2. Select **DHCP** from the **Obtain IP Address** drop-down list.

3. Click **Save**.

**IPv6**

1. Click **Setup > Network > Network**.

2. By default the **IPv6** mode is set to **Manual**.

3. Enter the IPv6 address; set the prefix length and default gateway. The IP address must be unique on the network.

4. Click **Save**.

**Port**

1. Click **Setup > Network > Port**.

2. Configure relevant port numbers.

3. Click **Save**.
FTP

All snapshots (except face detection) are saved through the general FTP service. After the configuration of FTP, you will be able to upload snapshots from network cameras to the specified FTP server.

**General**

1. Click **Setup > Storage > FTP**. Go to **General tab**.

2. Set the IP address and port for the FTP server, username and password used to upload images to the FTP server, select **Upload Images**, **Overwrite Storage** and set **Overwrite At** (threshold for overwriting images). Some camera models support FTP test. You may test FTP after completing FTP settings correctly.

3. Set the path for saving snapshots on the FTP server and the file name format. For example, set path as Date-YYYY\Date-MM\Date-DD\Hour(s), and set file name as Date-YYYY-Date-MM-Date-DD.jpg.

4. Click **Save**.
This function is used to store snapshots taken for smart functions such as face recognition. To use smart FTP, click Setup > System > Server > Intelligent Server and set Platform Communication Type to FTP.

1. Click Setup > Storage > FTP. Go to Smart tab.

2. Set the IP address and port of the FTP server, username and password used to upload images to the FTP server.

3. Set the path for saving snapshots on the FTP server and the file name format. For example, set path as Preset No.\IP Address\Date, and set file name as Preset No.-PTZ Latitude-PTZ Longitude-PTZ Zoom.jpg.

4. Click Save.
E-Mail

After the configuration of E-mail, when alarms are triggered, you will be able to send messages to the specified E-mail address.

1. Click Setup > Network > E-mail.

2. Configure relevant parameters of the sender and the recipient. Some camera models support Email test. You may test email after setting the recipient address. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS/SSL</td>
<td>When enabled, the e-mail will be encrypted using TLS (Transport Layer Security) or Secure Socket Layer (SSL) to protect privacy. First it tries to send through an SSL connection. If the SMTP server supports SSL, the e-mail will be sent through the SSL connection; otherwise, it tries to send using STARTTLS.</td>
</tr>
<tr>
<td>Attach Image</td>
<td>When enabled, the e-mail will contain 3 instant snapshots as attachment according to the Capture Interval.</td>
</tr>
<tr>
<td>Username/Password</td>
<td>Username and password of the registration email address. The password allows the following special characters \ / : * ’ ” &lt; &gt;</td>
</tr>
</tbody>
</table>

3. Click Save.
Port Mapping

1. Click **Setup > Network > Port.** Go to **Port Mapping** tab.

   ![Port Mapping Tab]

   2. Enable **Port Mapping** and select mapping type. If **Manual** is selected, then external ports must be configured (external IP is obtained automatically by the camera). If the configured port is occupied, then the **Status** will show Inactive.

   3. Click **Save.**

DNS

1. Click **Setup > Network > DNS.**

   - Preferred DNS Server: 8.8.8.8
   - Alternate DNS Server: 8.8.4.4

2. Set DNS server addresses.

3. Click **Save.**

DDNS

1. Click **Setup > Network > DDNS.**

   ![DDNS Settings]

2. Enable **DDNS Service.**

3. Select a DDNS type: DynDNS, NO-IP, or EZDDNS.

4. Complete other settings including server address, domain name, username and password.

5. Click **Save.**

SNMP

SNMPv3 is recommended when a camera needs to transfer configuration with the central server. Both the camera and the central server should support SNMPv3.
NOTE!

- Two options are available: SNMPv3 (default) and SNMPv2.
- If you choose SNMPv2, an onscreen message will remind you of potential risks and ask if you want to continue.

1. Click Setup > Network > SNMP

2. Select SNMPv3 and complete settings.

3. Click Save.

On the SNMPv2 setting page, Read-Only Community Name is used for two-way authentication between a camera and the central server. The default name is public, and you may change it as needed. If you change the Read-Only Community Name, you should change it into the same one on the central server, or the two-way authentication will not be completed.

802.1x

802.1x provides authentication to devices (e.g., cameras) trying to connect to a network. Only the authenticated devices can connect the network. This enhances security.

1. Click Setup > Network > 802.1x.

2. Select On and then complete other settings.

3. Click Save.
Image Configuration

Image Adjustment

NOTE!

- You may move the sliders to adjust settings or enter values in the text boxes directly.
- Clicking Default will restore all the default image settings.

Setting the Scene

Set image parameters to achieve the desired image effects based on live video in different scenes.

Click Setup > Image > Image.

The scene management page displays as follows; you can take the following steps to configure the scene.

1. Click Scenes.
2. Select a scene, and then set scene switching parameters. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
</table>
| Current         | Indicates the scene that is being used.  
                 **Note:**  
                 - Select an option button to switch to the scene and display the corresponding image parameters for the scene.  
                 - The camera switches the current scene automatically when Enable Auto Switching is selected.  
| Scene Name      | Name of the current scene. The device provides several preset scene modes. When you select a scene, the corresponding image parameters are displayed. You can adjust image settings according to actual needs.  
                 - Indoor: recommended for indoor scenes.  
                 - WDR: recommended for scenes with high-contrast lighting, such as window, corridor, front door or other scenes that are bright outside but dim inside.  
                 - Custom: set a scene name as needed.  
| Auto Switching  | Indicates whether to add a scene to the auto-switching list.  
                 **Note:**  
                 If Auto Switching is enabled, the system switches to a scene automatically when the condition for switching to the scene is met. By default the auto-switching list includes the default scene.  
| Setup           | Click to set conditions for auto-switching, including schedule and illumination. It means that auto-switching is triggered only when meets the set conditions. A condition is invalid if both the start and end values are set to 0.  


3. Select a scene and then click 🏕️ to set it as the default scene.
4. If auto-switching is enabled, the camera can switch to the scene automatically when the condition for switching to a non-default scene is met. Otherwise, the camera remains in the default scene. When auto-switching is not enabled, the camera remains in the current scene.

**NOTE!**
- If Auto Switching is enabled (scene settings will be unavailable), the device will switch between the set scenes. If not, the device will stay at the current scene. The device will stay at default scenes unless the non-default scenes are triggered.
- If multiple non-default scenes are triggered, then the device will switch to the scene with the minimum number (starts from 1 to 5).

**Image Enhancement**

1. Click **Setup > Image > Image** and then click **Image Enhancement**.

2. Use the sliders to change the settings. You may also enter values directly. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brightness</td>
<td>Set the degree of brightness of images.</td>
</tr>
<tr>
<td></td>
<td><img src="image1.jpg" alt="Low brightness" /> <img src="image2.jpg" alt="High brightness" /></td>
</tr>
<tr>
<td>Saturation</td>
<td>The amount of a hue contained in a color.</td>
</tr>
<tr>
<td></td>
<td><img src="image3.jpg" alt="Low saturation" /> <img src="image4.jpg" alt="High saturation" /></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Contrast</td>
<td>Set the degree of difference between the blackest pixel and the whitest pixel.</td>
</tr>
<tr>
<td></td>
<td><img src="image1.png" alt="Low contrast" /> <img src="image2.png" alt="High contrast" /></td>
</tr>
<tr>
<td>Sharpness</td>
<td>Contrast of boundaries of objects in an image.</td>
</tr>
<tr>
<td></td>
<td><img src="image3.png" alt="Low sharpness" /> <img src="image4.png" alt="High sharpness" /></td>
</tr>
<tr>
<td>2D Noise Reduction</td>
<td>Reduce the noise of images. The function may cause image blurring.</td>
</tr>
<tr>
<td>3D Noise Reduction</td>
<td>Reduce the noise of images. The function may cause motion blur (or ghosting in some applications).</td>
</tr>
<tr>
<td>Image Rotation</td>
<td>Rotation of the image.</td>
</tr>
<tr>
<td></td>
<td><img src="image5.png" alt="Normal" /> <img src="image6.png" alt="Flip Vertical" /> <img src="image7.png" alt="Flip Horizontal" /> <img src="image8.png" alt="180°" /></td>
</tr>
</tbody>
</table>
3. To restore default settings in this area, click Default.

**Exposure**

### NOTE!

- The default settings are scene-adaptive. Use default settings unless modification is necessary.

1. **Click Setup > Image > Image** and then click Exposure.

![Exposure Settings](image)

2. Set the parameters as required. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Exposure Mode** | Select the correct exposure mode to achieve the desired exposure effect.  
  - Automatic: The camera automatically adjusts exposure according to the environment.  
  - Custom: The user sets exposure as needed.  
  - Indoor 50Hz: Reduce stripes by limiting shutter frequency.  
  - Indoor 60Hz: Reduce stripes by limiting shutter frequency.  
  - Low Motion Blur: Control the minimum shutter to reduce motion blur in faces captured in motion. |
| **Shutter(s)** | Shutter is used to control the light that comes into the lens. A fast shutter speed is ideal for scenes in quick motion. A slow shutter speed is ideal for scenes that change slowly.  
  **Note:**  
  - You can set a shutter speed when Exposure Mode is set to Manual or Shutter Priority. |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gain (dB)</strong></td>
<td>Control image signals so that the camera outputs standard video signals according to the light condition.</td>
<td>You can set this parameter only when <strong>Exposure Mode</strong> is set to <strong>Manual</strong> or <strong>Gain Priority</strong>.</td>
</tr>
<tr>
<td><strong>Slow Shutter</strong></td>
<td>Improves image brightness in low light conditions.</td>
<td>You can set this parameter only when <strong>Exposure Mode</strong> is not set to <strong>Shutter Priority</strong> and when <strong>Image Stabilizer</strong> is disabled.</td>
</tr>
<tr>
<td><strong>Slowest Shutter</strong></td>
<td>Set the slowest shutter speed that the camera can use during exposure.</td>
<td>You can set this parameter only when <strong>Slow Shutter</strong> is set to <strong>On</strong>.</td>
</tr>
<tr>
<td><strong>Compensation</strong></td>
<td>Adjust the compensation value as required to achieve the desired effects.</td>
<td>You can set this parameter only when <strong>Exposure Mode</strong> is not set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Metering Control</strong></td>
<td>Set the way the camera measures the intensity of light.</td>
<td>You can set this parameter only when <strong>Exposure Mode</strong> is not set to <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Day/Night Mode</strong></td>
<td>- Automatic: The camera outputs the optimum images according to the light condition. In this mode, the camera can switch between night mode and day mode automatically.</td>
<td><strong>Automatic</strong>: The camera outputs the optimum images according to the light condition. In this mode, the camera can switch between night mode and day mode automatically.</td>
</tr>
<tr>
<td><strong>Day/Night Sensitivity</strong></td>
<td>Light threshold for switching between day mode and night mode. A higher sensitivity means that the camera is more sensitive to the change of light and becomes more easily to switch between day mode and night mode.</td>
<td>You can set this parameter only when <strong>Day/Night Mode</strong> is set to <strong>Automatic</strong>.</td>
</tr>
<tr>
<td><strong>Day/Night Switching(s)</strong></td>
<td>Set the length of time before the camera switches between day mode and night mode after the conditions for switching are met.</td>
<td>You can set this parameter only when <strong>Day/Night Mode</strong> is set to <strong>Automatic</strong>.</td>
</tr>
<tr>
<td><strong>WDR</strong></td>
<td>Enable WDR to distinguish the bright and dark areas in the same image.</td>
<td>You can set this parameter only when <strong>Exposure Mode</strong> is neither <strong>Customize</strong> nor <strong>Manual</strong> and when <strong>Image Stabilizer</strong> is disabled.</td>
</tr>
<tr>
<td><strong>Suppress WDR Stripes</strong></td>
<td>When enabled, the camera can automatically adjust slow shutter frequency according to the frequency of light to minimize stripes that may appear in images.</td>
<td></td>
</tr>
</tbody>
</table>

3. To restore the default settings, click Default.
**Smart Illumination**

1. Click **Setup > Image > Image** and then click **Smart Illumination**.

2. Select the correct IR control mode and set the parameters. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lighting Type</td>
<td><strong>Infrared</strong>: The camera uses infrared light illumination.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: When <strong>Control Mode</strong> is set to <strong>Manual</strong>, camera can set illumination level from 0~1000.</td>
</tr>
<tr>
<td>Control Mode</td>
<td><strong>Global Mode</strong>: The camera adjusts IR illumination and exposure to achieve balanced image effects. Some areas might be overexposed if you select this option. This option is recommended if monitored range and image brightness are your first priority.</td>
</tr>
<tr>
<td></td>
<td><strong>Overexposure Restrain</strong>: The camera adjusts IR illumination and exposure to avoid regional overexposure. Some areas might be dark if you select this option. This option is recommended if clarity of the central part of the image and overexposure control are your first priority.</td>
</tr>
<tr>
<td></td>
<td><strong>Manual</strong>: This mode allows you to manually control the intensity of IR illumination.</td>
</tr>
<tr>
<td>Illumination Level</td>
<td>Set the intensity level of the IR light. The greater the value, the higher the intensity. 0 means that the IR light is turned off.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You can set this parameter only when <strong>Control Mode</strong> is set to <strong>Manual</strong>.</td>
</tr>
</tbody>
</table>

3. To restore the default settings, click **Default**.

**White Balance**

White balance is the process of offsetting unnatural color cast in images under different color temperatures so as to output images that best suit human eyes.

1. Click **Setup > Image > Image** and then click **White Balance**.

2. Select a white balance mode as required. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>White Balance</td>
<td>Adjust the red or blue offset of the image:</td>
</tr>
<tr>
<td></td>
<td><strong>Auto/Auto2</strong>: The camera adjusts the red and blue offset automatically according to the light condition (the color tends to be blue). If the images are still unnaturally red or blue</td>
</tr>
</tbody>
</table>
in Auto mode, please try Auto2.
- Fine Tune: Allow you to adjust the red and blue offset manually.
- Outdoor: Suitable for outdoor environment with a relatively greater color temperature range.
- Locked: Lock the current color temperature without change.

<table>
<thead>
<tr>
<th>Red Offset</th>
<th>Adjust the red offset manually.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> You can set this parameter only when <strong>White Balance</strong> is set to <strong>Fine Tune</strong>.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blue Offset</th>
<th>Adjust the blue offset manually.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> You can set this parameter only when <strong>White Balance</strong> is set to <strong>Fine Tune</strong>.</td>
</tr>
</tbody>
</table>

3. To restore the default settings, click **Default**.

**Advanced**

Use the defog function to adjust the clarity of images captured in fog or haze conditions.

1. Click **Setup > Image > Image** and then click **Advanced**.

![Advanced Settings](image)

**NOTE!**
- You can set this parameter only when WDR is turned off.
- When **Defog** is set to **On**, defog intensity level 6-9 represent optical defog, and images change from color to black/white when defog intensity is set from level 5 to 6; if **Defog** is set to **Auto** and defog intensity level is somewhere between 6-9, images do not automatically change to black/white in light fog conditions; the camera automatically switches to optical defog only in heavy fog conditions.

2. Enable the defog function and then select a level for the scene. Level 9 achieves the maximum defog effects, and level 1 achieves the minimum.

![Defog Off](image) ![Defog On](image)

3. To restore the default settings, click **Default**.
OSD Setting

On Screen Display (OSD) is the text displayed on the screen with video images and may include time and other customized contents.

NOTE!
This function may vary with models. Please see the actual Web interface for details.

1. Click **Setup > Image > OSD.**

2. Select the position and content of the OSD.
   - **Position:** Click the desired box in the **Live View** area. After the cursor shape is changed, click and hold the button to move the box to the desired position. To set the position precisely, use the X and Y coordinates.
   - **Overlay OSD Content:** The drop-down list provides **Time, Date, Date & Time, People Counting, Scroll OSD, Picture Overlay** and **Network Port.** You may also select **Custom** and enter the content you want.
   - After you have set the position and OSD content, the ✔ symbol appears in the column, which means that the OSD is set successfully. You may set multiple lines of contents for each area.

3. After you have completed the settings, a message appears to indicate the successful settings. You can double-click the preview window to enter or exit full screen mode. To cancel OSD for an area, clear the OSD content in the **Overlay OSD Content** column.

The following shows an example time OSD.
Privacy Mask

In certain circumstances, you may need to set a mask area on the camera image to protect privacy, for example, the keyboard of an ATM machine. When camera changes its position, the Privacy Mask will be adjusted accordingly to protect the area all along.

NOTE!
- The camera supports up to 8 privacy masks.

1. Click Setup > Image > Privacy Mask.

2. Click Add button to add a privacy mask, and click Delete button to remove a mask.
   - To mask a position: Click the box (with Mask displayed on it) to activate the mask. After the cursor shape has changed, drag the box to the intended position.
   - To mask an area: After adding a privacy mask, use the mouse to shape and move the box on the area you want to mask.

When privacy mask is configured, the intended area is blocked. The following shows an example.
Audio and Video Configuration

Video Configuration

You can set video parameters that your camera supports; you may also enable sub-stream and third stream as required.

**NOTE!**
- After enabling the sub or third stream, modify the parameters as required. The parameters for the sub and third stream have the same meanings as that for the main stream.

1. Click Setup > Video & Audio > Video.

Modify the settings as required. The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video Compression</strong></td>
<td>Three options: H.265, H.264 and MJPEG.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>- Image Quality cannot be set when Video Compression is set to H.265 or H.264. When set to MJPEG, only three frame rates are available: 1, 3 and 5; Bit Rate, I Frame Interval, Smoothing, SVC and Smart Encoding cannot be set.</td>
</tr>
<tr>
<td></td>
<td>- The bit rate changes to the default when you change the setting between H.264 and H.265. The default bit rate for H.265 is half of that for H.264.</td>
</tr>
<tr>
<td><strong>Frame Rate</strong></td>
<td>Frame rate for encoding images. Unit: FPS (frame per second).</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>To ensure image quality, note that the frame rate should not be greater than the reciprocal of shutter speed.</td>
</tr>
<tr>
<td><strong>Bitrate Type</strong></td>
<td>- CBR: Constant Bit Rate, which means that the camera transmits data at a constant data rate.</td>
</tr>
<tr>
<td></td>
<td>- VBR: Variable Bit Rate, which means that the camera adjusts the bit rate dynamically according to image quality.</td>
</tr>
<tr>
<td><strong>Image Quality</strong></td>
<td>When Encoding Mode is VBR, you can move the slider to adjust quality level for images. Moving the slider toward Bit Rate decreases the bit rate and may affect image quality. Moving the slider toward Quality increases the bit rate and improves image quality.</td>
</tr>
</tbody>
</table>

2. Click Save.
Snapshot

1. Click Setup > Video & Audio > Snapshot.

2. Select **On**, and then set resolution, most large and schedule as needed. Some parameters are described in the table below.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snapshot Interval</td>
<td>Interval between two snapshots. For example, with Snapshot Interval set to 1 and Number of Snapshot set to 2, the camera will take 2 snapshots (take one first and then take another after 1 second).</td>
</tr>
<tr>
<td>Number to Snapshot</td>
<td>Currently 1, 2, and 3 snapshots are allowed.</td>
</tr>
<tr>
<td>Snapshot Mode</td>
<td><strong>Schedule</strong>: You need to set a snapshot time, e.g., 19:12:00, which means the camera takes a snapshot at 19:12:00. <strong>Repeat</strong>: Allows you to set an interval (unit: sec). The default value is 60, which means that 60 seconds must elapse before the camera takes another snapshot.</td>
</tr>
</tbody>
</table>

2. Click **Save**.

ROI

When Region of Interest (ROI) is enabled, the system ensures image quality for ROI first if the bit rate is insufficient.

1. Click **Setup > Video & Audio > ROI**.
2. Click and then drag the mouse to cover the intended part of the images. To delete, select the area and then click .

Media Stream Configuration

Media Stream
You can display the established media streams from a camera. You may also set the camera so it transmits code streams by the TS/UDP or ES/UDP protocol to a specified IP address and port number. The settings can be saved and take effect after the camera is restarted.

NOTE!
- Choose a transport protocol based on your actual needs and network performance. TS is Transport Stream and ES is Elementary Stream.

1. Click Setup > Video & Audio > Media Stream.

2. Click , select a stream type, and then set the IP address and port number of the unicast or multicast group for the decoding device that receives audio and video streams from the camera.
   If you want the device to establish the media stream that has been configured before automatically after the restart, select Enable for Persistent.

3. To delete a stream, click .
4. Click **OK** to complete the operations or Cancel the setting.

**RTSP Multicast Address**

After an RTSP multicast address is configured, the third-party player can request the RTSP multicast media stream from the camera through the RTP protocol.

1. Click **Setup > Video & Audio > Media Stream > RTSP Multicast Address**.

2. Set the multicast address (224.0.0.0 to 239.255.255.255) and port number (0 to 65535).

3. Click **Save**.

**Intelligent Alarm Configuration**

You can configure intelligent monitoring to count people and monitor moving objects. Intelligent monitoring includes people counting, perimeter protection, and face.

**Smart Settings**

Click **Setup > Intelligent > Smart Settings**.

**Perimeter Protection: Cross Line Detection**

Cross line detection detects objects that cross a virtual line in live video and triggers alarm when such an event is detected.
1. Click **Setup > Intelligent > Smart Settings**. Choose **Cross Line** and then click ![settings](image)

2. Select **Cross Line Detection**.

3. In the **Detection Rule** area, click ![add](image) to add a new detection area. To delete a detection area, click ![delete](image).

4. On the small preview window, drag the line to the intended position and set the detection range.

5. Set the direction and sensitivity for the camera to decide whether to report a cross line detection alarm.

6. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in Configuring Motion Detection Alarm.

7. Click **Save**.

**Perimeter Protection: Intrusion Detection**

Intrusion detection detects objects that enter a specified area in live video and triggers alarm when such an event is detected.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Intrusion** and then click ![settings](image).
2. Select **Intrusion Detection**.

3. In the **Detection Rule** area, click to add a new detection area. To delete a detection area, click .

4. Drag the borders of the box to set the intended position and range.

5. Set time threshold, sensitivity, and percentage for the camera to decide whether to report an intrusion detection alarm.
   - **Time Threshold**: The minimum length of time that the intruder stays in the detection area before an alarm will be reported.
   - **Sensitivity**: Sensitivity of detection. A greater value means higher detection sensitivity.
   - **Percentage**: The minimum ratio of the intruder’s size to the size of the specified detection area before an alarm will be reported.

6. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in **Configuring Motion Detection Alarm**.

7. Click **Save**.

**Exception Protection and Statistics: Object Moving**

Detect objects left behind in the specified area and trigger alarms.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Object Moving** and then click .
2. Select **Enable Object Moving Detection**.

3. In the Detection Rule area, click **+** to add a detection area. To delete, click **−**.

4. Drag the box to set the position and effective range.

5. Set time threshold and sensitivity to decide whether to report an intrusion detection alarm.
   - **Time threshold**: Minimum duration an object is detected in the specified area to trigger an alarm.
   - **Sensitivity**: The greater the number, the higher the sensitivity. An alarm is reported if an object is detected in the specified area for the specified length of time.

6. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in [Configuring Motion Detection Alarm](#).

7. Click **Save**.

**Exception Protection and Statistics: Object Left**

Detect objects left behind in the specified area and trigger alarms.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Object Left** and then click **Edit**.
2. Select **Enable Object Left Detection**.

3. In the **Detection Rule** area, click + to add a detection area. To delete, click -.

4. Drag the box to set the position and effective range.

5. Set time threshold and sensitivity to decide whether to report an intrusion detection alarm.
   - **Time threshold**: Minimum duration an object is detected in the specified area to trigger an alarm.
   - **Sensitivity**: The greater the number, the higher the sensitivity. An alarm is reported if an object is detected in the specified area for the specified length of time.

6. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in Configuring Motion Detection Alarm.

7. Click **Save**.

**Exception Protection and Statistics: Defocus Detection**

Use Defocus detection to detect defocus of the camera and to report an alarm when such an event is detected.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Defocus** and then click .
2. Select **Defocus Detection**.
3. Set detection sensitivity and alarm-triggered actions as required. For the detailed steps, see the descriptions of alarm-triggered actions in [Configuring Motion Detection Alarm](#).
4. Click **Save**.

### Exception Protection and Statistics: Scene Change Detection

Use Scene Change detection to detect the change of surveillance environment caused by external factors, such as intentional rotation of the camera, and to report an alarm when such an event is detected.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Scene Change** and then click ![Scene Change Detection](image).

![Scene Change Detection](image)

2. Select **Scene Change Detection**.
3. Set detection sensitivity. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in [Configuring Motion Detection Alarm](#).
4. Click **Save**.

### Face Detection

Face detection detects human faces in live video.

1. Click **Setup > Intelligent > Smart Settings**. Choose **Face** and then click ![Face Detection](image).
2. Drag the borders to set the intended position and range.
3. Set detection parameters according to actual needs.
4. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in Configuring Motion Detection Alarm.
5. Click Save.
6. Click Start Intelligent Analysis.
People Counting

1. Click **Setup > Intelligent > Smart Settings**. Choose **People Counting** and then click .


3. Click **Draw Detection Area**, and then draw a detection area on the preview window on the left, e.g., a square.

4. Click **Draw Entrance Direction**, and then draw the direction on the preview window on the left. The direction is usually vertical or sloping.

5. Set **Max. Size** and **Min. Size** under **Filter by Object Size**. Only objects within the size range will be counted; others will be filtered and not counted. The maximum width or height must be greater than the minimum width or height.

6. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in Configuring Motion Detection Alarm.

7. To reset counting results, click **Clear Counting Result**.

8. Click **Save**.

**Advanced Settings**

Advanced settings include photo clarity and detection mode for intelligent functions.

**Photo parameters**

Set clarity of snapshots.

1. Click **Setup > Intelligent > Advanced Settings**. Click **Photo parameters** tab.
2. Set the thumbnail image clarity.
3. Click Save.

**NOTE!**
Please turn off the Face Detection before setting the photo parameter.

**Detection Parameters**

**NOTE!**
- The default detection mode is **Normal Mode**. Set as required.

1. Click Setup > Intelligent > Advanced Settings. Click Detection parameters tab.

2. Choose a detection mode. Choose **Filter Repeated Motion Mode** to prevent repeated alarm reporting caused by repeated motion detected in the surveillance environment.
3. Click Save.

**Common Alarm Configuration**

You can schedule alarm reporting and set actions that can be triggered by other devices so that alarms and the triggered actions can be handled in time. Alarm reporting can be scheduled for motion detection alarm, tampering detection alarm, and audio detection alarm.

**Configuring Motion Detection Alarm**

Motion detection detects the object motion in a specified rectangular area during a period. You need to set a detection area, sensitivity of detection, object size, and history for the camera to decide whether to report a motion detection alarm when it detects motion.
Area Detection

1. Click Setup > Events > Common Alarm > Motion Detection. Set Detection Mode to Area.

2. In the Detection Area list, click + to add a new detection area. To delete a detection area, click -.

3. A box appears on the preview screen. Click and drag the mouse to size and position a detection area.

4. Set the detection sensitivity and object size.
   - Moving the slider to the right increases detection sensitivity. When the extent of motion within the detection area exceeds the set object size, the camera reports an alarm.
   - Object size specifies the minimum ratio of the object’s size to the size of the total detection area before an alarm will be reported. Therefore, to detect motion of tiny objects, you need to draw a small box (detection area) in the actual motion area.
   - Motion detection results are shown in real time. The red lines represent the raised motion detection alarms. The longer a line, the greater the extent of motion. The denser the lines, the greater the frequency of motion.

5. Set the alarm parameters.
   - Suppress Alarm(s): After an alarm is triggered, the same alarm will not be reported within the set time.
   - Clear Alarm(s): After an alarm is triggered:
     a. If the same alarm is not triggered within the set time, the alarm will be cleared and the same alarm can be reported again.
     b. If the same alarm is triggered within the set time, the alarm will not be cleared until the suppress alarm time expires. Then the same alarm can be reported again.

6. Set actions to be triggered by motion detection alarm and the plan.
The following table describes the triggered actions and how to set a plan.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recording</strong></td>
<td>With <strong>Recording</strong> selected, the camera will automatically start to record video when an alarm is triggered. <strong>Note:</strong> Make sure you have completed <strong>Recording</strong> before using this function.</td>
</tr>
<tr>
<td><strong>Upload to FTP</strong></td>
<td>With <strong>Upload to FTP</strong> selected, the camera will automatically upload snapshots to the specified FTP server when an alarm is triggered. <strong>Note:</strong> Make sure you have completed <strong>FTP</strong> and <strong>Snapshot</strong> before using this function.</td>
</tr>
<tr>
<td><strong>Trigger E-mail</strong></td>
<td>With <strong>Trigger E-mail</strong> selected, the camera will automatically send snapshots to the specified E-mail address when an alarm is triggered. <strong>Note:</strong> Make sure you have completed <strong>Smart</strong> function.</td>
</tr>
</tbody>
</table>

**Smart**

This function is used to store snapshots taken for smart functions such as face recognition. To use smart FTP, click Setup > System > Server > Intelligent Server and set Platform Communication Type to FTP.

1. Click **Setup > Storage > FTP**. Go to **Smart** tab.

   ![FTP Server Parameters](image)

   **Server Parameters**

   - Server IP: 192.168.0.150
   - Port No.: 21
   - Username: 
   - Password: 
   - Device Name: 
   - Device ID: 1
   - Intersection ID: 

   ![Snapshot Image](image)

   **Snapshot Image**

   - Save To: \[Preset No.\] \[IP Address\] \[Date\]
   - Root Directory: 
   - File Name: [Preset No.]: [PTZ Latitude]: [PTZ Longitude]: [PTZ Zoom].jpg
   - Separator: -

   **Naming Element**

   - No
   - Naming Element
   - Naming Rule

<table>
<thead>
<tr>
<th>No</th>
<th>Naming Element</th>
<th>Naming Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Preset No.</td>
<td>✔️</td>
</tr>
<tr>
<td>2</td>
<td>PTZ Latitude</td>
<td>✔️</td>
</tr>
<tr>
<td>3</td>
<td>PTZ Longitude</td>
<td>✔️</td>
</tr>
<tr>
<td>4</td>
<td>PTZ Zoom</td>
<td>✔️</td>
</tr>
<tr>
<td>5</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

2. Set the IP address and port of the FTP server, username and password used to upload images to the FTP server.

3. Set the path for saving snapshots on the FTP server and the file name format. For
example, set path as Preset No.\IP Address\Date, and set file name as Preset No.-PTZ Latitude-PTZ Longitude-PTZ Zoom.jpg.

4. Click Save.

**E-Mail** before using this function.

Select the check box and set the start and end times during which motion detection alarm is effective. Select Armed or Unarmed and then directly drag the mouse to draw a plan or click **Edit** to edit time periods in the table. The time periods cannot overlap. The camera reports alarms during the specified period(s) only. You can select from Monday to Sunday and set four periods for each day.

**Enable Plan**

Drag the mouse to draw a plan

Edit time periods in the table

**Note:**
Plan drawing using a mouse is only supported by IE versions later than 8.0. After setting the plan for one day, you can apply the same settings to other days by clicking **Copy** and **Paste**.

1. Click Save.
Grid Detection

1. Click **Setup > Events > Motion Detection**. Set Detection Mode to **Grid**.

2. Detection area(s) can be irregular on the grid.

3. Set detection sensitivity for the camera to decide whether to report a motion detection alarm (alarm visible on compatible NVR).

4. Set alarm parameters.
   - **Suppress Alarm(s):** After an alarm is triggered, the same alarm will not be reported within the set time.
   - **Clear Alarm(s):** After an alarm is triggered,
     a. If the same alarm is not triggered within the set time, the alarm will be cleared and the same alarm can be reported again.
     b. If the same alarm is triggered within the set time, the alarm will not be cleared until the suppress alarm time expires. Then the same alarm can be reported again.

5. Set actions to be triggered by motion detection alarm and the plan. For the detailed steps, see the descriptions of alarm-triggered actions in **Area Detection** in Configuring Motion Detection Alarm.

6. Click **Save**.
Configuring Tampering Alarm

Configure tampering alarm so that the camera reports a tampering alarm when the lens is blocked for a certain length of time.

1. Click **Setup > Events > Common Alarm > Tampering Alarm**.

2. Select **On** for **Tampering Alarm**.

3. Set detection sensitivity and duration for the camera to decide whether to report a tampering alarm.
   - Sensitivity is set using the slider bar or entering a specific number in the field; the higher the number, the more sensitive the camera is to tampering with the lens. The camera reports an alarm when the lens is blocked for a specified length of time.
   - Tampering alarm is effective on the whole screen. To disable tampering alarm, select Off for the **Tampering Alarm** check box.

4. Set actions to be triggered by tampering alarms and the plan. For the detailed steps, see the descriptions of alarm-triggered actions in [Configuring Motion Detection Alarm](#).

5. Click **Save**.
Configuring Audio Detection Alarm

The camera can detect input audio signals for exceptions. When the rise or fall of volume exceeds the set limit, or when the input volume reaches the threshold, the camera reports an alarm and triggers the set actions. Make sure that an audio input device is correctly connected to the camera and audio input is turned on in Error! Reference source not found..

1. Click Setup > Events > Common Alarm > Audio Detection.

![Audio Detection Setup Screen](image)

2. Select On for Audio Detection, select a detection type and set the difference or threshold. To disable audio detection, select the Off check box.

The following table describes some major parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection Type</td>
<td>• Sudden Rise: An alarm is reported when the rise of volume exceeds the difference.</td>
</tr>
<tr>
<td></td>
<td>• Sudden Fall: An alarm is reported when the fall of volume exceeds the difference.</td>
</tr>
<tr>
<td></td>
<td>• Sudden Change: An alarm is reported when the rise or fall of volume exceeds the difference.</td>
</tr>
<tr>
<td></td>
<td>• Threshold: An alarm is reported when the volume exceeds a threshold.</td>
</tr>
<tr>
<td>Difference</td>
<td>• Threshold: After a volume is set as the threshold, an alarm is reported when the threshold is exceeded.</td>
</tr>
<tr>
<td></td>
<td>• Difference: The difference between two volumes. When the rise or fall of volume exceeds the difference, an alarm is reported.</td>
</tr>
</tbody>
</table>

**Note:**
- The scale in the audio detection area is used to measure sound volume.
- Audio detection results are shown in real time. The red part indicates the reported audio detection alarms.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

3. Set the alarm-triggered actions and arming schedule as required. For the detailed steps, see the descriptions of alarm-triggered actions in Configuring Motion Detection Alarm.

4. Click Save.

**System Maintenance**

**Security**

**User Management**

There are two types of users in the system:

- Administrator: Referred to as “admin” in this manual. The default name of the administrator is admin, which cannot be modified. Admin has full permission and can manage all users and devices. Only one admin user is allowed in the system.
- Common user: Referred to as “user” in this manual. User only has permission to play live and recorded video. Up to 32 common users are allowed in the system.

You can add a user on the user management interface (under Setup > Security > User).

After the user is added successfully, you can change the password by entering the new password or delete the user by clearing the username.
NOTE!

- Only admin can change passwords. Changing the username or password for a user when the user is still logged in will force the user to log out. The user must use the new username or password to log in.
- Only admin can add and delete users. Deleting a user when the user is still logged in will force the user to log out. A deleted user cannot log in.

Setting Secure Data Transmission

Set a secure channel for data transmission to ensure security.

1. Click Setup > Network > Port.

2. Enter the port number in the HTTPS Port text box.

3. Click Save.

4. Click Setup > Security > Network Security > HTTPS.

5. Select On for HTTPS. You may import a custom SSL certificate as needed.

6. Click Save.

Next time you log in, enter the address in `https://IP:HTTPS port number` format, for example, `https://192.168.1.13:443` to enter secure channel mode. If you use the default HTTPS port, enter `https://IP`.

Authentication

RTSP (Real Time Streaming Protocol) is an application layer protocol. To transmit and control the audio and video, set RTSP authentication on the Web interface.

1. Click Setup > Security > Network Security > Authentication. HTTP authentication supports Basic mode, which is compatible with Digest mode and displayed as Basic/Digest on the Web.

2. Select an authentication mode and then click Save.

Hide Vendor Information

You can set to hide the vendor information of the network camera on the Web interface.

1. Click Setup > Security > Registration Info.

2. Under Registration Info, select On.

3. Click Save.
**ARP Protection**

This function protects a camera from ARP attacks. The gateway and the MAC address must be set properly before a PC can access the camera from another network; if an incorrect MAC is set, only PCs on the same LAN can access.

1. Click **Setup > Security > Network Security > ARP Protection**.

2. Select the check box **On** to enable the ARP binding function and set the gateway MAC address.

3. Click **Save**.

**IP Address Filtering**

Use IP address filtering to allow or forbid access from specified IP address(es).

1. Click **Setup > Security > Network Security > IP Address Filtering**.

2. Select **On** to enable IP address filtering.

3. Select a filtering mode, **Whitelist** or **Deny Access**, and then add IP address(es).

4. Click **Save**.

**NOTE!**

- If **Filtering Mode** is set to **Whitelist**, then only the added IP address(es) are allowed to access the camera. If **Filtering Mode** is set to **Deny Access**, then only the added IP address(es) are not allowed to access the camera.
- Up to 32 IP addresses are allowed. Each IP address can be added once only.
- The first byte of each IP address must be 1-223 and the fourth cannot be 0. For example, the following IP addresses are illegal and cannot be added: 0.0.0.0, 127.0.0.1, 255.255.255.255, 224.0.0.1.
Access Policy

NOTE!
Enabling friendly password does not affect use. If you turn it off and log in with a weak password, a page will pop up, prompting you to change the password. There is no Cancel or Close button on this page. The default password is treated as weak.


2. Select On to enable friendly password and MAC Authentication.
3. Click Save.

Watermark
Use watermark to encrypt custom information with video to prevent unauthorized deletions or alterations.

1. Click Setup > Security > Watermark.

2. Select On to enable watermark, and then input watermark content.
3. Click Save.

Setting the System Time
You can use the following methods to adjust the system time of your device.

Manually Setting or Synchronizing the System Time
1. Click Setup > Common > Time, and then click the Time tab.

2. Select a synchronization mode.
3. Set the correct time zone and system time. You may also click Sync with Computer Time to synchronize the time settings of your camera with that of your PC.
4. Click Save.
Setting the DST

1. Click **Setup > Common > Time**, and then click the **DST** tab.

2. Select **On** for **DST**, set the start time, end time, and DST bias.
3. Click **Save**.

Upgrading the Device

If the device is managed by the central management server and you want to upgrade the devices in batch mode, it is recommended to perform the upgrade operation on the central server. For detailed steps, see the user manual for the central management server.

1. Click **Setup > System > Maintenance**.

2. Under **Software Upgrade**, click **Browse** and select the correct upgrade file.
3. Click **Upgrade** and then confirm to start. The camera will restart automatically after the upgrade is completed.

**NOTE!**

- You must use the correct upgrade file for your camera. Otherwise, unexpected results may occur.
- The upgrade file is a ZIP file and must include all the necessary files.
- Ensure that the power supply is normal during upgrade. The device will restart after the upgrade is completed.

Restarting the System

1. Click **Setup > System > Maintenance**.

2. Under **Device Restart**, click **Restart**. The device will restart after you confirm the operation.
CAUTION!

Perform this operation with caution because restarting the system interrupts the ongoing service.

Importing and Exporting System Configuration File

Export the current configurations of the camera and save them to the PC or an external storage medium. You can also quickly restore configurations by importing backup configurations stored on the PC or an external storage medium back to the camera.

CAUTION!

- After you perform the Default operation, all settings are restored to factory defaults, except the following: login password of the system administrator, network settings, and system time.
- Make sure you import the correct configuration file for your camera. Otherwise, unexpected results may occur.
- The camera will restart when the configuration file is imported successfully.

1. Click **Setup > System > Maintenance**.

2. To import configurations that you have backed up, click **Browse** next to the **Import** button and select the configurations you want to import, and then click **Import**. The result will be displayed.

3. To export current system configurations, click **Browse** (next to the **Exporting** field), set the destination and then click **Export**.

4. To restore default configurations, click **Default** and then confirm the operation. The device will restart and restore the default configurations. Clicking **Default** with the check box selected will completely restore the device to factory default settings.

Collecting Diagnosis Information

Diagnosis information includes logs and system configurations. You can export diagnosis information to your PC.

1. Click **Setup > System > Maintenance**.

2. In the **Diagnosis Info** area, click **Browse** to set the destination and then click **Export**.

NOTE!

- Diagnosis information is exported to the local folder in form of a compressed file. You need to decompress the file using a tool such as WinRAR and then open the file using a text editor.
- By selecting **Collect Image Debugging Info**, you can display video with debugging information at the same time, which makes troubleshooting easier.
4 Live View

Live view means playing live video (real-time audio and video) received from a camera in a window through the Web interface.

If you log in with the Live View check box selected, live video appears by default when you are logged in. You may double-click the window to enter or exit full screen mode.

Live View Toolbar

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Play/stop live video" /></td>
<td>Play/stop live video.</td>
</tr>
</tbody>
</table>
| ![Take a snapshot](image) | Take a snapshot of the current image displayed on the PC.  
**Note:** The path for saving snapshots are set in System Configuration. |
| ![Start/stop local recording](image) | Start/stop local recording.  
**Note:** The path for saving local recordings is set in System Configuration. |
| ![Start/stop digital zoom](image) | Start/stop digital zoom. For more details, see Using Digital Zoom. |
| ![Set image display ratio](image) | Set image display ratio in the window. For example, to display high-definition images at original 16:9, select Scale; to display according to window size, select Stretch; to display with the original image size, select Original. |
| ![Reset packet loss rate to zero](image) | Reset the packet loss rate to zero.  
**Note:** After you move the mouse cursor on a live view window, this button appears on the floating toolbar. |
<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="button" /></td>
<td>Display packet loss rate and bit rate information at the bottom of the window. <strong>Note:</strong> After you move the mouse cursor on a live view window, this button appears on the floating toolbar. Click this button to always display the information. With another click, the information appears only when you move the mouse cursor over the window or place it at the bottom. If the mouse cursor rests on the window for around 3 seconds or leaves the window, the information disappears.</td>
</tr>
<tr>
<td><img src="image" alt="button" /></td>
<td>Click this button to open the image setting page.</td>
</tr>
<tr>
<td><img src="image" alt="button" /></td>
<td>Display in full screen mode.</td>
</tr>
<tr>
<td><img src="image" alt="button" /></td>
<td>Select a live video stream that the camera supports: main stream, sub stream or third stream.</td>
</tr>
</tbody>
</table>

**Viewing Certain Area of Images**

Digital zoom and area focus allow you to get more details of certain part of images. Digital zoom enlarges an image with loss in image quality.

**Using Digital Zoom**

1. On the **Live View** page, click ![button](image) on the toolbar.

![image](image)

2. Click and hold the mouse button, and then drag from top down (draw a rectangle) to specify an area. To restore the original image size and zoom in on other areas of the image, right-click the mouse.

To exit, click ![button](image).
Appendix FAQ

What to do if no message prompts me to install ActiveX when I log in on a Windows 7 PC the first time.
Answer: Follow these steps to turn off UAC and then log in again:
1. Click the Start button, and then click Control Panel.
2. In the search box, type uac, and then click Change User Account Control Settings.
3. Move the slider to the Never Notify position, and then click OK.
4. After UAC is turned off, log in again.

What to do if the installation of ActiveX failed.
Answer: If the installation failed, add the IP address of the camera as a trusted site: open Internet Option in IE, click the Security tab, click Trusted sites, and then click Sites to add the website.
If you use Windows 7, you need to save the setup.exe to your PC first, right-click the file, select Run as administrator, and then install it according to instructions.

What to do if live video fails when I log in for the first time.
Answer: Close the firewall on your PC and then log in to the Web interface again.
Shipping Instructions

Use the following procedure when returning a unit to the factory:

1. Call or write Vicon for a Return Authorization (R.A.) at one of the locations listed below. Record the name of the Vicon employee who issued the R.A.

   Vicon Industries Inc.
   135 Fell Court
   Hauppauge, NY 11788
   Phone: 631-952-2288; Toll-Free: 1-800-645-9116; Fax: 631-951-2288

   For service or returns from countries in Europe, contact:

   Vicon Industries Ltd
   Unit 4, Nelson Industrial Park,
   Hedge End, Southampton
   SO30 2JH, United Kingdom
   Phone: +44 (0)1489/566300; Fax: +44 (0)1489/566322

2. Attach a sheet of paper to the unit with the following information:

   a. Name and address of the company returning the unit
   b. Name of the Vicon employee who issued the R.A.
   c. R. A. number
   d. Brief description of the installation
   e. Complete description of the problem and circumstances under which it occurs
   f. Unit’s original date of purchase, if still under warranty

3. Pack the unit carefully. Use the original shipping carton or its equivalent for maximum protection.

4. Mark the R.A. number on the outside of the carton on the shipping label.
Vicon Standard Equipment Warranty

Vicon Industries Inc. (the “Company”) warrants your equipment to be free from defects in material and workmanship under Normal Use from the date of original retail purchase for a period of three years, with the following exceptions:

1. Access Control System Components: Two year from date of original retail purchase.
2. Uninterruptible Power Supplies: Two years from date of original retail purchase.
3. For PTZ cameras, “Normal Use” excludes prolonged use of lens and pan-and-tilt motors, gear heads, and gears due to continuous use of “autopan” or “tour” modes of operation. Such continuous operation is outside the scope of this warranty.
4. Any product sold as “special” or not listed in Vicon’s commercial price list: One year from date of original retail purchase.

NOTE:
• If the product is to be used outdoors or in dusty, humid, or other hostile environments, it must be suitably protected.
• Camera products must be protected, whether in use or not, from exposure to direct sunlight or halogen light as the light may damage the camera image sensor. This applies to both indoor and outdoor use of the cameras.
• Failure to comply with any of the aforementioned requirements will invalidate this Limited Hardware Warranty.

Date of retail purchase is the date original end-user takes possession of the equipment, or, at the sole discretion of the Company, the date the equipment first becomes operational by the original end-user.

The sole remedy under this Warranty is that defective equipment be repaired or (at the Company’s option) replaced, at Company repair centers, provided the equipment has been authorized for return by the Company, and the return shipment is prepaid in accordance with policy. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer. When a product or part is exchanged the replacement hardware becomes the property of the original purchaser and all hardware or part thereof that is replaced shall become the property of Vicon.

The warranty does not apply (a) to faulty and improper installation, maintenance, service, repair and/or alteration in any way that is not contemplated in the documentation for the product or carried out with Vicon consent in writing, operation adjustments covered in the operating manual for the product or normal maintenance, (b) to cosmetic damages, (c) if the product is modified or tampered with, (d) if the product is damaged by acts of God, misuse, abuse, negligence, accident, normal wear and tear and deterioration, improper environmental conditions (including, but not limited to, electrical surges, water damage, chemical exposure, an/or heat/cold exposure) or lack of responsible care, (e) if the product has had the model or serial number altered, defaced or removed, (f) to consumables (such as storage media or batteries) (g) to products that have been purchased “as is” and Vicon the seller or the liquidator expressly disclaim their warranty obligation pertaining to the product, (h) to any non-Vicon hardware product or any software (irrespective of packaged or sold with Vicon hardware product) and Vicon products purchased from an unauthorized distributor/reseller, (i) to damage that occurs in shipment or (j) to damages by any other causes not related to defective design, workmanship and/or materials.

The warranty for the products shall run from Vicon to End User customers only (including product purchased through authorized partners and resellers), Vicon is not obligated under any circumstances to honor warranties on product(s) purchases from internet auction sites including eBay, uBid or from any other unauthorized resellers. Except as explicitly provided herein, Vicon disclaims all other warranties, including the implied warranties of fitness for a particular purpose and merchantability.

Software supplied either separately or in hardware is furnished on an “As Is” basis. Vicon does not warrant that such software shall be error (bug) free. Software support via telephone, if provided at no cost, may be discontinued at any time without notice at Vicon’s sole discretion. Vicon reserves the right to make changes to its software in any of its products at any time and without notice.

The Warranty and remedies provided above are exclusive and in lieu of all other express or implied warranties including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Certain jurisdictions do not allow the exclusion of implied warranties. If laws under such jurisdictions apply, then all express and implied warranties are limited to the warranty period identified above. Unless provided herein, any statements or representations made by any other person or firm are void. Except as provided in this written warranty and to the extent permitted by law, neither Vicon nor any affiliated shall be liable for any loss, (including loss of data and information), inconvenience, or damage, including, but not limited to, direct, special, incidental or consequential
damages, resulting from the use or inability to use the Vicon product, whether resulting from breach of warranty or any other legal theory. Notwithstanding the foregoing, Vicon total liability for all claims under this warranty shall not exceed the price paid for the product. These limitations on potential liabilities have been an essential condition in setting the product.

No one is authorized to assume any liability on behalf of the Company, or impose any obligations on it in connection with the sale of any Goods, other than that which is specified above. In no event will the Company be liable for indirect, special, incidental, consequential, or other damages, whether arising from interrupted equipment operation, loss of data, replacement of equipment or software, costs or repairs undertaken by the Purchaser, or other causes.

This warranty applies to all sales made by the Company or its dealers and shall be governed by the laws of New York State without regard to its conflict of laws principles. This Warranty shall be enforceable against the Company only in the courts located in the State of New York.

The form of this Warranty is effective March 22, 2019.

THE TERMS OF THIS WARRANTY APPLY ONLY TO SALES MADE WHILE THIS WARRANTY IS IN EFFECT. THIS WARRANTY SHALL BE OF NO EFFECT IF AT THE TIME OF SALE A DIFFERENT WARRANTY IS POSTED ON THE COMPANY’S WEBSITE, WWW.VICON-SECURITY.COM. IN THAT EVENT, THE TERMS OF THE POSTED WARRANTY SHALL APPLY EXCLUSIVELY.

Vicon Part Number: 8006-9010-03-13  Rev 0319
VICON INDUSTRIES INC.

For office locations, visit the website: www.vicon-security.com