Voyager I
Megapixel IR IP Camera

User Manual

Software Version 1.27
## Contents

Contents ....................................................................................................................................2

Package Contents .....................................................................................................................4

Overview ...................................................................................................................................6

Features and advantages .........................................................................................................6

System Introduction .................................................................................................................7

Hardware Installation ..............................................................................................................11

Camera Setting from a Router .............................................................................................14

Enter the Main Page ..............................................................................................................18

Camera Main Page ................................................................................................................21

Basic Settings..........................................................................................................................30
  System (System info)......................................................................................................30
  Video/Image ....................................................................................................................32
  Audio ...............................................................................................................................43
  User(User) .......................................................................................................................43

Network (Network Settings) .................................................................................................46
  Network (Wired network setting page)........................................................................46
  Wireless (Wireless network setting page)....................................................................48
  Streaming (streaming Setting) ..................................................................................57
  PPPoE (dial-up networking setting)...........................................................................58
  DDNS (Dynamic Domain Name Server Setting) ....................................................59
  UPnP (Universal Plug and Play) ...............................................................................61
  SMTP Server (mail server setting) ...........................................................................63
  Samba ..............................................................................................................................64
  Multicast ............................................................................................................................66

Date/Time (date/time setting)..............................................................................................68

IP Filtering...............................................................................................................................69

Event (event trigger setting page).......................................................................................70

Firmware upgrade .................................................................................................................81

Factory Default ....................................................................................................................83

Reboot ......................................................................................................................................86

Attachment A: External Alarm .............................................................................................87
Package Contents

The package of this product contains the following items. Please contact your dealer if anything is missing.

1. Voyager IP Camera
2. 12V DC Power Adapter
3. Tripod and Screws Pack
4. Network Cable
5. Quick Installation Guide
6. CD ROM (Manual/Software)
## System Requirements

<table>
<thead>
<tr>
<th>Network Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN</td>
</tr>
<tr>
<td>10/100M Ethernet</td>
</tr>
<tr>
<td>Wireless LAN</td>
</tr>
<tr>
<td>802.11b or 802.11g</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitoring system resource requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
</tr>
<tr>
<td>Windows 2000 Professional SP4, XP Home/Professional SP2, VISTA</td>
</tr>
<tr>
<td>Browser</td>
</tr>
<tr>
<td>Internet Explorer 6.x or later versions</td>
</tr>
<tr>
<td>System hardware</td>
</tr>
<tr>
<td>CPU: Pentium 4, 2.4GHz or better</td>
</tr>
<tr>
<td>RAM: 512MB (1GB recommended)</td>
</tr>
<tr>
<td>VGA resolution: 1024x768 or higher</td>
</tr>
<tr>
<td>DirectX</td>
</tr>
<tr>
<td>DirectX 9.0C above</td>
</tr>
</tbody>
</table>
Overview

Voyager I is an IP camera which delivers high definition video. When connecting to the LAN or any broadband network, it provides professional remote monitoring functions for the user. In addition, the IR LEDs on the camera make a clear night vision possible.

Features and advantages

The IP camera can operate independently without the need for any other hardware or software. After the camera is connected to the network, the remote monitoring can be achieved via the IE browser (version 6.0 or above) of a computer to provide the best security.

The camera has the following features:

- 1/4”, 1.3 Megapixel, progressive scan CMOS sensor providing high definition video.
- MPEG4/MJPEG dual image compression modes and the dual encoding capability meet different requirements of the user.
- Comprises 6 IR LEDs for low light environment.
- 2-way audio.
- The video motion detection function can automatically monitor abnormal situations and make instant response and action according to the setting.
- The built-in web server allows an easy access via networks.
- Dynamic IP and DNS are supported. The camera can operate in a setting without any static IP.
- User permission can be set based on different levels to ensure the security of the camera and protection of the property.
- 3GPP support.
System Introduction

Product layout and connection diagram

DC power inlet
Please connect the product to a power supply from the DC Power Inlet.

Tripod
The product can be fixed on the wall (Fig. 1) or hung from the ceiling (Fig. 2).
When using the attached plastic anchor and screws to fix the product, make sure that no steel bars or power cables exist behind the position where the product is to be fixed. Some walls or ceilings may not be strong enough to support the tripod and the product. Pay attention during installation to avoid injury that might be brought about due to falling of the product.

Fixed on a wall (Fig. 1)  Fixed on a ceiling (Fig. 2)
**Line Out**
This product supports 2-way voice communication. You can connect a speaker to the Audio Out socket. See the Audio section for details.

[Image of Line Out connector]

**LAN socket**
An RJ-45 connector is provided for connection to the 10Base-T Ethernet cable or 100 Base-T High Speed Ethernet cable.
Please connect the product to your network from the LAN socket.

[Image of LAN socket]

**External alarm connector (I/O)**
See Appendix A for details of D1/DO.

[Image of External alarm connector (I/O)]
Default settings
After turning on the power, insert a slim plastic object into the reset orifice and press for five seconds to restore the unit to factory settings.

Built-in microphone
The product is provided with built-in microphone pickup function. Don't block this hole if you want to use this function to acquire the best audio response.

The status of Power LED and Link LED

<table>
<thead>
<tr>
<th>Status</th>
<th>color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>Orange</td>
<td>When power supply plug into the DC Power Inlet, the system will boot up and the orange LED will light up about 15 seconds then go out.</td>
</tr>
<tr>
<td>Link</td>
<td>Green</td>
<td>The green LED lights up when you transmit images after turning on the camera.</td>
</tr>
<tr>
<td>Event</td>
<td>Green</td>
<td>The green LED flashes when motion or alert detection is implemented after turning on the camera.</td>
</tr>
</tbody>
</table>

The LED Switch can be set to On or Off, please refer to the “Setting>Basic Setting[System[System[System Info” for more information.
Focus knob
You can rotate the focus knob clockwise or anticlockwise to acquire the sharpest image.

IR LED
When the light is out or under low illumination environment, IR LED will switch on automatically.

Note:
1. The effective range of IR distance is 5 meter. A reflex object located at the effective range will cause a black/white video changed to color in turn in darkness conditions.
2. The natural light or yellow light exist in the monitoring conditions will result in color shift.
3. To enhance the video quality by adjusting the Slow Shutter option. Please reference to Basic Setting > Video / image > Sensor > AE Setting > Slow Shutter for more information.
Hardware Installation

This product can be installed on any convenient flat surface or can be attached to the wall or ceiling. (Note: The product is provided with an image flip function to convert inverted images to normal. Refer to the “Setting/Basic Setting/Video/PreProc” for more information.)

1. Connect to the LAN cable
Plug one end of your LAN cable in the LAN socket on the back of the camera and connect the other end to the network that you want to access to.

2. Connect to power supply
Plug one end of the attached power cable in the power socket of the product and connect the other end to the AC power outlet. When the product has been connected and turned on, the LED lights orange about 15 seconds. When any link to the network is detected, the LED lights green.
Camera Settings

After the hardware has been installed, insert the supplied CD in the computer and execute the file IP Finder.exe following the steps below to search for and change the IP address of the camera.

1. **Start the machine.**
   Execute the IP Finder.exe from the supplied CD.

2. **Find the camera (Search)**
   Search for the product from your LAN. The factory IP setting 192.168.0.20 appears on the screen.

3. **Changing the IP address and related settings for the network environment**
   When you find the camera, click it and the settings will appear on the right side. Change the settings for the new network environment you need.
※ You must enter new settings in the IP, Netmask and Gateway fields and keep the settings in other fields unchanged.

4. **Submit data (Submit)**
   Click Submit to validate new settings.

5. **Confirmation**
   When all changes have been confirmed, click “Exit” to quit.

**Notes:**

1. The IP Finder can only find the IP addresses of cameras that share the same hub on the LAN. For information about finding IP addresses on the Internet, refer to the “DDNS setting”, or “UPnP Setting”.

2. All Alinking camera/network server products can be found and changed using the IP Finder software.

3. If the IP Finder software cannot be executed, check your antivirus software or firewall to remove the block.
4. Field description: You can give a name to your camera (such as “PT_IP” or “PT-IP”).
You can change the settings for IP, Gateway Address and Network Mask to meet the
requirements of your network environment. The product uses HTTP Port1 and does not
support Port2 settings.

MAC: Factory default network identity of the machine.

You can find 2 set of CMOS IR IPCAM in camera lists if the model is VOYAGER IW. One is
wired network, MAC number is 00:30:F0:XX:XX:XX; the other one is wireless, MAC
number is 00:0E:2E:XX:XX:XX.
Camera Setting from a Router

You can use DHCP when you want to use the camera on the Intranet (LAN). However, the IP must fixed when you want to use the camera on a WAN. For this application, it is required to set up a virtual server on the ADSL router. Follow the steps below to complete the setting:

1. Enter the camera setting page to set a fixed IP. (Refer to the “Network Setting”.) Ex.: 192.168.0.49
2. Enter the ADSL router main setting page. Ex.: Zonet ADSL router
3. Enter the Virtual Server setting page.
   a. Set “mapping of HTTP Port (80) to 192.168.0.49 ”.
   b. Restart ADSL router.

After completing the settings, you can operate the camera from a WAN IP Address via the ADSL router.

Example: The Virtual Server setting screen of the Zonet ADSL router

Note 1: The virtual server setting screen is not the same for all ADSL routers. Refer to the manual of the ADSL router you purchased for more information about the setting.

Note 2: Not all virtual servers on the ADSL routers support the external control. If possible, use the DMZ function to perform NAT and Firewall penetration.
DMZ stands for De-militarized zone. It is a small section of network between the internal network (militarized zone) and the external network. This zone can be sensed and protected by IDS, monitored by the firewall or detected by other safety mechanisms.
Change the Internet Explorer Setting

This product uses ActiveX Control to play images and sound on your PC. The ActiveX Control application software will be downloaded to your PC when you connect it to the Internet. To ensure successful download of the software, the Internet Explorer "security settings" must be changed accordingly. Make sure that the security level is set to **Medium**, the commonly used default security level.

**Steps:**
Open the IE browser ➔ Tools ➔ Internet Options ➔ Security ➔ Custom Level

1. This product supports IE 6.0 or above.
2. If you are using Firefox, please download and install the IE Tab kit first from https://addons.mozilla.org/en-US/firefox/addon/1419vu8y930.

An additional option will appear after the package is successfully installed. Left click the button (option) to run IE webpage simulation.
Install IE Tab.

Restart Firefox.

IE Tab online learning.
Enter the Main Page

1. Open the IE browser and key in the IP address of the product.

![Key in the IP address of the camera](image)

When the login screen appears, key in "root" in the User Name and Password fields. Click OK.

![Camera login screen](image)

2. Key in the default “username” and “password”.
   
   Default User Name: root
   
   Default Password: root
   
   You can access the camera as an administrator by default and set up for other users or privileges from the “Basic Settings” -> “User”.

3. Installation of Internet Explorer ad-hoc components
   
   When the username and password are confirmed, a control setup screen pops up under the IE address bar. Click “Install ActiveX Control” to install the controls.
4. The security warning screen appears. Click "Install".

The ActiveX Control is named "UIC ActiveX Control". This software is owned by UIC and well certified. You can use it without any doubts about its validity.
5. When the firewall block screen pop up, please select **Unblock**.

6. When ActiveX Control is installed successfully, you will see the camera image and interface.
Camera Main Page

Descriptions:

1. **Logo:** An alinking web page will show on another IE page when clicking the logo.

2. **Image area:** The streaming will show at the image area.

3. **Language (interface language selection):** This product currently supports three languages: English, Simplified Chinese, and Traditional Chinese.

**Attention:** Please change the streaming setting to HTTP if nothing appears in the image area.
Alert Message Description

1. Alert activation display
   When the position detection or alarm is activated, a red alert will blink on the screen to alert the user. Press to stop blinking.

2. Alert message
   Alert message: When the position detection or alert is activated, an alert message will display on the Alert Message box.
   Alert Snapshot: When it is ON, the alert video will be saved in the quick capture path. When it is OFF, the alert video will not be saved and only the alert message will display.
   Double click the message to view details. When an alert is activated, an alert message will display on the screen (50 messages, max.). When you exit this page, the message will be cleared automatically. You can also clear the message manually. (See Setup/Application Service Setup/Event/Event for details of alarm setup.)
Video Description

1. **Video Format:** sets the format for streaming
   - MPEG4 (main stream): Stream mode at MJPEG+MPEG4 or Dual MPEG4
   - MPEG4 (sub stream): Stream mode at Dual MPEG4
   - Motion JPEG: Stream mode at MJPEG+MPEG4
   Please refer to “Setting > Video / Image > Video” for details.

2. **View Size:** selects the size of the image
   Select the size of the image from 0.5 to 4 X.

   **Note:** It’s not recommended to use 4x zoom in size to view the video since the image will be abrasive due to the digital zoom effect.

3. **Streaming:** sets the video stream protocol (HTTP is recommended)
   This product provides three different video streaming protocols: UDP, TCP, and HTTP. HTTP is recommended because it allows the video stream to go through the firewall.
   (Refer to Setting/Basic Setting/Network/Streaming for more information).

   - **UDP:** provides the fastest but most unreliable transmission service. Video streams are transmitted through UDP Port (50000~60000 by default) to ensure the fastest image transmission. However, video fragment or mosaics may occur due to poor transmission quality.

   - **TCP:** provides reliable data transmission. Video streams are transmitted through RTSP Port (554 by default) to avoid video fragment or mosaics due to poor transmission quality.
quality.

HTTP: Video streams are transmitted through HTTP Port (80 by default) to ensure passing through firewalls.

<table>
<thead>
<tr>
<th></th>
<th>Tunneling</th>
<th>Pocket Loss</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>Easy</td>
<td>Fair</td>
<td>Fair</td>
</tr>
<tr>
<td>TCP</td>
<td>Fair</td>
<td>Lower</td>
<td>Fast</td>
</tr>
<tr>
<td>UDP</td>
<td>Hard</td>
<td>Lowest</td>
<td>Fastest</td>
</tr>
</tbody>
</table>

4. **Brightness/Hue/Contrast/Saturation**
Select the item you wish to adjust, then press the + or – button to adjust video display. Press + means to increase the value and – to decrease the value of the selected item.
Brightness: Adjusts the brightness of videos.
Hue: Adjusts the red and green tones of the image.
Contrast: Adjusts the contrast of colors.
Saturation: Adjusts the saturation of colors.
Set to default: Resets all items to default settings.

5. **DayNight Setting**
When select "Day" mode, the image is in color, however, it turns black and white when shift into "Night" mode. The image will be more clearly and smoothly when use Night mode. If the "Auto" mode has been selected, the Day/Night selection function will be concealed. Please refer to “Basic Setting>Video / Image>Sensor” for more information.
6. **ZOOM IN/OUT**: Click the image area and roll the mouse scroll front to zoom in or back to zoom out. Hold the mouse left button to drag the image.

7. **Full Screen**: Click Full screen to zoom image to whole screen.

8. **Jitter Time**: This function can help the video smoother. If the video lag caused by bad quality of network, please select 1 s to 5 s to add packet buffer.
Record Description

1. **REC**: executes the video recording function
   Click this button to start video recording and save the image file in the preset directory (C:\video). A red mark appears at the bottom left corner of the image when the recording function is running.

2. **Snapshot**: 
   Click this button to capture an image and save it to the preset directory. (C:\snapshot).

⚠️ The recording or snapshot functions might not be operated if you use VISTA operation system. Please select the WebPages into your trusted sites.
Select the WebPages into your trusted sites.

1. Select “Tools” on the IE browser.
2. Click Internet Options
3. Click Security
4. Select Trusted sites
5. Click Sites
6. Enter the IP Address of the product
7. Cancel the selection of the button
8. Click Add
9. Click Close
10. Close the entire IE browser then open a new IE. A "trusted sites" shall appear on the bottom of the banner.
3. **Path**: sets the save path and name for recorded images and snapshots. The filename is the recording date by default. You can identify the file by prefix of the filename.

Click the Path field to select the folder to save the file.

Save the path.
Audio Description

1. Voice communication
   When the speaker icon on the screen is green, it means the built-in microphone on the camera is receiving voice signals.
   When the microphone icon on the screen is green, it means the local microphone is sending voice signals to external speaker of a remote camera.
   Please refer to “Setting/Basic Setting/Audio” for details.

⚠️ You need a microphone and a speaker connected to your PC when using this function. A speaker must also be installed on the camera. Therefore, please check if the peripherals work properly before using this function.
System Settings
System setting contains basic and application settings. The basic setting is executed for basic system information, transmission speed, audio/video code, user authorization, date/time, and IP filter, while the application setting is executed for event triggering definition and other relevant settings, definition of the motion detection area, firmware update, reset to factory default, and reboot.

Basic Settings

Basic Setting > System (System info)

Basic Setting > System > System

- **Basic Setting > System > System > System Info**
  - **Device Name:** You can set the name for your camera here. Click Set to complete the setting.
  - Network information included MAC Address, IP Address, Network Mask, and Gateway. Firmware, Firmware Building time and Firmware Building Number are belong to Firmware version information.
  - **Current Viewers:** The number of viewers who are currently accessing the video stream.
  - **LED Switch:** Determine whether to enable or disable Status LED indicator or not.
**Status LED in link status:** When streaming video, status LED becomes green.

**Status LED in event status:** when an event is triggered, status LED blinks in orange

**Flash Time Interval:** Set the blink interval (unit: second).

- **Basic Setting > System > System Log**
  The administrator can view all login information of this camera, including boot record, video streaming mode, login IP, changes, and the date/time information. You can copy the entries to a Word document and save them manually. Please note that all information is deleted when you turn off the machine.

**Basic Setting > System > System Log**
This function can send log file to syslog server to monitor the situation of IP cam. You can download free software of syslog server from internet.

![Asante Megapixel IR IP Camera](image)

- **Basic Setting > System > System > System Log > System Log**
  Max Size: The numbers that log exist, the default is 100000.
  Critical Log: The most important log file.
  Warning Log: The medium level log file.
  Information Log: The general log file.

- **Basic Setting > System > System > System Log > Syslogd Service**
  Syslogd Service: click start to send log to server.
  Server: The IP address of syslog server.
  Port: Set the port number.
Basic Setting > Video/Image

Basic Setting > Video / Image > Video Format

You can select MPEG4 or MJPEG as the video format. It is recommended to select MPEG4 for real-time browsing to optimize the bandwidth. MJPEG is a good choice for the best resolution when video recording is required for collection of evidence.

Sensor Scan Mode: SXGA model will scan all sensor pixels (1.3 mega-pixels) and then output; while VGA mode will scan all sensor pixels and scale down into VGA (640 × 480) then output. Under the SXGA mode, the total frame rate (FPS) of MPEG4 + MJPEG can achieve up to maximum 15fps, and 3GPP is not supported under this mode, For example, if the total frame rate of MPEG4 and MJPEG is set to 15fps, each video encoder will reach 8fps approximately. Under the VGA mode, the frame rate can reach 30fps for each video encoder and 3GPP is supported, too.

Dual video encoders: Under SXGA mode, the primary video encoder is MPEG4, and the secondary encoder must be MJPEG. On the other hand, under VGA mode, the primary video encoder is MPEG4 while the secondary can be either MJPEG or MPEG4.
Generally speaking, selection of resolution is dependent on the bandwidth of the network you are using. This product offers different selections for video/audio settings. However, to ensure undisrupted image transmission, you need a higher uploading bandwidth. Generally, it is recommended to use QVGA resolution for normal bandwidth. To meet other requirements, refer to “Attachment B” for more information.
The product offers 5 image resolutions (PAL/NTSC):

1. SXGA (1280x1024)
2. XGA (1024x768)
3. VGA (640x480)
4. QVGA (320x240)
5. QQVGA (160x128)

Note that when choosing the video resolution to be SXGA (available in SXGA sensor scan mode, MJPEG encoder only), all pixels from the sensor will be shown. If choosing XGA resolution (available in SXGA sensor scan mode, MPEG4 encoder only), only the top left portion from the sensor pixels will be shown. Please refer to the figure below.
Basic Setting > Video / Image > Video Image > Frame per Second (FPS):

Users can set the frame rate from 1 ~ 12.5(PAL)/15(NTSC) in SXGA sensor scan mode, or 1~25(PAL)/30(NTSC) in VGA sensor scan mode. If the network upload bandwidth is insufficient, frame drops might happen such that the target frame rate may not be reached. Please refer to the Appendix B for details.

Basic Setting > Video / Image > Video Image > Video Quality

There are two video quality modes:

Fixed rate mode is suitable for use in a network environment that the upload bandwidth is limited. Please select the appropriate bit-rate according to your network environment. For example, if the network (upload) bandwidth available for the network camera is 500kbps, 500kbps multiplied 0.8 equals 400kbps (considering 20% overhead). This means that the largest fixed bit-rate should be set less than 400kbps; setting the bit-rate more than that might cause frame drops. Fixed quality mode is suitable for use if you want a constant video quality. If you want the best quality, Please choose the best option. The system will adjust the frame rate to fit the bandwidth available. There are 9 options to choose in fixed bit-rate drop-list. The higher the bit-rate, the better the video quality. There are 5 options to choose in fixed quality drop-list. The better the video quality, the higher the bit-rate is produced. Please refer to the “Appendix B” for more information.
Basic Setting > Video / Image > Video Image > 3GPP

To view the camera image using a 3G cellular phone, click Enable to enable the 3GPP mode.
(Note: When the 3GPP mode has been activated, all relevant parameters are set automatically and cannot be changed. This is for the sake of compatibility).

Note: the URI of 3GPP streaming is rtsp://IP address:554/cam1/3gpp
To use the 3GPP function, the following requirements must be met. Contact your telecom company to learn more about the connection conditions):

1. **3G phone**: Your cellular phone functions properly and supports 3G service. The compatible cellular phones that have passed our test are: Nokia (6630, 6500 classic, E61, E65, N70, N73, N80, N81, N93, N95-8G) Sony Ericsson (K608i, K800i, W810i) Wibo (WinII)
2. 3G phone number is available.
3. The 3G wireless networking service is available.
4. The camera has a fixed IP address.
5. The 3GPP mode is activated.

**Ex:** Nokia N71. Follow these steps to set up your 3G viewing function.

1. Enter multimedia data from the main screen.
2. Select a streaming link.
3. Add a new link.

4. Enter the link name.

5. Enter the IP address of the camera, e.g. rtsp://xxx.xxx.xxx.xxx:554/cam1/3gpp

6. Select OK to save the setting.

7. Select this stream name to proceed with linking.

8. Select “Yes” to connect.


10. Loading the image.
Note: Two ways to start 3GPP streaming

1. Without password
   Step 1: Enable anonymous login.

2. With password (if user name is root and password is root)

Basic Setting > Video / Image > PreProc

   Basic Setting > Video / Image > PreProc > PreProc Setting
   Camera position: Sets the position of camera on the screen.
   Default: Select this option when the product is in normal deployment.
   Flip position: Select this option when the product is mounted on the ceiling.
Mirror: Select this option when the product is in normal deployment, but from the reflection of a mirror.

Rotate 180°: Select this option when the product is installed on the ceiling and from the reflection of a mirror.

**Basic Setting > Video / Image > PreProc > Overlay Setting**

**Language:** choose the preferred language.

**Display mode:** You can select to display the date, time and text or not.

**Foreground color:** Selects the color for date, time and text display. Click on the color block to bring out the color palette. Move the pointer to the desired color and click on it.

**Display text:** Inputs the text you wish to display on the screen, e.g. Lobby IP Cam.

**Date/time position:** Selects the location where the date and time are displayed on the screen—any of the four corners.

**Text position:** Selects the location where text is displayed on the screen—any of the four corners.

**Alpha Blending:** Transparency available options are 0%, 50% and 100%.

Please don’t forget to press the Save button to save and apply the settings.
Basic Setting > Video / Image > Sensor
Adjust contrast and color. Displays date, camera ID and relevant information on the video. When the setting on this page is changed, a new image will immediately appear on the real-time display window.

Click the color block to call out the color palette.
Basic Setting > Video / Image > Sensor > DayNight Setting
When the ambient illumination becomes dim, IR LED will be switched on and the sensor image will become black and white. The Auto Day/Night mode is On by default. Select Manual if manual setting is required.

Mode:
- Auto: The camera will switch automatically into Day or Night mode based on the environment illumination.
- Manual: Set the Day or Night mode manually.
- External: Activate Day or Night Mode using external sensor. Connect the sensor with alarm input of the camera. Set up the activation in the "Event" function. Please refer to Application / Event for more information.

Switching Delay: This option is to set the time delay such that Day or Night mode switches. If it set 10 seconds, when system is in Night mode and detected the status that needs to shift Day mode, it will delay 10 seconds before switching to Day mode. This feature is in order to avoid switching modes due to misjudgment. This option is only applied to Auto Mode.

Sensitivity Level: The sensitivity to tell the difference between Day or Night. There are High, Mid and Low three levels.

Basic Setting > Video / Image > Sensor > AE setting
**Slow shutter:** The higher value correspond the slower shutter and the video will clear in dark place, but frame rate will drop.

**Flicker Control:** The screen flickers under fluorescent lamps when the lens is at 50Hz in the NTSC mode or 60Hz in the PAL mode. Activate this function to reduce flickers.

**Basic Setting > Audio**

**Basic Setting > Audio > Device Audio Setting**

**Audio:** Full duplex, half duplex, simplex microphone only, simplex amplifier only, and audio off.
- Full duplex: Allows using a microphone and amplifier at the same time, or turning them off.
- Half duplex: Allows using a microphone or amplifier by manual switch.
- Simplex microphone only: Allows using the microphone only.
- Simplex amplifier only: Allows using the speaker only.
- Audio off: Turns audio off; i.e. both the microphone and speaker are off.

---

**Audio input:** 1 formats

**Audio output:** 1 formats

G726/24: Uses G.726 24Kbps for audio encryption/decryption.

Gain: Adjust the volume of the audio.

---

**Basic Setting > User (User)**

The administration of the camera can set up access privileges by administrator, operator, and viewer to ensure the security and control of the camera. The access privileges and setting steps are described as below.

**Basic Setting > User > User List (access privilege list)**

The access privileges of the administrator, operator, and viewer are listed as follows. The
administrator has the right to define the privilege for each user depending on requirements.

<table>
<thead>
<tr>
<th>User</th>
<th>Administrator</th>
<th>Operator</th>
<th>Viewer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Live View</td>
<td>v</td>
<td>v</td>
<td>v</td>
</tr>
<tr>
<td>System Setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Video Setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>3GPP</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Audio Setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Date / Time Setting</td>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Setting</td>
<td>root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Setting</td>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>DDNS setting</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>PPPoE setting</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Streaming</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>UPnP</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>SAMBA</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Notification</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>IP Filter setting</td>
<td></td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Event Setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>schedule setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>event server</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>trigger setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Motion Setting</td>
<td>v</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>Firmware Upgrade</td>
<td>root</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Factory default</td>
<td>v</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reboot Setting</td>
<td></td>
<td>v</td>
<td></td>
</tr>
</tbody>
</table>

Steps: Click Add (to add a new user), Update (to change the privilege or password of a user on the list), or Delete (to delete a user from the list) and complete required fields. Then Click "Save" to complete the setting.

Options:
- Add: Add a new user and set up a different privilege.
- Update: Change the privilege or password of a user. You cannot change the name of the user.
- Delete: Delete a user from the list.
Add a new user and set up a different privilege.

Change the privilege or password of a user. You cannot change the name of the user.

Delete a user from the list.

Log in the username, password and privilege as required.

Basic Setting > User > User Setting (privilege setting)
For special business situations, this product allows you to log in to browse without the need of keying in your username and password. For this purpose, you need to check “Enable” at Anonymous Login. However, “Disable” for this option is recommended for the sake of security. Depending on the bandwidth and requirements, a limit up to 10 viewers who are allowed to view the camera simultaneously can be defined.
The default user name and password have been set as “root”. The root user cannot be deleted but root’s password can be changed. For the safety consideration, it’s recommended change the root’s password when the first time login. You can press the reset bottom to reset to factory default.

**Basic Setting > Network (Network Settings)**

**Basic Setting > Network > Network (Wired network setting page)**

- Basic Setting > Network > Network > IP Assignment
DHCP setting:
DHCP (Dynamic Host Configuration Protocol) is a protocol that enables automatic assignment of TCP/IP information to the client. Each DHCP client connects to the DHCP server to access its network setting information, including IP address, gateway, and DNS server.
The IP address of the camera is 192.168.0.20 by default when DHCP is "OFF". When you select "DHCP ON" and access the DHCP network environment, the camera will automatically send a DHCP packet to request an IP address. This IP address is assigned automatically from the DHCP server on the network. No additional settings are required for this page unless you need to change the network configuration. The DHCP status of the camera is "OFF" by default.

Other settings:
For IP address, Subnet mask, Default gateway, DNS 1, and DNS 2, the DHCP server will assign these values automatically when DHCP is in "ON" status; otherwise, you need to key in the values manually.

Note: Where no IP address is assigned from the DHCP server, the system will set the Link-Local Address automatically.
Basic Setting > Network > Wireless (Wireless network setting page)

Attention: Only wireless model provides this wireless function. (VOYAGER IW)

Basic Setting > Network > Wireless Setting > AP information

Scan: Scan the nearby wireless station; you can acquire most of the information of those stations (such as SSID, Mode, Channel, Encryption, Quality and BSSID).

Basic Setting > Network > Wireless Setting > Wireless

Enable: Turn on or off the wireless function.

Mode: Selection of the wireless networking mode.

1. Infrastructure: Infrastructure networking mode.

This camera uses the wireless Access Point (AP) as the hub when set to infrastructure networking mode and connects to the network via the wireless AP.

2. AdHoc: Point-to-point networking mode.

This camera connects to other wireless devices via a wireless network when it is in the AdHoc point-to-point networking mode; i.e. the product connects to other devices equipped with built-in wireless connection function without the need to access from any AP.
Note: Where no IP address is assigned from the DHCP server, the system will set the Link-Local Address automatically.

Authentication Type: Network authentication type

1. WEP (Wired Equivalent Privacy): it is an algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are thus more
susceptible to eavesdropping than wired networks. WEP uses a simple algorithm to provide confidentiality comparable to that of a traditional wired network.

**WEP Encryption: WEP encryption function**

When the base station (AP), which you want to access, has enabled the encryption function, you need to acquire the following information by accessing its encryption settings. You can use a computer equipped with wireless networking function to view the available wireless networks from the Windows system.

1. Encryption mode (64Bit or 128Bit)
2. Authentication type
3. Group (KEY1, KEY2, KEY3, KEY4)

Then change the settings on the wireless networking setting page to make them conform to the settings of the base station.

2. **Wi-Fi Protected Access (WPA and WPA2)** is a certification program administered by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks.
Note: Refer to the user setting instructions of your wireless IP sharer for more information.

SSID: Service Set Identifier

Enter the name of the base station (AP) to which you want to connect.
Encryption: The choice of different Authentication Type will show a different Encryption.
WEP security mode:
Select an encryption mode from the list. The format is “None” by default, indicating that the security function is disabled.

Authentication mode: One of the following authentication modes is required when you select a WEP encryption mode from the security list.
1. 64 Bit (10 Hex chars)
2. 64 Bit (5 ASCII chars)
3. 128 Bit (26 Hex chars)
4. 128 Bit (26 ASCII chars)
WEP key password encryption mode:

You can set up 64 Bit or 128 Bit WEP key password encryption mode. A set of 64 Bit encryptions is equivalent to 10 sets of hexadecimal digits or 5 sets of ASCII characters. A set of 128 Bit encryptions is equivalent to 26 sets of hexadecimal digits or 13 sets of ASCII characters.

<table>
<thead>
<tr>
<th>Encoding</th>
<th>HEX</th>
<th>ASCII</th>
</tr>
</thead>
<tbody>
<tr>
<td>Available characters</td>
<td>0<del>9, a</del>f, A~F</td>
<td>0<del>9, a</del>f, A~Z</td>
</tr>
<tr>
<td>64 Bit</td>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>128 Bit</td>
<td>26</td>
<td>13</td>
</tr>
</tbody>
</table>

WPA-PSK Mode:

Unlike in WEP mode that the key field can be left blank, you must input password in the key.
field if you choose WPA-PSK or WPA2-PSK authentication mode. The SSID input here must be the same as that of the wireless AP which this camera connects to. Passwords can be 8-64 characters, and which may also include special characters and space, and it will generate 4 Groups of WEP key automatically. WPA-PSK key should be a string of characters (uppercase or lowercase letters, numeric or punctuation), at least 20 characters above or at least 24 Hex digits. You must enter the same passwords or a 16 bit key as that of the wireless AP which this camera connects to. The more random the WPA-PSK password, the more secure when use.

Note: Refer to the user setting instructions of your wireless IP access point for more information.

WPA2-PSK Mode:

TKIP (Temporal Key Integrity Protocol) and AES: You can choose to use either TKIP or AES as the key encryption algorithm.
Note: Refer to the user setting instructions of your wireless IP access point for more information.

Ex.: Wireless mode setting (applicable to most situations)
Selection:
1. Mode: Select Infrastructure to connect the camera to a wireless base station.
2. Authentication Type: Select Shared Key.
3. SSID: Enter the server name of the base station.
4. WEP Encryption: Select the encrypted key that is the same as the base station.
5. KEY: Select a group that is the same as the wireless base station. You must select KEY1 for base stations that only have a set of keys.
6. DHCP ON/OFF: DHCP ON is recommended.
7. Save the settings.
8. Restart the equipment.

Basic Setting > Network > Wireless Setting> Wireless IP Assignment (IP setting in the wireless networking mode)

DHCP setting:
DHCP (Dynamic Host Configuration Protocol) is a protocol that enables automatic assignment of TCP/IP information to the client. Each DHCP client connects to the DHCP server to access its network setting information, including IP address, gateway, and DNS server.
The IP address of the camera is 192.168.0.20 by default when DHCP is “OFF”. When you select “DHCP ON” and access to the DHCP network environment, the camera will automatically send a DHCP packet request an IP address. This IP address is assigned automatically from the DHCP server on the network. No additional settings are required for this page unless you need to change the network configuration. The DHCP status of the camera is “OFF” by default.

Other settings:
For IP address, Subnet mask, Default gateway, DNS 1, and DNS 2, the DHCP server will assign these values automatically when DHCP is in "ON" status; otherwise, you need to key in the values manually.
Basic Setting > Network > Streaming (streaming Setting)

Setting of the video streaming port (HTTP and factory default are recommended)

1. HTTP: Port 80 can pass through most firewalls. Video streams are transmitted through HTTP Port (80 by default) to ensure passage through firewalls.

2. RTSP: Port 554 uses a fixed port (i.e. TCP) or can be defined by users to ensure reliable data transmission. Video streams are transmitted through RTSP Port (554 by default) to avoid video fragment or mosaics due to poor transmission quality.

3. RTP: Port 50000 to 60000 are UDP ports and can be defined by users. They provide the fastest but also most unreliable transmission service. Video streams are transmitted through UDP Port (50000–60000 by default) to ensure the fastest image transmission. However, video fragment or mosaics may occur due to poor transmission quality.
Basic Setting > Network > PPPoE (dial-up networking setting)

**PPPoE:** Point to Point Protocol over Ethernet is applicable to networking via a xDSL or cable modem. PPPoE setting must be executed in the LAN environment for your PC to connect to ADSL. Follow the steps below to complete the setting:

1. **Dial:** You can select whether or not to dial when you boot the machine.
2. **Use DHCP or fixed IP for connection to the LAN environment.**
3. **Key in the IP address of the camera and enter "PPPoE Setting" following the route Setting ➔ Basic Setting ➔ Network ➔ PPPoE.**
4. **Key in the xDSL "Username" and "Password" acquired from your ISP. Click Save to confirm the setting.**
5. **Where the ADSL modem and the camera is connected via a switch-hub, you can press “Reboot” or restart the machine manually to try PPPoE dialing when the setting of the camera has been completed.**
6. **A different IP address is obtained after each dial-up network connection. You can get the new IP address from Setting ➔ Basic Settings ➔ System. If you want to know the new IP address anytime, you must enter Setting ➔ Basic Settings ➔ Notification to set some settings. There are three ways to get information: 1. SMTP 2. FTP 3. HTTP. For details, refer to the Notification Setup Menu.**

**Note:** You can use the DDNS function to access the camera. Refer to the “DDNS Setting” page for more information.
- **Basic Setting > Network > PPPoE**
  Dial: You can select whether or not to dial when you boot the machine (On Boot or Off).
  Username: Enter the username provided by your ISP.
  Password: Enter the password.

- **Basic Setting > Network > PPPoE Information**
  IP Address: The IP address acquired when dialing has been executed successfully.
  Subnet Mask: The subnet mask information acquired when dialing has been executed successfully.
  Default Gateway: The gateway information acquired when dialing has been executed successfully.
  DNS: The ISP domain name acquired when dialing has been executed successfully.

**Basic Setting > Network > DDNS (Dynamic Domain Name Server Setting)**
The IP address (Ex. 210.168.0.22) is like a telephone number, while the website address is like a name in an address book. The DDNS allows the user to access the website by entering the name of the website without memorizing a bunch of cold numbers.

When you apply for an Internet service, you will have at least one IP address from your ISP that is either fixed or dynamic. Most of the ADSL service providers will give you a dynamic IP for ADSL environments, which means your IP address will constantly change each time you connect to the Internet. As a result, users from WAN environments will have much
difficulty finding the correct IP address. The DDNS (Dynamic DNS service) is created for exactly this kind of moment. By updating your WAN IP address each time you connect to the Internet, the DDNS helps you locate your website and access your website easily. You can find a lot of free DDNS service providers on the Internet, such as www.no-ip.com and www.DynDNS.org.

Some gateway-routers can directly communicate with DDNS. In this case, you may directly enter your DDNS account on the setting page in the Internet router, and then the router will update your WAN IP status whenever it is changed and report to the DDNS. If your router does not support direct communication with the DDNS, you can download a small application program on the DDNS service page to help you update your WAN IP.

**Item Description:**

Active: enables/disables DDNS

DDNS Server: currently we only support [http://dyndns.org](http://dyndns.org). This is a free domain name server provided by DynDNS. You may log on this website for relevant information and apply for free domain names.

Username: your account for the domain name you applied for

Password: your password for the domain name you applied for

Domain Name: the domain name you applied for.
Basic Setting > Network > UPnP (Universal Plug and Play)

If you connect your camera to a router, IP allocator, or wireless AP, your camera will possibly be blocked by the NAT and can’t be located on the Internet. To penetrate the firewall, activate the supportive item- UPnP. The Link URL shows the external IP address and the port of the router. Enter the IP address in the Internet Explorer to penetrate the NAT.

- **Basic Setting > Network > UPnP > UPnP Device**
  
  Active: yes (enable)/no (disable)
  Device Name: the name of the UPnP device

- **Basic Setting > Network > UPnP > UPnP Traversal**
  
  Active: yes (enable)/no (disable)
  Port Range: the range of the usable ports, from 32768 to 65535 as default
  Link URL: After the network camera penetrates the firewall successfully, the actual external IP address and port will be shown.
  Click “Save” to confirm when you finish.

![UPnP setting](image_url)
To activate the UPnP function in Windows OS:
Ex: Windows XP:
1. Windows component installation.
   - Step 1: Click Control Panel
   - Step 2: Click Add/Remove Programs
   - Step 3: Click Add/Remove Windows Components
   - Step 4: Click Networking Services
   - Step 5: Click Detail
   - Step 6: Check UPnP User Interface
2. Open Windows firewall option
Basic Setting > Network > SMTP Server (mail server setting)

This camera is able to transmit images to a particular email address when a motion detection event occurs or a sensor is triggered. To use this function, a mail server setting for the camera is required.

Enter the following information in sequential order to complete the setting:

- SMTP server: the SMTP server IP address.
- SMTP From: the email of the sender, i.e. xxx@xxx.com
- SMTP Authentication: enables/disables

3. View the connection device using “My Network Place”

1. Open “My Network Place”

2. The LAN camera appears.

Double-click to access the main page.

2. Click Exceptions

Step 1: Click Windows Firewall in the Control Panel

Step 3: Check UPnP Configuration.

1. Open “My Network Place”

2. The LAN camera appears.

Double-click to access the main page.
- User name: the SMTP server username.
- Password: the password of the SMTP server.
- Select **Save** to save the setting.

**SMTP Setting**

This camera is able to upload the snapshots to a specified shared folder when an event is triggered. To use this function, a Samba setting is required.

**Options:**
- **Active:** Enable/Disable
- **Samba Authentication:** Enable/Disable
- **Username:** the username
- **Password:** the password
- **Path:** specify the IP address of the computer you want to share with and the file name, i.e. 192.168.0.X/xxx
- **Recycle Record:** Enable for the last record file to mantle the first record file.
- **Remaining SAMBA Capacity:** the remaining capacity can be record.
- **Shared Folder Size (MB):** the total capacity of the folder. Always remember to set the size of the folder to avoid exhaustion of disk capacity.

**Basic Setting > Network > Samba**

This camera is able to upload the snapshots to a specified shared folder when an event is triggered. To use this function, a Samba setting is required.

**Options:**
- **Active:** Enable/Disable
- **Samba Authentication:** Enable/Disable
- **Username:** the username
- **Password:** the password
- **Path:** specify the IP address of the computer you want to share with and the file name, i.e. 192.168.0.X/xxx
- **Recycle Record:** Enable for the last record file to mantle the first record file.
- **Remaining SAMBA Capacity:** the remaining capacity can be record.
- **Shared Folder Size (MB):** the total capacity of the folder. Always remember to set the size of the folder to avoid exhaustion of disk capacity.
Basic Setting > Network > Notification of IP address Change (IP address change notice)

This setting is not necessary for a fixed IP. For a dynamic IP, you need to update the IP address every time you connect to the Internet to access the camera. This setting allows you to update the IP address by the automatic notification of IP address change. Choose one of the following three notice options to update the IP address:

1. Notification via SMTP mail server

   - **Basic Setting > Network > Notification of IP Address Change > SMTP Notification**
     - SMTP Notification: notification via SMTP mail server
     - SMTP SendTo: the recipient, i.e. xxx@xxx.com
     - SMTP Subject: mail subject
     - Select **Save** to complete and activate your settings.

2. Notification via FTP server

   - **Basic Setting > Network > Notification of IP Address Change > FTP Notification**
     - FTP Server: FTP Server name.
     - FTP Port: FTP port. The default setting is 21 (recommended).
     - FTP Upload path: the path to upload files.
     - FTP Login name: the name to log in the FTP.
FTP Login Password: the password to log in the FTP.
Select [Save] to complete and activate your settings.

3. Notification via HTTP server

- **Basic Setting > Network > Notification of IP Address Change > HTTP Notification**
  - Server: the address of the server, i.e. http://.
  - Port: the port to access HTTP. The default setting is 80 (recommended).
  - Parameter: the setting of the parameters, refer to the installation setting of your HTTP server.

Refer to the installation setting of your HTTP server for the setting of the parameters (such as Username, Password, and Proxy).
Select [Save] to complete and activate your settings.

---

**Basic Setting > Network > Multicast**

This function allows multiple people to watch video streaming without limitation on the number of users, but is only applicable in the LAN environment. The video streaming format (MPEG4/MJPEG) depends on the selected image format setting in Basic Setting → Video/Image → Video Format.
**Basic Setting > Network > Multicast > MPEG4**
This function allows multiple users to view the MPEG4 video stream free from restrictions on the number of users. However, this is only effective within the LAN.

**Basic Setting > Network > Multicast > Motion JPEG**
This function allows multiple users to view the Motion JPEG video stream free from restrictions on the number of users. However, this is only effective within the LAN.
Basic Setting > Date/Time (date/time setting)

1. **Synchronize the time with PC’s time:**
   - The preset method of time synchronization of the camera time with your PC time.

2. **Get Time from an NTP server: synchronize the time with the NTP (Network Time Protocol)**
   - Click on the “NTP” Button
   - Enter the NTP server’s IP address.
   - Press “SAVE” to activate it.
   - The camera will update its time once obtaining the NTP time.

   **Note:** The default NTP servers are:
   - A. NTP Server 1: 198.123.30.132
   - B. NTP Server 2: 192.43.244.18
   - C. NTP Server 3: 133.100.9.2

3. **Change the time manually:**
   - Click the “User Input”.
   - Select the format of date display, i.e. “yyyy/mm/dd” format.
   - Select the format of date display, “hh:mm:ss” by 24 hours format.
Select the time zone.
Select “Adjust” to adjust time.

**Basic Setting > IP Filtering**

This function filters IP addresses and is able to allow or deny visits from particular addresses/target addresses.

**IP filter setting**

**Basic Setting > IP Filter > General**

IP Filtering: enables/disables the IP filter
Policy: allows/denies access

**Basic Setting > IP Filter > Filter IP Address (Overview of the set IPs)**

- **Add**: enter the IP address you want to allow or deny the access of in the front field.
- **Remove**: removes a set IP addresses
- **Remove All**: removes all the set IP address

**Special Attention**

**Setting rules:**

1. Actions that may cause a limited connection are to be denied.
2. Improper use of this function may cause disconnection from Internet. You might need to use hardware reset to reset to the factory default. Please refer to the “Factory Default” for details.
Application Setting

**Application Setting > Event (event trigger setting page)**

This camera is equipped with intelligent security management functions. It ensures security monitoring by allowing user to define “trigger events” based on particular times and situations, and sets the camera respond to the event.

**Application Setting > Event > Event Setting**

[Image of the interface]

Click [Add Event] to enter the trigger event setting
### Event Setting

#### General
<table>
<thead>
<tr>
<th>Name</th>
<th>New0</th>
</tr>
</thead>
</table>

#### Response to event trigger
- **Always**
  - During time: [ ] Sun, [ ] Mon, [ ] Tue, [ ] Wed, [ ] Thu, [ ] Fri, [ ] Sat
  - Start from: [ ] 00:00 Duration: [ ] 00:00 (max 16:00 hours/minutes)
- **Never**

#### Trigger by
- [ ] Alarm input
- [ ] Motion Detection
- [ ] Area 1, [ ] Area 2, [ ] Area 3
- [ ] On boot

#### Response process
- [ ] Active alarm out
  - [ ] Alarm Out1
  - [ ] Duration 1 [ ] Seconds

#### Upload video/image to server
- Base file name: [ ]
- File format: [ ] MP4 [ ] Main Stream
- [ ] Add data/time suffix
- [ ] Add sequence number suffix up to [ ] and then start over.

#### Upload Server Type:
- [ ] HTTP
  - Include pre-trigger buffer: [ ] [ ] Seconds
  - Include post-trigger buffer: [ ] [ ] Seconds
  - Continue video upload: [ ] [ ] Seconds

#### Recording Storage Device:
- [ ] SD Card
  - Include pre-trigger buffer: [ ] [ ] Seconds
  - Include post-trigger buffer: [ ] [ ] Seconds
  - Continue video upload: [ ] [ ] Seconds

---

**In order to get a better quality of your recording, please make sure the target bitrate of recording channel is under 1500 Kbps**

### HTTP notification
- [ ] Send HTTP notification
  - Custom parameters
  - Message

### TCP notification
- [ ] Send TCP notification
  - Message

### NTP notification
- [ ] Send NTP notification
  - Device ID

### Day Night
- [ ] Day
- [ ] Night

[Save] [Cancel]
Add Event: Add Event setting page

Options:

• General:
  Name: Name the trigger event here.

• Response to event trigger: the time setting of the trigger event
  Always: Always monitoring
  During time: Check the date you want to monitor (Sun–Sat) and the duration of monitoring here. For example, if you want to set the camera to monitor from 7 pm after work to 7 am next morning from Monday to Friday, check the boxes from Monday to Friday, enter “19:00” in the “Start From” field, and enter “12:00” in the “Duration” field.
  Never: Do not set the time.

• Trigger by: sources of trigger events (Note: You can only set one trigger event once.)
  Alarm input: The alarm is triggered by the security equipment connected from the DI terminals behind the machine, such as door/window detectors, infrared sensors.
  Motion Detection: The alarm is triggered when motion is detected. The camera will send an alarm when any objects appear in the set detection area.
  On boot: The alarm is triggered by reboot. The camera will send an alarm when the system is rebooted due to power shortage, sabotage, or other reasons.

• Response process: trigger event response (Note: Multiple selections are available)
  Active alarm out: An event is detected by the security equipment connected from the DI terminal behind the machine, such as high-decibel alarms, light projectors. You can set the alarm duration in the “Duration” field.
Upload video to: The camera will send the capture Motion JPEG or MPEG4 video of the event to the FTP server or Samba you specified.

Include pre-trigger buffer: When an event is detected, the camera will record the previous video image up to 10 seconds.

Include post-trigger buffer: When an event is detected, the camera will record the post video image up to 10 seconds.

Continue video upload: When the event is continue, the camera will record the video image up to 10 seconds.

For example: If the pre-trigger 5 seconds, post-trigger 5 seconds and continue video upload 5 seconds have been selected, the total file size will be 15 seconds.

Upload img to: The camera will send the capture photo of the event to the FTP server or Samba you specified.

Send HTTP notification: The alarm will be sent to the HTTP server you specified. To use this function, set the coordinative HTTP server in the Event Server setting page in advance.

Send TCP notification: The alarm will be sent to the TCP Server you specified. To use this function, set the coordinative TCP server in the Event Server setting page in advance.

Send NAP notification: The alarm will be sent to the NAP Server you specified. To use this function, set the coordinative NAP server in the Event Server setting page in advance.

Day Night: Force the camera turn into Day/Night Mode when the trigger is detected.

Click [Save] to save and activate your settings when you completed setting.

[Add Schedule]: Add Schedule setting page
The Add Event setting page and the Add Schedule setting page are basically the same except that the Add Schedule setting page does not have the option “Trigger by” to indicate the sources of the trigger event.
Click [Save] to save and activate your settings when you complete setting.

**Delete**: delete the event cluster setting.
**Modify**: modify the event cluster setting.

**Application Setting > Event > Trigger (manual test of trigger response)**

Whenever the camera detects abnormal events during the scheduled time, it will automatically respond by performing trigger response. There are 2 types of trigger responses: alarm sending and emailing the alarm or recorded image to the specified server. To use this function, enter the server information by accessing Application Setting > Event > Event Server. You may perform manual test as specified in this section once you complete the setting to ensure that all functions are working properly.

The default status of the digital input pin is set as “Normal Open”, but users can change it to “Normal Ground” by setting the page “Setting > Application > Event > Trigger”:

1. When alarm input is set to be “Normal Open”, then the external device connected to alarm input pin should be in open status. So when the external device is triggered to close status, the alarm input pin will be triggered.
2. On the contrary, when alarm input pin is set to be “Normal Grounded” then the external device connected to alarm input pin should be in close status. So when the external device is triggered to open status, the alarm input pin will be triggered.
(Please refer to Attachment A for detailed explanation.)

**Note:** It is recommended to set up the Trigger Setting page (Setting-> Application Setting-> Event-> Trigger) before installing the hardware alarm I/O!

**Trigger Alarm output: Alarm output**
Click “Set” to trigger the alarm. Click “Clear” to stop the alarm. (Please make sure to click “Clear” for closing the alarm testing when the trigger testing is done).

**Trigger mail: Sending mail**
Click “Set” after you enter the email address and subject to test the integrity of the sent mail.

**Trigger FTP: Sending AVI file to FTP Server**
Upload AVI files to FTP server to test the file integrity.

**HTTP Server: Sending message to HTTP Server**
Upload message to HTTP server to test the message integrity. Enter the message in the “Message” field. You may go to Application Setting > Event > Event Server to make a complete custom parameters settings.

**TCP Server: Sending message to TCP Server**
Enter the message in the “Message” field.

**Trigger SAMBA: Sending message to Samba shared folder**
Path: Enter the path of the shared folder in your PC.

**Application Setting > Event > Event Servers (setting for uploading trigger event file to the server)**
Here you can perform a complete setting for uploading files to the server. Please set servers (SMTP, FTP, SAMBA…etc) in the Event Server setting by the instructions below:
Click **Add FTP** to go to the setting page and enter the information of the FTP server you specified.

Name: the name of the FTP
Network Address: IP address of the FTP
Login: Log-in name
Password: Log-in password
Upload Path: Uploading path
Port: Port
Passive: Check to set the FTP status as passive

Click [Add Http] to go to the setting page and enter the information of the HTTP server you specified.

Name: HTTP name
Network Address: HTTP IP address
Login: Log-in name
Password: Log-in password
Proxy: Proxy server name
Proxy Port: Proxy server port
Proxy Login: Proxy server log-in name
Proxy Password: Proxy server log-in password

Click [Add TCP] to go to the setting page and enter the information of the TCP server you specified.
Name: TCP server name
Network Address: TCP IP address
Port: TCP port

Click **Add UDP** to go to the setting page and enter the information of the UDP server you specified.
Name: UDP server name
Network Address: UDP IP address of UDP.
Port: UDP port

Modify: Modifies the setting value
Remove: Removes the setting value

**Application Setting > Motion Detection**

You can open the setting frame by clicking on the area to monitor. To move area to monitor, drag the area with your mouse; to adjust the size of the frame, drag the arrow to adjust after you move the mouse to the edge of the area and left-click; There are 3 frames available for setting. You may adjust the sensitivity of the area by entering the degree of sensitivity in the “Detect Level” field. “Lower” is least sensitive, “Highest” is extremely sensitive.

Exclusive: User can set some areas that are not willing to be detected. The function appear as number 4 (blue frame) in the picture.

Select Save to complete and activate your settings.
Application Setting > Privacy mask

The privacy zone function can mask the image in the mask zone to ensure confidentiality. First, select a mask zone (1 to 3) and a mask color in the privacy zone. Then, move the green frame to the area you want to mask. Moving the cursor to the bottom right corner of the frame can change the size of the frame. When the setting is completed, click Save to make the setting effective, and the screen will automatically refresh within a few seconds after the setting is effective.
Application Setting > Firmware upgrade

Contact your dealer for more information about firmware upgrade. Please follow the steps below to execute the upgrade.

**Important! Read Carefully!!**

1. Close all active applications on your PC.
2. Select “Firmware Upgrade”.
   
   The Firmware Upgrade Setting page appears.
3. Click **Browse...** to select the location where the firmware file is stored.
4. Click **Submit**
5. The auto upgrade runs. The Upgrade Status shows the progress of the upgrade.

When the firmware upgrade has been completed, the machine reboots automatically. Reconnect to the server after 60 seconds.
Note: The new firmware is burned into the Flash ROM during the upgrade, so you must take care during the process and make sure it is not interrupted during the operation. The system may be damaged seriously and need to be returned to the factory for repair if the power cable is removed or becomes loose during the upgrade. Firmware upgrading in a wireless network environment is not recommended because unstable packet transmission may bring about loss of data.

When the firmware upgrade has been completed, you don't need to restart the camera manually. The camera will reboot automatically after 60 seconds (Reboot OK). Then open the IE browser and key in the IP address (The original IP address remains undeleted).

**Application Setting > Factory Default**

You can use this function to reset to factory default, but all changes, including the IP address, you have made are deleted.
Factory Default: Reset to factory default.

Resets all parameters, except the IP parameters:
You can use this function to reset to factory default. All changes you have made are deleted but the IP address and all settings relevant to networking remain valid, including cable and wireless network settings. Click Set to complete the reset.

Resets all parameters:
You can use this function to reset to factory default. All changes, including the IP address, you have made are deleted. Click Set and a warning window appears to ask if you really want to reset to factory default. Click “OK” to complete the reset.
**Backup: Data backup**

**Back all parameters:**

Back up all changes you have made. When you click [Backup], a file download window appears. Back up the file named param.bin (⚠️ Don't change the file name; otherwise, the backup may fail.)

![Backup window](image)

**Restore backup parameters:**

You can select this function to restore the changes you have made. To do this, click [Browse…] to select a backup file and click [Submit] to confirm the restoration.

![Restore window](image)
**Application Setting > Reboot**

You can enable this function for the camera to reboot automatically.
Attachment A: External Alarm

In addition to the motion detection executed by the internal software application, the product can connect to external infrared detectors, beepers, and smoke detectors. For more information about these external devices, contact to your local retailer, dealer or installation service provider. This product provides a standard Alarm I/O for you.

This camera provides 2 sets of digital inputs (DIs) and 1 set of digital outputs (DOs). Pins 1 and 2 are designed for connection to external Sensor 1; Pins 2 and 3 for external Sensor 2. All 3 pins are designed for connection to the C connection equipment and should not access to voltage or current. Otherwise, the product will be damaged. Pins 4, 5 and 6 are relays to normally open (NO) or close (NC) these external devices. These 3 pins only act as relay output contacts and no power is output (dry contacts).

The default status for this DI sets is NO. The gray color indicates the current status. NC status can be selected by selecting Setting/ Application Setting/ Event/ Trigger/ Alarm Input Setting.

Applications:
1. When the status is NO, the connected C connection equipment should be NO as well. When the C connection equipment is triggered, the status will change to NC. The machine will detect this change and inform the system.
2. When the status is NC, the connected C connection equipment should be NC as well. When the C connection equipment is triggered, the status will change to NO. The machine will detect this change and inform the system.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alarm Input #1</td>
</tr>
<tr>
<td>2</td>
<td>Alarm Input #1/2 (K).Ground</td>
</tr>
<tr>
<td>3</td>
<td>Alarm Input #2</td>
</tr>
<tr>
<td>4</td>
<td>Alarm Output #1 (NC).Max 24VDC, 1A</td>
</tr>
<tr>
<td>5</td>
<td>Alarm Output #1 (COM)</td>
</tr>
<tr>
<td>6</td>
<td>Alarm Output #1 (NO)</td>
</tr>
</tbody>
</table>
External Alarm I/O Circuit Diagram

**Warning!** The alarm will be triggered when alarm pin 1 & 2 are formed as a short circuit. Please do not connect the electric voltage or current into alarm input pin because the electronic current might burn the product.

**Warning!** The alarm will be triggered when alarm pin 2 & 3 are formed as a short circuit. Please do not connect the electric voltage or current into alarm input pin because the electronic current might burn the product.

- **Warning!** Where connecting of a low or high current loop to the external alarm input/output of the product is required, the wiring and connection shall be conducted by a qualified electrician. Incorrect wiring may bring about damage to the product fatal electric shock.
- **Warning!** Direct connection of the external alarm input/output terminal to high-current equipment is not allowed and a customized repeat circuit might be required (provided by the customer) for some cases to isolate the terminal and the high-current equipment. Where the voltage/current of an external device exceeds the loading capability (DC 50V) of the Alarm I/O, the product would be damaged seriously.
Attachment B: Bandwidth Estimation

Since the FPS is dependent on the bandwidth of the camera, the relationship between the size of an image file and the bandwidth is always the major concern of the system construction engineer.

The table below shows the relation between the resolution and size of an MJPEG file in the NTSC system. Please note that the values in the table are for reference only, because the size of an image file is closely related to the complexity of the environment and the actual situation of the place being monitored.

<table>
<thead>
<tr>
<th>Image Resolution</th>
<th>Average range of Data Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>160 x 120 (QQVGA)</td>
<td>20k - 50k bit</td>
</tr>
<tr>
<td>320 x 240 (QVGA)</td>
<td>50k - 150k bit</td>
</tr>
<tr>
<td>640 x 480 (VGA)</td>
<td>150k - 350k bit</td>
</tr>
<tr>
<td>1280 x 1024 (SXGA)</td>
<td>400k – 900k bit</td>
</tr>
</tbody>
</table>

The table below shows the relation between the resolution and size of an MPEG4 file in the NTSC system.

<table>
<thead>
<tr>
<th>Image Resolution</th>
<th>Average range of Data Sizes</th>
</tr>
</thead>
<tbody>
<tr>
<td>160 x 120 (QQVGA)</td>
<td>10k - 40k bit</td>
</tr>
<tr>
<td>320 x 240 (QVGA)</td>
<td>20k - 100k bit</td>
</tr>
<tr>
<td>640 x 480 (VGA)</td>
<td>60k - 210k bit</td>
</tr>
<tr>
<td>1024 x 768 (XGA)</td>
<td>100k – 300k bit</td>
</tr>
</tbody>
</table>

Ex.: The transmission speed on the Internet is 2fps under 320 x 240, i.e. 50k*2=100k to 150*2=300k per second. It is suggested to apply for 512K "upload" bandwidth.

**Note 1:** What the camera needs at the client end is the “upload” bandwidth. However, most ISPs in Taiwan provide download bandwidth that is wider than the upload bandwidth. Therefore, symmetrical bandwidth is a good choice for users who need wider upload bandwidth. Ex. download/upload = 521K/512K

**Note 2:** 32 kbps to 64kbps is required for transmission of audio signals.
## Attachment C: Troubleshooting and FAQs

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Function</strong></td>
<td></td>
</tr>
<tr>
<td>What encoder and decoder are used by the camera for sounds and images?</td>
<td>The camera uses MJPEG or MPEG4 compression technology to provide quality images. MJPEG is a standard image compression technology applicable to different browsers without the need to install additional software. MPEG4 is next-generation image compression standard and can provide high image quality at low bandwidth. The sound decoder uses G.726 compression technology.</td>
</tr>
<tr>
<td>How many users are allowed to view the camera simultaneously?</td>
<td>The maximum number of viewers depends on the bandwidth of the client accessing the camera. About 5–6Mbps are used to process data of the camera, so the maximum number of viewers changes in proportion to FPS and the resolution of the image. Obviously, the higher the number of viewers, the lower the performance at each client ends.</td>
</tr>
<tr>
<td>Is it possible to catch the image from the camera in a real-time manner?</td>
<td>Yes, you can use the snapshot function from the main control page.</td>
</tr>
</tbody>
</table>

### Camera Installation

<table>
<thead>
<tr>
<th>Question</th>
<th>Answer and Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can the camera be used outdoors?</td>
<td>The camera is not waterproof, so a special waterproof cover must be available for outdoor use. Please note that the waterproof cover may affect the built-in pickup function of the camera.</td>
</tr>
<tr>
<td>What network cable is used for the camera?</td>
<td>The camera uses a 10 or 100 Base-T Category 5 UTP network cable.</td>
</tr>
<tr>
<td>How to install and operate the camera behind a firewall?</td>
<td>If you have a firewall in your network environment, please select HTTP mode (Port80). Generally the port 80 is always open for the browser to access the Internet.</td>
</tr>
</tbody>
</table>
| What are the username and password for the first use and after reset to factory default? | Username = root  
Password = root. Please change your password immediately after entering the system to ensure information security.                                                                                      |
| I forgot the username and password I used for the setting. What should I do? | Please proceed as follows:  
1. Hold the Reset button for 4 seconds after booting to reset the password to preset.  
2. Change the username and the password.                                                                                                               |
| I forgot the IP address of the camera. What should I do?               | Use IP Finder to locate the IP address of the camera. Please connect the camera and the PC on which the IP finder is executed to the same hub.                                                                        |
| IP Finder cannot find the camera.                                      | • When the camera still can’t be located over 1 minute, re-activate the camera.  
• Do not connect the camera to more than one router. The IP Finder will not be able to detect the camera.  
• If the IP of PC on which the IP Finder is executed is not correctly set, the IP Finder will not be able to locate the camera. Please confirm that the IP address has been properly set.  
• The anti-virus applications on the PC or the firewall might block the IP Finder from execution. If you can not execute the IP Finder, please disable your anti-virus applications or firewall. |
<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer does not display the camera screen correctly.</td>
<td>Please be sure that the version of your Internet Explorer is 6.0 or later. Should you have any difficulties, please log on the Microsoft website to update your browser. Microsoft website: <a href="http://www.microsoft.com/windows/ie">http://www.microsoft.com/windows/ie</a>.</td>
</tr>
<tr>
<td>IP Finder cannot store network parameters.</td>
<td>• Your connection might have problems. Please ensure that the network parameters and the camera connection are correctly set.</td>
</tr>
</tbody>
</table>
| I cannot enter the login screen and camera page from Internet Explorer. | • The IP address of the camera is possibly being used by another PC or device. Please disconnect the network cable from the camera and execute PING to confirm if the IP address has been used.  
• It is possibly due to the network cable. Please use the cross-line network cable to connect the PC and the camera, and see if the log-in screen appears.  
• Be sure that the network connection and the settings are properly configured.  
• Be sure to enter correct IP address in the Internet Explorer. If you use dynamic IP address, the address might have been changed after your last check.  
• Internet traffic might slow down the webpage access. Please wait.  
• Be sure that you are using http port. The default setting is Port 80. It will be converted to the private camera IP address.  
• The port assigned for your camera might not able to access the Internet. Contact your ISP to acquire a usable port.  
• The proxy server might be blocking you from connecting to the camera. Do not set the proxy server.  
• Please be sure that the default gateway address is correct.  
• Your router might need Port conversion. Refer to the user manual of your router for details.  
• The package filtering function of the router might have blocked the access to the external Internet. Refer to the user manual of your router for details.  
• If you are using DDNS, please remember to set the default gateway and server address.  
• If none of the procedures above is working, please reset to the factory default values and re-install.  
• If the problem still persists, there might be some problems with the product. Contact the dealer who sold you the product for more help. |
| No image appears on the main control screen.                           | • When using PC to connect to the camera for the first time, a security warning window will tell you that you need to download the ActiveX control. When you are using Windows 2000 or Windows XP, you might need a properly-authorized user account to install the application  
• Network traffic might slow down the video streams. If the video is extremely slow, select a lower resolution for a lower bandwidth requirement. |
| Check whether the Active X control of the camera has been installed in your computer. | Select C:\Windows\Downloaded Program Files to check if the file “Media Viewer Class” is registered. The status bar should indicate the file has been installed. If you do not see this file, be sure that your Internet Explorer security is properly set (the default value is moderate). Re-connect to the camera main page and download the file again. Incomplete download or installation of the camera ActiveX control is the major reason for this problem. Check |
the security setting of your Internet Explorer. Close and re-open Internet Explorer, and enter the main page to see if you can log in.

<table>
<thead>
<tr>
<th>Problem Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer displays the following message:</td>
<td>Change the IE security setting to allow downloading unsigned ActiveX control.</td>
</tr>
<tr>
<td>Downloading the ActiveX control is prohibited under the current security setting.</td>
<td>IE → Tools → Internet Options → Security → Custom Level. Change &quot;Inactive&quot; to &quot;Tips&quot; for the ActiveX control if required.</td>
</tr>
<tr>
<td></td>
<td>• A firewall mechanism might have been activated. Check the setting of your system or ask your network administrator. To access the camera from the Internet, you may need to change the setting of the firewall.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that your camera does not conflict with other servers on the same LAN.</td>
</tr>
<tr>
<td></td>
<td>• Check the router and make sure that its setting allows it to access your camera from the Internet.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>The camera can operate only in the LAN rather in the Internet environment.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Congestion of the network or objects of the image may affect the number of frames transmitted. The number of frames may be less than the defined value when they are transmitted via a congested network.</td>
</tr>
<tr>
<td></td>
<td>• The number of frames transmitted may become less when multiple users are viewing the video stream.</td>
</tr>
<tr>
<td></td>
<td>• The network hub might be another reason for this problem, especially when multiple camera video streams are viewed simultaneously.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>The number of frames transmitted is less than the defined value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• When you connect your PC to the camera, no sufficient bandwidth is available to support more frames with the current resolution of video streams. Reduce the resolution to QQVGA (176x144) or QVGA (320x240) and deactivate the audio function.</td>
</tr>
<tr>
<td></td>
<td>• The audio signal needs 32 to 64 kbps of your bandwidth. You can deactivate the audio function to improve the image quality. Your Internet service may have not sufficient bandwidth to support audio transmission.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>When the audit function is activated, the video streaming area becomes black or the transmission becomes slower.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Make sure the IP address of the gateway and domain server (DNS) has been defined correctly.</td>
</tr>
<tr>
<td></td>
<td>• Where FTP still fails, contact your ISP or network administrator to check the FTP server.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Images cannot be transmitted via e-mail or FTP.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Camera Image Quality</strong></td>
<td></td>
</tr>
<tr>
<td>Camera has a problem focusing.</td>
<td>• The lens might be contaminated with dust, fingerprints, or other dirt. Use a special cleaning cloth to clean the lens or adjust the focus manually.</td>
</tr>
<tr>
<td></td>
<td>• Focusing might be impossible in some cases. If the object is too close to the lens, more it away from your camera.</td>
</tr>
<tr>
<td>Color of the video stream is too deep or light.</td>
<td>• Please confirm that the image you are watching has the best quality. Adjust the setting of your display card (color quality) to at least 16 bits (24 bits or more are recommended).</td>
</tr>
<tr>
<td></td>
<td>• Incorrect camera video setting. You may need to adjust some parameters, such as brightness, contrast, color, and saturation.</td>
</tr>
<tr>
<td>Video stream flashes.</td>
<td>• Incorrect power cord frequency may cause flashing of the image. Confirm that your camera uses NTSC or PAL system.</td>
</tr>
<tr>
<td></td>
<td>• The image flashes if the objects are black. In this case, adjust the illumination brighter around your camera.</td>
</tr>
<tr>
<td>This is noise problem</td>
<td>Noise may be produced if you install your camera at a very dark location.</td>
</tr>
<tr>
<td>Others</td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
</tr>
<tr>
<td>How to reboot my camera? If you only need to re-boot the system and don't want to change any setting, enter the Setting page and select the Reboot option at the bottom of the screen. The system will reboot automatically.</td>
<td></td>
</tr>
<tr>
<td>I can't replay recorded files. Confirm that you have installed Microsoft*’s DirectX 9.0 or above and use Windows Media Player 9 or above.</td>
<td></td>
</tr>
</tbody>
</table>
FCC Class B Announcement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
—Reorient or relocate the receiving antenna.
—Increase the separation between the equipment and receiver.
—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
—Consult the dealer or an experienced radio/TV technician for help.

You are cautioned that any change or modifications to the equipment not expressly approved by the party responsible for compliance could void your authority to operate such equipment.