

GV-Fisheye IP Camera H.264

GV-FE111/GV-FE421 User's Manual



Before attempting to connect or operate this product,
please read these instructions carefully and save this manual for future use.



© 2010 GeoVision, Inc. All rights reserved.

Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of GeoVision.

Every effort has been made to ensure that the information in this manual is accurate. GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
<http://www.geovision.com.tw>

Trademarks used in this manual: *GeoVision*, the *GeoVision* logo and GV series products are trademarks of GeoVision, Inc. *Windows* and *Windows XP* are registered trademarks of Microsoft Corporation.

December 2010

Preface

Welcome to the *GV-Fisheye IP Camera User's Manual*.

The GV-Fisheye IP Camera has two models with different resolutions. This Manual is designed for the following models and firmware versions:

Model	Model Number	Firmware Version
Fisheye Camera	GV-FE111	V1.06
	GV-FE421	V1.01

Contents

Naming and Definition	1
Note for Recording	2
Note for Firmware Upgrade	3
1.1 Key Features	4
1.2 Packing List	5
1.3 System Requirement	6
1.4 Options	6
1.5 Physical Description	7
1.6 Lens Adjustment	8
1.7 Installation	9
1.7.1 Hard Ceiling Mount	9
1.7.2 In-Ceiling Mount	10
1.7.3 Wall Mount and Ground Mount	12
1.8 Connecting the Data Cable	13
Chapter 2 Getting Started	15
2.1 Installing on a Network	15
2.2 Assigning an IP Address	15
2.3 Configuration Basics	17
Chapter 3 Accessing the Camera	18
3.1 Accessing Your Surveillance Images	18
3.2 Functions Featured on the Main Page	19
3.2.1 The Live View Window	20
3.2.2 Fisheye View	22
3.2.3 The Control Panel of the Live View Window	26
3.2.3 The Control Panel of the Live View Window	26
3.2.4 Snapshot of a Live Video	29
3.2.5 Video Recording	30
3.2.6 Picture-in-Picture and Picture-and-Picture View	30
3.2.7 Alarm Notification	33
3.2.8 Video and Audio Configuration	34

3.2.9	Remote Configuration	34
3.2.10	Camera Name Display	35
3.2.11	Image Enhancement	35
3.2.12	I/O Control	36
3.2.13	Visual Automation	37
3.2.14	Network Status	37

Chapter 4 Administrator Mode38

4.1	Video & Motion	40
4.1.1	Video Settings	40
4.1.2	Motion Detection	43
4.1.3	Privacy Mask	44
4.1.4	Tampering Alarm	45
4.1.5	Visual Automation	47
4.2	I/O Control	48
4.2.1	Input Settings	48
4.2.2	Output Settings	49
4.3	Events & Alerts	50
4.3.1	E-mail	50
4.3.2	FTP	52
4.3.3	Center V2	54
4.3.4	VSM	56
4.3.5	ViewLog Server	58
4.3.6	RTSP	59
4.4	Monitoring	60
4.5	Recording Schedule	61
4.5.1	Recording Schedule Settings	61
4.5.2	I/O Monitoring Settings	62
4.6	Remote ViewLog	63
4.7	Network	64
4.7.1	LAN	64
4.7.2	Advanced TCP/IP	66
4.7.3	IP Filtering	69
4.7.4	SNMP Setting	70
4.8	Management	71
4.8.1	Date and Time Settings	71
4.8.2	GPS Maps Settings	73
4.8.3	Storage Settings	75

4.8.4	User Account.....	77
4.8.5	Log Information	78
4.8.6	Tools	79

Chapter 5 Recording and Playback80

5.1	Recording	80
5.2	Playback.....	80
5.2.1	Playback Using the Memory Card.....	81
5.2.2	Playback over Network	82
5.2.3	Access to the Recorded Files through FTP Server	83
5.2.4	Playback of Daylight Saving Time Events.....	84

Chapter 6 Advanced Applications85

6.1	Upgrading System Firmware	85
6.1.1	Using the Web Interface.....	86
6.1.2	Using the IP Device Utility	87
6.2	Backing Up and Restoring Settings.....	89
6.2.1	Backing Up the Settings.....	89
6.2.2	Restoring the Settings.....	90
6.3	Restoring to Factory Default Settings.....	91
6.4	Verifying Watermark	92
6.4.1	Accessing AVI Files	92
6.4.2	Running Watermark Proof.....	92
6.4.3	The Watermark Proof Window	93

Chapter 7 DVR Configurations94

7.1	Setting Up IP Cameras.....	95
7.1.1	Previewing Video and Setting Audio	97
7.2	Remote Monitoring with Multi View	99
7.2.1	Connecting to the IP Camera	99
7.3	Remote Monitoring with E-Map	100
7.3.1	Creating an E-Map for the IP Camera.....	100
7.3.2	Connecting to the IP Camera	101

Chapter 8 CMS Configurations.....	102
8.1 Center V2	102
8.2 VSM.....	104
8.3 Dispatch Server	105
 Specifications	 106
Camera	106
Optics Lens	106
Operation	107
Network.....	107
Mechanical	108
General	108
Power over Ethernet	108
Web Interface.....	109
Application.....	109
 Appendix	 110
A. Settings for Internet Explore 8	110
B. RTSP Protocol Support	111

Naming and Definition

GV-System	GeoVision Analog and Digital Video Recording Software. The GV-System also refers to Multicam System , GV-NVR System , GV-Hybrid DVR System and GV-DVR System at the same time.
------------------	--

Note for Recording

The GV-Fisheye IP Camera is designed to work with GV-System, a hybrid or digital video management system. Normally, the images are recorded to the memory card inserted in the camera. Once the camera is connected to GV-System for video management or its Live View (Figure 3-3) is accessed through the Web browser, recording to the memory card will be stopped and GV-System will take over the recording. When the connection between the camera and GV-System is interrupted, the recording to the memory card will be resumed to back up the images on the camera.

When connecting from the GV-System, GV-FE421 is only supported on 64-bit operating systems.

Note for Firmware Upgrade

Before you upgrade the firmware, please follow these instructions:

1. The firmware upgrade must be performed on the LAN.
2. Stop monitoring of the camera.
3. Stop all the remote connections including Center V2, VSM and ViewLog Server.
4. Stop the connection to GV-System.

Failure to follow the above instructions may cause damages to the camera. For details on firmware upgrade, see *6.1 Upgrading System Firmware* in the User's Manual.

If firmware upgrade fails, you will need to restore the camera to the default settings. For details, see *6.3 Restoring to Factory Default Settings* in the User's Manual.

Chapter 1 Introduction

The GV-FE111/GV-FE421 is a fisheye camera that allows you to monitor all angles of a location using just one camera. The distorted hemispherical image of the fisheye camera will be converted into the conventional rectilinear projection.

Without installing any software, you can watch live view and utilize functions such as motion detection, privacy mask, and alert notification through the Web interface using an IE browser. In addition, the GV-Fisheye IP Camera seamlessly integrates with the GV-System, providing advanced monitoring and video management features.

1.1 Key Features

- 360 degree fisheye view
- 1/3" progressive scan CMOS for GV-FE111 and 1/2.5" progressive scan CMOS for GV-FE421
- Built-in Web server for monitoring through IE browser
- Different angle of view controllable by multiple users at the same time
- H.264, MPEG4 and MJPEG video compression for GV-FE111 and H.264 and MJPEG video compression for GV-FE421
- Up to 15 frames per second at 1280 x 1024 for GV-FE111 and 2048 x 1944 for GV-FE421
- Built-in microphone and speaker
- Motion detection triggering actions, e.g. image upload and output trigger
- Privacy mask to cover parts of the image that should not be viewable.
- IP address filtering
- PoE (Power over Ethernet)
- 16 languages on web interface

1.2 Packing List

- Camera Body



- Support Bracket x 3



- Camera Cover (Hard Ceiling Mount)



- Camera Cover (In-Ceiling Mount)



- Screw (Hard Ceiling Mount) x 3



- Screw (In-Ceiling Mount) x 3



- Security Torx



- Plastic Screw Anchor x 3



- 3-Pin Terminal Block
- GV-FE421 Software DVD
- GV-NVR Software DVD

- DC 12V Power Adapter
- Installation Sticker
- GV-NVR Quick Start Guide

1.3 System Requirement

To operate the camera through a web browser, make sure your PC has good network connection, and meet this system requirement:

- Microsoft Internet Explorer 7.x or later

Note: If you are using Microsoft Internet Explorer 8.0, additional settings are required. Please refer to *Settings for Internet Explorer 8* in Appendix A.

1.4 Options

Optional devices can expand your camera's capabilities and versatility. Contact your dealer for more information.

GV-PA191	The GV-PA191 is a Power over Ethernet (PoE) adapter designed to provide power to the IP device through a single Ethernet cable.
-----------------	---

1.5 Physical Description

To access the Default button, LED indicators and micro SD card slot, unscrew the three screws indicated below and then remove the outer shell of the camera.



Figure 1-1

You can now access the Default button, LED indicators, and the micro SD card slot.

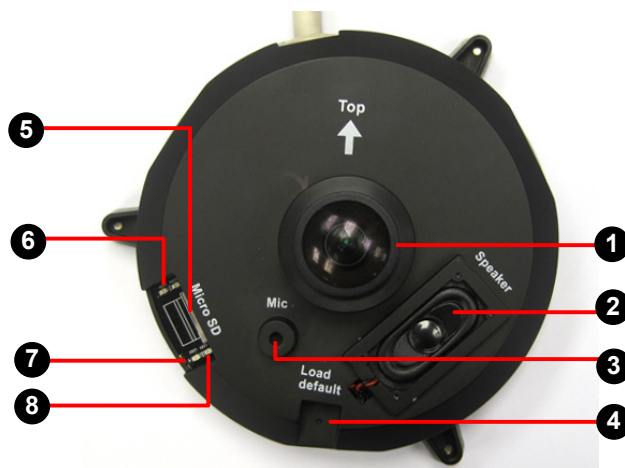


Figure 1-2

No.	Name	Function
1	Lens	Rotates the lens to adjust focus.
2	Speaker	Talks to the surveillance area from the local computer.
3	Microphone	Receives the sound from the camera.
4	Default Button	Resets all configurations to default factory settings. See 6.3 <i>Restoring to Factory Default Settings</i> .
5	Micro SD Card Slot	Inserts a micro SD/SDHC memory card to store recorded data.
6	Network status LED	Indicates the network status.
7	Power status LED	Indicates whether the camera is powered on or off.
8	System status LED	Indicates whether the system is booted successfully or not.

1.6 Lens Adjustment

By default, the lens should already be adjusted to produce clear image. If not, you can adjust the focus by removing the outer shell of the camera and then rotating the lens (No.1, Figure 1-2). To see how to remove the outer shell of the camera, refer to *1.5 Physical Description*.

Set an object about 50 cm (19.7 in) in front of the camera and rotate the lens until the image becomes clear. You can access the live images of the camera by connecting to its Web interface. Refer to Chapter 2 to see how to install the camera on the network and refer to Chapter 3 to see how to access the Web interface.

1.7 Installation

The GV-FE1111/GV-FE421 is designed to be mounted on the ceiling, wall or ground. There are two ways to mount the camera on the ceiling, **Hard Ceiling Mount** and **In-Ceiling Mount**. Make sure the ceiling has enough strength to support the fisheye camera.



Hard Ceiling Mount



In-Ceiling Mount



Wall Mount



Ground Mount

Note: The fisheye camera is designed for indoor use only.

1.7.1 Hard Ceiling Mount

1. Place the installation sticker on the ceiling board. The 3 red dots indicate the location of the screws.

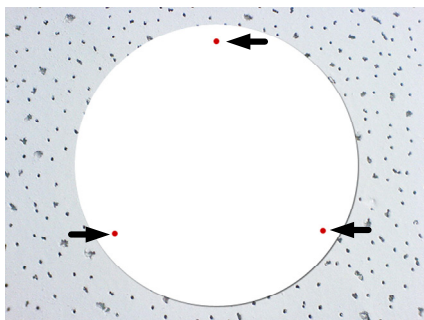


Figure 1-5

2. At the 3 red dots, drill a hole slightly smaller than the plastic screw anchors provided.
3. Insert the 3 plastic screw anchors in the drilled holes.
4. Secure the fisheye camera with the 3 hard ceiling mount screws provided.



Figure 1-6

5. Place the camera cover for hard ceiling mount on top of the camera and tighten the screws with the security torx provided.



Figure 1-7

1.7.2 In-Ceiling Mount

In-Ceiling Mount allows the camera to be mounted into the ceiling, revealing a small portion of the camera. In-Ceiling Mount requires the ceiling board to be between 0.5 – 3.0 cm (0.2 – 1.18 in) thick.

1. Place the installation sticker on the ceiling board, and cut the circle part out of the ceiling.

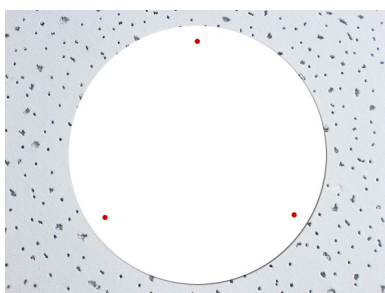


Figure 1-8

2. Align the 3 support brackets with the holes on the back of the camera as shown below and secure using the in-ceiling mount screws provided.

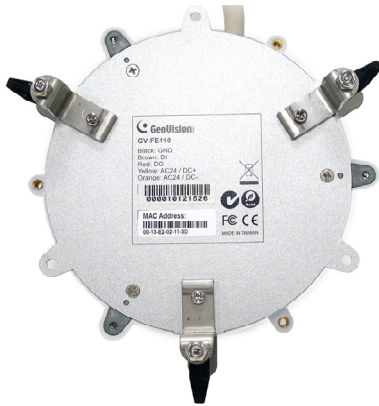


Figure 1-9

3. Place the fisheye camera into the ceiling opening as shown below.



Figure 1-10

4. On the back side, make sure the black plastic clips are slightly above the ceiling board and pointing outward.



Figure 1-11

5. From the front side of the camera, tighten the screws.



Figure 1-12

6. Place the camera cover for in-ceiling mount on top of the camera and tighten the 3 screws.



Figure 1-13

1.7.3 Wall Mount and Ground Mount

To mount the camera on a wall, follow the instructions in *Hard Ceiling Mount*. For ground mount, simply place the camera on a flat surface such as a conference table.

Hint: Mount the fisheye camera in the middle of the wall to have an excellent overview. Or ensure the camera is focused on the most important areas of the room as directly as possible to have the desired detailed recognition.

1.8 Connecting the Data Cable

The fisheye camera comes with a 5-pin data cable that allows you to connect to the power and any I/O devices.

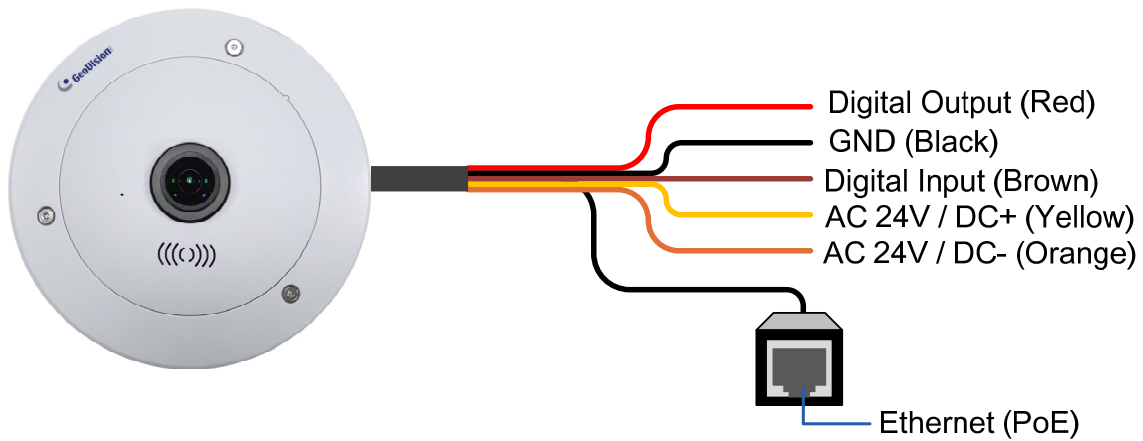


Figure 1-14

Wire Definition

No.	Wire Color	Definition
1	Yellow	AC 24V+ / DC 12V+
2	Orange	AC 24V- / DC 12V-
3	Brown	Digital Input
4	Red	Digital Output
5	Black	GND

Connecting to Power

You can connect to power using either the power adapter provided or a Power over Ethernet (PoE) adapter. See “Power over Ethernet” in Specifications later in this manual before purchasing a PoE adapter. To connect to power using the power adapter, follow the steps below to connect the orange and yellow wires of the camera to the 3-pin terminal block provided.

1. Insert the yellow wire to the pin on the right-side of the terminal block and the orange wire to the pin on the left-side of the terminal block.
2. Use a small flat-tip screwdriver to secure the screws above the pins.

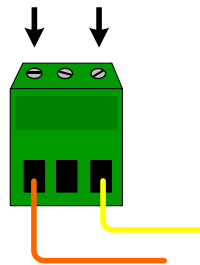


Figure 1-15

3. Connect the DC 12V Power Adapter to the 3-Pin Terminal Block.



Figure 1-16

Note:

1. A DC 12V power adapter has been provided, but both AC 24V power adapter and DC 12V power adapter are compatible.
 2. The power status LED will not be visible unless the outer shell of the camera body is removed.
-

Chapter 2 Getting Started

This section provides basic information to get the camera working on the network.

2.1 Installing on a Network

These instructions describe the basic connections to install the camera on the network.

1. Using a standard network cable, connect the camera to your network.
2. Connect power using one of the methods:
 - Using the supplied power adapter, connect to power. For details, see *1.7 Connecting the Data Cable*.
 - Use the Power over Ethernet (PoE) function. The power will be provided over the network cable.
3. Set the IP address for the unit.

Note: See “Power over Ethernet” in Specifications later in this manual before purchasing a PoE adapter.

2.2 Assigning an IP Address

Designed for use on the network, the camera must be assigned an IP address to make it accessible.

Note: The camera has a default IP address of **192.168.0.10**. The computer used to set the IP address must be under the same network assigned to the unit.

1. Open your web browser, and type the default IP address <http://192.168.0.10>
2. In both Login and Password fields, type the default value **admin**. Click **Apply**.
3. In the left menu, select **Network** and then **LAN** to begin the network settings.

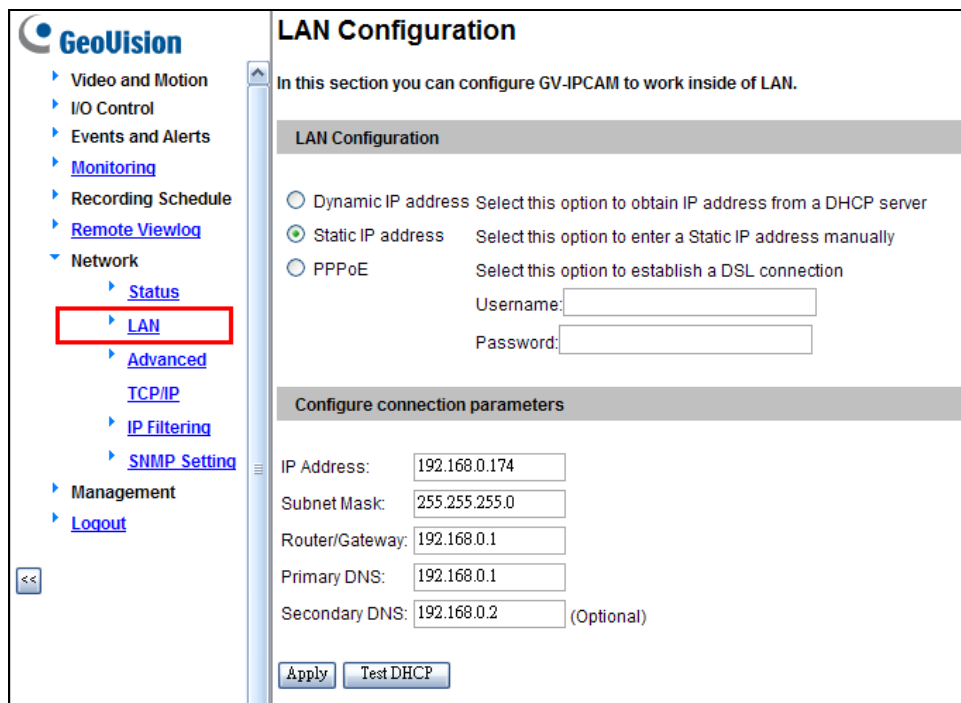


Figure 2-2

4. Select **Static IP address**. Type IP Address, Subnet Mask, Router/Gateway, Primary DNS and Secondary DNS in the **Configure connection parameters** section.
5. Click **Apply**. The camera is now accessible by entering the assigned IP address on the web browser.

IMPORTANT:

- **Dynamic IP Address** and **PPPoE** should only be enabled if you know which IP address the camera will get from the DHCP server or ISP. Otherwise, you must use the Dynamic DNS service to obtain a domain name linked to the camera's changing IP address first.

For details on Dynamic DNS Server settings, see *4.7.2 Advanced TCP/IP*.

- If **Dynamic IP Address** and **PPPoE** is enabled and you cannot access the unit, you may have to reset it to the factory default settings and then perform the network settings again.

To restore the factory settings, see *6.3 Restoring to Factory Default Settings*.

2.3 Configuration Basics

Once the camera is properly installed, the following important features can be configured using the browser-based configuration page and are discussed in the following sections in this manual:

- **Date and time adjustment:** see *4.8.1 Date and Time Settings*.
- **Login and privileged passwords:** see *4.8.4 User Account*.
- **Network gateway:** see *4.7 Network*.
- **Camera image adjustment:** see *3.2.3 The Control Panel of the Live View Window*.
- **Video format, resolution and frame rate:** see *4.1.1 Video Settings*.

Chapter 3 Accessing the Camera

Two types of users are allowed to log in to the camera: **Administrator** and **Guest**. The Administrator has unrestricted access to all system configurations, while the Guest has the access to live view and network status only.

3.1 Accessing Your Surveillance Images

Once installed, your camera is accessible on a network. Follow these steps to access your surveillance images:

1. Start the Internet Explorer browser.
2. Type the IP address or domain name of the camera in the **Location/Address** field of your browser.

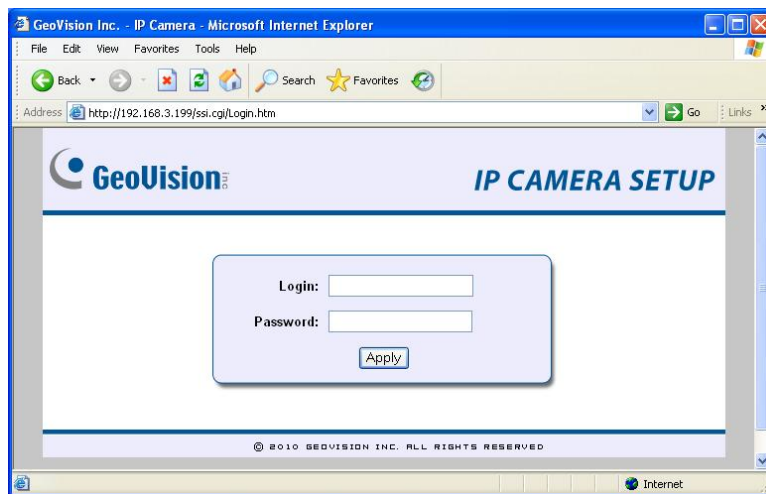


Figure 3-1

3. Enter the login name and password.
 - The default login name and password for Administrator are **admin**.
 - The default login name and password for Guest are **guest**.
4. A video image, similar to the example in Figure 3-2, is now displayed in your browser.

Note: To enable the updating of images in Microsoft Internet Explorer, you must set your browser to allow ActiveX Controls and perform a one-time installation of GeoVision's ActiveX component onto your computer.

3.2 Functions Featured on the Main Page

This section introduces the features of the **Live View** window and **Network Status** on the main page. The two features are accessible by both Administrator and Guest.

Main Page of Guest Mode

- ▼ Video and Motion
 - ▼ Live View
 - ▶ Camera
 - ▼ Network
 - ▶ Status

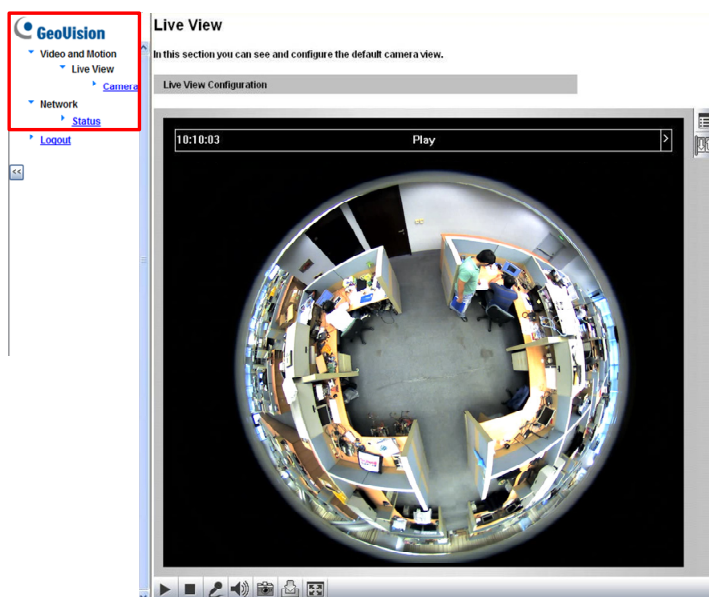


Figure 3-2

3.2.1 The Live View Window

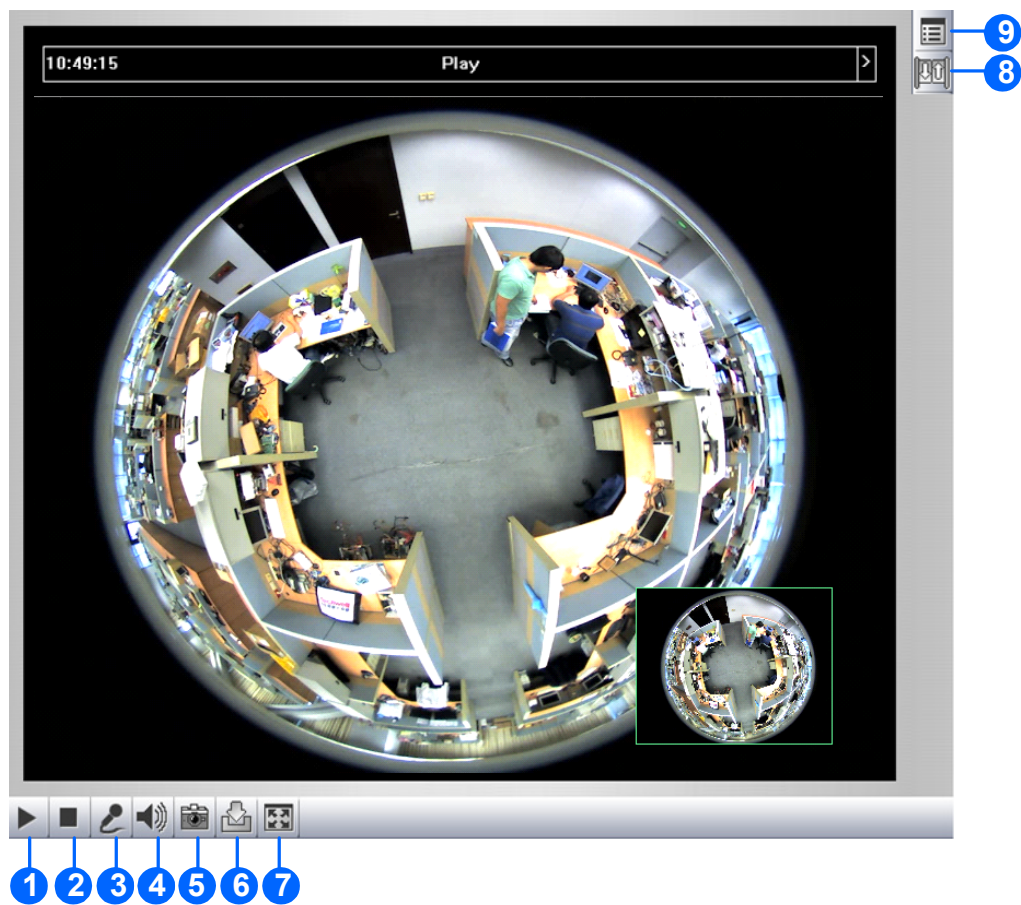


Figure 3-3

No.	Name	Function
1	Play	Plays live video.
2	Stop	Stops playing video.
3	Microphone	Talks to the surveillance area from the local computer.
4	Speaker	Listens to the audio around the camera.
5	Snapshot	Takes a snapshot of live video. --- See 3.2.4 <i>Snapshot of a Live Video</i> .
6	File Save	Records live video to the local computer. --- See 3.2.5 <i>Video Recording</i> .
7	Full Screen	Switches to full screen view. Right-click the image to have these options: Snapshot , Resolution , PIP , PAP , Geo Fisheye , Google Maps , Zoom In and Zoom Out . --- See 3.2.6 <i>Picture-in-Picture and Picture-and-Picture View</i> --- See 3.2.2 <i>Fisheye View</i> --- See 4.8.2 <i>GPS Maps Settings</i>

8	I/O Control	Enables the I/O Control Panel or the Visual Automation. --- See 3.2.12 <i>I/O Control</i> .
9	Show System Menu	Brings up these functions: Alarm Notify, Video and Audio Configuration, Remote Config, Show Camera Name and Image Enhance . --- See 3.2.7 <i>Alarm Notification</i> , 3.2.8 <i>Video and Audio Configuration</i> , 3.2.9 <i>Remote Configuration</i> , 3.2.10 <i>Camera Name Display</i> and 3.2.11 <i>Image Enhancement</i> respectively.

3.2.2 Fisheye View

To enable the fisheye options, right-click the live view and select **Geo Fisheye**. Right-click the image again and select **Fisheye Option** to see the following options.

- **Image Alignment:** By default, the image should be properly aligned already. If not, follow the steps below to align the image for each model:
 - **GV-FE111 (Firmware V1.06):** Align the dotted circle with the outer edge of the camera image, and then align it with the inner edge of the image frame to achieve optimal results.



Figure 3-4

- **GV-FE421:** Align the white circle with the edge of the camera image. You can eliminate the darker areas toward the edge of the image by making the white circle smaller, but the field of view will be slightly reduced.

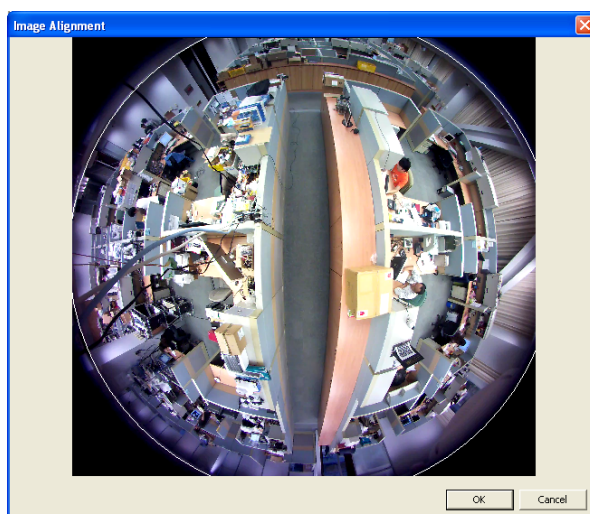
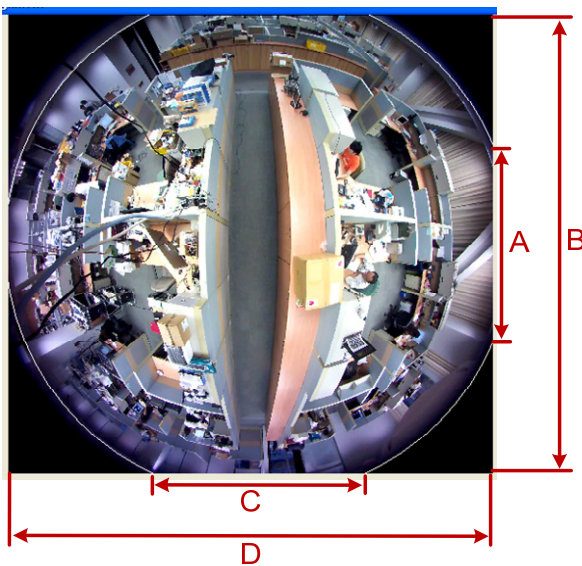


Figure 3-5

Note:

The circular source image of GV-FE421 should be centered and slightly cropped on all four edges. If the image is not centered, please contact your sales representative and send your device back to GeoVision for adjustment.

To determine whether your device needs adjustment, measure the length of a longer cropped edge and the length of that entire edge. Divide the length of the cropped edge by the length of the entire edge. The ratio for left and right edges should be less than or equal to 5/9 and the ratio for the top and bottom edges should be less than or equal to 5/8.



Left and right:

$$\frac{A}{B} \leq \frac{5}{9}$$

Top and bottom:

$$\frac{C}{D} \leq \frac{5}{8}$$

■ **Camera Modes:** You can choose among four view modes.

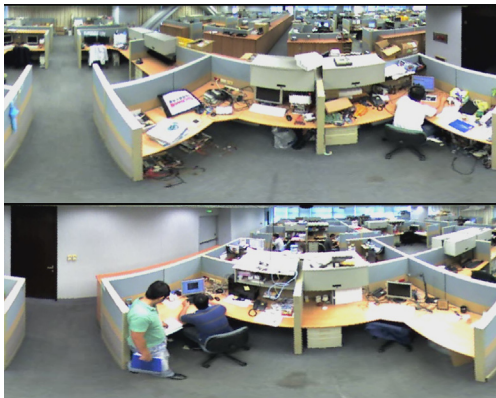
- **Quad view:** Composed of four PTZ views.
- **360 degree:** Composed of two PTZ view and one 360° panoramic view.
- **Dual 180 degree:** Composed of two 180° views.
- **Single view:** Composed of one PTZ view.



Quad view: 4 PTZ views



360 degree: 2 PTZ views & 1 360° view



Dual 180 degree: 2 180° views



Single view: 1 PTZ view

Figure 3-5

Note: When wall mount is selected for **Camera Position**, only one 180° view will be displayed.

- **Camera Position:** Select **Ceiling**, **Wall** or **Ground** according to where the camera is mounted.
- **Adjust AutoPan Speed At Top-Left Channel:** Select low, medium, or high speed to enable Auto Pan for one PTZ view at the rotation speed of your choice. This option applies to **Quad view**, **360° degree** and **Single view**.

- **Zoom:** Select **Zoom In** or **Zoom Out** and then click on the image.
- **Show Source Video at Top-Right Channel:** Shows the circular source image in the top-right quadrant when **Quad view** is selected.
- **Fisheye Settings:** The following settings are available.
 - **Frame Rate Control:** You can set the frame rate of the live view image.
 - **Show Original Video in Low Resolution:** Shows circular source image when the resolution is low. This option only works on the GV-System when the fisheye camera is connected to a GV-System.
 - **Screen Ratio Setting:** Select a ratio that best fits the display ratio of your computer.

You can drag and drop PTZ view or 180° view to adjust the viewing angle.

3.2.3 The Control Panel of the Live View Window

To open the control panel of the Live View window, click the arrow button on top of the viewer. You can access the following functions by using the left and right arrow buttons on the control panel.

Click the arrow button to display the control panel.

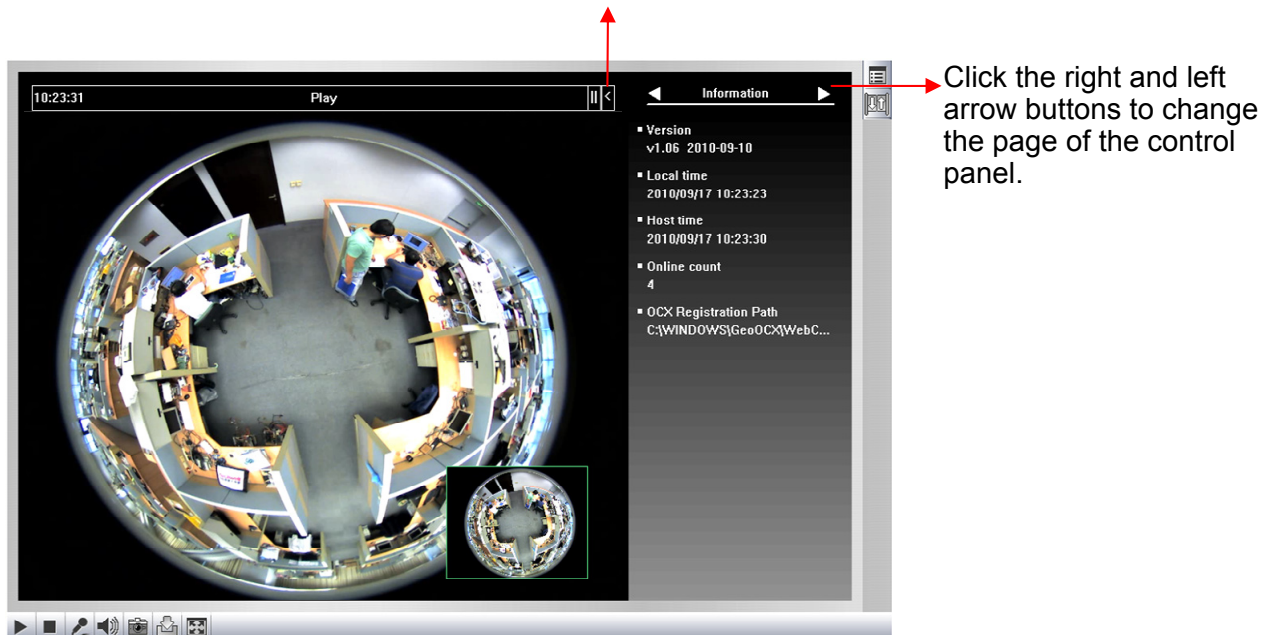


Figure 3-6

[Information] Displays the version of the camera, local time of the local computer, host time of the camera, and the number of users logging in to the camera.

[Video] Displays the current video codec, resolution and data.

[Audio] Displays the audio data rates when the microphone and speaker devices are enabled.

[I/O Control] Provides a real-time graphic display of the input and output status. You can force the output to be triggered by double-clicking its icon.

[Alarm Notify] Displays the captured images by sensor triggers and/or motion detection. For this function to work, you must configure the Alarm Notify settings first. See 3.2.7 *Alarm Notification*.

[Camera Adjustment] Allows you to adjust the image quality.

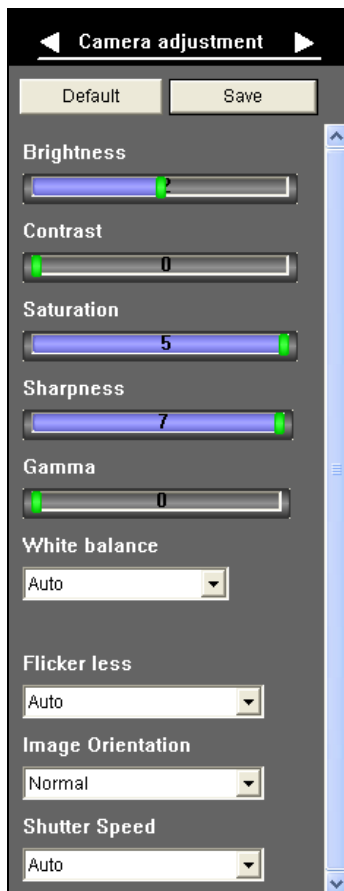


Figure 3-7

- **Brightness:** Adjusts the brightness of the image.
- **Contrast:** Adjusts the relative differences between one pixel and the next.
- **Saturation:** Adjusts the saturation of the image.
- **Sharpness:** Adjusts the sharpness of the image.
- **Gamma:** Adjusts the relative proportions of bright and dark areas.
- **White balance:** The camera automatically adjusts the color to be closest to the image you are viewing. You can choose one of the three presets: **Indoor**, **Fluorescent**, and **Outdoor**. You can also choose **Manual** to adjust the white balance manually.
- **Flicker less:** The camera automatically matches the frequency of your camera's imager to the frequency of indoor light sources, e.g. fluorescent lighting. You can also select 50 Hz or 60 Hz manually. If these don't match, faint light and dark bars may appear in your images. Check the power utility to determine which frequency is used.
- **Image Orientation:** Changes the image orientation on the Live View window.

- **Shutter Speed:** Determines how long the image sensor is exposed to light. The range of shutter speed is from 1/5 to 1/8000 sec.

Shutter	Speed	Balanced	Quality
Image Brightness	Poor	Good	Excellent
Image Clarity	Poor	Good	Excellent
Image Smoothness	Excellent	Good	Poor

[GPS] For details see 4.8.2. *GPS Maps Setting*.

[Temperature] Click the **Monitor** button to see the current temperature of the chipset in Celsius and Fahrenheit.

[Download] Allows you to install the programs from the hard drive.

3.2.4 Snapshot of a Live Video

To take a snapshot of live video, follow these steps:

1. Click the **Snapshot** button (No. 5, Figure 3-3). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and select **JPEG** or **BMP** as **Save as Type**. You may also choose whether to display the name and date stamps on the image.
3. Click the **Save** button to save the image in the local computer.

3.2.5 Video Recording

You can record live video for a certain period of time to your local computer.

1. Click the **File Save** button (No. 6, Figure 3-3). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and move the **Time period** scroll bar to specify the time length of the video clip from 1 to 5 minutes.
3. Click the **Save** button to start recording.
4. To stop recording, click the **Stop** button (No. 2, Figure 3-3).

3.2.6 Picture-in-Picture and Picture-and-Picture View

Two types of close-up views are available to provide clear and detailed images of the surveillance area: **Picture-in-Picture (PIP)** and **Picture-and Picture (PAP)**. After entering the live view window, the image is displayed in PIP mode by default. The PIP and PAP views can only be displayed on the hemispherical source image.

To enable this feature:

- Click the **Full Screen** button (No. 7, Figure 3-3). Right-click the full screen to have the options of **PIP** and **PAP**.
- Right-click the live view to have the options of **PIP** and **PAP**.

Picture-in-Picture View

With the Picture in Picture (PIP) view, you can crop the video to get a close-up view or zoom in on the video.

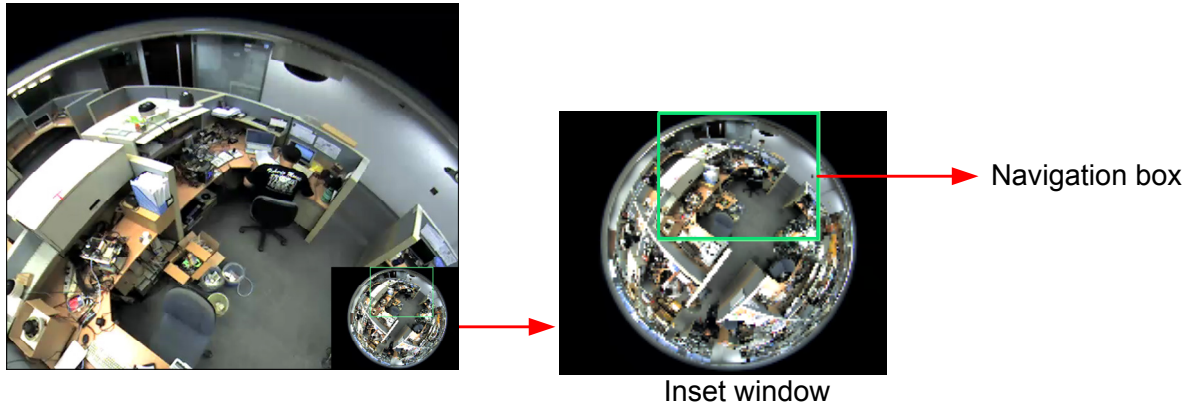


Figure 3-8

1. Select **PIP**. An inset window appears.
2. Click the inset window. A navigation box appears.
3. Move the navigation box around in the inset window to have a close-up view of the selected area.
4. To adjust the navigation box size, move the cursor to any of the box corners, and enlarge or diminish the box.
5. To exit the PIP view, right-click the image and click **PIP** again.

Picture-and-Picture View

With the Picture and Picture (PAP) view, you can create a split video effect with multiple close-up views on the image. A total of 7 close-up views can be defined.

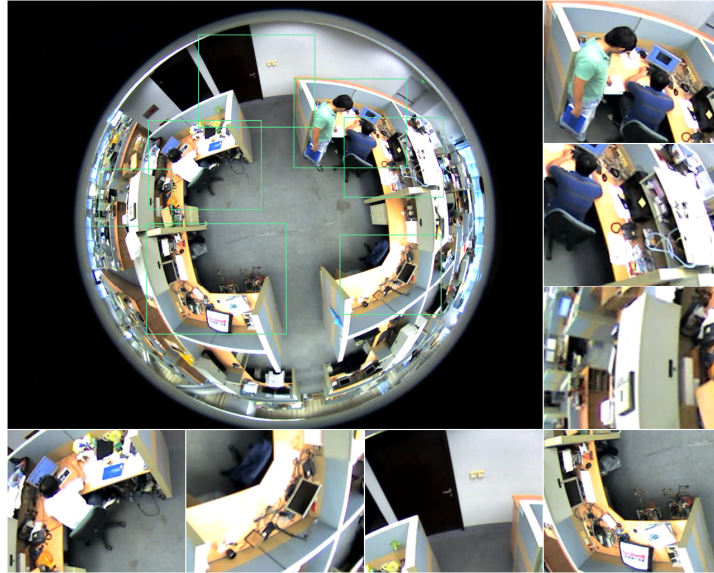


Figure 3-9

1. Select **PAP**. A row of three inset windows appears at the bottom.
2. Draw a navigation box on the image, and this selected area is immediately reflected in one inset window. Up to seven navigation boxes can be drawn on the image.
3. To adjust a navigation box size, move the cursor to any of the box corners, and enlarge or diminish the box.
4. To move a navigation box to another area on the image, drag it to that area.
5. To change the frame color of the navigation box or hide the box, right-click the image, select **Mega Pixel Setting** and click one of these options:
 - **Display Focus Area of PAP Mode:** Displays or hides the navigation boxes on the image.
 - **Set Color of Focus Area:** Changes the color of the box frames.
6. To delete a navigation box, right-click the desired box, select **Focus Area of PAP Mode** and click **Delete**.
7. To exit the PAP view, right-click the image and click **PAP** again.

3.2.7 Alarm Notification

After input triggers and motion detection, you can be alerted by a pop-up live video and view up to four captured images.

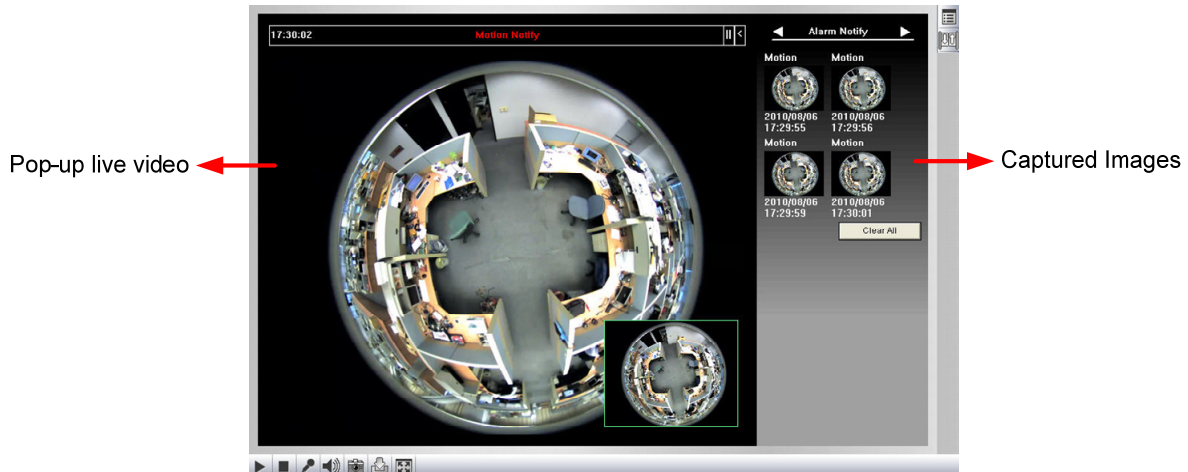


Figure 3-10

To configure this function, click the **Show System Menu** button (No. 11, Figure 3-3), and select **Alarm Notify**. This dialog box appears.

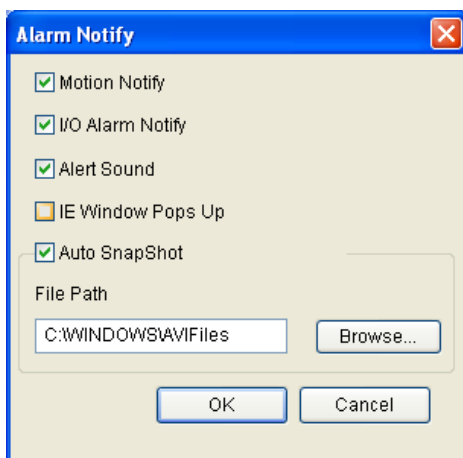


Figure 3-11

- **Motion Notify:** Once motion is detected, the captured images are displayed on the control panel of the Live View window.
- **I/O Alarm Notify:** Once the input device is triggered, the captured images are displayed on the control panel of the Live View window. For this function to work, the Administrator needs to install the input device properly. See 4.2.1 *Input Settings*.
- **Alert Sound:** Activates the computer alarm on motion and input-triggered detection.
- **IE Window Pops up:** The minimized Live View window pops up on motion and input-triggered detection.

- **Auto Snapshot:** The snapshot of live video is taken every 5 seconds on motion and input-triggered detection.
- **File Path:** Assigns a file path to save the snapshots.

Note: The Administrator can adjust the motion detection area by using the Motion Detection function. See *4.1.3 Motion Detection* for more details.

3.2.8 Video and Audio Configuration

You can enable the microphone and speaker for two-way audio communication and adjust the audio volume. To change audio configuration, click the **Show System Menu** button (No. 9, Figure 3-3), and select **Video and Audio Configuration**.

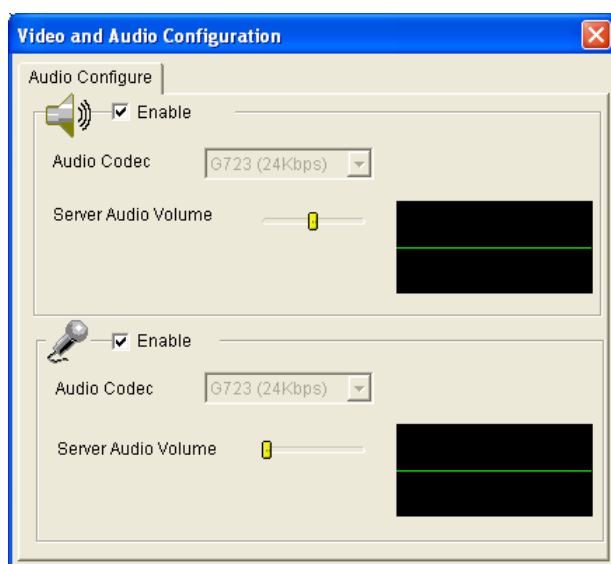


Figure 3-12

3.2.9 Remote Configuration

You can view the connection status of the central monitoring stations and upgrade firmware over the Internet. Click the **Show System Menu** button (No. 9, Figure 3-3), and select **Remote Config**. The Remote Config dialog box will appear.

[Firmware Upgrade] In this tab, you can upgrade the firmware over the network. For details, see *Chapter 6 Advanced Applications*.

3.2.10 Camera Name Display

To display the camera name on the image, click the **Show System Menu** button (No. 9, Figure 3-3), and select **Show Camera Name**.

3.2.11 Image Enhancement

To enhance the image quality of live video, click the **Show System Menu** button (No. 9, Figure 3-3), and select **Image Enhance**. This dialog box appears.

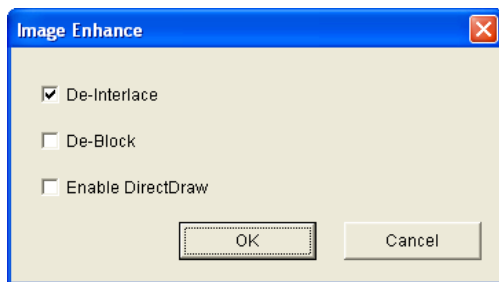


Figure 3-13

- **De-Interlace:** Coverts the interlaced video into non-interlaced video.
- **De-Block:** Removes the block-like artifacts from low-quality and highly compressed video.
- **Enable DirectDraw:** Activates the DirectDraw function.

3.2.12 I/O Control

The I/O Control window provides real-time graphic displays of camera status, I/O status, and alarm events. Additionally, you can remotely force output to be triggered.

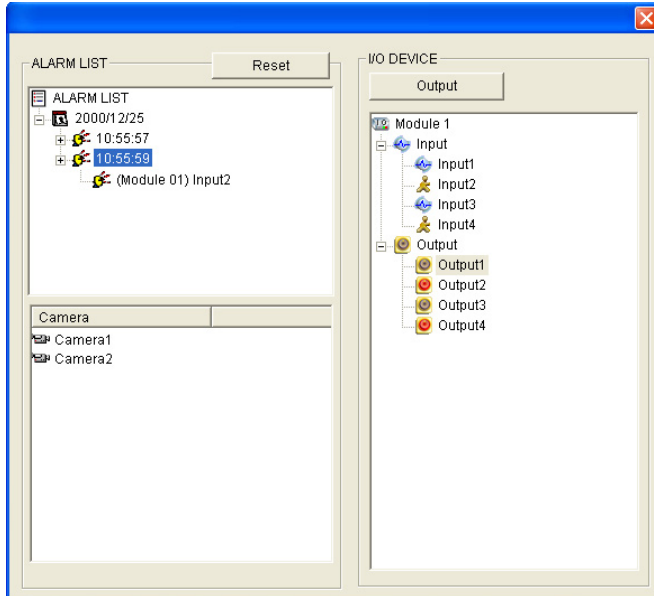


Figure 3-14

- To display the I/O control window, click the **I/O Control** button (No. 8, Figure 3-3).
- The Alarm List is displayed in three levels. The first level indicates date, the second indicates time, and the third indicates alarm ID. Clicking the **Reset** button will clear the list.
- To trigger an output device, highlight an output and then click the **Output** button.

3.2.13 Visual Automation

The Visual Automation allows you to change the current state of the electronic device by simply clicking on its image, e.g. turning the light ON. This feature is only available when the Visual Automation is set ahead by the Administrator. For details, see 4.1.5 *Visual Automation*.



Figure 3-15

- To access this feature, click the **I/O Control** button (No. 8, Figure 3-3) and select **Visual Automation**.
- To change the style of the set areas, right-click the image and select **Visual Automation**. Right-click the image again to see these options:
 - **Show All:** Displays all set areas.
 - **Rect Float:** Embosses all set areas.
 - **Set Color:** Changes the frame color of all set areas.

3.2.14 Network Status

To view the network status, in the left menu, click **Network** and select **Status**.

Network Status Information	
In this section you can see an overview of GV-IPCAM status.	
Current Status Information	
Interface:	Wired
IP Acquisition:	Fixed
MAC Address:	0013E201E1A1
IP Address:	192.168.2.115
Subnet Mask:	255.255.252.0
Gateway:	192.168.0.1
Domain Name Server 1:	192.168.0.1
Domain Name Server 2:	192.168.0.2

Figure 3-16

Chapter 4 Administrator Mode

The Administrator can access the system configuration through the network. Eight categories of configurations are involved in the system configuration: **Video and Motion**, **I/O Control**, **Events and Alerts**, **Monitoring**, **Recording Schedule**, **Remote ViewLog**, **Network** and **Management**.



Figure 4-1

List of Menu Options

Find the topic of interest by referring to the section number prefixed to each option.

4.1 Video and Motion	4.1.1 Video Settings 4.1.2 Motion Detection 4.1.3 Privacy Mask 4.1.4 Tampering Alarm 4.1.5 Visual Automation
4.2 I/O Control	4.2.1 Input Setting 4.2.2 Output Setting
4.3 Events and Alerts	4.3.1 Email 4.3.2 FTP 4.3.3 Center V2 4.3.4 VSM 4.3.5 ViewLog 4.3.6 RTSP
4.4 Monitoring	
4.5 Recording Schedule	4.5.1 Recording Schedule Settings 4.5.2 I/O Monitor Settings
4.6 Remote Viewlog	
4.7 Network	4.7.1 LAN 4.7.2 Advanced TCP/IP 4.7.3 IP Filtering 4.7.4 SNMP Setting
4.8 Management	4.8.1 Date and Time Settings 4.8.2 GPS Maps Settings 4.8.3 Storage Settings 4.8.4 User Account 4.8.5 Log Information 4.8.6 Tools

4.1 Video & Motion

This section includes the video image settings and how the images can be managed by using Motion Detection, Privacy Mask, Tampering Alarm and Visual Automation.

4.1.1 Video Settings

Video Settings

In this section you can define compression art, broadcasting method and privacy mask.

Name
Name

Connection template

Video Signal Type

In this section you can configure camera's video signal, also the resolution and frame per second to be transmitted through the network

Video Format

Resolution

Frame per second

Bandwidth Management

In this section you can configure the bit rate used by MPEG-4 video stream. Using VBR (Variable Bit Rate) is an intelligent method to compensate between image quality and bandwidth control. But if you want to provide consistently the same image quality at bandwidth cost, please set to CBR (Constant Bit Rate).

☒ VBR

Quality
Maximal Bit Rate Mbit

☐ CBR

Maximal Bit Rate

GOP Structure and Length

In this section you can configure the composition of the MPEG-4 video stream (GOP structure). By using I-Frame only will increase video quality dramatically but also the bandwidth.

Group of Picture(GOP) Size (1 indicates to generate I-VOP only and disable motion detection)

Alarm Settings

In this section you can configure pre-alarm and post-alarm settings.

Pre-alarm recording time seconds

Post-alarm recording time seconds with hard disk installed (1~30)

Split interval minutes

☐ Record audio

☐ Overlayd with camera name

☐ Overlayd with date stamps

☐ Overlayd with time stamps

☐ Overlay with digital input description name

Watermark Setting

In this section you can set Watermark function.

☐ Enable

LED Control

Ready LED ☒ Enable ☐ Disable

BLC ☒ Off ☐ On

Figure 4-2

[Name]

Rename the video stream. The camera name will appear on the Live View. To display the name of the video stream on the Live View window, see *3.2.10 Camera Name Display*.

[Connection Template]

Select the type of your network connection. Unless you select **Customized**, this option will automatically bring up the recommended video resolution, frame rate, bandwidth and GOP size.

[Video Signal Type]

The codec options, resolution and maximum frame rate available for GV-FE111 and GV-FE421 are listed as below:

	GV-FE111	GV-FE421
Codec Options	H.264, MPEG4, MJPEG	H. 264, MJPEG
Image Resolution	1280 x 1024	2048 x 1944
Maximum Frame Rate	15 fps	15 fps

[Bandwidth Management]

When using MPEG-4 or H.264, it is possible to control the bitrate, which in turn allows the amount of bandwidth usage to be controlled.

- **VBR (Variable Bitrate):** The quality of the video stream is kept as constant as possible at the cost of a varying bitrate. The bandwidth is used much more efficiently than a comparable CBR. You can set a limit to the bit rate by specifying a **Maximal Bit Rate**.

Set the image quality to one of the 5 standards: **Poor**, **Fair**, **Good**, **Great**, and **Excellent**.

- **CBR (Constant Bitrate):** CBR is used to achieve a specific bitrate by varying the quality of the stream. Use the **Maximal Bit Rate** drop-down list to select a bitrate.

[GOP Structure and Length]

Use the **Group of Picture(GOP) Size** drop-down list to set the number of frames between every key frame. This option is only available when H.264 or MPEG-4 is selected for codec. The limit is 1 key frame for every 30 frames.

[Alarm Settings]

The alarm settings allow you to capture images before and/or after the motion or I/O event happens.

- **Pre-alarm recording time:** Activates video recording before an event occurs. Set the recording time to 1 or 2 seconds. The recording is saved in the buffer of the camera.
- **Post-alarm recording time:** Activates video recording onto the inserted memory card after an event occurs. Set the recording time from 1 to 30 seconds.
- **Split Interval:** Sets the time length of each event file from 1 to 5 minutes.
- **Record Audio:** Activates audio recording when an event occurs.
- **Overlaid with camera name:** Includes camera names on live and recorded videos.
- **Overlaid with date stamps:** Includes date stamps on live and recorded videos.
- **Overlaid with time stamps:** Includes time stamps on live and recorded videos.
- **Overlaid with digital input description name:** Includes the names of selected inputs on live and recorded videos.

[Watermark] Enable this option to watermark all recordings. The watermark allows you to verify whether the recorded video has been tampered with. See *6.4 Verifying Watermark*.

[Ready LED] You can select to enable or disable the Ready LED.

[BLC] Enable backlight compensation to adjust the exposure when the subject is positioned in front of a bright light source.

4.1.2 Motion Detection

Motion detection is used to generate an alarm whenever movement occurs in the video image. You can configure up to 8 areas with different sensitivity values for motion detection.

Motion Detection

In this section you can define different region(s) for motion detection.

Camera: Streaming1

Sensitivity: 2

Reset

Save

Please advise which action(s) should be taken when motion detection is activated.

Trigger digital output relay ☐ Output 1

Apply

Figure 4-3

1. The default detection area is set to the entire camera view with a sensitivity level of 2. To define a different detection area, click **Reset**.
2. Select the desired sensitivity level by moving the slider. The higher the value, the more sensitive the camera is to motion.
3. Drag an area on the image. Click **Add** when you are prompted to confirm the setting.
4. To create several areas with different sensitivity values, repeat Steps 2 and 3.
5. Click **Save** to save the above settings.
6. To trigger the alarm output when motion is detected, select **Output1** and click the **Apply** button. To activate the output settings, you must also start **Input** monitoring manually or by schedule. For related settings, see *4.4 Monitoring*.

Note: Since the area of the moving subject needs to exceed a certain percentage of the selected detection area to be counted as motion detection, it is recommended to set one or multiple small motion detection areas instead of selecting the entire camera view as one detection area for better detection results.

4.1.3 Privacy Mask

The Privacy Mask can block out sensitive areas from view, covering the areas with dark boxes in both live view and recorded clips. This feature is ideal for locations where displays, keyboard sequences (e.g. passwords), and confidential information might be visible.



Figure 4-4

1. Select the **Enable** option.
2. Drag the area(s) where you want to block out on the image. Click **Add** when you are prompted to confirm the setting.
3. Click the **Save** button to save the settings.

4.1.4 Tampering Alarm

The Tampering Alarm is used to detect when the camera is being physically tampered with. An alarm can be generated when the camera is moved, covered up, or out of focus. The alarm methods include triggering the output device and e-mail alert. To enable the tampering alarm, first set up these alarm methods properly:

- To trigger the output device when a tampering event occurs, enable the output setting and select **Tampering Alarm**. See *Output Setting* in 4.2.2 *Output Settings*.
- To trigger the e-mail alert when a tampering event occurs, enable the e-mail setting and select **Tampering Alarm**. See 4.3.1 *E-Mail*.

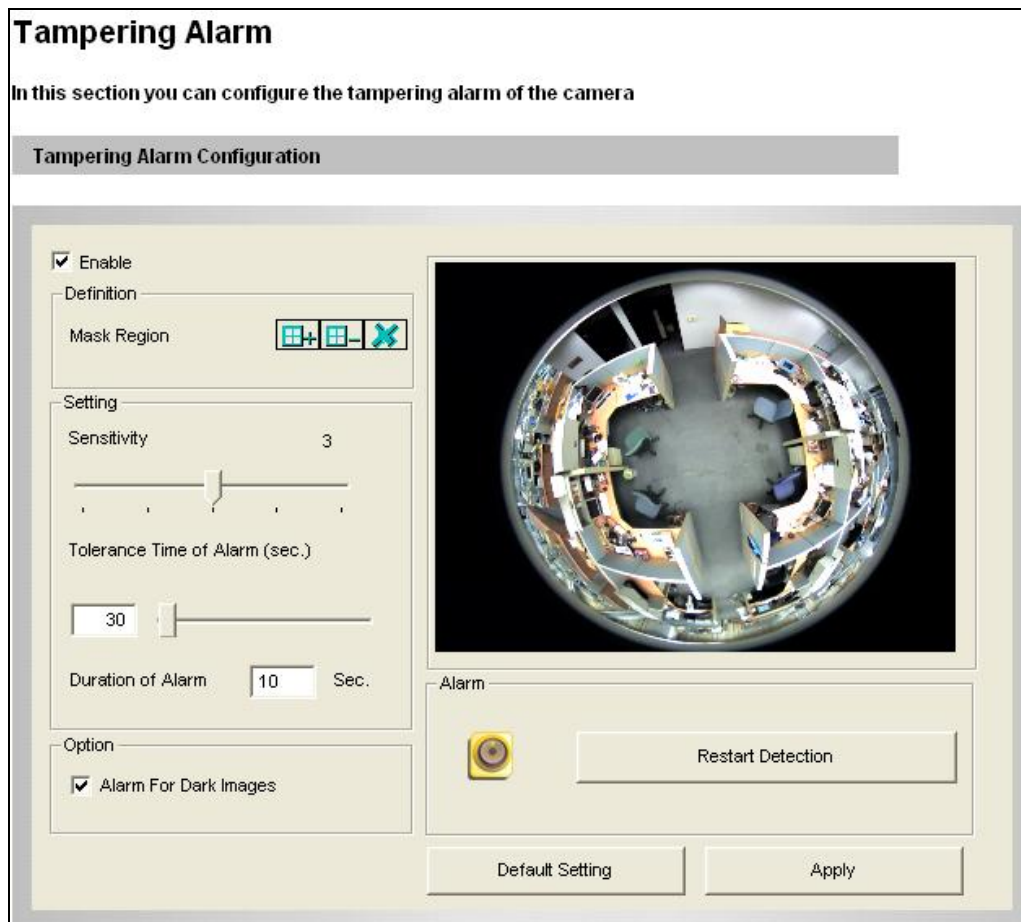



Figure 4-5

To configure the tampering alarm:

1. Select **Enable**.
2. If you want the camera to ignore any movement or scene change in certain areas, click the  button to drag areas on the camera view.
3. Select the desired detection sensitivity by moving the slider. The higher the value, the more sensitive the camera is to scene changes.
4. In the **Tolerance Time of Alarm** field, specify the time length allowed for scene changes before an alarm is generated.
5. In the **Duration of Alarm** field, specify the duration of the alarm after which the triggered output device will be turned off.
6. To trigger an alarm when the scene turns dark, e.g. the lens of camera has been covered, select **Alarm for Dark Images**.
7. Click **Apply** to save all the settings.
8. Start monitoring to enable the function. To have output alarm, it is required to start **Input** monitoring. See *4.4 Monitoring*.

When the camera has been tampered with, the output device can be activated. To turn off the output device immediately, return to this setting page, and click **Restart Detection**.

4.1.5 Visual Automation

This intuitive feature helps you automate any electronic device by triggering the connected output device. When you click on the image of the electronic device, you can change its current state, e.g. turning the light on.

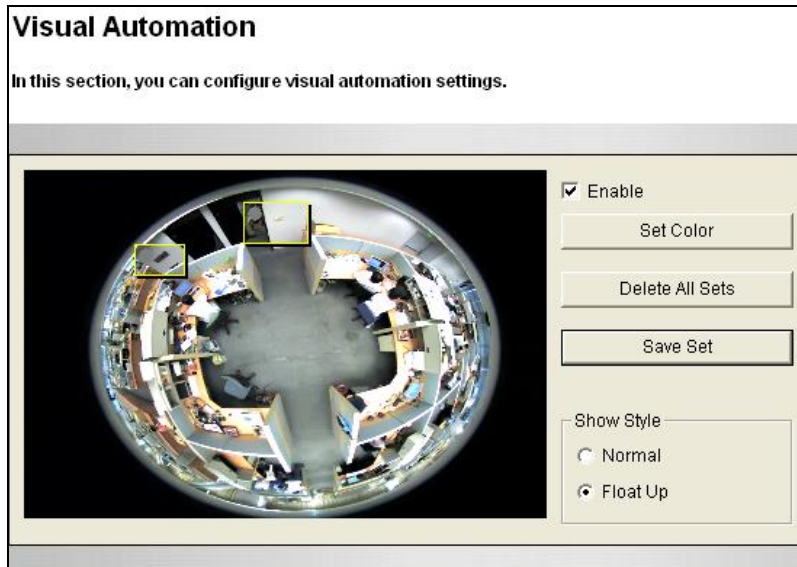


Figure 4-6

1. Select the **Enable** option.
2. Drag an area on the image of the electronic device. This dialog box appears.

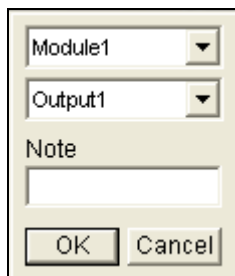


Figure 4-10

3. Assign the connected module and output device. In the Note field, type a note to help you identify the device. Click **OK** to save the settings.
4. To change the frame color of the set area, click the **Set Color** button.
5. To emboss the set area, select **Float Up**; or keep it flat by selecting **Normal**.
6. Click the **Save Set** button to apply the settings.

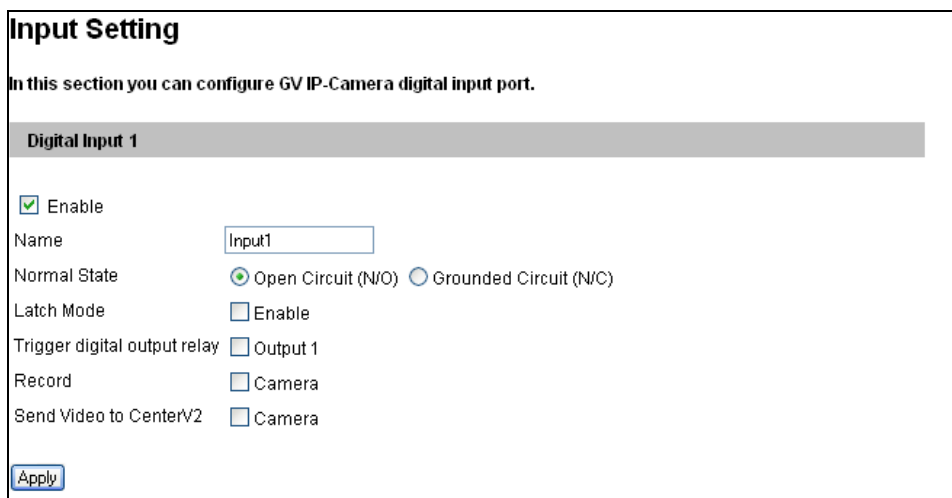
To perform the function, see 3.2.13 *Visual Automation*.

4.2 I/O Control

The I/O wires connected to the camera provide the interface for one input device and one output device.

4.2.1 Input Settings

To activate the sensor input, select **Enable**.



Input Setting

In this section you can configure GV IP-Camera digital input port.

Digital Input 1

☒ Enable

Name

Normal State ☒ Open Circuit (N/O) ☐ Grounded Circuit (N/C)

Latch Mode ☐ Enable

Trigger digital output relay ☐ Output 1

Record ☐ Camera

Send Video to CenterV2 ☐ Camera

Figure 4-7

- **Normal State:** You can set the input state to trigger actions by selecting **Open Circuit (N/O)** or **Grounded Circuit (N/C)**.
- **Latch Mode:** Enable this option to have a momentary output alarm.
- **Trigger digital output relay:** When this option is enabled, the output will be triggered once the input is activated.
- **Record:** Enable this option to start recording when the input is triggered.
- **Send Video to Center V2:** Enable this option to send the images to Center V2 when the input is triggered.

Note: Triggering the output, recording the images and sending video to Center V2 are enabled only after you start **Input** monitoring manually or by schedule. To configure the input monitoring, see [4.4 Monitoring](#).

4.2.2 Output Settings

Select **Enable** to start the output device. Choose the output signal that best suits the device you are using: N/O (Open Circuit), N/C (Grounded Circuit), N/O Toggle, N/C Toggle, N/O Pulse or N/C Pulse. For **Toggle** output type, the output continues to be triggered until a new input trigger ends the output. For **Pulse** output type, the output is triggered for the amount of time you specify in the Trigger Pulse Mode for x Seconds field.

[Alarm Settings] You can choose to automatically trigger the digital output under these conditions: tampering alarm, disk write error (Rec Error) and hard disk full (HD Full).

Output Setting

In this section you can configure GV IP-Camera digital output port.

Digital Output 1 - Normal State

☒ Enable

Name

General Mode ☒ Open Circuit (N/O) ☐ Grounded Circuit (N/C)

Toggle Mode ☐ Open Circuit (N/O) ☐ Grounded Circuit (N/C)

Pulse Mode ☐ Open Circuit (N/O) ☐ Grounded Circuit (N/C)

Trigger Pulse Mode for seconds(1~60)

Digital Output 1 - Alarm Settings

☐ Tampering Alarm

☐ Rec Error

☐ HD Full

Figure 4-8

4.3 Events & Alerts

The Administrator can set up the following alert methods to receive notifications when motion is detected or I/O devices are triggered:

1. Send a captured still image by e-mail or FTP.
2. Notify Center Monitoring Station, Center V2, VSM or GV-GIS, by video or text alerts.

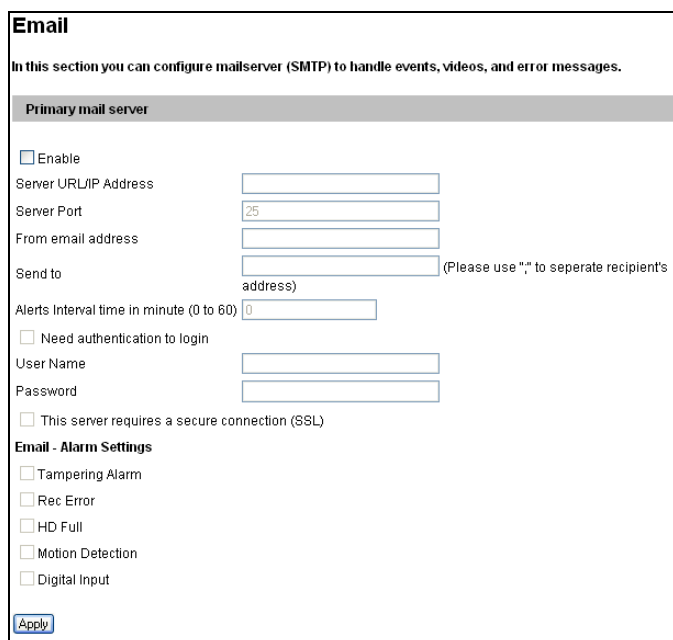
To activate the above alert methods, you must set the following functions in advance:

- Motion Detection (See 4.1.2 *Motion Detection*)---optional
- Input Setting (See 4.2.1 *Input Settings*)
- For e-mail and FTP alerts, it is required to start monitoring (See 4.4 *Monitoring*).

Note: Setting the Motion Detection function is optional since it is activated by default.

4.3.1 E-mail

After a trigger event, the camera can send an e-mail to a remote user containing a captured still image.



Email

In this section you can configure mailserver (SMTP) to handle events, videos, and error messages.

Primary mail server

☐ Enable

Server URL/IP Address:

Server Port:

From email address:

Send to: (Please use "," to separate recipient's address)

Alerts Interval time in minute (0 to 60):

☐ Need authentication to login

User Name:

Password:

☐ This server requires a secure connection (SSL)

Email - Alarm Settings

☐ Tampering Alarm

☐ Rec Error

☐ HD Full

☐ Motion Detection

☐ Digital Input

Figure 4-9

[Enable] Select to enable the e-mail function.

- **Sever URL/IP Address:** Type the SMTP Server's URL address or IP address.
- **Server Port:** Type the SMTP Server's port number. Or keep the default value 25.

- **From email address:** Type the sender's e-mail address.
- **Send to:** Type the e-mail address(s) you want to send alerts to.
- **Alerts Interval Time:** Specify the interval between e-mail alerts. The interval can be between 0 and 60 minutes. The option is useful for frequent event occurrence. Any event triggers during the interval period will be ignored.

[Need authentication to login] If the SMTP Server needs authentication, select this option and type a valid username and password to log in the SMTP server.

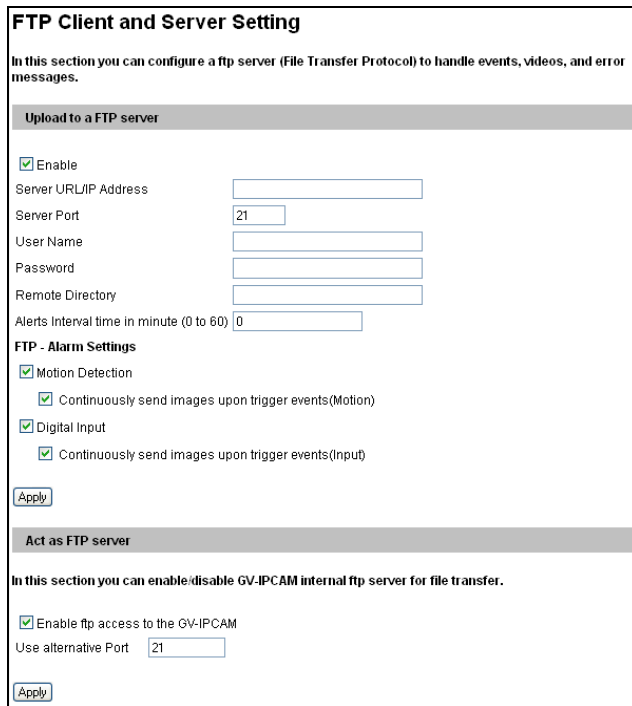
[This server requires a secure connection] If the SMTP Servers needs a secure connection (SSL), select this option.

[Email-Alarm Settings] You can choose to automatically send an e-mail alert under these conditions: motion detection, digital input triggered, tampering alarm, disk write error (Rec Error) and hard disk full (HD Full).

For related settings to send e-mail alerts, see *4.1.2 Motion Detection*, *4.2.2 Output Settings* and *4.4 Monitoring*.

4.3.2 FTP

You can also send the captured still image to a remote FTP server for alerts.



FTP Client and Server Setting

In this section you can configure a ftp server (File Transfer Protocol) to handle events, videos, and error messages.

Upload to a FTP server

☒ Enable

Server URL/IP Address

Server Port

User Name

Password

Remote Directory

Alerts Interval time in minute (0 to 60)

FTP - Alarm Settings

☒ Motion Detection

☒ Continuously send images upon trigger events(Motion)

☒ Digital Input

☒ Continuously send images upon trigger events(Input)

Act as FTP server

In this section you can enable/disable GV-IPCAM internal ftp server for file transfer.

☒ Enable ftp access to the GV-IPCAM

Use alternative Port

Figure 4-10

[Enable] Select to enable the FTP function.

- **Server URL/IP Address:** Type the URL address or IP address of the FTP Server.
- **Server Port:** Type the port number of the FTP Server. Or keep the default value 21.
- **User Name:** Type a valid user name to log into the FTP Server.
- **Password:** Type a valid password to log into the FTP Server.
- **Remote Directory:** Type the name of the storage folder on the FTP Server.
- **Alerts Interval time in minute:** Specify the interval between FTP alerts. The interval can be between 0 and 60 minutes. The option is useful for frequent event occurrence. Any event triggers during the interval period will be ignored.

[FTP-Alarm Settings]

- **Motion Detection:** Once motion is detected on the camera, a still image will be sent to the FTP Server.
 - ⊙ **Continuously send images upon trigger events (Motion):** A sequence of snapshots is uploaded to the FTP Server when motion is detected on the camera.
- **Digital Input:** When the input is triggered, a still image will be sent to the FTP Server.
 - ⊙ **Continuously send images upon trigger events (Input):** A sequence of snapshots is uploaded to the FTP Server when the input is triggered.

[Act as FTP Server]

- **Enable FTP access to GV-IPCAM:** The camera acts as a FTP server, enabling users to download AVI files. The memory card must be inserted for the camera to act as an FTP server.
- **Use alternative port:** The default port is set to 21.

To access the internal FTP server through a web browser, type the IP address or the domain name of the camera in your browser like this:

ftp://192.168.0.10

When you are prompted for Username and Password, type the default value **ftpuser** in both fields. Then you should find the AVI files recorded after trigger events.

To change login information of the internal FTP server, see *4.8.4 User Account*. For the related settings to send FTP alerts, see *4.1.2 Motion Detection*, *4.2.1 Input Settings* and *4.4 Monitoring*.

4.3.3 Center V2

After a motion or an I/O triggered event, the central monitoring station Center V2 can be notified by live videos and text alerts. For the live monitoring through Center V2, you must already have a subscriber account on Center V2. The camera can connect with up to two Center V2.

Connection 1

Connection 2

Center V2

In this section you can configure the connection to Center V2 and tasks to perform.

Center V2 server

Activate Link

☒

Host name or IP Address:

192.168.0.217

Port number:

5551

User Name:

0

Password:

•

Cease motion detection messages from

☐ Camera

Cease input trigger message from

☐ Input 1

Enable schedule mode

☐

Apply

Select schedule time

☐ Span 1

00

:

00

~

00

:

00

Next Day

☐ Span 2

00

:

00

~

00

:

00

Next Day

☐ Span 3

00

:

00

~

00

:

00

Next Day

☐ Weekend

☒ Saturday and Sunday

☐ Only Sunday

Apply

Connection Status

Status: Connected. Connected Time: Wed May 26 04:31:30 2010

Figure 4-11

To enable the Center V2 connection:

1. **Activate Link:** Enable the monitoring through Center V2.
2. **Host Name or IP Address:** Type the host name or IP address of Center V2.
3. **Port Number:** Match the port to **Port 2** on Center V2. Or keep the default value 5551.
For details, see *8.1 Center V2*.
4. **User Name:** Type a valid user name to log into Center V2.
5. **Password:** Type a valid password to log into Center V2.
6. Click **Apply**. The Connection Status should display “Connected” and the connected time.

These options can also be found on this Center V2 setting page:

- **Cease motion detection messages from:** Stops notifying Center V2 of motion-triggered events.
- **Cease input trigger messages from:** Stops notifying Center V2 of input-triggered events.
- **Enable schedule mode:** Starts the monitoring through Center V2 based on the schedule you set in the **Select Schedule Time** section. Refer to *4.5 Recording Schedule* for the same settings.

For related settings to activate the monitoring through Center V2, see *4.1.2 Motion Detection*, *4.2.1 Input Settings*, and *8.1 Center V2*.

4.3.4 VSM

After a motion detection or an I/O triggered event, the central monitoring station VSM can get notified by text alerts. For the live monitoring through VSM, you must already have a subscriber account on VSM. The camera can be connected with up to two VSM.

Connection 1
Connection 2

Vital Sign Monitor Server Setting

In this section you can configure the connection to VSM Server and tasks to perform.

Vital Sign Monitor Server

Activate Link
☐

Host name or IP Address:

Port number:

User Name:

Password:

Cease motion detection messages from
☐ Camera

Cease input trigger message from
☐ Input 1

Enable schedule mode
☐

Apply

Select schedule time

☐ Span 1
 : ~ : Next Day

☐ Span 2
 : ~ : Next Day

☐ Span 3
 : ~ : Next Day

☐ Weekend
☒ Saturday and Sunday
☐ Only Sunday

☐ Special Day (MM/DD)

01. 02. 03. 04.
05. 06. 07. 08.
09. 10. 11. 12.

Apply

Connection Status

Status: Disconnected

Figure 4-12

To enable the VSM connection:

1. **Activate Link:** Enable the monitoring through VSM.
2. **Host Name or IP Address:** Type the host name or IP address of VSM.

3. **Port Number:** Match the port to **Port 2** on VSM. Or keep the default value 5609. For details, see *8.2 VSM*.
4. **User Name:** Type a valid user name to log into VSM.
5. **Password:** Type a valid password to log into VSM.
6. Click **Apply**. The Connection Status should display “Connected” and connected time.

These options you can also find on this VSM setting page:

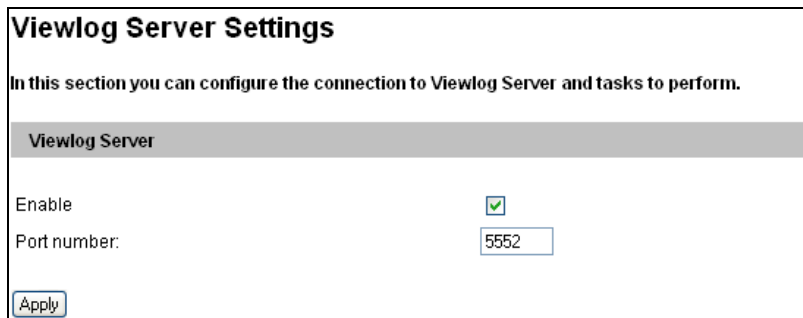
- **Cease motion detection messages from:** Stops notifying VSM of motion-triggered events.
- **Cease input trigger messages from:** Stops notifying VSM of input-triggered events.
- **Enable schedule mode:** Starts the monitoring through VSM based on the schedule you set in the **Select Schedule Time** section. Refer to *4.5 Recording Schedule* for the same settings.

For related settings to activate the monitoring through VSM, see *4.1.2 Motion Detection*, *4.2.1 Input Settings*, and *8.2 VSM*.

4.3.5 ViewLog Server

The ViewLog Server is designed for remote playback function. This server allows you to remotely access the recorded files saved in the camera and play back video with the player ViewLog.

Select **Enable** to activate the built-in server. Keep the default port **5552** or modify it if necessary. For details on the remote playback, see *5.2.2 Playback over Network*.

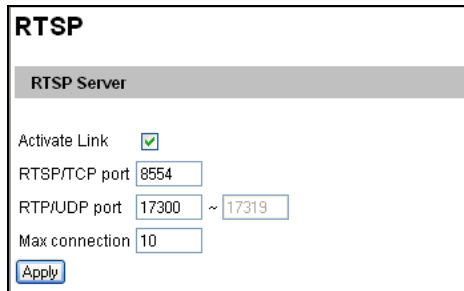


The screenshot shows a web-based configuration window titled "Viewlog Server Settings". Below the title is a subtitle: "In this section you can configure the connection to Viewlog Server and tasks to perform." There is a section header "Viewlog Server" in a grey bar. Below this, there are two settings: "Enable" with a checked checkbox, and "Port number:" with a text input field containing "5552". At the bottom left of the settings area is an "Apply" button.

Figure 4-13

4.3.6 RTSP

The RTSP Server enables RTSP protocol for video streaming.



The screenshot shows a configuration window titled "RTSP". Inside, there is a sub-header "RTSP Server". Below this, there are four settings: "Activate Link" with a checked checkbox, "RTSP/TCP port" with a text box containing "8554", "RTP/UDP port" with a range of text boxes showing "17300" and "17319" separated by a tilde, and "Max connection" with a text box containing "10". At the bottom left is an "Apply" button.

Figure 4-14

- **Activate Link:** Enable the RTSP protocol.
- **RTSP/TCP Port:** Keep the default value 8554, or modify it if necessary.
- **RTP/UDP Port:** Keep the default range from 17300 to 17319, or modify it if necessary.
The number of ports for use is limited to 20.
- **Max Connection:** Set the maximum number of connections to the camera.

For details on the RTSP command, see *RTSP Protocol Support* in Appendix B.

4.4 Monitoring

You can start recording manually, by schedule or by input trigger.

Note: See **Note for Recording** at the beginning of the manual.

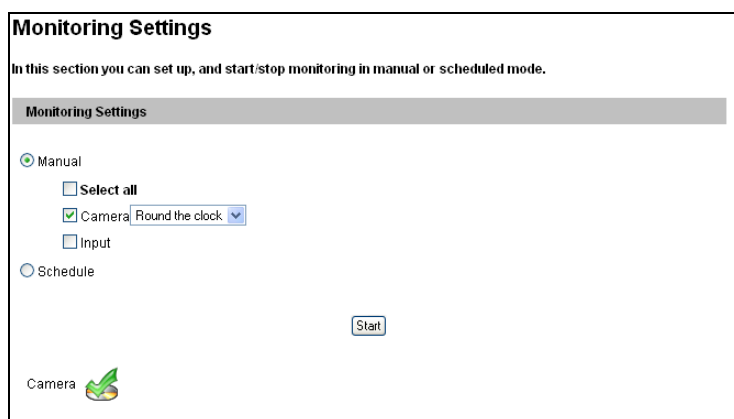


Figure 4-15

[Manual] Manually activates motion detection and I/O monitoring. Select one of the following options and then click the **Start** button.

- **Select all:** Manually starts both motion detection and I/O monitoring.
- **Camera x:** Manually starts recording. Select the desired recording mode for recording.
- **Input:** Manually starts I/O monitoring. When the sensor input is triggered, the camera and output will also be activated for recording and alerting. For input settings, see 4.2.1 *Input Settings*.

[Schedule] The system starts recording and input monitoring based on the schedule you set. For schedule settings, see 4.5 *Recording Schedule*.

[Camera Status Icon]



: On standby



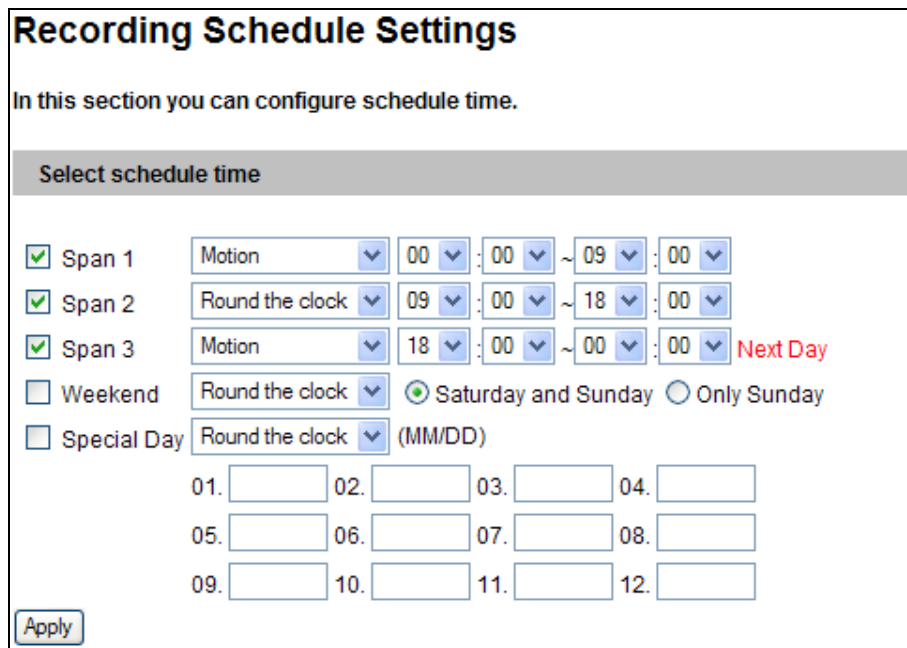
: Enabled for motion detection and input trigger

4.5 Recording Schedule

The schedule is provided to activate recording and I/O monitoring on a specific time each day.

4.5.1 Recording Schedule Settings

You can set up the schedule for recording.



Recording Schedule Settings

In this section you can configure schedule time.

Select schedule time

☒ Span 1 Motion 00 : 00 ~ 09 : 00

☒ Span 2 Round the clock 09 : 00 ~ 18 : 00

☒ Span 3 Motion 18 : 00 ~ 00 : 00 **Next Day**

☐ Weekend Round the clock ☒ Saturday and Sunday ☐ Only Sunday

☐ Special Day Round the clock (MM/DD)

01. 02. 03. 04.

05. 06. 07. 08.

09. 10. 11. 12.

Figure 4-16

- **Span 1- Span 3:** Set a different recording mode for each time span during the day. Each day can be divided into 3 time spans, shown as Span 1, Span2, and Span 3. The time span settings will apply to Monday through Sunday.
- **Weekend:** Enable this option to start monitoring all day on the weekend and select a recording mode to be used. Define whether your weekend includes **Saturday and Sunday** or **Only Sunday**.
- **Special Day:** Set the recording mode on a specified day.

4.5.2 I/O Monitoring Settings

You can set the schedule for I/O monitoring to start.

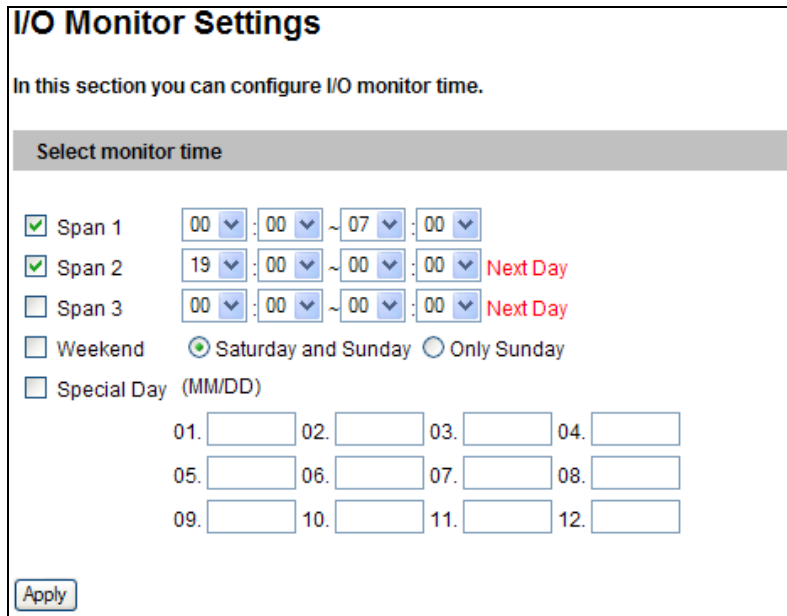


Figure 4-17

- **Span 1-3:** Set different time spans during the day to enable I/O monitoring. Each day can be divided into 3 time spans, shown as Span 1, Span2, and Span 3. The time span settings will work from Monday through Sunday.
- **Weekend:** Enable this option to start I/O monitoring all day on the weekend and select whether your weekend includes **Saturday and Sunday** or **Only Sunday**.
- **Special Day:** Enable I/O monitoring on a specified day.

Note: In Recording Schedule and I/O Monitoring Schedule, if the settings for Special Day conflict with those for Span 1-3 or Weekend, the Special Day settings will get priority.

4.6 Remote ViewLog

With the Remote ViewLog function, you can play back the files recorded at the camera over TCP/IP network.

For first-time users, you need to install the Remote ViewLog program from the Software DVD to the local computer. For remote access to the camera, the **ViewLog Server** built in the unit must be enabled. See *4.3.5 ViewLog Server*.

For details on connecting to the camera for playback, see *5.2.2 Playback over Network*.

4.7 Network

The Network section includes some basic but important network configurations that enable the camera to be connected to a TCP/IP network.

4.7.1 LAN

According to your network environment, select among Static IP, DHCP and PPPoE.

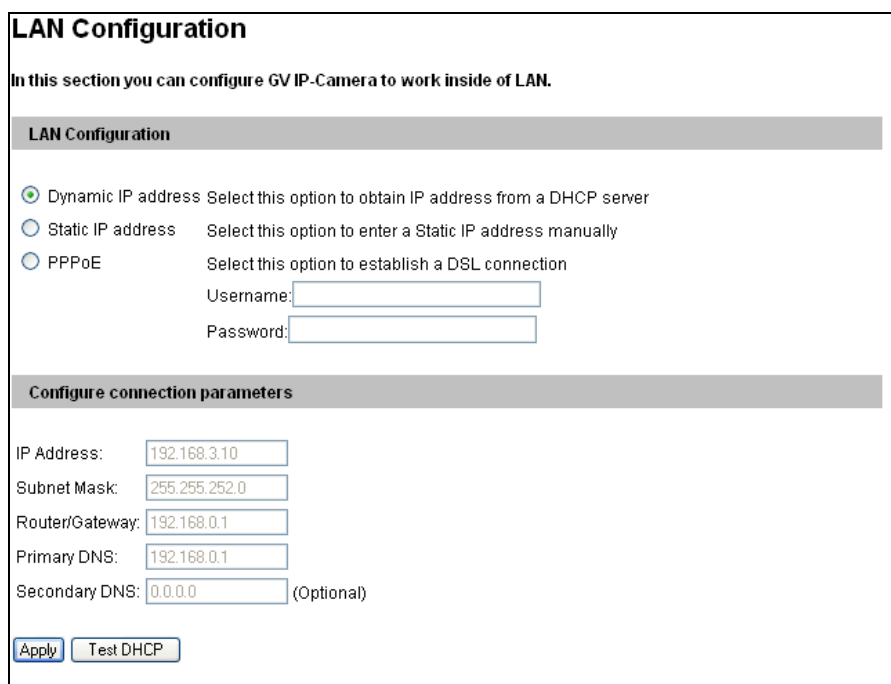


Figure 4-18

[LAN Configuration]

- **Dynamic IP address:** The network environment has a DHCP server. This option should only be enabled if you know which IP address the camera will get from the DHCP server, or you have obtained a domain name from the DDNS service provider that always links to the camera's changing IP address.
- **Static IP address:** Assign a static IP or fixed IP to the camera. Type the camera's TCP/IP and DNS parameters in the **Configure connection parameters** section.
- **PPPoE:** The network environment is xDSL connection. Type the Username and Password provided by ISP to establish the connection. If you use the xDSL connection with dynamic IP addresses, first use the DDNS function to obtain a domain name linking to the camera's changing IP address.

[Configure connection parameters]

Type the camera's IP address, Subnet Mask, Router/Gateway, Primary DNS server and Secondary DNS server.

Parameters	Default
IP address	192.168.0.10
Subnet Mask	255.255.255.0
Router/Gateway	192.168.0.1
Primary DNS server	192.168.0.1
Secondary DNS server	192.168.0.2

For details on Dynamic DNS Server Settings, see *4.7.2 Advanced TCP/IP*.

4.7.2 Advanced TCP/IP

This section introduces the advanced TCP/IP settings, including DDNS Server, HTTP port, streaming port and UPnP.

Advanced TCP/IP

In this section you can set the advanced TCP/IP configuration

Dynamic DNS Server Settings

In this section you can configure your GV-IPCAM to obtain a domain name by using a dynamic IP.

☒ Enable

Service Provider: Geovision DDNS Server ex: [Register Geovision DDNS Server](#)

Host Name:

User Name:

Password:

Update Time : Fri Nov 19 11:41:06 GMT8:00 2010 [Refresh](#)

[Apply](#)

HTTP Port Settings

In this section you can change the default HTTP port number (80) to any port within the range 1024-65535. It is a simple method to increase system security using port mapping. You can configure HTTP connection to an alternative port.

HTTP Port:

[Apply](#)

HTTPS Settings

In this section you can change the default HTTPS port number (443) to any port within the range 1024-65535. It is a simple method to increase system security using port mapping. You can configure HTTPS connection to an alternative port.

External storage is not available. Cannot upload customized certification and private key.

☐ Enable

HTTP Port:

☐ Use customized certification and private key. External storage is necessary.

Certification: [Browse...](#)

Private Key: [Browse...](#)

Password:

[Apply](#)

GV-IPCAM Streaming Port Settings

In this section you can configure Streaming connection from a determine port. The default setting is 10000.

VSS Port:

[Apply](#)

UPnP Settings

In this section you can enable or disable UPnP function.

UPnP: ☒ Enable ☐ Disable

[Apply](#)

Figure 4-19

[Dynamic DNS Server Settings]

DDNS (Dynamic Domain Name System) provides a convenient way of accessing the camera when using a dynamic IP. DDNS assigns a domain name to the camera, so that the Administrator does not need to go through the trouble of checking if the IP address assigned by DHCP Server or ISP (in xDSL connection) has changed.

Before enabling the following DDNS function, the Administrator should have applied for a Host Name from the DDNS service provider's website. There are 2 providers listed in the camera: GeoVision DDNS Server and DynDNS.org.

To enable the DDNS function:

1. **Enable:** Enable the DDNS function.
2. **Service Provider:** Select the DDNS service provider you have registered with.
3. **Host Name:** Type the host name used to link to the camera. For users of GeoVision DDNS Server, it is unnecessary to fill the field because the system will detect the host name automatically.
4. **User Name:** Type the user name used to enable the service from the DDNS.
5. **Password:** Type the password used to enable the service from the DDNS.
6. Click **Apply**.

[HTTP Port Settings]

The HTTP port enables connecting the camera to the web. For security integration, the Administrator can hide the server from the general HTTP port by changing the default HTTP port of 80 to a different port number within the range of 1024 thru 65535.

[HTTPS Settings]

By enabling the HTTPS settings, you can access the camera through a secure protocol. You can use your own generated Certificate and Private Key or ones verified by the SSL authority. Click **Browse** to locate the Certificate file and Private Key file, and type the password if the .pem files are protected by a password. Click **Apply**. The Web interface will be restarted automatically and you will need to log in again.

Note: Only .pem file format is supported for Certification and Private Key.

[GV-IPCAM Streaming Port Settings]

The VSS port enables connecting the camera to the GV-System. The default setting is 10000.

[UPnP Settings]

UPnP (Universal Plug & Play) is a networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. It means that they are listed in the network devices table for the operating system (such as Windows XP) supported by this function. Enabling this function, you can connect to the camera directly by clicking on the camera listed in the network devices table.

4.7.3 IP Filtering

The Administrator can set IP filtering to restrict access to the camera.

IP Filter Setting

In this section you can allow or deny network connection listed in the table. (Filter Table support only 4 entries.)

IP Filtering

☒ Enable IP Filtering

No.	IP Address Range in CIDR format	Action	Customize
1	192.168.0.66	Allow	Remove

Filtered IP:

ex: 192.168.1.2 or 192.168.1.0/24

Action to take:

Allow

Apply

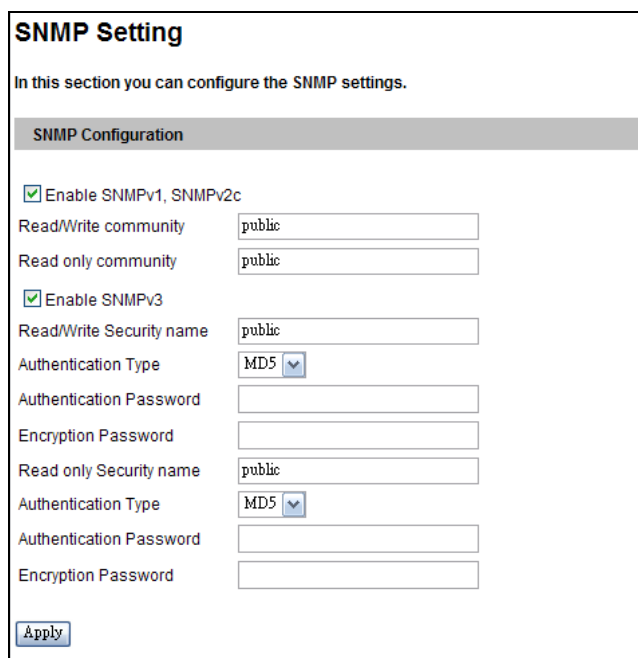
Figure 4-20

To enable the IP Filter function:

1. **Enable IP Filtering:** Enable the IP Filtering function.
2. **Filtered IP:** Type the IP address you want to restrict the access.
3. **Action to take:** Select to **Allow** or **Deny** the IP address(es) you have specified.
4. Click **Apply**.

4.7.4 SNMP Setting

The Simple Network Management Protocol (SNMP) allows you to monitor the status of the camera with SNMP network management software.



SNMP Setting

In this section you can configure the SNMP settings.

SNMP Configuration

☒ Enable SNMPv1, SNMPv2c

Read/Write community:

Read only community:

☒ Enable SNMPv3

Read/Write Security name:

Authentication Type:

Authentication Password:

Encryption Password:

Read only Security name:

Authentication Type:

Authentication Password:

Encryption Password:

Figure 4-21

To set up the SNMP settings:

1. Select **Enable SNMPv1 SNMPv2c** to enable the function.
2. To enable access to **Read/Write community**, type a community string. This will serve as a password to allow read and write access to the camera from the SNMP software.
3. To enable **Read only community**, type a community string to allow read only access to the camera from the SNMP software.
4. For a more secured connection, select **Enable SNMPv3** to enable SNMP version 3.
5. To enable access to SNMPv3 Read/Write community, type a **Read/Write Security name**.
6. Select an **Authentication Type** to use for SNMP requests.
7. Type the **Authentication Password** and **Encryption Password**. You will need to type these passwords in the SNMP software to be able to access the camera.
8. To enable access to SNMPv3 Read only community, type a **Read only Security name** and follow steps 6 – 7.
9. Click **Apply** to save the settings.

4.8 Management

The Management section includes the settings of data and time, GPS maps, storage device and user account. Also you can view the firmware version and execute certain system operations.

4.8.1 Date and Time Settings

The date and time settings are used for date and time stamps on the image.

Date and Time Settings

In this section you can configure time and date or just synchronize with a NTP server.

Date and Time on GV IP-Camera

Mon Feb 14 17:22:49 2000

Time Zone

(GMT+08:00) China,Hong Kong,Australia Western,Singapore,Taiwan,Russia

☐ Enable Daylight Saving Time

Start (MM/dd/hh/mm)

End (MM/dd/hh/mm)

Synchronized with a Network Time Server

☒ Synchronized with Network Time Server (NTP)

Host name or IP Address:

Update period: 24 hours; Update Time: AM 05:10

Synchronized with your computer or modify manually

☐ Modify manually

Date (yyy/mm/dd)

Time (hh:mm:ss)

☐ Synchronized with your computer

Date and time overlay setting

Show date as

(This is a format of date where yyyy stands for year in 4 digits or yy in 2 digits, mm stands for month, and dd stands for day)

Display order

☒ Date prior to time (Ex.2007/05/21 17:00:00)

☐ Time prior to date(Ex.17:00:00 2007/05/21)

Figure 4-22

[Date & Time on GV-IPCAM] Displays the current date and time on the camera.

[Time Zone] Sets the time zone for local settings. Select **Enable Daylight Saving Time** to automatically adjust the camera for daylight saving time. Type the Start Time and End Time to enable the daylight saving function. Also see *5.2.4 Playback of Daylight Saving Time Events*.

[Synchronized with a Time Server] By default, the camera uses the timeserver of time.windows.com to automatically update its internal clock every 24 hours. You can also change the host name or IP setting to the timeserver of interest.

[Synchronized with your computer or manually] Manually changes the camera's date and time. Or, synchronize the camera's date and time with those of the local computer.

[Date and time overlay setting] Select the display format of date and time stamps on the image. For this function to work, you must also enable the **Overlaid with date stamps** and **Overlaid with time stamps** options in Figure 4-2.

4.8.2 GPS Maps Settings

The Maps Settings allows you to see the location of your camera on Google maps, without a GPS device.

To see the location of your camera on maps:

1. It is required to sign up for a Google Maps API key before using the Google Maps. Click **Link to the Google Maps API**.

GPS Maps

In this section you can configure the GPS Maps settings.

GPS Maps Settings

Sign up for a Google Maps API key [Link to the Google Maps API](#)

Google Maps API Key

Longitude (Ex.121.565=E121.565. -10.25=W10.25)

Latitude (Ex.25.081=N25.081. -10.25=S10.25)

Location Name

Figure 4-23

2. Enter the registered Maps API Key, the longitude and latitude of your camera, and location name. Click **Apply** to enable this function.
3. Open the control panel of the Live View window.



Figure 4-24

- Click **Open**. A warning message appears.

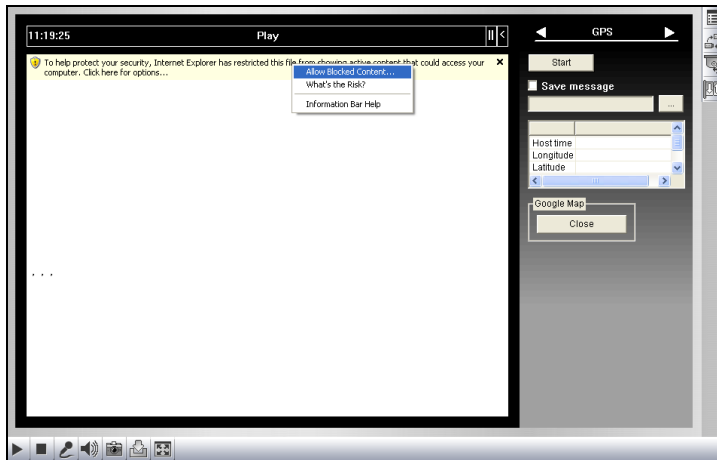


Figure 4-25


- Right-click the warning message and select **Allow Blocked Content**. The map will be displayed. The  icon indicates the location of your camera. At the upper right corner you have options to view different map formats, such as Satellite and Hybrid.



Figure 4-26

4.8.3 Storage Settings

Based on Linux ext3 file system, the camera supports memory cards for video and audio recordings. You need to format the memory card by using the following Storage Settings. After being formatted, the memory card will be ready to use by Linux OS of the camera.

Storage Settings

In this section you can configure the disk storage to archive videos and events.

Storage Settings

☒ Enable recycling

Stop recording or recycle disk when free space of disk is smaller than

256M

☐ Keep days (1-255)

30

Apply

Disk Information

Disk No.	Total Size	Used Size	Free space	Utilization	Remove	Format
Disk11	3.910	0.070	3.840	1%	<div>Remove</div>	<div>Format</div>

Partition Information

Disk No.	Partition No.	Total Size	Used Size	Free space	Utilization	Format
Disk11	1	3.910	0.069	3.840	1%	<div>Format</div>

(Unit: Gigabyte)

Figure 4-27

[Storage Settings]

If the **Enable recycling** option is selected, when the space of the storage device is lower than the specified space, the system will either write the data to another device or overwrite the oldest recorded files.

If the **Enable recycling** option is not selected, the system will stop recording when the specified space is reached.

- Keep days (1-255):** Specify the number of days to keep the files from 1 day to 255 days. When both **Keep days** and **Enable recycling** are selected, the system applies whichever condition comes first. For example, if the specified smallest amount of storage space comes earlier than the designated keep days, then recycle is applied first.

[Disk Information]

This section shows the details of the attached storage devices.

[Partition Information]

This section shows the partition details of the attached storage devices.

To add a memory card:

1. Insert the memory card to the camera.
2. Click the **Format** button.
3. After the format is complete, the partition information will display. The maximum space for one partition is 200 GB.

To remove a memory card:

1. Click the **Remove** button.
2. When you are prompted to confirm the action, click **Yes**. The page will be refreshed and the partition information will be cleaned.
3. Remove the memory card from the camera.

Note:

1. If **Enable Recycle** is selected, the available space of the storage device must be higher than the space you specified at the **Stop recording or recycle disk when free space of disk is smaller than x** option. Otherwise no video will be recoded.
 2. The recording data may be lost if you remove the storage device during recording.
 3. If you do not remove the storage device properly, the data cannot be read in another computer. In this case, re-plug the storage device back to the camera. The system will repair the data automatically. When the system is repairing the data, the **Remove** field will display "Repairing".
-

4.8.4 User Account

You can change the login name and password of Administrator, Guest and FTP Server User.

- The default Administrator login name and password are **admin**.
- The default Guest login name and password are **guest**. To allow a Guest user log in without entering name and password, select **Disable authentication for guest account**.
- The default FTP Server login name and password are **ftpuser**.

User Account
In this section you can change the administrator account and password

Administrator Account
Username:
Old Password:
New Password:
Confirm Password:

Guest User Account
Username:
Old Password:
New Password:
Confirm Password:

☐ Disable authentication for guest account

FTP Server User Account
Username:
Old Password:
New Password:
Confirm Password:

Figure 4-28

4.8.5 Log Information

The log information contains dump data that is used by service personnel for analyzing problems.

Log Information

In this section you can see all system activities.

Startup time log

In this section you can see latest booting time of system.

[0] Mon Feb 14 14:59:02 2000

System Log

In this section you can see all system activities.

```

Jan 1 00:00:07 FIE8180 syslog.info syslogd started: BusyBox v1.1.3
Jan 1 00:00:07 FIE8180 user.warn kernel: it isn't (<NULL>); looks
like an initrd
Jan 1 00:00:07 FIE8180 user.info kernel: Freeing initrd memory:
13487K
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc000e790: ptrace_break_init+0x0/0x2c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc000fb68: consistent_init+0x0/0xe8()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0012bd8: helper_init+0x0/0x38()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0012d80: ksysfs_init+0x0/0x40()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0014d54: filelock_init+0x0/0x54()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0015728: init_aout_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0015744: init_script_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc0015760: init_elf_binfmt+0x0/0x1c()
Jan 1 00:00:07 FIE8180 user.debug kernel: Calling initcall
0xc001ec8c: netlink_proto_init+0x0/0x214()
Jan 1 00:00:07 FIE8180 user.info kernel: NET: Registered protocol

```

Clear

Figure 4-29

4.8.6 Tools

This section allows you to execute certain system operations and view the firmware version.

Additional Tools

In this section you can set the additional tools

Host Settings

In this section you can determine a hostname and camera name for identification.

Host Name

Firmware Update

In this section you can see GV-IPCAM firmware version.

System Settings

Restore to factory default settings

Current chipset temperature inside camera is °C / °F

Reboot

Do you wish to reboot now?

Figure 4-30

[Host Settings] Type a descriptive name for the camera.

[Firmware Update] This field displays the firmware version of the camera.

[System Settings] Clicking the **Load Default** button will restore the camera to factory default settings. You can also see the **Current chipset temperature inside the camera**.

Note: After applying the default function, you will need to configure the camera's network setting again.

[Reboot]

Clicking the **Reboot** button will make the camera perform software reset.

Chapter 5 Recording and Playback

The camera can record video and audio directly to the memory card. You can play back the recorded files on the GV-System or over the TCP/IP network.

Note: See *Note for Recording* at the beginning of the manual.

5.1 Recording

To enable the recording function:

1. Insert the memory card to the camera. See “To add a memory card,” 4.8.3 *Storage Settings*.
2. If you like to set up pre-recording, post-recording or audio recording, see 4.1.1 *Video Settings*.
3. If you like to set up the schedule for video recording or I/O monitoring, see 4.5 *Recording Schedule*.
4. If you like to configure the areas and sensitivity values for motion detection, see 4.1.2 *Motion Detection*.
5. If you want the recording to be triggered by input device, configure the operation of I/O devices. See 4.2.1 *Input Settings*.
6. To start recording and I/O monitoring, see 4.4 *Monitoring*.

The camera will start recording in case of motion detection, I/O trigger, or during the scheduled time.

5.2 Playback

These methods are available to play back the video files recorded at the camera:

- Playback using the memory card by connecting it directly to the GV-System through a memory card reader
- Playback using the Remote ViewLog function over the TCP/IP network
- Playback using the recorded files downloaded from built-in FTP Server

5.2.1 Playback Using the Memory Card

You can play back the files recorded at the camera by attaching the memory card to the GV-System. However, the GV-System is run on Windows system while the files recorded at camera is of Linux file system. To enable Windows to recognize the files, you need to install the program **Ext2 Installable File System** included on the Software DVD.

1. Insert the Software DVD, select **IFS Drives** and follow the onscreen instructions for installation.
2. Run **IFS Drives** from Control Panel and assign the drive name(s) to each available partition in the storage device.

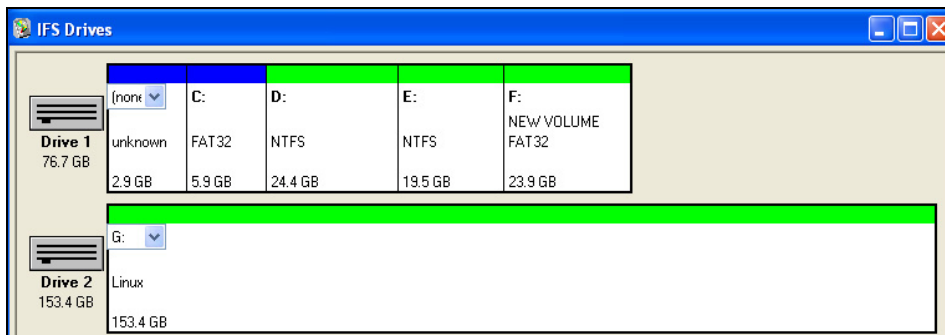


Figure 5-1

3. Run **ViewLog**.
4. Click the **Advanced** button , select **Reload Database** and click **Video Server/Compact DVR**. This dialog box appears.

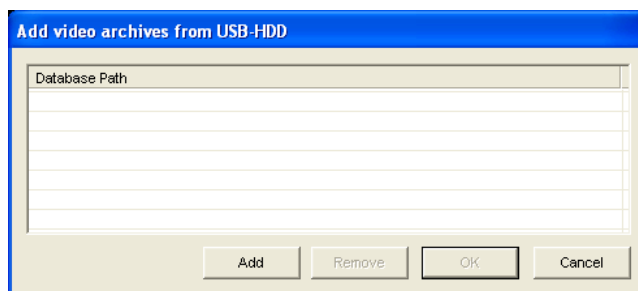


Figure 5-2

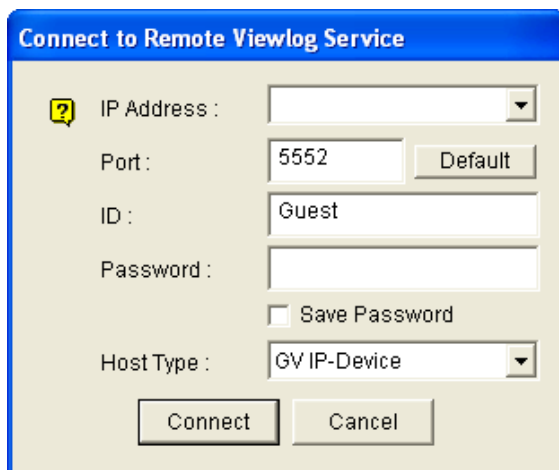
5. Click **Add** to assign the hard drive.
6. Click **OK** to load the data to the ViewLog for playback.

Note: IFS Driver supports Windows NT/2000/XP/Windows 7. For Windows 7, refer to ftp://geo-demo-japan.dipmap.com/Technote/GV_IP_Devices/Run_IFS_Driver_Win7.pdf to see how to configure the settings.

5.2.2 Playback over Network

With the Remote ViewLog function, you can play back the files recorded at the camera over TCP/IP network.

1. The camera must allow remote access with **ViewLog Server** activated. See 4.3.5 *ViewLog Server*.
2. For first time users, run the **Remote ViewLog** program from the Software DVD. Next time whenever you would like to use this function, access this option from the camera's Web interface.
3. When this dialog box appears, type the camera's IP address, login ID and password. Keep the default port **5552** or modify it if necessary.



The dialog box titled "Connect to Remote Viewlog Service" contains the following fields and controls:

- IP Address :** A text input field with a dropdown arrow on the right.
- Port :** A text input field containing "5552" and a "Default" button to its right.
- ID :** A text input field containing "Guest".
- Password :** A text input field.
- Save Password :** An unchecked checkbox.
- Host Type :** A dropdown menu with "GV IP-Device" selected.
- Buttons:** "Connect" and "Cancel" buttons at the bottom.

Figure 5-3

3. In the **Host Type** field, select **GV IP-Device**.
4. Click **Connect** to access the files of the camera for playback.

5.2.3 Access to the Recorded Files through FTP Server

The built-in FTP Server allows you to download the recorded files saved on the memory card. You can play back the downloaded files of AVI format with any multimedia player. For details to download files, see [Act as FTP Server], 4.3.2 *FTP*.

5.2.4 Playback of Daylight Saving Time Events

On GV-System, you can retrieve the events recorded during the Daylight Saving Time (DST) period from the camera for playback. You can also connect the memory card with the recorded files to GV-System for playback.

The following instructions describe how to retrieve the recorded files from the camera over Internet. If you like to use the memory card for playback, first follow the instructions in 5.2.1 *Playback Using the Memory Card* to load the recorded files to ViewLog, and then follow Steps 4-5 below to play back DST events.

1. The camera must allow the remote access with **ViewLog Server** activated. See 4.3.5 *ViewLog Server*.
2. To remotely connect to the camera from GV-System, click the **Tools** button and select **Remote ViewLog Service**. The Connect to Remote ViewLog Service dialog box appears.
3. Enter the connection information of the camera, and click **Connect**. Once the connection is established, the video events will be displayed on the Video Event list.
4. On the Date Tree, select the date of Daylight Saving Time. A separate DST subfolder will be displayed as illustrated below.

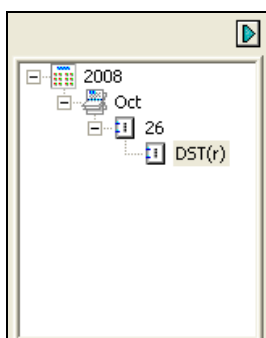


Figure 5-6

5. On the Video Event list, select desired events, and click the **Play** button to start.

Note:

1. The playback function is only compatible with GV-System version 8.4 or later.
 2. The AVI file recorded during the DST period is named with the prefix “GvDST”, e.g. GvDST20081022xxxxxxxxx.avi, to differentiate from the regular AVI file named with the prefix “Event”, e.g. Event20081022xxxxxxxxx.avi.
-

Chapter 6 Advanced Applications

This chapter introduces more advanced applications.

6.1 Upgrading System Firmware

GeoVision will periodically release the updated firmware on the website. The new firmware can be simply loaded into the camera using the Web interface or the **IP Device Utility** included on the Software DVD.

Important Notes before You Start

Before you start updating the firmware, please read these important notes:

1. While the firmware is being updated,
 - A. the power supply must not be interrupted, and
 - B. do not unplug the Ethernet cable if the cable is the source of power supply (Power over Ethernet or PoE supported).
2. Do not turn the power off for 10 minutes after the firmware is updated.
3. If you use the IP Device Utility for firmware upgrade, the computer used to upgrade firmware must be under the same network of the camera.

WARNING: The interruption of power supply during updating causes not only update failures but also damages to your camera. In this case, please contact your sales representative and send your device back to GeoVision for repair.

6.1.1 Using the Web Interface

1. In the Live View window, click the **Show System Menu** button (No. 9, Figure 3-3) and select **Remote Config**. This dialog box appears.

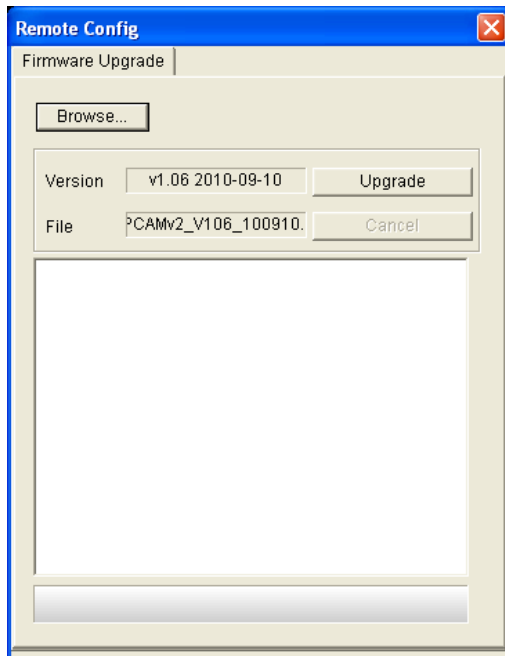


Figure 6-1

2. Click the **Browser** button to locate the firmware file (.img) saved at your local computer.
3. Click the **Upgrade** button to process the upgrade.

6.1.2 Using the IP Device Utility

The IP Device Utility provides a direct way to upgrade the firmware for multiple cameras. Note the computer used to upgrade firmware must be under the same network of the camera.

1. Insert the Software DVD, select **IP Device Utility**, and follow the onscreen instructions to install the program.
2. Double-click the **GV IP Device Utility** icon created on your desktop. This dialog box appears.

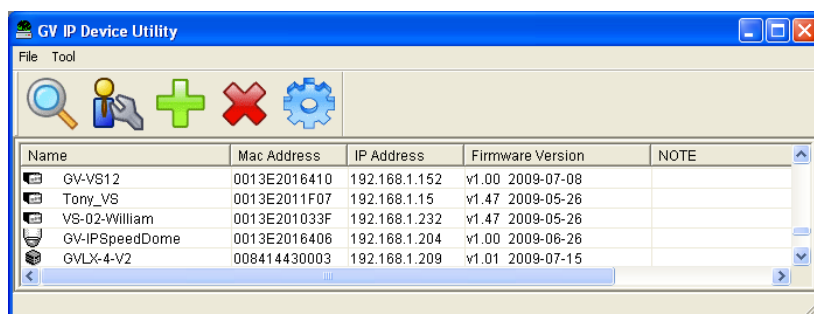



Figure 6-2

3. Click the **Search** button  to locate the available cameras on the same LAN. Or click the **New** button and assign the IP address to locate the camera over the Internet. Or highlight a camera in the list and click the **Delete** button to remove it.
4. Double-click a camera in the list. This dialog box appears.

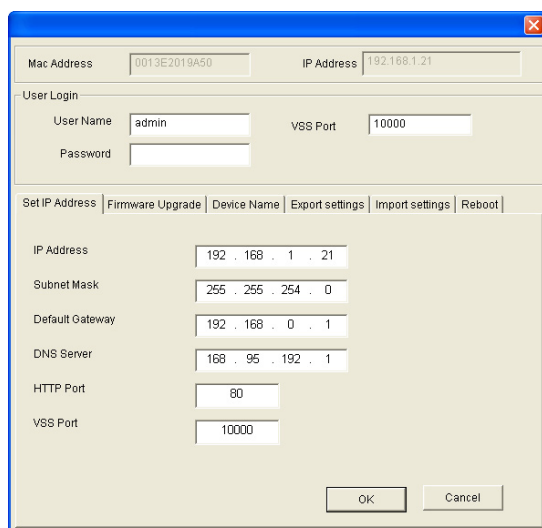
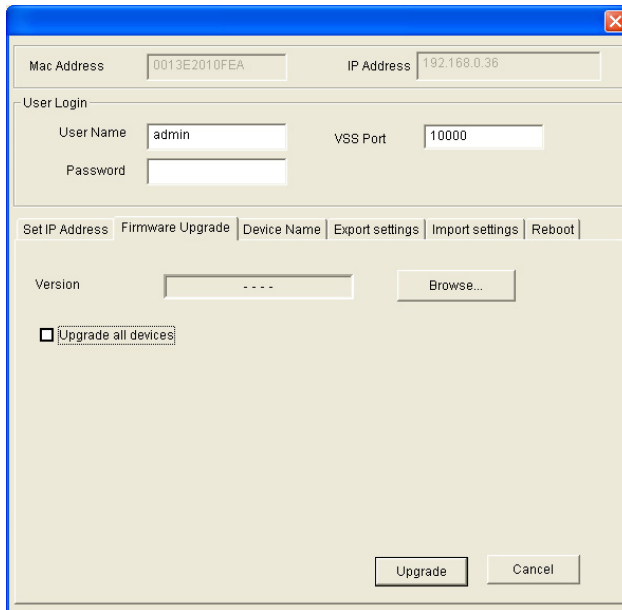


Figure 6-3

5. Click the **Firmware Upgrade** tab. This dialog box appears.



The dialog box is titled "Firmware Upgrade" and has a blue title bar. It contains the following fields and controls:

- Mac Address:** 0013E2010FEA
- IP Address:** 192.168.0.36
- User Login:**
 - User Name:** admin
 - Password:** (empty)
 - VSS Port:** 10000
- Tabs:** Set IP Address | **Firmware Upgrade** | Device Name | Export settings | Import settings | Reboot
- Version:** (empty) with a "Browse..." button next to it.
- ☐ Upgrade all devices
- Buttons:** Upgrade, Cancel

Figure 6-4

6. Click the **Browse** button to locate the firmware file (.img) saved at your local computer.
7. If you like to upgrade all cameras of the same model in the list, check **Upgrade all devices**.
8. Type **Password**, and click **Upgrade** to process the upgrade.

6.2 Backing Up and Restoring Settings

With the IP Device Utility included on the Software DVD, you can back up the configurations in the camera, and restore the backup data to the current unit or import it to another unit.

6.2.1 Backing Up the Settings

1. Run **IP Device Utility** and locate the desired camera. See Steps 1-3 in *6.1.2 Using the IP Device Utility*.
2. Double-click the camera in the list. Figure 6-3 appears.
3. Click the **Export Settings** button. This dialog box appears.

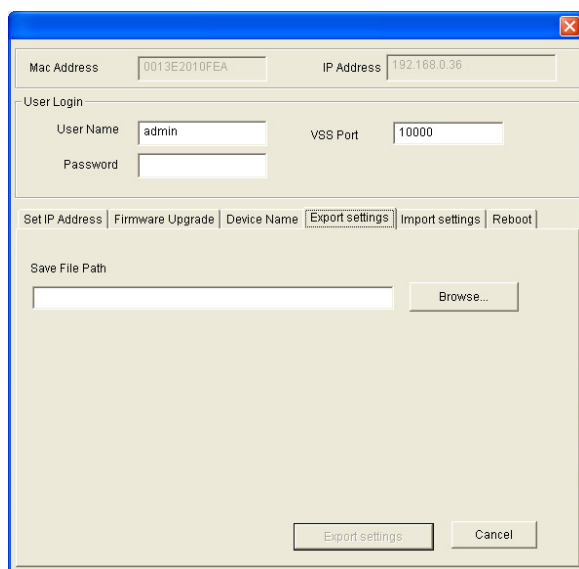
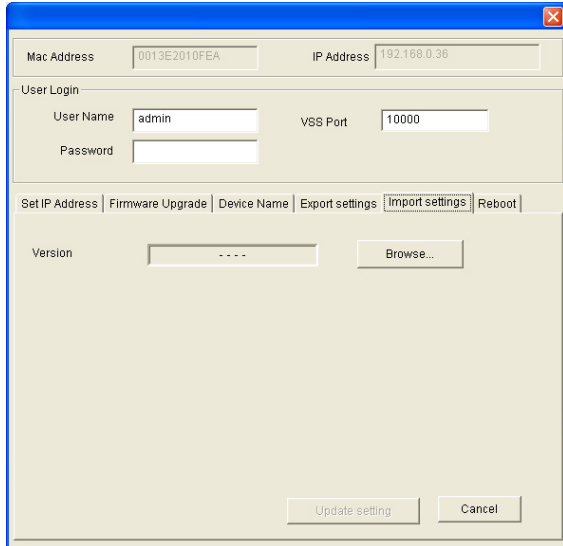


Figure 6-5

4. Click the **Browse** button to assign a file path.
5. Type **Password**, and click **Export Settings** to save the backup file.

6.2.2 Restoring the Settings

1. In Figure 6-3, click the **Import Settings** tab. This dialog box appears.



The dialog box titled "Import Settings" contains the following fields and controls:

- Mac Address: 0013E2010FEA
- IP Address: 192.168.0.36
- User Login section:
 - User Name: admin
 - Password: (empty)
 - VSS Port: 10000
- Tabbed interface with the following tabs: Set IP Address, Firmware Upgrade, Device Name, Export settings, **Import settings** (selected), and Reboot.
- Version: (empty) with a "Browse..." button.
- Buttons at the bottom: "Update setting" and "Cancel".

Figure 6-6

2. Click the **Browse** button to locate the backup file (.dat).
3. Click the **Update Settings** button to start restoring.

6.3 Restoring to Factory Default Settings

You can restore the camera to factory default settings using the Web interface or directly on the camera.

To restore to default settings using the Web interface:

1. In the left menu, select **Management** and select **Tools**.
2. Under the **System Settings** section, click the **Load Default** button.

To restore to default settings directly on the camera:

1. Unplug the power cable and the network cable.
2. To access the **Load default** button, first remove the outer shell of the camera. Refer to *1.6 Physical Description* for details.
3. Use a pointy object such as the tip of a pen to hold down the **Load default** button (No. 3, Figure 1-2) while plugging the power cable and the network cable.
4. Wait until the network status LED turns off momentarily to release the **Load default** button. This may take about 40 seconds.
5. The system status LED should turn back on.

6.4 Verifying Watermark

The watermark is an encrypted and digital signature embedded in the video stream during the compression stage, protecting the video from the moment of its creation. Watermarking ensures that an image is not edited or damaged after it is recorded. To enable the watermark function, see [Watermark], *4.1.1 Video Settings*.

The **Watermark Proof** is a watermark-checking program. It can verify the authenticity of the recording before you present it in court.

6.4.1 Accessing AVI Files

To verify watermark, first you have to access the recorded AVI files by one of these methods:

1. Use the **File Save** function on the Live View window (Figure 3-3) to start recording on the local computer.
2. Use the **Act as FTP Server** function to download AVI files from the camera. See *4.3.2 FTP*.
3. Use the files recorded on the memory card. Since the files saved on the memory card are of Linux file system, remember to run **IFS Drives** from the Software DVD to convert the Linux-based files to Windows-based files. For the instructions, see Steps 1 to 2 in *5.2.1 Playback Using the Memory Card*.

6.4.2 Running Watermark Proof

1. Install **Watermark Proof** from the Software DVD. After installation, a **WMProof** icon is created on your desktop.
2. Double-click the created icon. The Water Mark Proof window appears.
3. Click **File** from the menu bar, select **Open** and locate the recording (.avi). The selected recording is then listed on the window. Alternatively, you can drag the recording directly from the storage folder to the window.
4. If the recording is unmodified, a check will appear in the **Pass** column. On the contrary, if the recording is modified or does not contain watermark during recording, a check mark will appear in the **Failed** column. To review the recording, double-click the listed file on the window.

6.4.3 The Watermark Proof Window

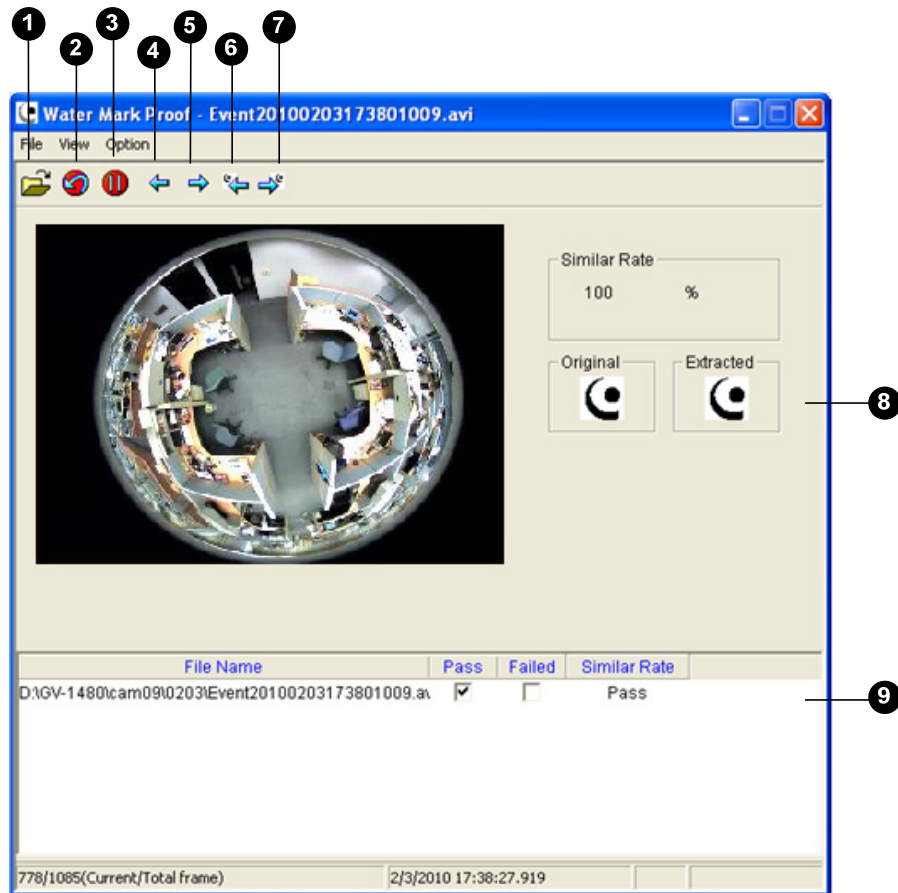


Figure 6-8

The controls in the window:

No.	Name	Description
1	Open File	Opens the recorded file.
2	First Frame	Goes to the first frame of the file.
3	Play	Plays the file.
4	Previous Frame	Goes to the previous frame of the file.
5	Next Frame	Goes to the next frame of the file.
6	Previous Watermarked Frame	Goes to the previous frame that contains watermark.
7	Next Watermarked Frame	Goes to the next frame that contains watermark.
8	Original vs. Extracted	The Extracted icon should be identical to the Original icon. If not, it indicates the recording has been tampered with.
9	File List	Displays the proof results.

Chapter 7 DVR Configurations

The GV-System provides hybrid solution, integrating the digital videos from IP cameras with other analog videos. For digital videos, the GV-System provides complete video management, such as video viewing, recording, playback, alert settings and almost every feature of the system. The integration specifications are listed below:

- GV-System version 8.4 or later is required (For GV-FE421, GV-System version 8.4 and an additional patch file are required).
- The maximum number of connections to the fisheye camera is 7 for GV-FE111 and 5 for GV-FE421. When one GV-System connects to one fisheye camera, it takes up 2 connections. When one user connects to the fisheye camera via browser, it takes up 1 connection. When users operate the **Camera/Audio Control** on Center V2 to connect the fisheye camera, it takes up 1 connection.

	GV-FE111	GV-FE421
Maximum number of connections	7	5
Connection from one GV-System	Takes up 2 connections	
One connection to Web interface	Takes up 1 connection	
Connection from one Center V2	Takes up 1 connection	

- When connecting from the GV-System, GV-FE421 is only supported on 64-bit operating systems.
- The hardware compression and the “Pre-Recording Using RAM” feature cannot work on the videos from the fisheye camera.

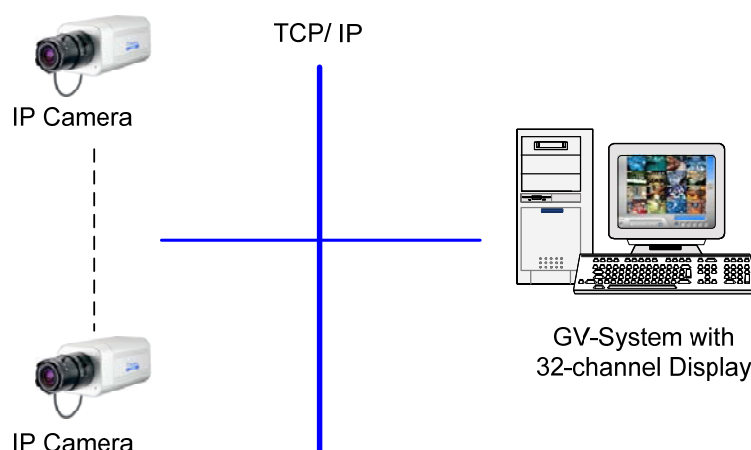


Figure 7-1

3. Type the IP address, username and password of the camera. Modify the default HTTP port if necessary. Select **GeoVision** from the **Brand** drop-down list and select **GeoVision_GV-FE111** or **GeoVision_GV-FE421** from the **Device** drop-down list. This dialog box appears.

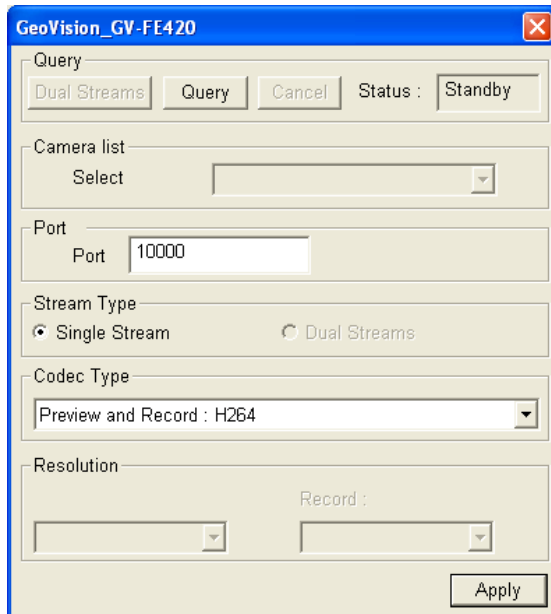


Figure 7-4

4. Click **Query** to acquire the information from the IP camera. You can change the video streaming port number if needed.
5. Click **Apply**. The IP camera is added to the connection list.
6. Click the listed camera and select **Display position** to map the IP camera to a channel on the GV-System.

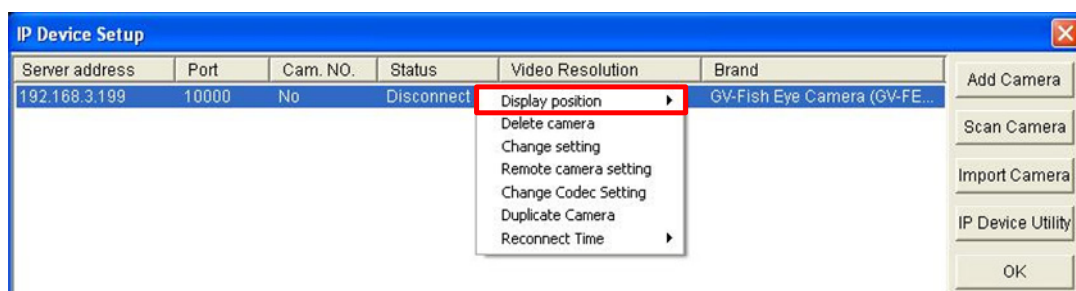


Figure 7-5

7. The Statue column should display "Connected". Click **OK**.

7.1.1 Previewing Video and Setting Audio

To preview video and activate audio, click the desired camera (see Figure 7-5) on the connection list and select **Preview & Audio Setting**. This dialog box appears.

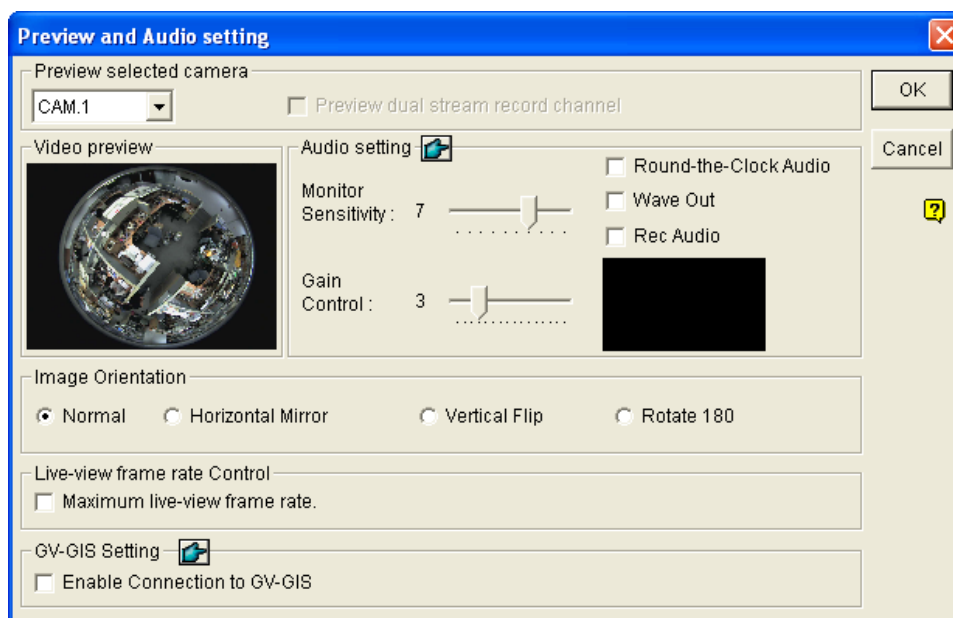


Figure 7-6

[Preview selected camera]

- **Drop-down List:** Select the desired camera for live preview.

[Audio Setting]

- **Monitor Sensitivity:** Adjust the sensitivity of the audio that will be detected. The higher the value, the more sensitive the system is to the surrounding sound.
- **Gain Control:** Increase or decrease the gain of the microphone.
- **Round-the-Clock Audio:** Enables round-the-clock audio recording. The **Rec Audio** option must also be selected to enable this function.
- **Wave Out:** Select this option to listen to live audio from the camera.
- **Rec Audio:** Select this option to activate the audio recording.

[Image Orientation] You can adjust the image orientation of the camera according to your preference.

- **Normal:** Select to view the camera image as it is.
- **Horizontal Mirror:** Select to view the mirror image of the camera image.

- **Vertical Flip:** Select to view the camera image flipped vertically.
- **Rotate 180:** Select to view the camera image rotated by 180 degrees.

[Live-view Frame Rate Control] Set the frame rate of live view to reduce the CPU usage.

- **Maximum live-view frame rate:** This option is available when the recording codec of the IP camera is set to JPEG. Select the frame rate of live view from 1 to 15 fps.
- **Live-view key frame only:** This option is available when the recording codec of the IP camera is set to MPEG4 or H.264. Select this option to see the video of key frames only on the live view to reduce the CPU usage. This option is related to the GOP setting of the IP camera. For example, if the GOP value is set to 30, there is only one key frame among 30 frames. For the GOP setting, see *4.1.2 Video Settings*.

[GV-GIS Setting]

Receive the GPS data from the IP device. To receive the GPS data, remember to also enable the GIS function of the GV-System (Configure button < Accessories < Enable Local GIS).

7.2 Remote Monitoring with Multi View

You can use the Multi View to monitor and manage the camera.

7.2.1 Connecting to the IP Camera

1. On the Multi View window, click the **Edit Host** button. The Edit Host window appears.
2. To create a host, click the **New** button. You need to create a group before creating a host.
3. Select **GV-IP Camera**, **GV-IP Speed Dome** from the Device drop-down list. Type the host name, IP address, user name and password of the camera. Modify the default VSS port **10000** if necessary.

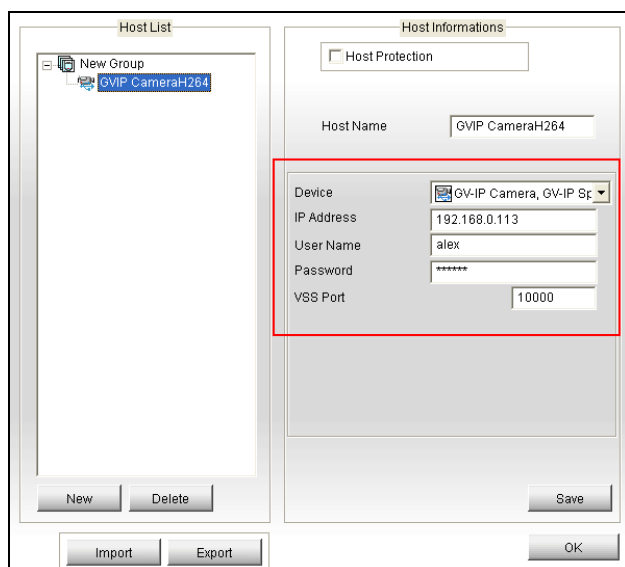


Figure 7-7

4. Click **Save** to establish connection.

For details on the Multi View functions, see “Multi View Viewer”, *Remote Viewing*, *DVR User’s Manual* on the Surveillance System Software DVD.

7.3 Remote Monitoring with E-Map

You can use the Remote E-Map to monitor and manage the camera.

7.3.1 Creating an E-Map for the IP Camera

With the E-Map Editor, you can create an E-Map for the camera. The E-Map Editor is available in the two applications: Main System and E-Map Server. The following is an example of running the E-Map Editor included in the Main System.

1. Go to Windows **Start** menu, point to **Programs**, select **GV folder** and click **E-Map Editor**.
2. To create an E-Map, click the **Add Map** button on the toolbar. A New Map file appears.
3. Double-click the New Map file, and click the **Load Map** button on the toolbar to import a graphic file.
3. To create a host, click the **Add Host** button on the toolbar and select **Add Camera**.
4. Right-click the created New Host in the Host View, and select **Host Settings**. This dialog box appears.

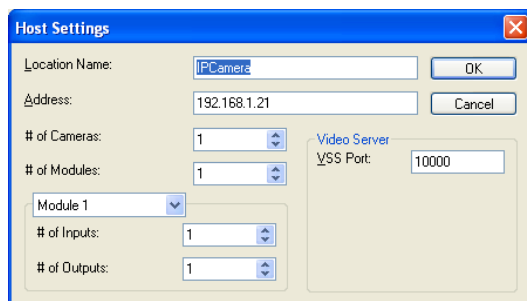


Figure 7-8

4. Give the camera a location name, and type its IP address (or domain name). Modify the default VSS port **10000** if necessary.
5. Click **OK** to save the settings.
6. Expand the created host folder. Drag and drop the icons of cameras and I/O devices onto the imported E-Map.
7. Close the E-Map Editor. Click **Yes** when you are promoted to save the file.

For details on creating an E-Map file on the E-Map Server, see “E-Map Server”, *E-Map Application, DVR User’s Manual* on the Surveillance System Software DVD.

7.3.2 Connecting to the IP Camera

Depending on where you save the created E-Map file (DVR, E-Map Server or Control Center), the steps to open the Remote E-Map window for monitoring may vary slightly. The following is the connection example when you store the E-Map file on the DVR.

1. To enable the remote access to the DVR, click the **Network** button, select **WebCam Server** to display the Server Setup dialog box, and click **OK** to start the WebCam server.
2. At the local computer, open the web browser and type the address of the DVR. The Single View page appears.
3. Select **Emap**. A valid user name and password are required for login. For the first-time user, you will be directed to the Download page. Install the E-Map program before you can run it.
4. On the Remote E-Map window, click the **Login** button and select the camera host to access its videos and I/O devices. A valid user name and password are required to log in the camera.

For details on the Remote E-Map functions, see “The Remote E-Map Window”, *E-Map Application*, *DVR User’s Manual* on the Surveillance System Software DVD.

Chapter 8 CMS Configurations

This section introduces settings on connecting the camera in the central monitoring stations Center V2, VSM and Dispatch Server.

8.1 Center V2

The Center V2 can monitor and manage the camera and I/O devices connected to the camera.

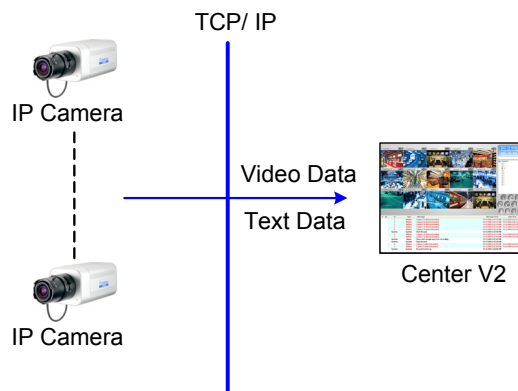


Figure 8-1

- To set the appropriate port connecting to the IP camera, click the **Preference Settings** button, select **System Configure**, click the **Network** tab, and check **Accept connections from GV-Compact DVR, Video Server & IP Cam**. Keep the default port 5551 for the Port 2 option, or modify it to match the Center V2 port on the camera.

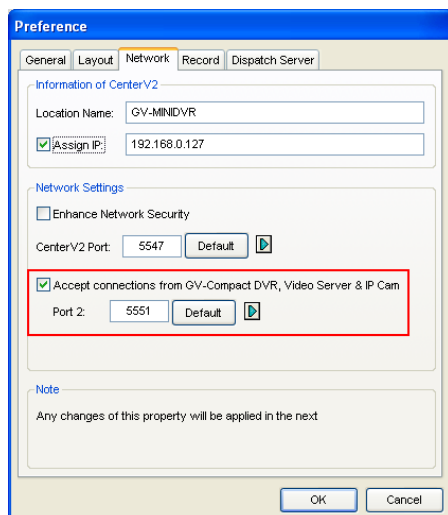


Figure 8-2

- To define how to display the received video on motion detection and input trigger from the camera, click the **Preference Setting** button and select **System Configure**. This dialog box appears.

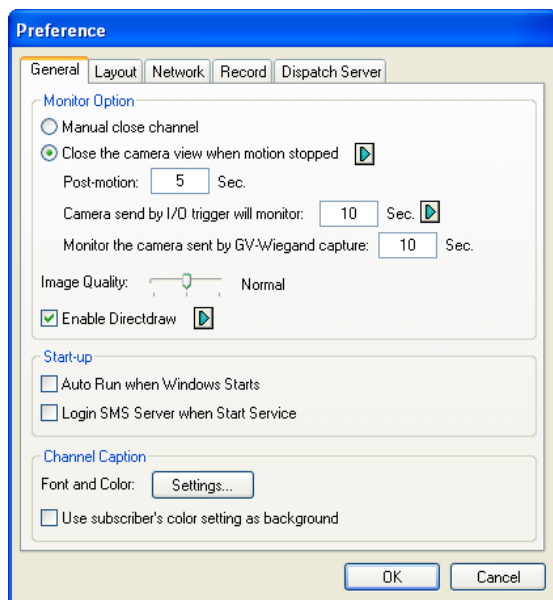


Figure 8-3

- **Manual close channel:** Closes the triggered camera view manually.
- **Close the camera view when motion stopped:** Closes the triggered camera view automatically when motion stops.
- **Post Motion:** Specify the duration of the camera view remaining on the monitoring window after motion stops.
- **Camera send by I/O trigger will monitor:** Specify the duration of the camera view remaining on the monitoring window when an I/O device is triggered.

To keep the camera view remaining on the monitoring window even after the alarm is finished, click the right-arrow button, and uncheck **Latch Trigger**. Then the camera view will keep remaining on the monitoring window for the specified time. For example, the alarm is triggered for 5 minutes and you set 10 minutes, which means the total display time will be 15 minutes.

For further information on how to manage the video received from the camera, see *GV-CMS Series User's manual*.

8.2 VSM

The VSM can monitor and manage the camera and I/O devices connected to the camera.

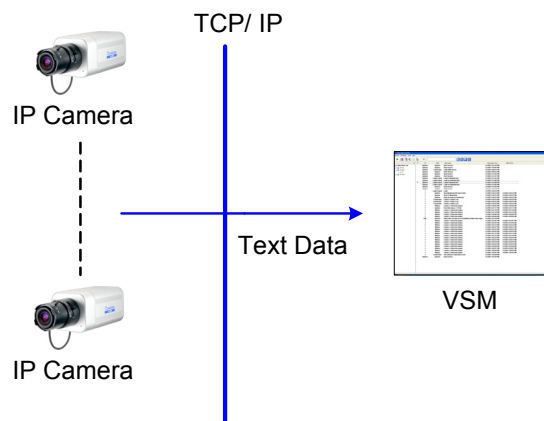


Figure 8-4

To set the appropriate port connecting to the camera, click **Configure** on the window menu, and select **System Configure** to display this dialog box. In the **Connective Port** field, keep the default value **5609** for the Port 2 option, or modify it to match the VSM port on the camera.

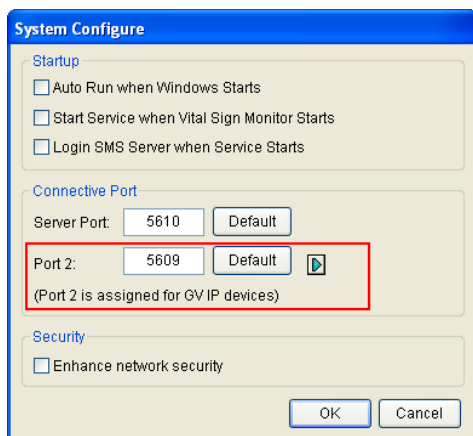


Figure 8-5

For further information on how to manage the video received from the camera, see *GV-CMS Series User's manual*.

8.3 Dispatch Server

The Dispatch Server can manage the camera and I/O devices connected to the camera, and distribute them to the Center V2.

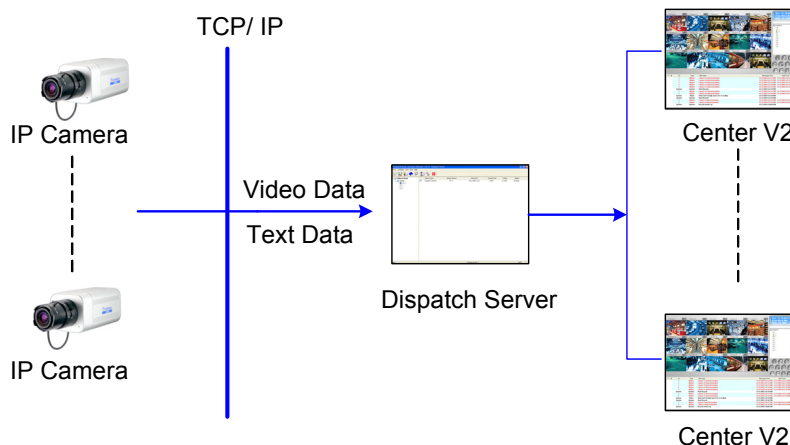


Figure 8-6

To enable connecting to the camera, click the **Server Setting** button on the toolbar, and enable **Allow GV IP devices to login as subscriber from port**. Keep the default port **5551**, or modify it to match the Center V2 port on the camera.

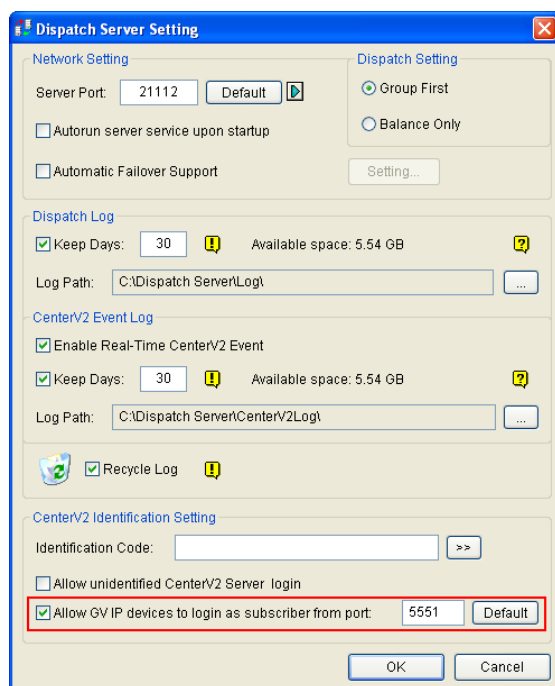


Figure 8-7

For further information on how to manage the video received from the camera, see *GV-CMS Series User's manual*.

Specifications

Camera

Image Sensor	GV-FE111	1/3" progressive scan CMOS	
	GV-FE421	1/2.5" progressive scan CMOS	
Picture Elements	GV-FE111	1280 (H) x 1024 (V)	
	GV-FE421	2048 (H) x 1944 (V)	
Minimum Illumination	GV-FE111	1.5 Lux (1/60 sec), 0.1 Lux (1/5 sec), (30 IRE, F/2.0, AGC-ON, slow shutter-Off.)	
	GV-FE421	Color	4 Lux (1/30 sec), 2 Lux (1/5 sec)
		B/W	
Shutter Speed	GV-FE111	Automatic (Balanced, Speed Priority, Quality Priority), (1/5 ~ 1/4000 sec)	
	GV-FE421	Automatic, Manual (1/5 ~ 1/8000 sec)	
White Balance	GV-FE111	Automatic, Manual (2800K ~ 8500K)	
	GV-FE421	Automatic, Manual (2800K ~ 8500K)	

Note: Although the GV-FE421 supports day/night function, it is not equipped with an IR-cut filter and therefore cannot work with infrared illuminators.

Optics Lens

Megapixel		Yes
Iris		Fixed Iris
Focal Length	GV-FE111	1.25 mm
	GV-FE421	1.27 mm
Aperture	GV-FE111	F/2.0
	GV-FE421	F/2.8
Mount		M12, Pitch 0.5 mm

Specifications

Image Format		GV-FE111	1/3”
		GV-FE421	1/2"
Angle of View	Diagonal	GV-FE111	185°
		GV-FE421	180°
	Horizontal	GV-FE111	185°
		GV-FE421	180°
	Vertical	GV-FE111	185°
		GV-FE421	180°
Operation		Focus	None
		Zoom	None
		Iris	Fixed

Operation

Video Codec	GV-FE111	H.264, MPEG4, MJPEG
	GV-FE421	H.264, MJPEG
Video Resolution	GV-FE111	1280 x 1024
	GV-FE421	2048 x 1944
Frame Rate		15 fps
Image Setting		Brightness, Contrast, Sharpness, Gamma, White Balance, Flicker-less, Image Orientation
Audio Codec		G.711
Digital Input		1 Input (Dry Contact)
Digital Output		1 Output

Network

Interface	10/100 Ethernet
Protocol	HTTP, TCP, UDP, SMTP, FTP, DHCP, NTP, UPnP, DynDNS, RTSP, PSIA

Mechanical

Connectors	Power	Terminal block (3 pin)
	Ethernet	Ethernet (10/100 Base-T), RJ-45 Connector
	Audio	Built-in microphone and speaker
	Digital I/O	I/O Wire
	Auto Iris	None
	Local Storage	Micro SD/SDHC memory card slot
	TV-Out	None

General

Operating Temperature		0°C ~ 50°C / 32 °F ~ 122 °F
Humidity		10% to 90% (no condensation)
Power Source		12V DC / 24V AC / PoE (IEEE802.3af)
Power Consumption	GV-FE111	7.2 W (max. 600mA at 12V DC)
	GV-FE421	4.1 W (max. 335mA at 12V DC)
Regulatory		CE, FCC, C-Tick, RoHS compliant
Dimension (Diameter x Height)		Ø 160 x 47.66 mm / 6.29 x 1.83 in
Weight		650 g / 1.43 lb

Power over Ethernet

PoE Standard	IEEE 802.3af Power over Ethernet / PSE
PoE Power Supply Type	End-Span
PoE Power Output	Per Port 48V DC, 350mA. Max. 15.4 watts

Web Interface

Installation Management	Web-based configuration
Maintenance	Firmware upgrade through Web Browser or Utility
Access from Web Browser	Camera live view, video recording, change video quality, bandwidth control, image snapshot, digital I/O control, audio, picture in picture, picture and picture, motion detection, privacy mask, visual automation, tampering alarm, auto pan function, virtual PTZ
Language	Czech / Danish / English / French / German / Hebrew / Hungarian / Italian / Japanese / Polish / Portuguese / Russian / Serbian / Simplified Chinese / Spanish / Traditional Chinese

Application

Network Storage	GV-NVR, GV-System
Live Viewing	IE
CMS Server Support	GV-Control Center, GV-Center V2, GV-VSM

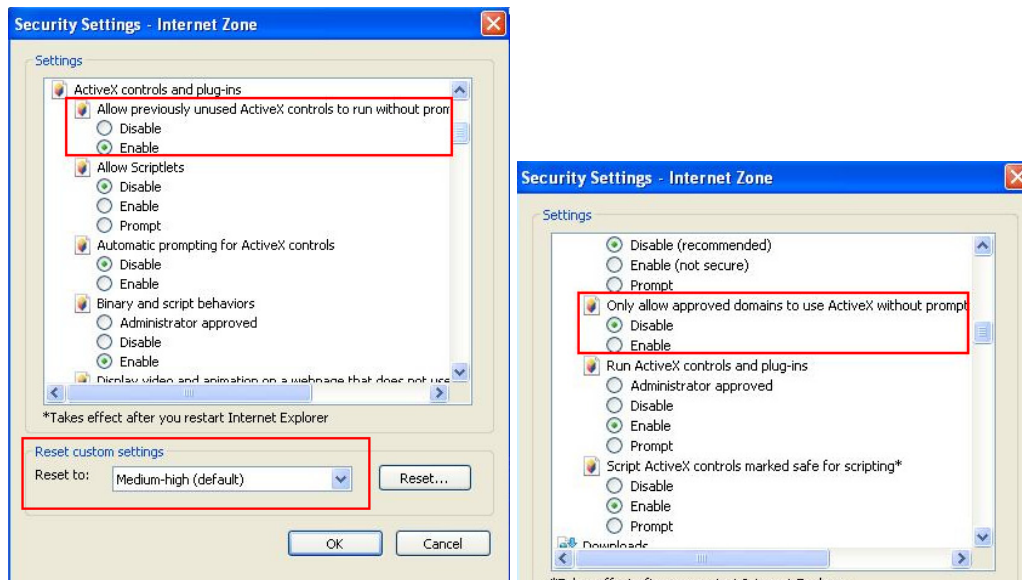
Note: All specifications are subject to change without notice.

Appendix

A. Settings for Internet Explore 8

If you use Internet Explorer 8, it is required to complete the following setting.

1. Set the Security to **Medium-high (default)**.
2. Enable **Allow previously unused ActiveX controls to run without prompt**.
3. Disable **Only allow approved domains to use ActiveX without prompt**.



B. RTSP Protocol Support

The fisheye camera can support RTSP protocol for video streaming.

For the RTSP command, enter:

rtsp://<IP of the fisheye camera>:8554/<CH No.>.sdp

For example, rtsp://192.168.3.111:8554/CH001.sdp

Note:

1. The RTSP streaming provides source video images only.
 2. The RTSP server must be enabled on the Web interface. See [4.3.6 RTSP](#).
-