GeoVision Inc.
The Vision of Security

GV-IP Camera

Firmware Manual

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

ICH265-FW-B

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. Note: no memory card slot or local storage function for Argentina.

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

December 2019

Contents

Notice

The GV-IPCAM has a variety of models designed to meet different needs. **The features described in the manual vary among camera models and versions. Some features may not be available in your camera.**

Note:

1. To upgrade the camera firmware from V2.07 or earlier to the latest version, back up the files in the camera's storage device first before upgrading and it is required to reformat the memory card after the upgrade.
2. The following models are not supported by firmware V3.10 or later:
   - GV-BX120D / 130D / 140DW / 220D / 320D / 520D
   - GV-CB120 / 220
   - GV-CBW120 / 220
   - Models installed with a 32 MB NAND flash

Creating GV-IP Camera's Login Credentials

The default **Administrator** and **Guest** accounts are not supported by **GV-IPCAM H.265 Firmware V1.14 or later**. When purchasing new cameras or after resetting them, you need to set up a login username and password for the cameras.

1 Download and install GV-IP Device Utility from the company website.

2 On the GV-IP Device Utility window, click to search for your GV-IP camera.

3 Double-click your GV-IP camera in the GV-IP Device Utility list. This dialog box appears.

4 Click the **Change Password** tab to type a new username and password. Note that the new password must meet the password strength requirements.

5 Optionally, click **Upgrade all devices** to use the same username and password on all other devices of the same model.

Note for Connecting to GV-DVR / NVR / VMS

The GV-IPCAM is designed to work with GV-DVR / NVR / VMS, a video management system. Note the following when the camera is connected to GV-DVR / NVR / VMS:

1. By default, the images are recorded to the memory card inserted in the **GV-IPCAM** (except for GV-IR Arctic Box Camera, which is not equipped with a memory card slot).
2. Once the camera is connected to the GV-DVR / NVR / VMS, the resolution set on the GV-DVR / NVR / VMS will override the resolution set on the camera's Web interface. You can only change the resolution settings through the Web interface when the connection to the GV-DVR / NVR / VMS is interrupted.

Note for Recording

1 By default, the images are recorded to the memory card inserted in the **GV-IP Camera** (except for GV-IR Arctic Box Camera, which is not equipped with a memory card slot). Make sure the **Write recording data into local storage** option (see *3.1.1 Video Settings*) is enabled. If this option is disabled, the camera will stop recording to the memory card while the live view is accessed through Web browsers or other applications.

2 Mind the following when using a memory card for recording:

- Recorded data on the memory card can be damaged or lost if the data are accessed while the camera is under physical shock, power interruption, memory card detachment or when the memory card reaches the end of its lifespan. No guarantee is provided for such causes.
- The stored data can be lost if the memory card is not accessed for a long period of time. Back up your data periodically if you seldom access the memory card.
- Memory cards are expendable and their durability varies according to the conditions of the installed site and how they are used. Back up your data regularly and replace the memory card annually.
- Replace the memory card when its read/write speed is lower than 6 MB/s or when the memory card is frequently undetected by the camera.

3 It is recommended to use memory cards of the following setting and specifications:

- Apply a battery backup (UPS) to avoid power outage.
- Use Micro SD card of MLC NAND flash, Class 10 for better performance.

Note for GV-EVD5100 / EFD5101 / EBL5101

When the resolution is set at 2592 x 1944:

1 If the camera is switched to single stream (while stream two is deselected) and Noise Reduction is disabled, the frame rate can reach up to 30 FPS.

2 If the camera is switched to dual streams and Noise Reduction is disabled, the frame rate can reach up to 25 FPS.

3 As long as Noise Reduction is enabled, whether the camera is switched to single stream or dual streams, the frame rate will be 15 FPS.

Chapter 1 Introduction

The GV-IPCAM series offers a comprehensive range of IP cameras for IP surveillance in various environmental conditions.

1.1 System Requirement

To perform the cameras' operations through Web browser, ensure your PC is in good network connection, and use one of the following Web browsers:

- Microsoft Internet Explorer 8.0 or later
- Google Chrome
- Mozilla Firefox
- Safari

Note:

1 For users of **Internet Explorer 8**, additional settings are required. For details, see *Appendix A*.

2 With non-IE browsers,

A. Motion Detection, Tampering Alarm, Visual Automation, Text Overlay and two-way audio are not supported.

B. only the Play function is available on the live view window (Figure 19-3)

C. RTSP streaming must be kept as enabled. For more details, see *3.3.8 RTSP*.

To access GV-BX12201 images, the following PC specs should be met:

CPU	Intel Core i5-4670, 3.40 GHz
Memory	DDR3 8 GB RAM
On Board Graphics	Intel HD Graphics 4600 (Versions of driver from year 2014 or later required)

Chapter 2 Getting Started

This section provides the basic configurations of the GV-IPCAM.

2.1 Accessing the Live View

When the camera is connected to a network with a DHCP server, it will be automatically assigned with a dynamic IP address. See *2.1.1 Checking the Dynamic IP Address* to look up this IP address.

However, if you do not have a DHCP server on your network, access the camera by its default IP address **192.168.0.10** and see *2.1.2 Configuring the IP Address* for more details.

Note: By default, GV-PTZ010D is assigned with the fixed IP address 192.168.0.10.

2.1.1 Checking the Dynamic IP Address

Follow the steps below to look up the IP address and access the Web interface.

1. Install the GV-IP Device Utility program from the company website.

Note: The PC installed with GV-IP Device Utility must be as the same LAN with the camera you wish to configure.

---

2. On the GV-IP Utility window, click the button to search for the IP devices connected in the same LAN. Click the **Name** or **Mac Address** column to sort.
3. Find the camera with its Mac Address, click on its IP address and select **Web Page**.

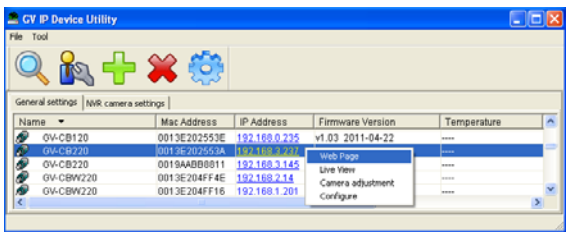


Figure 2-1

4. The login page appears.

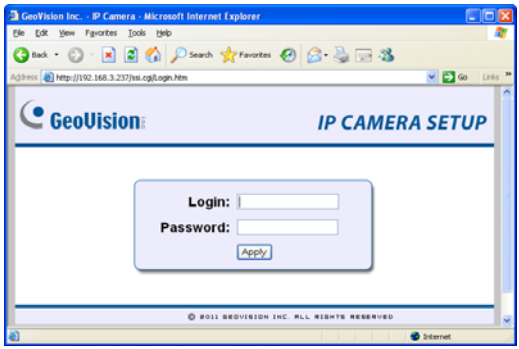


Figure 2-2

5. Type the default ID and password **admin** and click **Apply** to log in.

Note: For **GV-IPCAM H.265 firmware V1.14 or later**, the default Administrator and Guest accounts are no longer supported.

2.1.2 Configuring the IP Address

Follow the steps below to configure the IP address.

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. This page appears.

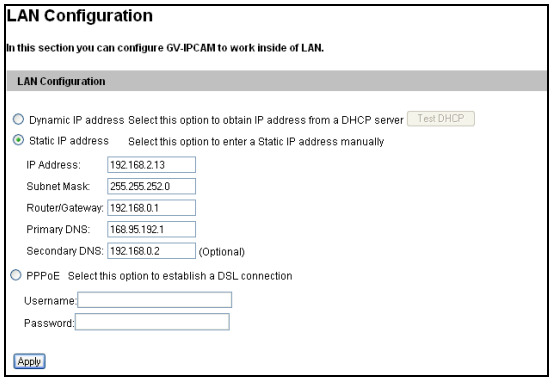


Figure 2-3

4. Select **Dynamic IP address**, **Static IP address** or **PPPoE** and type the required network information.
5. Click **Apply**.

IMPORTANT:

1. If **Dynamic IP Address** or **PPPoE** is enabled, you need to know which IP address the camera will get from DHCP server or ISP to log in. If your camera is installed in the LAN, use the GV-IP Device Utility to look up its current dynamic IP address. See *2.1.1 Checking the Dynamic IP Address*. If your camera uses a public dynamic IP address via PPPoE, use the dynamic DNS Service to obtain a domain name that is linked to the camera's changing IP address first. For details on Dynamic IP Address and PPPoE, see *4.7.1 LAN Configuration* and *4.7.3 Advanced TCP/IP.*
2. If **Dynamic IP Address** or **PPPoE** is enabled and you cannot access the camera, you may have to reset it to the factory default and then perform the network settings again.

   To restore your camera to default settings, see *Loading Factory Default* in the corresponding *Quick Guide.*

2.1.3 Configuring the Wireless Connection

All models supporting wireless connection require GV-WiFi Adaptor except for GV-CAW and GV-CBW models, which come with built-in wireless modules.

1. To set up the wireless LAN for the first time, power on and connect a standard network cable to the camera.
2. An IP address will be automatically assigned to the camera. Use GV IP Device Utility to search for the device. For details, see *2.1.1 Checking the Dynamic IP Address*.
3. Configure the wireless settings.
   A. On the Web interface, select **Network**, select **Wireless** and **Client Mode**. This dialog box appears.

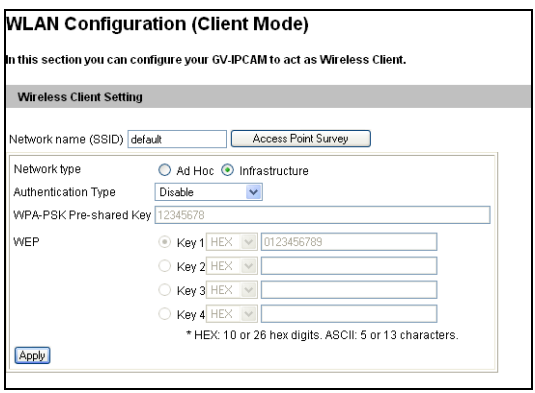


Figure 2-4

   B. Type the Network Name (SSID) or click the **Access Point Survey** button to search and select for the available Access Points/wireless stations.
   C. Select **Ad-Hoc** or **Infrastructure** for the Network type.

D. Select the **Authentication Type** using the drop-down list. You can also obtain this information by clicking the **Access Point Survey** button.

E. Type the **WPA-PSK Pre-shared Key** or **WEP** depending on the encryption setting for the Access Point.

F. Click **Apply** to save the configuration.

Note:

1. Your encryption settings must match those used by the Access Points or wireless stations with which you want to associate.
2. When **Ad Hoc** is used, only **WEP** encryption is supported.
3. When you lose the wireless access, you can still access the unit by connecting it to a LAN and using the GV IP Device Utility to search for the device.
4. For detailed information on configuring the wireless LAN, see *4.7.2 Wireless Client Mode*.

---

4. Enable wireless LAN.
   A. On the Web interface, select **Network** and **LAN**. This page appears.

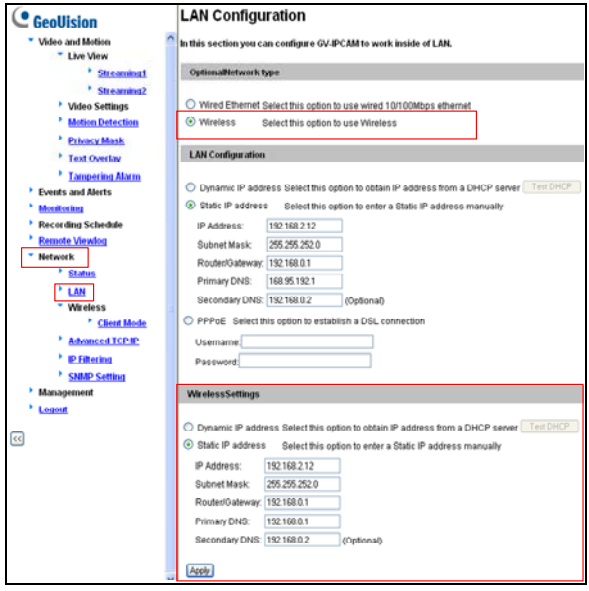


Figure 2-5

   B. Select **Wireless** for Optional Network Type.
   C. To use a dynamic IP address assigned by the DHCP server, select **Dynamic IP address**. To use a fixed IP address, select **Static IP address** and type the IP address information.

5. Click **Apply**. The Camera will start creating a wireless connection to the access point.

Note: For GV-CAW120/220, the LAN LED turns blue when the connection is established.

6. Unplug the Ethernet cable.

2.2 Adjusting Image Clarity

Note the procedures described in this section only apply to the cameras that allow manual focus adjustment. To adjust focus of a PTZ camera, refer to *Focus Adjustment* in corresponding *Quick Guide*; for Cube Camera and Advanced Cube Camera, refer to Camera Adjustment in *3.2.2 The Control Panel on the Live View Window*.

After you have connected your camera to the network, follow the steps below to adjust image clarity.

1. Make sure you have installed the GV-IP Device Utility program from the company website.

Note: The PC installed with GV-IP Device Utility must be under the same LAN with the camera you wish to configure.

---

2. On the GV-IP Utility window, click the button to search for the IP devices connected in the same LAN. Click the IP Address of the camera you desire. A drop-down list appears.

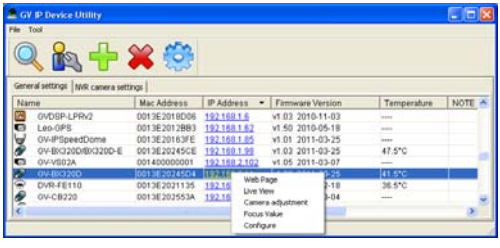


Figure 2-6

3. Select Focus Value. The Login dialog box appears.
4. Type the user name and password of the camera selected. The default is **admin** for both user name and password. This window appears.

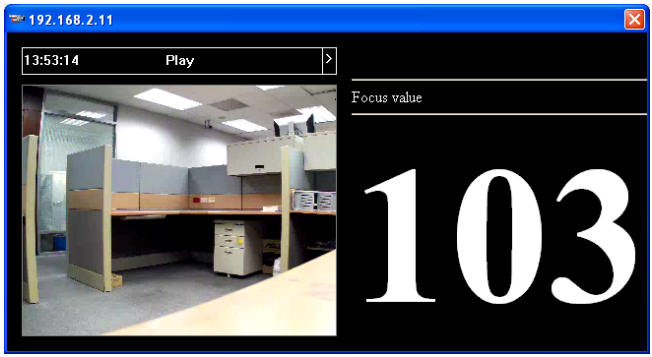


Figure 2-7

5. For IK10+ models **(GV-VD120D / 121D / 220D / 221D / 320D / 321D / 1500 / 2400 / 2500 / 3400 / 1530 / 2430 / 2530 / 3430 / 4711 / 5711**), hold the supplied Focus Adjustment Cap over the camera view. For details, see *2.2.1 Using Focus Adjustment Cap* for details.

6. For **Target Mini Fixed Dome** and **Target Mini Fixed Rugged Dome**, hold the camera cover close to the lens and use the supplied focus adjustment tool for precise focus adjustment.

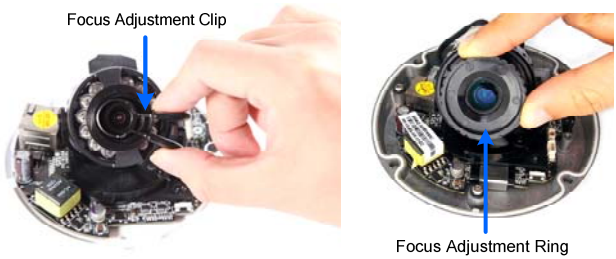


Figure 2-8

7. For **Mini Fixed Dome** and **Mini Fixed Rugged Dome**, hold the camera cover close to the lens for precise focus adjustment. For locations of adjustment screws and rings in each model, see *2.2.2 Locations of Adjustment Screws*.
8. Adjust the Focus Screw and the Zoom Screw of the camera slowly until the focus value reaches the maximum. For example, the maximum focus value in Step 4 is 103. For locations of adjustment screws in each model, see *2.2.2 Locations of Adjustment Screws*.

Note:

1. Do not over tighten the screws. The screws only need to be as tight as your fingers can get them to be. Do not bother using any tool to get them tighter. Doing so can damage the structure of lens.
2. The maximum focus value may vary when the environment changes.

2.2.1 Using Focus Adjustment Cap

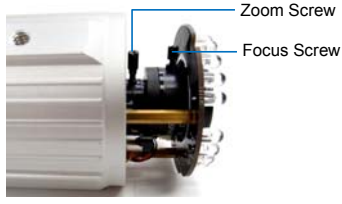
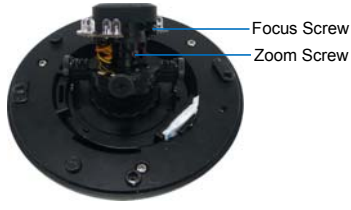
The Focus Adjustment Cap is only supplied for IK10+ models (**GV-VD120D / 121D** / **220D / 221D** / **320D / 321D** / **1500** / **2400 / 2500 / 3400 / 1530 / 2430 / 2530 / 3430 / 4711 / 5711)**.

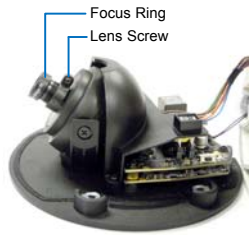
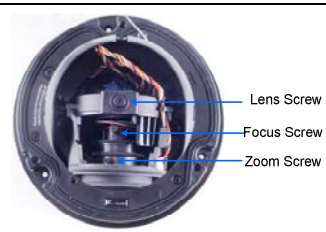
Hold the Focus Adjustment Cap on top of the camera view and keep it close to the camera.

Do not leave a distance between the Focus Adjustment Cap and the camera.

Figure 2-9

2.2.2 Locations of Adjustment Screws

Models	Adjustment Screws
Box Camera	
Bullet Camera	
Vandal Proof IP Dome	
Fixed IP Dome	

Models	Adjustment Screws
GV-MFD3401 / 5301	
GV-MDR320	
GV-MDR1500 / 3400	
GV-VD3700 / 5700	

Note:

1. The adjustment screws of Box Camera may vary for different models.
2. To focus GV-MFD and GV-MDR, loosen the lens screw first and slowly adjust the focus ring. Some models may need a T6 screw driver to loosen the camera lens. If you have a problem of obtaining this type of screw driver, please contact our overseas offices for further assistance.

2.3 Configuring the Basics

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

- **Date and time adjustment:** see *4.8.1 Date & Time Settings*.
- **Login and privileged passwords:** see *4.8.3 User Account*.
- **Network gateway:** see *4.7 Network*.
- **Camera image adjustment:** see *3.2.2 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 on to the GV-IPCAM: **Administrator** and **Guest**. The Administrator has full access to all system configurations, while the Guest can only access the live view (except the Camera Adjustment settings) and network status.

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 your Web browser.
2. Enter the IP address or the domain name of the camera in the **Location/Address** field of your browser.

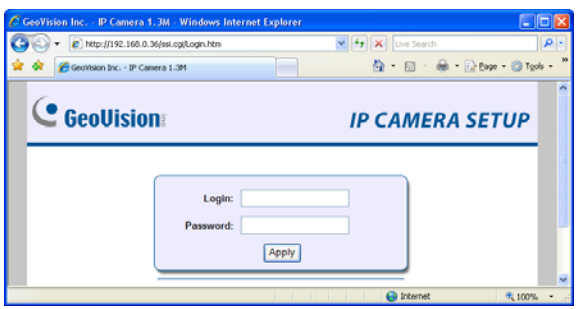


Figure 3-1

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. Click **Apply**. A video image, similar to the example on Figure 3-2, is now displayed in your browser.

Note:

1. To enable the updating of images in Internet Explorer, you must set your browser to allow ActiveX Controls and perform a once-only installation of GeoVision's ActiveX component onto your computer.
2. The default Administrator and Guest accounts are no longer supported by **GV-IPCAM H.265 Firmware V1.14 or later**.

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

Figure 3-2

The GV-IPCAM can process one video stream in two different codec and image settings. In the Administrator mode, both streams are available. Click **Streaming 1** or **Streaming 2** in the left menu to access the live view. In the Guest mode, only one stream is available, as shown in *Figure 3-2*.

3.2.1 The Live View Window

Internet Explorer

When accessing the live view using Internet Explorer, the following window appears.

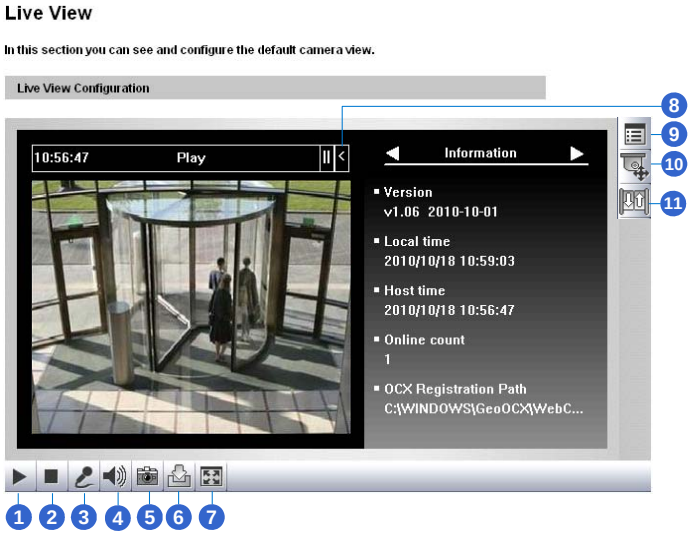


Figure 3-3A

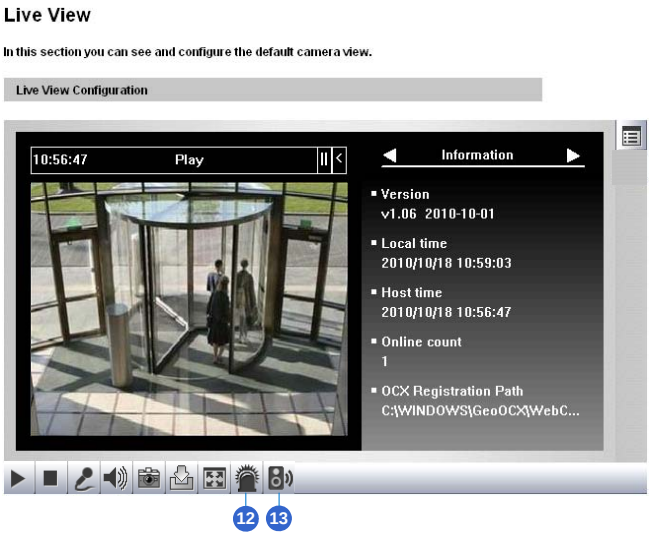

Live View
In this section you can see and configure the default camera view.
Live View Configuration
10:56:47
Play
Information
Version
v1.06 2010-10-01
Local time
2010/10/18 10:59:03
Host time
2010/10/18 10:56:47
Online count
1
OCX Registration Path
C:\WINDOWS\GeoOCX\WebC...
12
13

Figure 3-3B

No.	Name	Function
1	Play	Plays live video.
2	Stop	Stops playing video.
3	Microphone	Broadcasts to the surveillance site from a remote PC. Note this function is not available for **Ultra Bullet Camera** and **Target Series**. For **Cube Camera** and **Advanced Cube Camera**, you can click the **Push to talk** button (from the pop-up menu) for the camera to switch between audio transmission and reception, where only one party can speak at a time.
4	Speaker	Transfers sounds of the surveillance site to a remote PC. Note this function is not available for **Mini Fixed Rugged Dome**, **Ultra Bullet Camera**, **Target Bullet Camera**, and **Target Mini Fixed Rugged Dome**, and **Pinhole Camera.**
5	Snapshot	Takes a snapshot of live video. --- See *3.2.3 Snapshot of Live Video*.
6	File Save	Records live video to the local computer. --- See *3.2.4 Video Recording*.
7	Full Screen	Switches to full screen view. Right-click the image to have these options: Snapshot, Full Screen, Resolution, Zoom In, Zoom Out, PIP and PAP. --- See *3.2.5 Picture-in-Picture and Picture-and-Picture View for PIP and PAP views*

No.	Name	Function
8	Control Panel	Displays the camera information, video settings, audio data rate, I/O device status, images captured upon alarm, and GPS location of the camera. Also allows you to adjust image quality and install the program from the hard drive.
9	Show System Menu	Brings up these functions: Alarm Notify, Video and Audio Configuration, Remote Config, Show Camera Name and Image Enhance. --- See *3.2.6 Alarm Notification*, *3.2.7 Video and Audio Configuration*, *3.2.8 Remote Configuration,* *3.2.9 Camera Name Displa*y, and *3.2.11. Image Enhancement.*
10	PTZ Control Panel	Enables the PTZ Control Panel or the Visual PTZ. Note this function is supported by **PTZ Camera** and **PT Camera**, and only partially supported by **GV-IP Cameras with motorized varifocal lens**. --- See *The PTZ Control Panel* (Hardware Manual) --- See *3.2.11 Visual PTZ*
11	I/O Control	Enables the I/O Control Panel or the Visual Automation. Note this function is only supported by cameras with I/O function. --- See *3.2.13 I/O Control*.
12	LED Control	Click to turn the Alarm LED on and/or adjust the brightness sensitivity. Note this function is only available for **Advanced Cube Camera**.

No.	Name	Function
13	Alarm Speaker	Click to sound the alarm and/or adjust its volume. To sound the alarm upon motion or tampering events, see *4.3.9 Speaker* for setup steps. Note this function is only available for **Advanced Cube Camera**.

Non-IE Browsers

When accessing the live view using Google Chrome, Firefox or Safari, this window appears. Note the following functions are not supported on non-IE browsers: Motion Detection, Tampering Alarm, Visual Automation, Text Overlay and Two-Way Audio.

Note: Non-IE browsers do not support OCX plugin, so the smoothness of the live view is obstructed. For users of non-IE browsers, to enjoy smooth live view, download GV-WebViewer right after you log on and you can also have access to the features of Motion Detection, Tampering Alarm, Visual Automation, Text Overlay and Two-Way Audio.

3.2.2 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 window. You can access the following functions by using the right and left arrow buttons on the control panel.

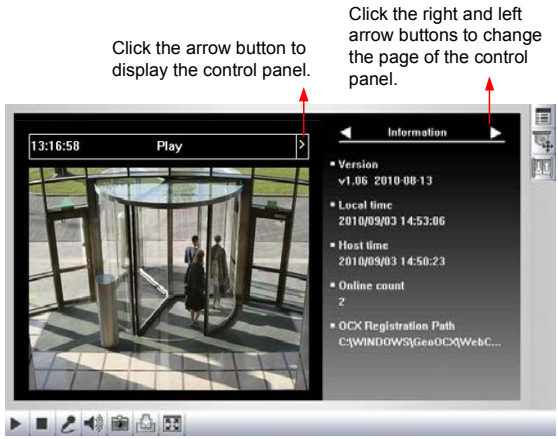


Figure 3-4

[Information] Displays the version of the camera, time of the local computer, time of the camera (host time), the number of users logging in the camera and the OCX registration path.

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

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

[I/O Control] Note this function is only supported by cameras with I/O function. 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 motion detection. For this function to work, you have to configure the Alarm Notification settings first. See *3.2.6 Alarm Notification*.

[Camera Adjustment] Allows you to adjust the image quality settings. Click **Save** to store the changes to the settings. Note that this function is only accessible for Administrator.

- **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 four presets: **Auto**, **Outdoor**, **Fluorescent**, and **Tungsten Lamp**. You can also choose **Manual** to adjust the white balance manually.
- **Color Temperature:** Adjust the camera image to have a warmer or cooler color tone. Note this function is only available for **GV-IPCAM H.265 Firmware V1.14 or later**, and only appears when you choose **Manual** for White Balance.
- **Tint:** Move the slider to remove undesired color cast for a more neutral color. Note this function is only available for **GV-IPCAM H.265 Firmware V1.14 or later**, and only appears when you choose **Manual** for White Balance.
- **Flicker less:** The camera automatically matches the frequency of your camera's image 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.

Note: For GV-IPCAM H.265 firmware V1.14 or later, the function of **Flicker** is listed in *Video Signal Type*, *4.1.1 Video Settings*.

- **Image Orientation:** Changes the image orientation on the Live View window.
- **Slowest Shutter Speed**: Shutter speed controls the amount of the lights enters the image sensor and directly impacts the quality of image presentation. A slow shutter speed allows higher light exposure that creates a brighter overall image by blurring moving objects and bringing out background details, and a faster shutter speed lowers color and image clarity in order to capture motions. The minimum shutter speed ranges from 1/5 to 1/8000 sec. In low light conditions, a fast shutter speed will lower color quality and image clarity. In this case, select the **Auto** option for automatic shutter control or select **Auto (High Speed Mode)** for a faster automatic shutter control.
- **D/N:** Sets the Day/Night mode of the camera. Select **Auto** for automatic switch between day mode and night mode depending on the amount of light detected. Select **Black and white** to switch the camera to night mode. Select **Color** to switch the camera to day mode. Sets the light sensor's sensitivity of switching between day mode and night mode. The value 10 is the most light-sensitive. Select **Trigger by Input** to switch between day mode and night mode once an input device (e.g. sensor or button) is triggered. Select **Schedule** to configure specific period(s) of time when day mode is activated.
- **3D Noise Reduction:** Denoise / Space Domain Strength / Time Domain Strength are all used to reduce the noise of the image depending on the surveillance environment
- **Wide Dynamic Range:** adjusts and generates clear live view when the scene contains very bright and very dark areas at the same time. Select **Auto (Strong)** to bring out details of the dark areas of the

scene, select **Auto (Weak)** to bring out fewer details of the dark areas and at the same time keep the bright areas from overexposure, or select **Auto (Normal)** for a balanced effect. Select **Close** to disable the function.

- **Defog:** Select **Auto** to automatically enhance the visibility of images. Select **Close** to disable the function.
- **Zoom:** Click **Zoom In** and **Zoom Out** to adjust the apparent distance of the scene. After zooming the camera, re-focus the camera manually or automatically. For details, see *Focus Change* and *Focus Mode* below.
- **Focus Change:** Click **Focus In** and **Focus Out** to adjust the focus. To focus automatically, click **Auto Focus**.
- **Focus Mode:** Select **Normal Scan**, **Regional Scan** or **Full Scan** and then click **Start** to automatically adjust the camera focus. The **Normal Scan** mode focuses the camera the fastest. The **Regional Scan** mode focuses the area selected on the live view. The **Full Scan** mode performs a detailed checkup and applies the best focus.
- **Day Night Focus:** Saves focus settings for day mode and night mode. Select **Auto** to automatically focus, or **Close** to disable the function. To configure fixed settings for day mode and night mode, select **Manual** and follow the steps below:
  1. Make sure the **D/N** is in **Auto** mode for the best effect. The following focus setting will be applied to the current D/N mode.
  2. Adjust the focus using **Focus In** and **Focus Out** and/or **Focus Mode**.
  3. Click **Day Mode Save** or **Night Mode Save** depending on the current D/N mode.
- **Metering:** Controls the camera's exposure. Select **Normal** for the camera to adjust exposure based on the full live view. Select **Regional Metering** for the camera to adjust exposure of specified zones. Draw directly on the live view and a block marked with "AE

(automatic exposure)" appears. You can establish up to 4 zones. To remove the block, right-click the block and select **Delete**.

- **Low Lux Enhancement:** Select **Auto** for the camera to automatically enhance the live view under insufficient light, or **Close** to disable the function. The default setting for cameras without Super Low Lux is **Close**. The default setting for cameras with Super Low Lux is **Auto**.
- **IR Light:** Select **Auto** for automatic switch between day mode and night mode depending on the amount of light detected. Select **Off** to completely disable IR LEDs
- **Maximum IR Strength**: Adjusts the intensity of the IR Light.
- **Denoise:** Reduces image noise especially under low-light conditions. The higher the denoise value, the stronger the effect.

Note: For GV-EVD5100, GV-EFD5101 and GV-EBL5101, refer to the description of **Noise Reduction** in *4.1.1 Video Settings.*

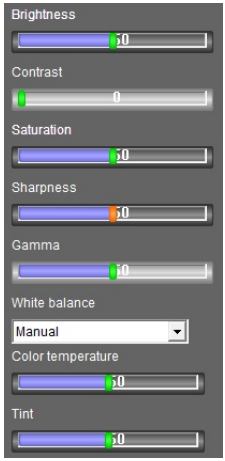


Figure 3-5A

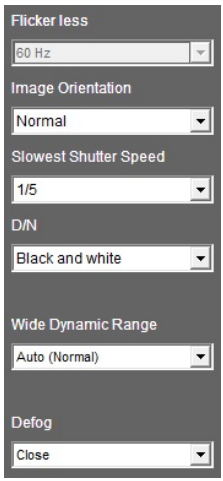


Figure 3-5B

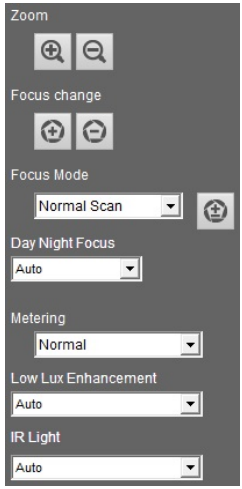


Figure 3-5C

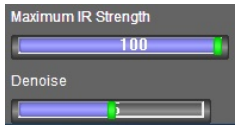


Figure 3-5D

Note:

1. For GV-PTZ010D**, Brightness, Contrast, Saturation**, **Sharpness, D/N**, **Slowest Shutter Speed**, **Wide Dynamic Range** and **Defog** are not available.
2. **Zoom**, **Focus Change**, **Focus Mode** and **Day Night Focus** settings are only available for models with motorized varifocal lens.
3. All **Target Series** support **Denoise** and **Metering;** for other cameras, **Denoise** and **Metering** settings are only available for firmware V2.14 or later.
4. **3D Noise Reduction** are only supported by GV-BX2600-FD / BX2700-FD / BX4700-FD / BX8700 / BX8700-FD / MD8710 / MD8710-FD.
5. **Maximum IR Strength** is not available for GV-BX Series.

3.2.3 Snapshot of 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.

3.2.4 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** slider 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).

3.2.5 Picture-in-Picture and Picture-and-Picture View

The full screen mode provides two types of close-up views: **Picture-in-Picture (PIP)** and **Picture-and Picture (PAP)**. The two views are useful to provide clear and detailed images of the surveillance area.

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 3-6

1. Right-click the live view and select **PIP**. An inset window appears.
2. Click the insert 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 3-7

1. Right-click the live view and 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 add more navigation boxes, to show or hide navigation boxes or to change the frame color of the navigation boxes, right-click the image, select **Mega Pixel Setting** and click one of these options:
   - **Enable Add-Focus-Area Mode:** Allows the user to add more navigation boxes on the image. This option is not available when 7 navigation boxes have been drawn.
   - **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.

3.2.6 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 3-8

To configure this function, click the **Show System Menu** button (No. 9, Figure 3-3), and select **Alarm Notify**. This dialog box appears.

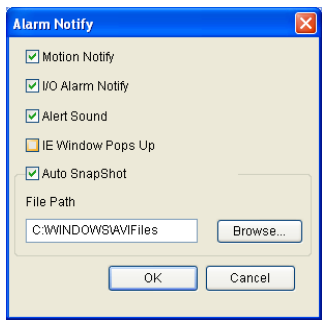


Figure 3-9

- **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 Setting*.
- **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.

3.2.7 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**.

- **Camera:** Sets the number of frames to keep in live view buffer. Keeping more frames for live view buffer can ensure a smooth live view, but the live view will be delayed for the number of frames specified.

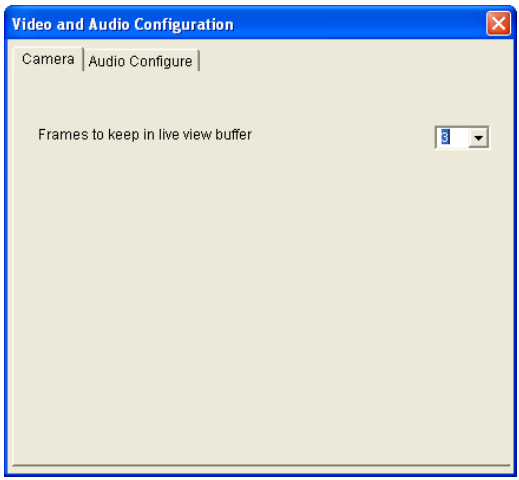


Figure 3-10

- **Audio Configure:** You can enable the microphone and speaker, and adjust the audio volume.

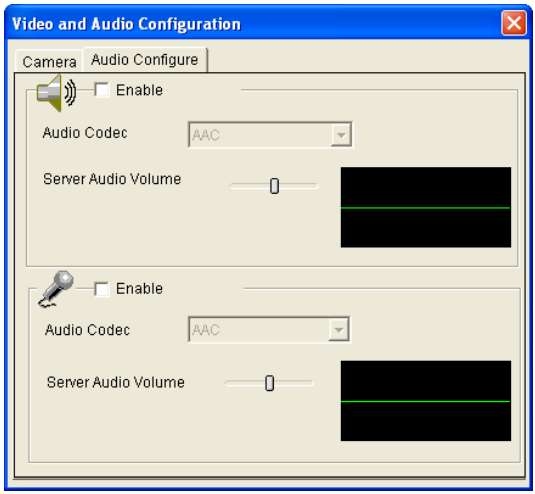


Figure 3-11

3.2.8 Remote Configuration

You can upgrade firmware over the network. 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 Internet. For details, see *Advanced Applications, Chapter 5.*

3.2.9 Camera Name Display

To display the streaming name on the image, click the **Show System Menu** button (No. 9, Figure 3-3), and select **Show Camera Name**. Note this function is not available for GV-VD3700 / 5700.

3.2.10 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.

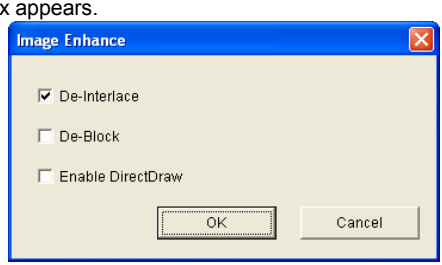


Figure 3-12

- **De-Interlace:** Converts 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.

3.2.11 Visual PTZ

Note this feature is only available in **PTZ Camera** and **PT Camera**.

The Visual PTZ provides two types of PTZ control panels on live images for easy and direct PTZ operation.

Activating Visual PTZ

Click the **PTZ Control** button  (No. 10, Figure 3-3) and select **Visual PTZ**. Alternatively right-click anywhere on the live view and select **Visual PTZ**.

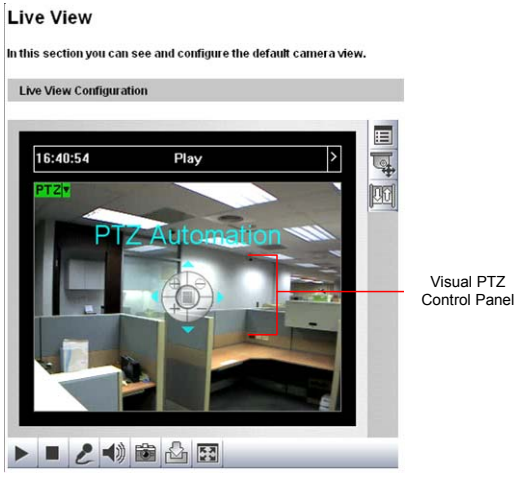


Figure 3-13

Figure 3-14

The Visual PTZ Panel provides the following features:

No.	Name	Description
1	Zoom In	Shortens the apparent distance between the camera and the view.
2	Zoom Out	Lengthens the apparent distance between the camera and the view.
3	Focus In	Adjusts the sharpness of the camera view.
4	Focus Out	
5	Home	Brings the camera to the home point.
6	Auto Focus	Automatically adjusts the sharpness of the camera view.
7	Preset Go	Starts a single movement in which the PTZ Camera moves towards a point in live view.
8	Go Sequence	Starts a series of movements in which the PTZ Camera moves towards at least two Preset points in live view.
9	Auto Pan	Starts a horizontal movement of the PTZ Camera in live view.

Setting Visual PTZ Panel

Click the  .button on the top left corner and select Visual PTZ, the following options will appear.

- **PTZ Control Type:** Two types of visual PTZ control panels are available.
  - ⊙ **Type 1:** Appears only when a movement of the cursor is detected and disappears when it is static. When you place the cursor in one of the eight directions, i.e. up, down, left, right, left up, left down, right up and right down, a 5-level arrow appears. Click and hold onto the required level to move the camera. The speed level is indicated at the top right corner of the live view.
  - ⊙ **Type 2:** Appears with a click on the live view and disappears with the second click. As the cursor points to one of the eight directions, a 5-level arrow head appears. The further the arrow is away from the visual PTZ control panel, the faster the movement and vice versa. The speed level is indicated at the top right corner of the live view.
- **Set Color:** Changes the color of the arrow line and the speed indicated at the top right corner of the live view. Alternatively, you can right-click the live view (with Visual PTZ enabled). Three colors are available: **Red**, **Green** and **Blue**.
- **Transparency:** Changes the transparency level of the Visual PTZ Control Panel. Ten levels range from 10% (fully transparent) to 100% (fully opaque).

3.2.12 Digital PTZ

Note this function is only supported by **GV-IPCAM H.264 firmware V2.06** and the **GV-IPCAM H.265**.

This function allows non-PTZ cameras to simulate PTZ movements on live view.

1. Right-click the live view and select **Digital PTZ**. The live view is labeled with “DPTZ” at the top left corner.

Figure 3-15

2. To zoom in / out, move the cursor to the live view and click the corresponding buttons. To bring the view back to its default image, click **Home**.

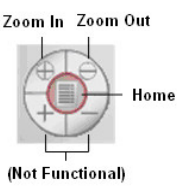


Figure 3-16

3. To pan and tilt the view, zoom the image first and then click and hold the arrow on the image. The arrow appears when you place the cursor in one of the eight directions, i.e. up, down, left, right, left up, left down, right up and right down.

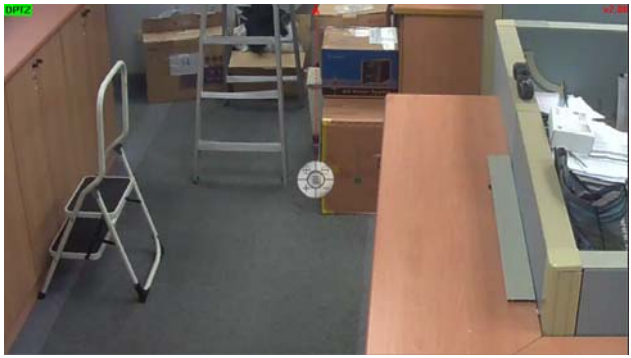


Figure 3-17

4. To adjust the transparency level of the control panel, click the green **DPTZ** button and select **Transparency**. Ten levels range from 10% (fully transparent) to 100% (fully opaque) are available.

Note: The Focus In / Out and the speed level are not functional for Digital PTZ.

3.2.13 I/O Control

Note this function is only supported by cameras with I/O function.

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

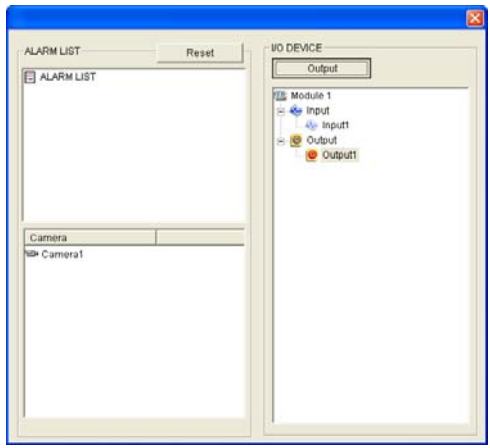


Figure 3-18

- To display the I/O control window, click the **I/O Control** button (No. 11, Figure 3-3) and select **I/O Control**.
- 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.

3.2.14 Visual Automation

Note this function is only supported by cameras with I/O function.

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 *4.1.6 Visual Automation.*

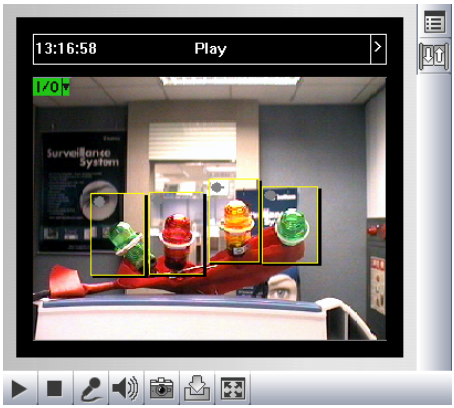


Figure 3-19

- To access this feature, click the **I/O Control** button (No. 11, Figure 3-3) and select **Visual Automation**.
- To change the style of the set areas, click the green **I/O** button on the top left corner. You will have these options:
  - **Show All:** Displays all set areas.
  - **Rect Float:** Embosses all set areas.
  - **Set Color:** Changes the frame color of all set areas

3.2.15 Network Status

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

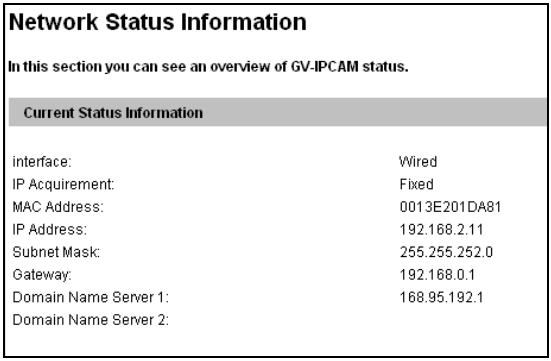


Figure 3-20

Chapter 4 Administrator Mode

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

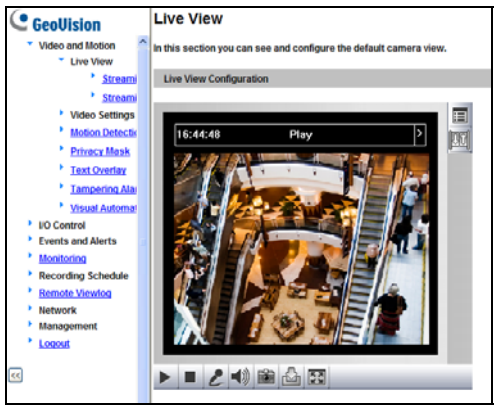


Figure 4-1

List of Menu Options

Find the topic of interest by referring to the corresponding section listed below.

Note: The available options may vary among camera models and firmware versions.

4.1 Video and Motion	4.1.1 Video Settings 4.1.2 Motion Detection 4.1.3 Privacy Mask 4.1.4 Text Overlay 4.1.5 Tampering Alarm 4.1.6 Visual Automation 4.1.7 Face Detection
4.2 Digital I/O and PTZ	4.2.1 Input Settings 4.2.2 Output Settings 4.2.3 PTZ Settings
4.3 Events and Alerts	4.3.1 Email 4.3.2 FTP 4.3.3 Center V2 4.3.4 Vital Sign Monitor 4.3.5 Backup Center 4.3.6 Video Gateway/Recording Server 4.3.7 ViewLog Server 4.3.8 RTSP/ONVIF 4.3.9 Speaker
4.4 Monitoring	
4.5 Recording Schedule	4.5.1 Camera 4.5.2 I/O Monitor
4.6 Remote ViewLog	
4.7 Network	4.7.1 LAN 4.7.2 Wireless-Client Mode 4.7.3 Advanced TCP/IP 4.7.4 HTTPS

	4.7.5 IEEE 802.1x 4.7.6 UMTS Settings 4.7.7 IP Filtering 4.7.8 SNMP Settings
4.8 Management	4.8.1 Date and Time Settings 4.8.2 Storage Settings 4.8.3 User Account 4.8.4 Security 4.8.5 Privacy 4.8.4 Log Information 4.8.5 Tools 4.8.6 Language

4.1 Video and Motion

The GV-IPCAM can simultaneously process one video source in multiple codec and resolutions. The dual / triple-stream design benefits for lower bandwidth environment, allowing Streaming 2 / 3 to be set with lower resolution and codec for live streaming, and Streaming 1 set with higher resolution and H.264 / H.265 for optimal recording quality. **Streaming 1**, **Streaming 2** and **Streaming 3** each have its own setting pages for separate setup.

Comparison between Streaming 1, Streaming 2 and Streaming 3

<table>
<tr><th>Video Setting Options</th><th>Streaming 1</th><th>Streaming 2 / 3</th></tr>
<tr><td>Watermark Setting</td><td rowspan="3">Yes</td><td rowspan="3">Not open for configuration. But settings in Streaming 1 are automatically applied to Streaming 2 / 3</td></tr>
<tr><td>Audio in Source</td></tr>
<tr><td>Special View Setting</td></tr>
<tr><td>Video Resolution</td><td colspan="2">Yes. Different resolutions can be applied to Streaming 1 and Streaming 2 / 3.</td></tr>
<tr><td>Audio Settings</td><td>Yes</td><td>No</td></tr>
<tr><td>TV Out</td><td>Yes</td><td>No</td></tr>
<tr><td colspan="3">Note:
1. Streaming 3 is only supported by GV-IPCAM H.265 firmware V1.14 or later. By default, Streaming 3 is disabled.
2. Audio In Source is only available in GV-PTZ010D.
3. Audio Settings are not available for GV-PTZ010D.
4. TV Out is only available for Box Camera, IR Arctic Box Camera, Vandal Proof IP Dome and Fixed IP Dome.</td></tr>
</table>

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

4.1.1 Video Settings

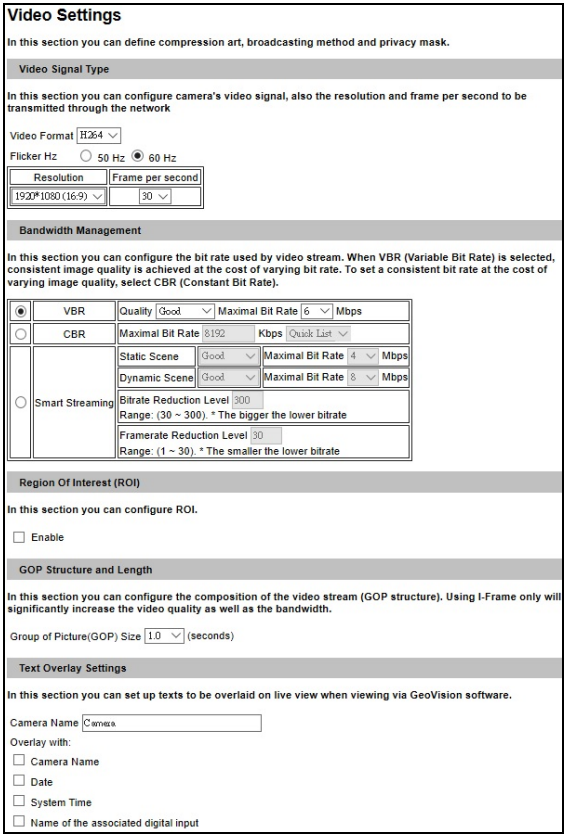


Figure 4-2A

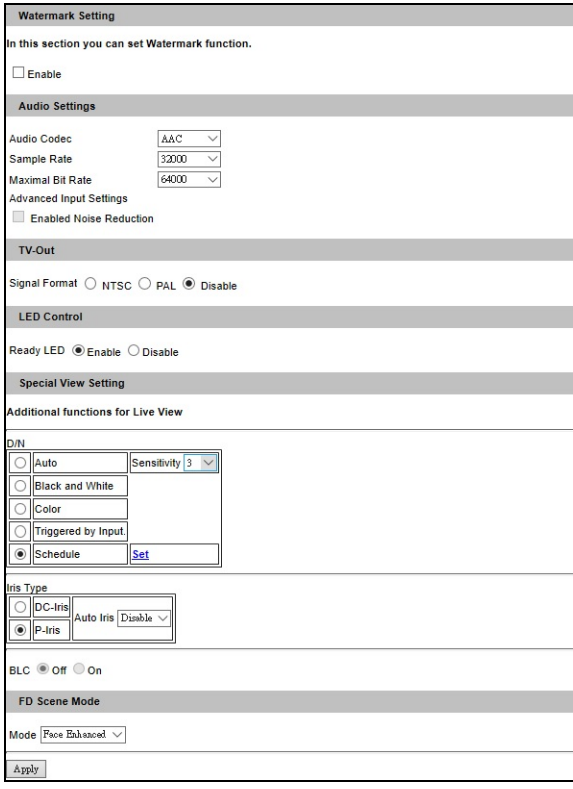

Watermark Setting
In this section you can set Watermark function.
Enable
Audio Settings
Audio Codec
AAC
Sample Rate
32000
Maximal Bit Rate
64000
Advanced Input Settings
Enabled Noise Reduction
TV-Out
Signal Format
NTSC
PAL
Disable
LED Control
Ready LED
Enable
Disable
Special View Setting
Additional functions for Live View
D/N
Auto
Sensitivity
3
Black and White
Color
Triggered by Input.
Schedule
Set
Iris Type
DC-Iris
P-Iris
Auto Iris
Disable
BLC
Off
On
FD Scene Mode
Mode
Face Enhanced
Apply

Figure 4-2B

[Name] Rename the video stream. To display the name of video stream on the Live View window, see *3.2.9 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] Select the video signal type, resolution and frame rate. Select among **H.265**, **H.264** or **MJPEG** as the codec type.

Note that for all the cameras (except GV-PTZ010D), the resolution options available for sub stream vary with the resolution selected for its main stream. For example, if a 4:3 resolution is selected for the main stream in GV-EVD5100, three options, 960 x 720, 640 x 480 and 320 x 240 will be available for its sub stream.

- **Flicker:** Choose the Flicker Hz value between 60 Hz or 50 Hz. This function is only supported by GV-BX4700 Series / 5700 Series.

Note:

1. For GV-BX4700 series, to reach 25 fps at 2560 x 1440, Flicker Hz value must be set at 50 Hz.
2. For WDR Pro or WDR option of other cameras, see Camera Adjustment in *3.2.2 The Control Panel on the Live View Window* to adjust the setting.

[Bandwidth Management] When using the H.264 / H.265 codec, 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 much more efficiently used than a comparable CBR.

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

  Maximal Bit Rate: When the actual bitrate exceeds the specified Maximal Bit Rate, the system will automatically lower its bitrate so as not to exceed it. Select one of the bitrates from the drop-down list or select **Auto** if you do not want to enable this function. The default maximal bitrate values are detailed as follows:

Camera Type	Default Max. Bitrate of VBR
1.3 MP	6 Mbps
2 MP	5 Mbps / 6 Mbps (Face Detection models)
3 MP	6 Mbps
4 MP	5 Mbps / 7 Mbps (Face Detection models)
5 MP	5 Mbps
8 MP	6 Mbps / 6 Mbps (Face Detection models)
12 MP	16 Mbps

- **CBR (Constant Bitrate):** CBR is used to achieve a specific bitrate by varying the quality of the H.264 / H.265 stream. Type the bitrate or select one of the bitrates from the drop-down list.

- **Smart Streaming:** When the option is enabled, the bitrates will be automatically reduced in static scenes, significantly maximizing bandwidth and lowering file size.

  You can choose the image quality of **Static Scene** and **Dynamic Scene** to one of the 5 standards: **Standard**, **Fair**, **Good**, **Great** and **Excellent**. You can even choose the maximum bitrate to optimize the bandwidth.

  Bitrate Reduction Level: The default value is 254. The bigger the value the more bitrates can be reduced in static scenes, thus saving the recording size.

Note: It takes either GV-NVR V8.7 or GV-VMS V16.10.3.0 or later to enable **Smart Streaming**. Refer to the technical notice for the models supporting the feature:

[Region of Interest (ROI)] Enhance image clarity to your defined regions with level High to Low . A total of **5** ROI can be set. This function is disabled by default and is not supported by **Target Series**.

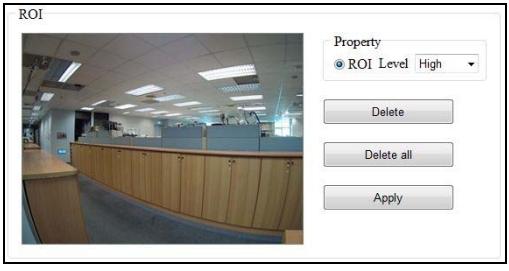


Figure 4-3

[GOP Structure and Length] Set the maximum number of seconds between every key frame.

[Video Slice Mode] Note this function is only supported by firmware V2.12 or earlier and is not supported by **Target Series** and **GV-IPCAM H.265**. Corrects the display mode of the camera when it is displayed on third-party NVR/DVR software and the live view is incomplete or broken. Select **Single Slice** or **Multi Slice** to display the live view. The default is **Auto**.

[H.264 Video Entropy Coding Setting] Note this function is not supported by **GV-IPCAM H.265**, **GV-BX12201** and **Target Series**. By default, the entropy coding is set to CAVLC. To change it to **CABAC**, click and select from the drop-down list.

[Record Settings] Note for **GV-BX12201** firmware V1.02 or later and **GV-IPCAM H.265**, see Recording Settings in 4.4 *Monitoring Settings* to adjust the setting.

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

- **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 (Max. Video Clip):** Sets the maximum time length of each recorded file from 1 to 5 minutes.
- **Record Profile:** Note this function is only available for firmware V2.14 or later. This setting is only applicable for recording to the camera's memory card. Select **Performance** to maximize the lifespan of the memory card by restricting the maximum bit rate to 4 Mbps and Sharpness value to 30. Select **Quality** to adopt your current settings.
- **Record audio:** Activates audio recording when an event occurs.

- **Write recording data into local storage:** Select this function for uninterrupted recording to the memory card while the live view is accessed through the Web interface or other applications. This option is enabled by default.

IMPORTANT: To ensure the quality of simultaneous recording and live view access, make sure you connect no more than two connections to the camera using Web interface or any other applications.

[Text Overlay Settings] Displays camera name, date, time and/or the triggered input's name on the live view and recorded videos when viewing through GeoVision software.

[Text Overlay Settings (OSD)]

Displays camera name, date, and/or time on the live view and recorded videos when viewing through GeoVision software and third-party software through ONVIF and RTSP.

[Watermark Setting] Note this function is not supported for **Target Series**. Enable this option to watermark all recordings. The watermark allows you to verify whether the video has been tampered while it was recorded. See *6.4 Verifying Watermark*.

[Audio In Source] Note this function is only available in **GV-PTZ010D** which contain a built-in microphone and also allow you to install an external microphone. By default, the built-in microphone is enabled to record sounds.

[TV Out] Note this function is only available for the camera with TV-out connector. Select the signal format of the Video Output on the camera as either NTSC or PAL.

[Audio Settings] Enable Noise Reduction to reduce the background noise in the audio file. All H.265 cameras applying firmware V1.02 or later support this function.

[LED Control] Note this function is not available for **GV-PTZ010D**.

- **Ready LED:** Select **Disable** if you do not wish to use the Status LED.
- **LAN LED, WAN LED, Monitoring LED:** Note this option is only available in **Advanced Cube Camera**. Select **Disable** if you do not wish to use the LEDs. For details on LED status, see *Overview* in the corresponding *Hardware Manual*.
- **Alarm LED:** Sets the **white illumination LED** in **Advanced Cube Camera**. The LED is enabled by default.
  - **Auto:** Select **Auto** for the white illumination LED to illuminate the scene automatically when the PIR sensor detects any motion within 5 meters.
  - **Sensitivity:** Set the sensitivity for low light detection. The higher the value, the easier the white illumination LED is to be triggered. The default value is **5**.
  - **The Interval between triggering:** Select the duration for the white illumination LED to light up at full intensity. If a motion persists over the specified period, the white illumination LED will light up with less intensity. This option is designed to keep the camera temperature within its precautious range. The default value is **60** seconds.
  - **Off:** Select to disable the white illumination LED.

[Special View Setting]

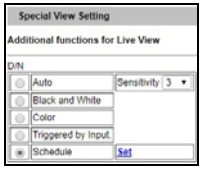


Figure 4-4

- **D/N:** Sets the sensitivity of day-night mode switch. The higher the sensitivity value, the more sensitive the switch is from day mode to night mode. The default value is 5.
  - ⊙ **Auto:** Select **Auto** for the camera to detect the amount of light present and automatically switch to monochrome in a poorly-lit scene. Move the slider to adjust the sensitivity level from 0 to 10.
  - ⊙ **Black and White:** Select this option for the live view to be in monochrome.
  - ⊙ **Color:** Select this option for the live view to be in color.
  - ⊙ **Triggered by Input:** Select this option to switch between day mode and night mode once an input device (e.g. sensor or button) is triggered.

Note: If you select **Triggered by Input**, make sure you enable **Trigger Day/Night Mode** in *4.2.1 Input Settings*.

  - ⊙ **Schedule:** Select this option to determine specific period(s) of time when day mode is activated. See *4.5.1 Recording Schedule Settings* for the details on the setting of the schedule.

Note: If you select **Schedule**, make sure you start **Schedule** monitoring in *4.4 Monitoring*.

- **IR Check Function:** Note this option is only available for **Box Camera**. This function determines whether the surveillance area is illuminated by an externally installed infrared illuminator.
  - ⊙ **Off:** The default setting. The infrared illuminator will be constantly off. It is advisable to enable this option when the color temperature of outdoor lighting is 6000 K or above.
  - ⊙ **On:** The infrared illuminator will be constantly on.
  - ⊙ **Trigger by Input / Trigger IR by D/N:** Select this option for the infrared illuminator to turn on under low light and turn off under sufficient light.

Note:

1. If an infrared illuminator is installed for outdoor surveillance, it is suggested to use the **Trigger by Input** or the **Trigger IR by D/N** function to avoid incorrect judgment of lighting and hence the action of the IR cut filter. See *Infrared Illuminators* in the *Hardware Manual*.
2. If you select **Trigger by Input** / **Trigger IR by D/N** option, make sure you have set D/N as **Auto** and configured its sensitivity level.

- **Iris Type:** Note this function is not supported for the camera with fixed lens or iris. This field shows the iris type (DC-Iris or P-Iris) of your GV-IP Camera.
  - ⊙ **Auto Iris:** The option is designed for auto iris lens (DC-Iris or P-Iris). Enable the auto iris function when the scene appears fuzzy and the Flicker Less function does not help to improve the situation.
- **BLC:** Select **On** to enable Backlight Compensation (BLC). This function is used to adjust the color intensity of scenes with strong light at the background.

Note: To access the BLC function in PTZ camera, see *Other*, *Image Settings* in the *Hardware Manual*.

- **IR Light:** Note this function is only available for **Target Series**, **Ultra Box Camera**, **IR Arctic Box Camera**, **Bullet Camera**, **Ultra Bullet Camera**, **PT Camera**, **Vandal Proof IP Dome** and **Fixed IP Dome**. Select **Auto** for automatic switch between day mode and night mode depending on the amount of light detected. Select **Off** to completely disable IR LEDs.
- **Noise Reduction:** Note this function is only supported by **GV-EVD5100**, **GV-EFD5101** and **GV-EBL5101**. Reduces image noise especially under low-light conditions.

Note: When the Noise Reduction is enabled, the frame rate will be affected. For details see *Note for GV-EVD5100 / EFD5101 / EBL5101* at the beginning of the manual.

[FD Scene Mode]

Note this function is only supported by **GV-BX2700 / GV-BX2700-FD / GV-BX4700 / GV-BX4700-FD / GV-BX8700-FD / GV-MD8710-FD**. For applying face detection, select **Face Enhanced**. If not, select **Normal**.

[Advanced Setting] Note this function is only supported by GV-IPCAM H.265 firmware V1.14 or later. You can enable AES encryption for enhanced security of the contents streamed.

Figure 4-5

Note: This function only works with GV-VMS V18.1, GV-DVR / NVR V8.8 or later versions.

4.1.2 Motion Detection

Motion detection is disabled by default except for GV-PTZ010D.

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. Set up at least one area to enable this function.

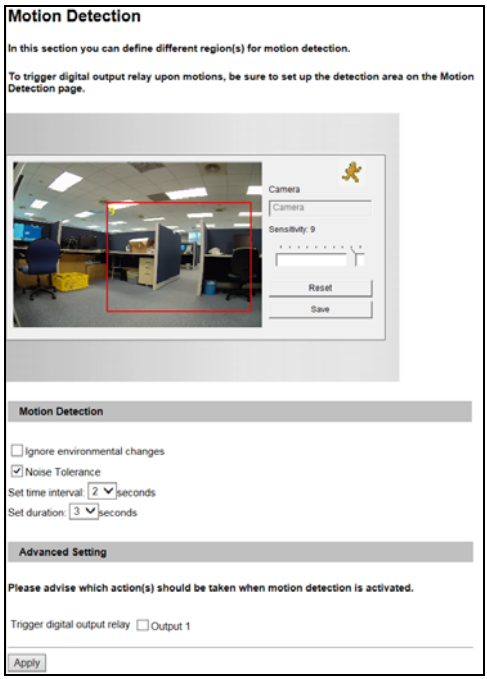


Figure 4-6

1. Select the desired sensitivity by moving the slider. There are ten values. The higher the value, the more sensitive the camera is to motion.
2. Drag an area on the image. Click **Add** when you are prompted to confirm the setting.
3. To create several areas with different sensitivity values, repeat steps 1 and 2.
4. Click **Save** to save the above settings.
5. Click **Reset** to delete all the selected areas.
6. If you want to detect motion using the PIR sensor (for **Advanced Cube Camera** only), select **Use PIR to detect motion**.
7. If you want to ignore environmental changes such as rain or snow, select **Ignore environmental changes**.
8. The **Noise Tolerance** function is enabled by default. It ignores video noise when the light intensity changes.
9. To set a period of time before a motion is to be detected, select **Set time interval**. The choices available range from 0-3 second(s).
10. To set a period of time for a motion to last, select **Set duration**. The choices available range from 1-5 second(s).
11. If you want to trigger the alarm output when motion is detected, select **Output 1** 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: Set time interval and **Set duration** are only supported by GV-BX12201 firmware V1.02 or later.

4.1.3 Privacy Mask

The Privacy Mask function is used to block out sensitive areas on live view and recorded clips for cameras connecting to GeoVision software. This feature is ideal for locations with displays, keyboard sequences (e.g. passwords), and for anywhere else you don't want sensitive information visible.

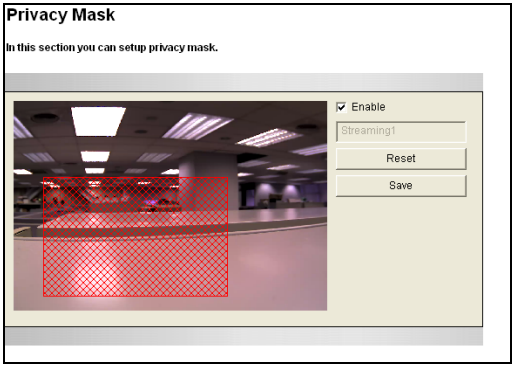


Figure 4-7

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 all the settings.

4.1.4 Text Overlay

The Text Overlay allows you to overlay any text in any place on the camera view. Up to 16 text messages can be created on one camera view. The overlaid text will be saved in the recordings.

Figure 4-8

1. Select the font, font style and font size in a pop-up window.
2. Select the **Enable** option.
3. Click any place on the image. This dialog box appears.

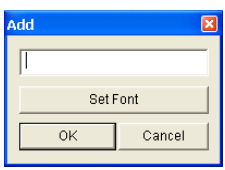


Figure 4-9

4. Type the desired text, and click **OK**. The text is overlaid on the image.
5. Drag the overlaid text to a desired place on the image.

6. Click **Set Font** to modify the font settings.
7. Click **Save** to apply the settings, or click **Load** (Undo) to revert to the last saved setting.
8. Click **Preview** to see how the text will appear on the image. Click **Close** to end the preview.

4.1.5 Tampering Alarm

Note this function is not available for **PTZ Camera** and **PT Camera**.

Tampering Alarm is used to detect whether a camera is being physically tampered. An alarm can be generated when the camera is moved, covered up, or out of focus. The alarm types include triggered the output device, e-mail alert and notifying the connected GV-Center V2, GV-Vital Sign Monitor and GV-DVR / NVR / VMS.

Note: This function is not available for **PTZ Camera** and **PT Camera**.

To establish the tampering alarm, set up at lest one alarm type:

- To trigger the output device when a tampering event occurs, enable the output setting and select **Tampering Alarm**. See *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.*
- To notify GV-Center V2, GV-Vital Sign Monitor and GV-DVR / NVR / VMS when a tampering event occurs, enable the connection to these systems. See *4.3.3 Center V2*, *4.3.4 Vital Sign Monitor*, *7.1 Setting up an IP Camera on GV-DVR / NVR*, and *7.2 Setting Up IP Cameras on GV-VMS*.

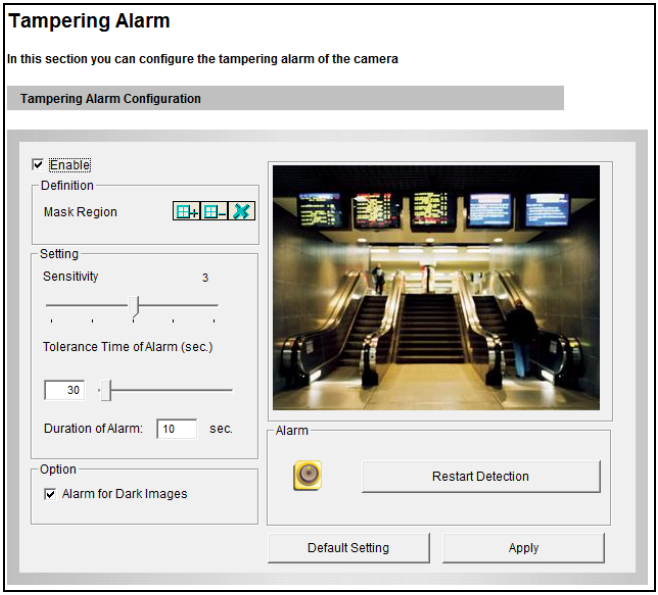


Figure 4-10

To configure the tampering alarm:

1. Select the **Enable** option.
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. when the lens of camera is covered, make sure the **Alarm for Dark Images** option is enabled. By default, this function is enabled.
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, the output device can be activated. To turn off the output device immediately, return to this setting page, and click **Restart Detection**.

4.1.6 Visual Automation

Note this function is only supported by cameras with I/O function.

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 simply change its current state, e.g. light ON.

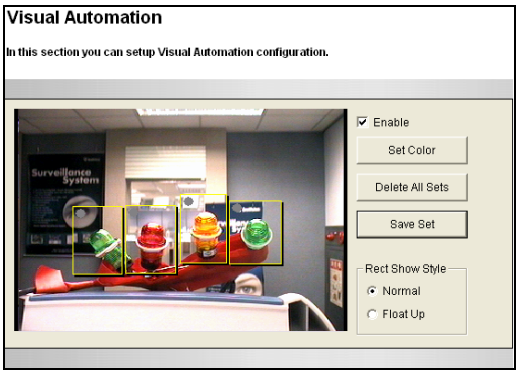


Figure 4-11

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

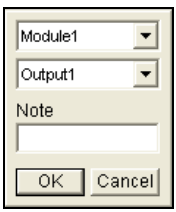


Figure 4-12

3. Assign the connected module and output device. In the Note field, type a note to help you manage 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.
7. To perform the function, see *3.2.14 Visual Automation*.

4.1.7 Face Detection

Face Detection is used to record events when human faces appear in the image, which can work with GV-VMS to generate alarms and/or trigger other actions on the server site.

Note:

1. This function is only supported by cameras with face detection function and GV-VMS 18.1 or later.
2. To receive the optimal quality of the captured face image, ensure to disable the smart streaming option when using the face detection feature

[Basic]

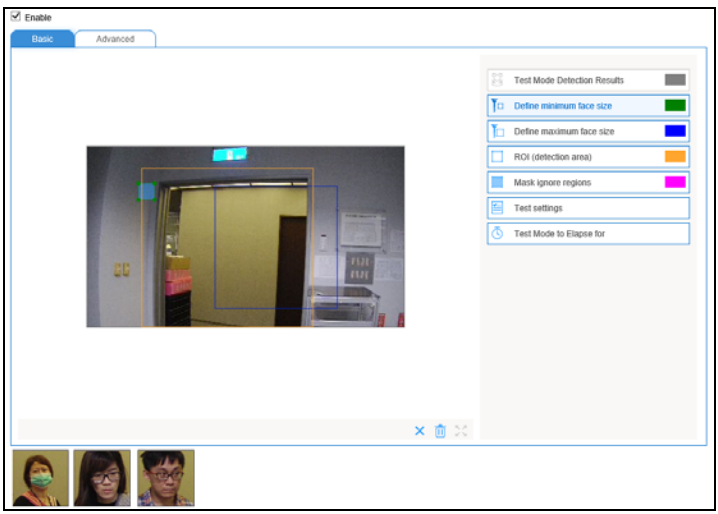


Figure 4-13

1. Select **Enable** to adjust the face detection settings. If you want the minimum face size, maximum face size and ROI settings to be automatically configured, click **Apply** and skip to step 4.
2. Draw areas to define the **minimum face size** and **maximum face size** so the system can detect faces within that size range.
3. Draw at least one **ROI** (region of interest) to specify the detection area(s).
4. If necessary, click **Mask ignore regions** to specify the area(s) where you do not wish the faces to be detected.
5. Click **Test settings** to test if a face can be detected or otherwise click **Apply** to initiate the settings. The detected face(s) will be highlighted with a red box and appear below the test screen.
6. If you want to adjust the test duration for the current face detection settings, click **Test Mode to Elapse for**.

[Advanced]

Face Count / Detection: Specify the maximum number of faces that can be detected at a time.

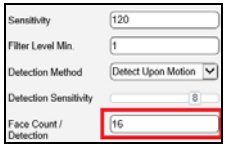


Figure 4-14

- **Face Count Max (1~16):** GV-BX2700 / 2700-FD / 4700 / 4700-FD.
- **Face Count Max (1~32):** GV-BX2600-FD / 8700-FD, GV-MD8710-FD.

Note: To achieve the optimal face detection results, avoid modifying other advanced settings.

4.2 I/O Settings

Note the I/O settings are only available for **Box Camera**, **Bullet Camera, Ultra Bullet Camera**, **PTZ Camera**, **PT Camera**, **Vandal Proof IP Dome**, and **Fixed IP Dome**.

After installing the I/O device, you need to enable the I/O settings on the camera. For how to install the I/O device on the camera, see the following reference sections in the corresponding Hardware Manual:

GV-IPCAM	Reference section
Box Camera	*I/O Terminal Block*
Bullet Camera	*Connecting the Camera* *Connecting the Camera*
PTZ Camera	*I/O Terminal Block*
PT Camera	*I/O Terminal Block*
Vandal Proof IP Dome	*Connecting the Camera*
Fixed IP Dome	*I/O Terminal Block*

4.2.1 Input Settings

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

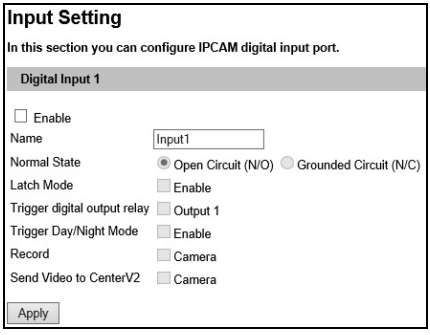


Figure 4-15

- **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.
- **Trigger Day/Night Mode:** Enable this option when **Triggered by Input** of D/N function is selected in *4.1.1 Video Settings*
- **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.

- **PTZ Settings:** Note this function is only available for **PTZ Camera** and **PT Camera**.
  - ⊙ **Input On:** Select a preset point to which the camera turns when an input is triggered.
  - ⊙ **Input Off:** Select a preset point to which the camera returns when the input triggering is off.
  - ⊙ **Duration to set preset after input off:** Specify the duration that the camera stays at the Input On point before returning to the Input Off point.

Note:

1. The GV-IP Cameras support dry-contact input device.
2. The functions “triggering the output”, “starting the recording when the input is triggered” and “sending video to Center V2” only work 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 mostly 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 (not available for **PTZ Camera**), disk write error (Rec Error) and full memory card (HD Full).

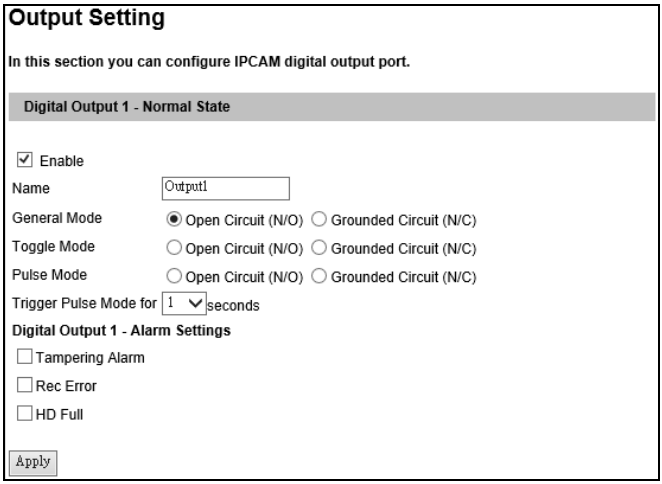


Figure 4-16

4.2.3 PTZ Settings

Note this function is only available in **PTZ Camera** and **PT Camera**.

You can change the image settings, configure sequences, and access settings including autopan speed, motor reset, digital zoom and system default loading. For details, see *Accessing the VISCA OSD Configuration* in the *Hardware Manual*.

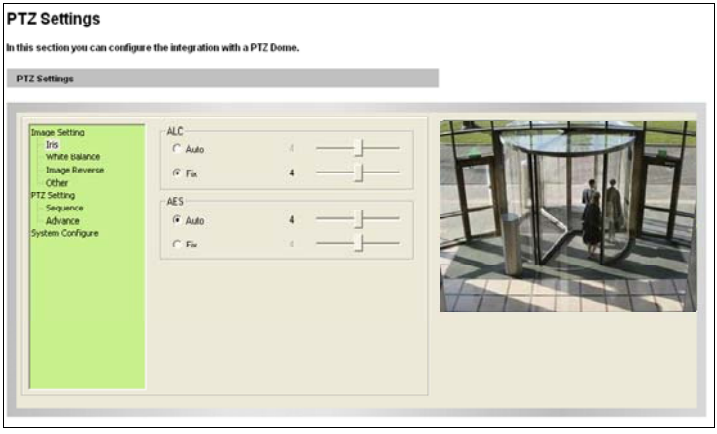


Figure 4-17

4.3 Events and Alerts

For the events of motion detection or I/O trigger, the Administrator can set up two trigger actions:

1. Send a captured still image by E-mail or FTP.
2. Notify Center Monitoring Station, Center V2 or Vital Sign Monitor, by video or text alerts.

To have the above trigger actions, you must set the following functions in advance:

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

4.3.1 E-mail

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

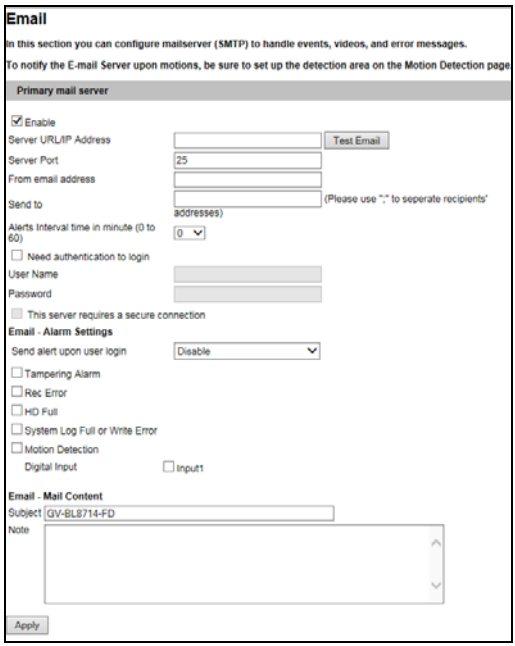


Figure 4-18

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

- **Sever URL/IP Address:** Type the URL address or IP address of the SMTP Server.
- **Server Port:** Modify the port number of the SMTP Server. 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 is between 0 and 60 minutes. The option is useful for the frequent event occurrence, by which any event triggers during the interval period will be ignored.

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

[E-Mail Alarm Settings] You can choose to automatically send an e-mail alert under these conditions: Login success / failure, tampering alarm, disk write error (Rec Error), full memory card (HD Full), System Log Full or Write Error, motion detection and input trigger. Note that the alert condition is only supported if the corresponding function is supported in that camera model.

IMPORTANT: To send e-mail alerts upon motions, be sure to set up detection area on the Motion Detection's page.

For the related settings to send e-mail alerts, see *4.1.2 Motion Detection*, *4.2.1 Input Setting* and *4.4 Monitoring*.

Note: For GV-BX12201, the maximum resolution of the captured still image sent by E-mail alert is 1 MP.

[E-Mail Mail Content] You can type the mail subject and mail content in the **Subject** and **Note** columns. The default mail subject is the camera model name.

4.3.2 FTP

You can also send the captured images to a remote FTP server as alerts.

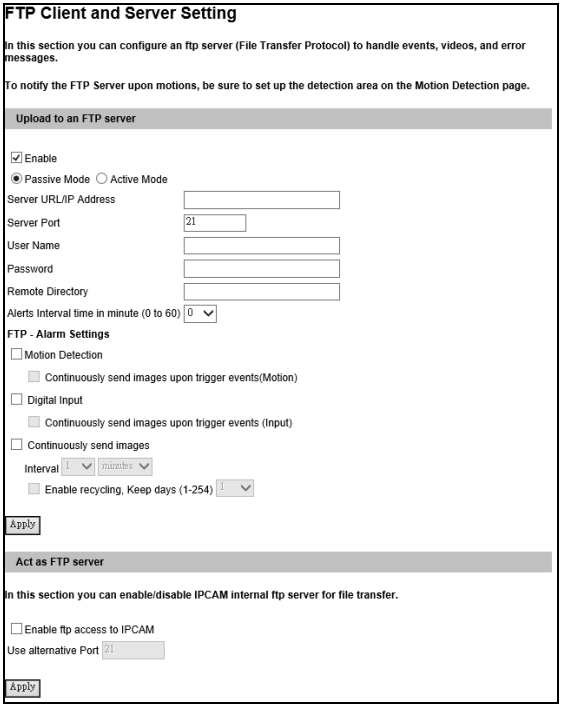


Figure 4-19

[Upload to an FTP Server]

- **Enable:** Select to enable the FTP function and then select **Active Mode** or **Passive Mode**, depending on the setting of your FTP server.
- **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 username 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 the frequent event occurrence by which any event triggers during the interval period will be ignored.

[Alarm Settings]

- **Motion Detection:** When a 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 a motion is detected. This stops as soon as no motion is detected.
- **Digital Input:** Note this function is only supported by cameras with I/O function. Once 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.

- **Continuously send images:** Sends images to the FTP server at the specified interval.
  - ⊙ **Interval:** Use the drop-down list to specify how frequent the images are sent to the FTP server.

- **FTP Schedule:** Select this option to define specific period(s) of time for images to be sent to the FTP Server. For details on the schedule option, see *4.5.1 Recording Schedule Settings*. Note this function is only supported by GV-IPCAM H.265 firmware V1.14 or later.
- **Enable Recycling:** Select this option to recycle the FTP storage at the specified Keep Day.
- **Keep Days:** Specify how frequent the images saved at the FTP server are recycled. By default, the Keep Day is set to **1**.

IMPORTANT: To send FTP alerts upon motions, be sure to set up detection area on the Motion Detection's page.

[Act as FTP Server] Note this function is not available for **Target Series**.

- **Enable FTP access to the GV-IP Cam:** The camera acts as an FTP server, enabling users to download AVI files.
- **Use alternative port:** The default port is set to 21.

To access the internal FTP server through a Web browser, enter 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, enter the default value username **ftpuser** and password **123456**. Then you should find the AVI files recorded after trigger events.

To change login information of the internal FTP server, see *4.8.3 User Account*. For related settings to send FTP alerts, see *4.1.2 Motion Detection*, *4.2.1 Input Settings*, and *4.4 Monitoring*.

Note: For GV-BX12201, the maximum resolution of the captured still image sent by FTP alert is 1 MP.

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. A camera can connect to up to 2 Center V2 stations simultaneously.

IMPORTANT: To notify Center V2 server upon motions, be sure to set up detection areas on the Motion Detection's page,

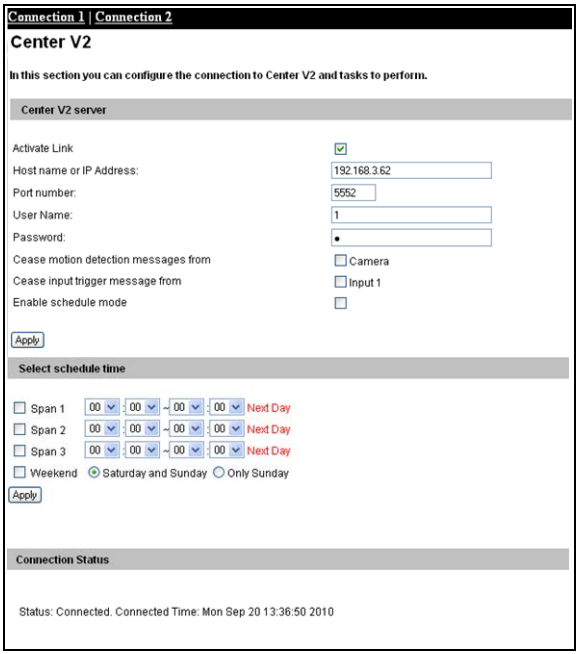


Figure 4-20

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 the Port 2 value on Center V2 or keep the default value **5551**.
4. **User Name:** type a valid username 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 connected time.
7. To establish connection to the second Center V2 server, click the **Connection 2** tab and repeat the above steps for setup.

You can also find the following options on this Center V2 setting page:

- **Cease motion detection messages from:** Stops notifying Center V2 of motion-triggered events.
- **Cease input trigger messages from:** Note this function is only supported by cameras with I/O function. 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 Setting* and *8.1 Center V2*.

4.3.4 Vital Sign Monitor

After a motion or an I/O triggered event, the central monitoring station Vital Sign Monitor can get notified by text alerts. For the monitoring through Vital Sign Monitor, you must already have a subscriber account on Vital Sign Monitor. A camera can connect up to 2 Vital Sign Monitors simultaneously.

IMPORTANT: To notify GV-Vital Sign Monitor server upon motions, be sure to set up detection areas on the Motion Detection's page.

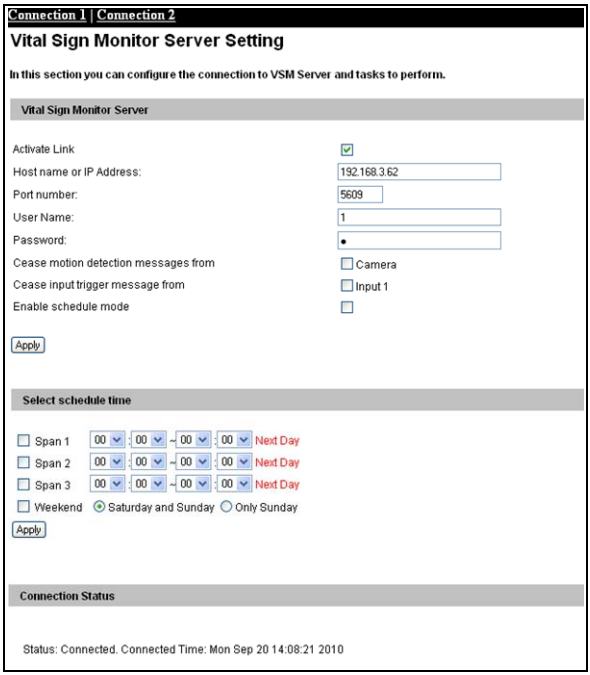


Figure 4-21

To enable the Vital Sign Monitor connection:

1. **Activate Link:** Enable the monitoring through Vital Sign Monitor.
2. **Host Name or IP Address:** Type the host name or IP address of Vital Sign Monitor.
3. **Port Number:** Match the port to the Port 2 value on Vital Sign Monitor. Or keep the default value 5609.
4. **User Name:** Type a valid username to log into Vital Sign Monitor.
5. **Password:** Type a valid password to log into Vital Sign Monitor.
6. Click **Apply.** The Connection Status should display “Connected” and connected time.
7. To establish connection to the second Vital Sign Monitor , click the **Connection 2** tab and repeat the above steps for setup.

These options you can also find on this Vital Sign Monitor setting page:

- **Cease motion detection messages from:** Stops notifying Vital Sign Monitor of motion-triggered events.
- **Cease input trigger messages from:** Note this function is only supported by cameras with I/O function. Stops notifying Vital Sign Monitor of input-triggered events.
- **Enable schedule mode:** Starts the monitoring through Vital Sign Monitor 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 Vital Sign Monitor, see *4.1.2 Motion Detection* and *4.2.1 Input Settings,* and *8.2 Vital Sign Monitor*.

4.3.5 Backup Center

Note that Backup Center is not supported for **Target Series**.

The connection to the GV-Backup Center allows you to back up another copy of recordings and system log to the GV-Backup Center on an offsite location while the camera is saving these data to the memory card. The GV-Backup Center provides a PC-based storage and backup solution. For details on the GV-Backup Center, see *GV-Backup Center User's Manual*.

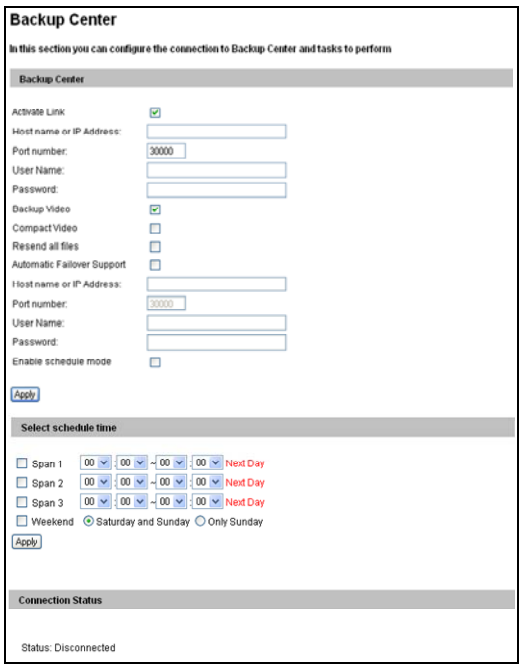


Figure 4-22

To enable connection to GV-Backup Center:

1. **Activate Link**: Enable the connection to the GV-Backup Center.
2. **Host Name or IP Address**: Type the host name or IP address of the GV-Backup Center.
3. **Port Number**: Match the communication port on the GV-Backup Center or keep the default value **30000**.
4. **User Name**: Type a valid user name to log into the GV-Backup Center.
5. **Password**: Type a valid password to log into the GV-Backup Center.
6. **Backup Video**: Select the streams to back up their recordings to the GV-Backup Center.
7. **Compact Video**: Select the streams to only back up their Key Frames to the GV-Backup Center, instead of full recordings. This option is useful to save the backup time.
8. **Resend all files**: Select this option to send all the recorded files that have received by the Backup Center again.
9. **Enable Schedule Mode**: Enable the GV-Backup Center connection on the schedule you set in the Select Schedule Time section. Refer to *4.5 Recording Schedule* for the same settings.
10. Click **Apply**. The Connection Status should display “Connected” and connected time.

If you have a failover GV-Backup Center server which provides uninterrupted backup services in case the first GV-Backup Center failed, configure the failover GV-Backup Center as below.

1. **Automatic Failover Support**: Enable the automatic connection to the failover GV-Backup Center once the connection between camera and the first GV-Backup Center is interrupted.

2. **Host Name or IP Address**: Type the host name or IP address of the failover GV-Backup Center.
3. **Port Number**: Match the communication port on the failover GV-Backup Center or keep the default value **30000**.
4. **User Name**: Type a valid user name to log into the failover GV-Backup Center.
5. **Password**: Type a valid password to log into the failover GV-Backup Center.
6. Click **Apply**.

4.3.6 Video Gateway / Recording Server

The GV-Video Gateway / GV-Recording Server is a video streaming server designed for large-scale video surveillance deployments. The GV-Video Gateway / GV-Recording Server (with recording capability) can receive up to **128** channels from various IP video devices, and distribute up to **300** channels to its clients. With the GV-Video Gateway / GV-Recording Server, the desired frame rate can be ensured while the CPU loading and bandwidth usage of the IP video devices are significantly reduced.

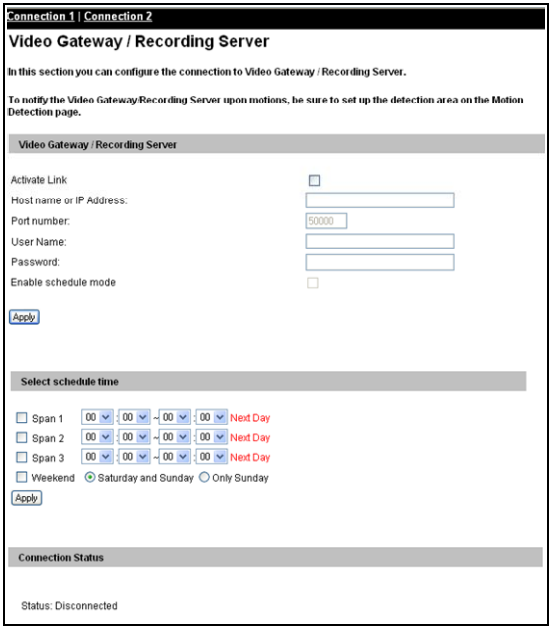


Figure 4-23

The supported GV-IPCAM can connect up to two GV-Video Gateway / GV-Recording Server. To send the video images to the GV-Video Gateway or GV-Recording Server, follow the steps below.

1. **Activate Link**: Enable the connection to the GV-Video Gateway / GV-Recording Server.
2. **Host Name or IP Address**: Type the host name or IP address of the GV-Video Gateway / GV-Recording Server.
3. **Port Number**: Match the communication port on the GV-Video Gateway / GV-Recording Server or keep the default value **50000**.
4. **User Name**: Type a valid user name to log into the GV-Video Gateway / GV-Recording Server.
5. **Password**: Type a valid password to log into the GV-Video Gateway / GV-Recording Server.
6. **Enable Schedule mode**: Enable the GV-Video Gateway / GV-Recording Server on the schedule you set in the **Select Schedule Time** section. Refer to *4.5 Recording Schedule* for the same settings.
7. Click **Apply**. The Connection Status should display “Connected” and the connected time.
8. To establish connection to the second GV-Video Gateway / GV-Recording Server, click the **Connection 2** tab and repeat the above steps for setup.

4.3.7 ViewLog Server

Note that ViewLog Server is not supported for **Target Series**.

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

This function is enabled by default using port **5552**. Keep the default setting and only modify it when necessary. For details on the remote playback, see *5.2.2 Playback over Network*.

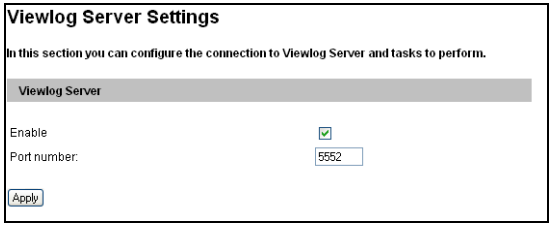


Figure 4-24

4.3.8 RTSP/ONVIF

The RTSP and ONVIF settings enable video and audio streaming to your 3G-enabled mobile phone or the third-party software. The RTSP and ONVIF streaming is enabled by default.

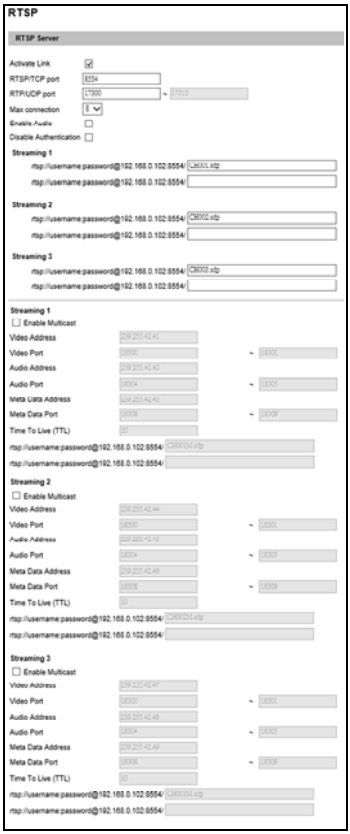


Figure 4-25

[RTSP]

- **Activate Link:** Enable the RTSP service.
- **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:** Select the maximum number of RTSP and 3GPP connections to the camera. The maximum value is 8.
- **Enable Audio:** Note this function is not available for **Target Bullet Camera**, **Target Mini Fixed Rugged Dome** and **Ultra Bullet Camera**. Turns audio streaming on or off.
- **Disable Authentication:** By default, when accessing live view through RTSP command, the ID and password of the camera are required. Select this option to disable the authentication prompt.

[Streaming 1/2/3]

Set up the Multicast function through RTSP.

Note:

1. The RTSP Multicasting function is only supported by **GV-EFD2101 / 3101 / 5101**, **GV-EVD2100 / 3100 / 5100**, **GV-EBL5101 firmware V1.04 or later**, and **Target cameras firmware V1.09 or later.**
2. The Multicast streaming name is customizable on **GV-IPCAM H.265 firmware V1.14 or later**.

For details on remote monitoring with mobile phones, see *Mobile Phone Connection, Chapter 26*. For details on RTSP / Multicast command, see *Appendix B*.

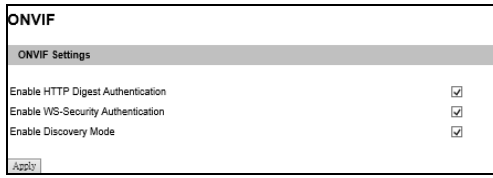


Figure 4-26

[ONVIF]

- **Enable HTTP Digest Authentication:** The compatibility with HTTP Digest Authentication is required to access the camera by a third-party DVR through ONVIF. This function is disabled by default. Note this function is only supported by GV-IPCAM H.265 fiirmware V1.14 or later.
- **Enable WS-Security Authentication:** The ID and password of the camera are required to access the camera by a third-party DVR through ONVIF. This function is enabled by default.
- **Enable Discovery Mode:** Allows the third-party DVR to browse this camera. This function is enabled by default.

4.3.9 Speaker

Note this function is only available for **Advanced Cube Camera**.

The Advanced Cube camera is equipped with an alarm. With the Speaker settings, your camera can sound the speaker when the camera is being tampered or when motions are detected. This function is disabled by default.

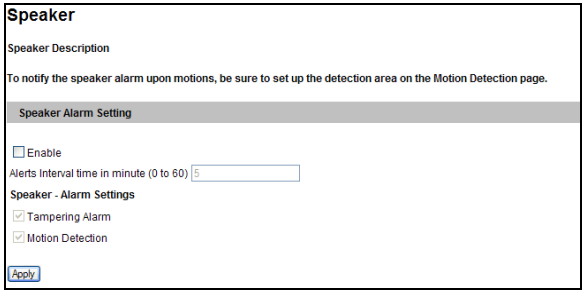


Figure 4-27

1. Select **Enable**.
2. Type the duration time in the Alerts Interval time field. The default value is **5** (minutes). When a motion is detected, the alarm will be on for the specified amount of time.
3. Select **Tampering Alarm** and/or **Motion Detection** under Alarm Settings.

To sound the alarm upon motion events, make sure you have enabled motion detection. For details, see *4.1.2 Motion Detection*.

4.4 Monitoring

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

Note:

1. See *Note for Connecting to GV-DVR / NVR / VMS* at the beginning of the manual.
2. For GV-**EBL2101 / 2111 / 3101**, see *4.4.1 Monitoring Settings for GV-EBL2101 / 2111 / 3101* for corresponding page.

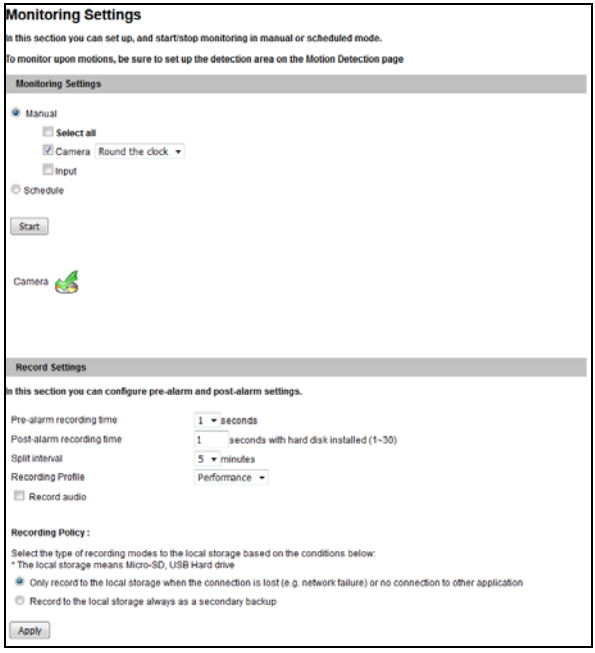


Figure 4-28-1

[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:** Manually starts recording. Select the desired recording mode for recording.
- **Input:** Note this function is only supported by cameras with I/O function. Manually starts I/O monitoring. When the sensor input is triggered, its associated camera and output will be activated for recording and alerting. For this setting, see *4.2.1 Input Setting.*

[Schedule] The system starts motion detection and I/O monitoring according to the schedule you have set. For schedule settings, see *4.5 Recording Schedule*.

[Camera Status Icon]

 **:** On standby

 : Enabled for motion detection and input trigger

 : Recording is on.

[Recording Settings] Note this function is only supported by **GV-BX12201** firmware V1.02 or later and **GV-IPCAM H.265**. Configure recording settings for motion and I/O events, and the condition to record.

- **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 between each event file from 1 to 5 minutes.
- **Recording Profile**: This setting is only applicable for recording to the camera's memory card. Select **Performance** to maximize the lifespan of the memory card by restricting the frame rate to 30 fps and maximum bit rate to 4 Mbps. Select **Quality** to adopt your current settings. The default setting is **Performance**.
- **Record audio:** Activates audio recording when an event occurs.
- **Recording Policy**: By default, the camera will only record to the memory card when the camera is not streaming live view to other applications (e.g. GV-VMS) or Web browser. Alternatively, you can set the camera to always record to the memory card as a secondary backup.

Note: When the camera is recording to the memory card, it is recommended to connect no more than two connections to the camera using Web interface or other applications.

- **Encryption:** Stores the recordings as encrypted files that can only be played back by GV-Remote ViewLog player. For details on playback, see *5.2.2 Playback over Network*.

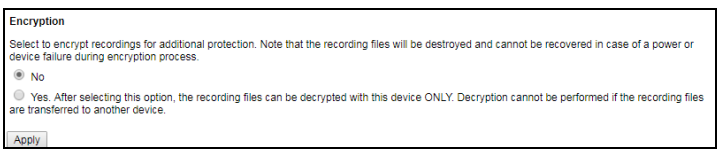


Figure 4-28-2

4.4.1 Monitoring Settings for GV-EBL2101 / 2111 / 3101

In the Monitoring Settings page for **GV-EBL2101 / 2111 / 3101**, click **Start** to activate e-mail and FTP alert functions. Be sure to complete related settings on the Motion Detection, email and FTP pages.

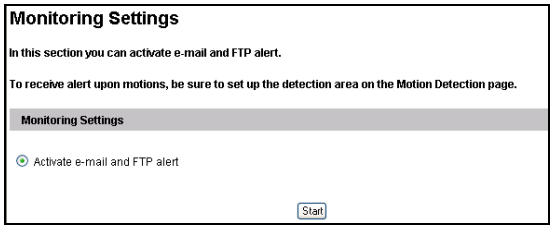


Figure 4-29

4.5 Recording Schedule

Note this function is not available for **GV-EBL2101 / 2111 / 3101**.

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 the schedule for recording.

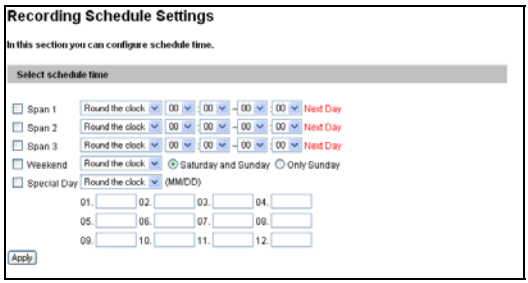


Figure 4-30

- **Span 1- Span 3:** Set a different recording mode for each time frame during the day. Each day can be divided into 3 time frames, represented by Span 1 to Span 3.
- **Weekend:** Enable this option to start monitoring all day on the weekend and select the 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

Note this function is only supported by cameras with I/O function.

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

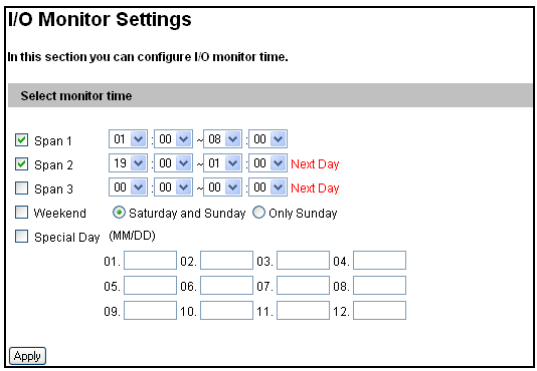


Figure 4-31

- **Span 1- Span 3:** Set different time frames during the day to enable I/O monitoring. Each day can be divided into 3 time frames, represented by Span 1 to Span 3.
- **Weekend:** Enable this option to start I/O monitoring all day on the weekend and define 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 the priority.

4.6 Remote ViewLog

Note this function is not available for **Target Series**.

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

For the first-time user, you need to download and install the Remote ViewLog program from the company website. To allow remote access to the camera, make sure the ViewLog Server function is enabled. See *4.3.7 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 Configuration

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

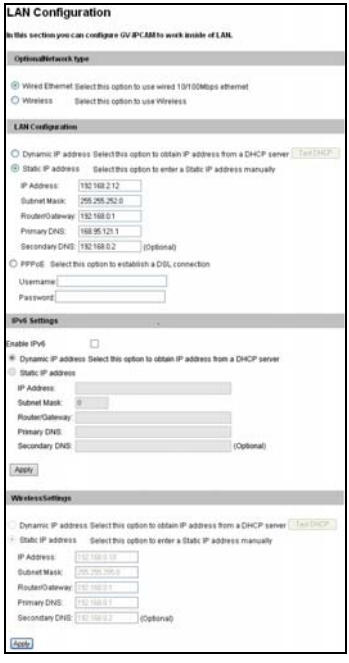


Figure 4-32

[Optional Network Type]

Note the Wireless Settings are only available in **GV-BX1200 Series / 2400 Series / 2700 Series / 4700 Series / 5700 Series**, **GV-CAW120 / 220, GV-FER5700** and **GV-MFD3401 Series / 5301 Series**. According to the network environment, select **Wired Ethernet** or **Wireless**. Before enabling the **Wireless** option, follow the steps in *2.1.3 Configuring the Wireless Connection* to configure the wireless settings first.

[LAN Configuration]

- **Dynamic IP address:** The network environment has a DHCP server which will automatically assign a dynamic IP address to the camera. Click the **Test DHCP** button to see the currently assigned IP address or look up the dynamic IP address using GV-IP Device Utility.
- **Static IP address:** Assign a static IP or fixed IP to the camera and fill out the required settings. The default values are as below.

	Wired Ethernet	Wireless
IP address	192.168.0.10	192.168.100.10
Subnet Mask	255.255.255.0	255.255.255.0
Router/Gateway	192.168.0.1	192.168.0.1
Primary DNS server	192.168.0.1	192.168.0.1
Secondary DNS server	192.168.0.2	192.168.0.2

- **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.

[IPv6 Settings]

Select **Enable IPv6** and click **Apply** to enable this function.

Note this function is only available for **Target firmware V1.07**, **Target firmware V1.03**, and **GV-IPCAM H.265 firmware V1.14** or later versions.

- **Dynamic IP address:** The network environment has a DHCP server which will automatically assign a dynamic IP address to the camera.
- **Static IP address:** Assign a static IP or fixed IP to the camera and fill out the required settings.

Note: To enable this function, make sure your network environment and hardware specifications support IPv6.

For details on Dynamic DNS Server Settings, *see 4.7.3 Advanced TCP/IP.*

4.7.2 Wireless Client Mode

Note this function is only supported in the models supporting wireless connection, and when GV-WiFi Adapter is installed. Set up the client mode before enabling the wireless function.

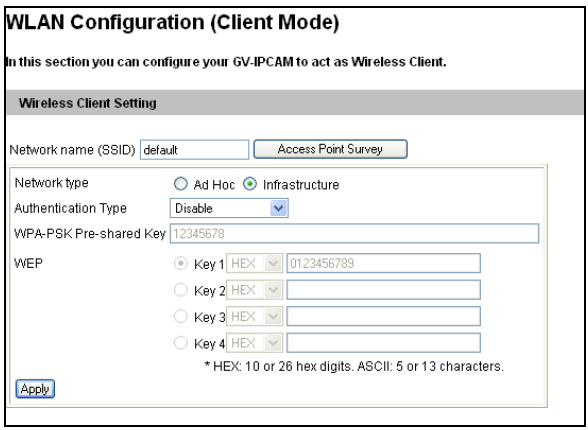


Figure 4-33

- **Network type:** Select the network mode **Ad Hoc** or **Infrastructure**.
  - **Infrastructure:** Connect to the Internet via the Access Point. This mode further gives wireless access to the Internet or data sharing under a previously wired environment.
  - **Ad-Hoc:** A Peer-to-Peer mode. This mode connects to other computer with the WLAN card, and does not need the Access Point to connect to each other.
- **Network name (SSID):** The SSID (Service Set Identify) is a unique name that identifies a particular wireless network. Type SSID of the Wireless LAN group or Access Point you are going to connect to.

- **Access Point Survey:** Click this button to search all the available Access Points (Infrastructure mode) and wireless stations (AD-Hoc mode) within the LAN.
- **Authentication Type:** Select one of these network authentication and data encryption: **Disable**, **WEP**, **WPAPSK-TKIP**, **WPAPSK-AES**, **WPA2PSK-TKIP** or **WPA2PSK-AES**.
  - ⊙ **Disabled:** No authentication is needed within the wireless network.
  - ⊙ **WEP (Wired Equivalent Privacy):** A type of data encryption. Type up to four WEP Keys in HEX or ASCII format. Note that if you use HEX format, only digits 0-9 and letters A-F, a-f are valid.
  - ⊙ **WPAPSK-TKIP and WPA2PSK-TKIP:** Type WPA-PSK (Pre-Shared Key) for data encryption.
  - ⊙ **WPAPSK-AES and WPA2PSK-AES:** Type WPA-PSK (Pre-Shared Key) for data encryption.

For step-by-step instruction on wireless connection, see *2.1.3 Configuring the Wireless Connection*.

Note:

1. Your encryption settings must match those used by the Access Points or wireless stations with which you want to associate.
2. When you lose the wireless access, you can still access the unit by connecting it to a LAN and search for the camera using GV IP Device Utility.
3. When **Ad Hoc** is used, only **WEP** encryption is supported.

4.7.3 Advanced TCP/IP

This section provides the advanced TCP/IP settings, including DDNS Server, HTTP port, HTTPS, streaming port, UPnP, QoS and network connection check.

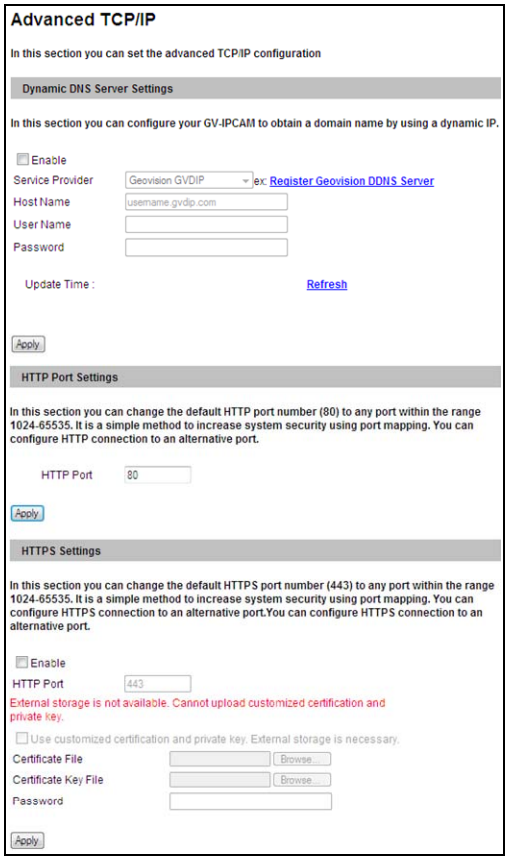


Figure 4-34-1

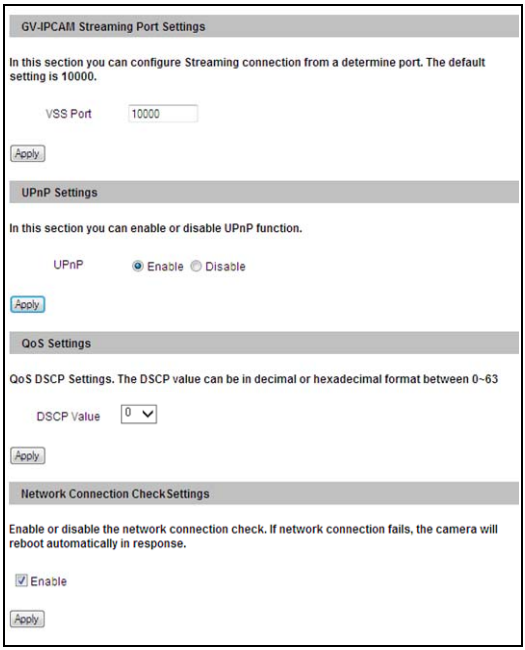


Figure 4-34-2

[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 3 providers listed in the camera: GeoVision GVDIP, 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 the users of GeoVision DDNS Server, it is unnecessary to fill the field because the host name will be detected and brought up automatically.
4. **User Name:** Type the username used to enable the service from the DDNS. The username should look similar to your host name. Depending on your service provider, you should add domain name (.dipmap.com, .gvdip.com or .org) after your user name, for example, alice.dipmap.com
5. **Password:** Type the password used to enable the service from the DDNS.
6. Click **Apply**.

[HTTPS Settings] For face detection camera models, see *4.7.4 HTTPS* for similar HTTPS settings. By enabling the HTTPS settings, you can access the camera through a secure protocol. The default HTTPS port is 443. 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 **Certificate 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: The .pem file format is supported by Certificate and Private Key.

[HTTP Port Settings] The HTTP port enables connection of 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 through 65535.

[GV-IPCAM Streaming Port Settings] The VSS port enables connecting the camera to the GV-DVR / NVR / VMS. 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 means you can connect to the camera directly by clicking on the camera listed in the network devices table.

[QoS Settings] The Quality of Service (QoS) is a bandwidth control mechanism that guarantees delay-sensitive data flows such as voice and video streams, obtain a certain amount of bandwidth to keep the streaming smooth.

To apply QoS to the camera, all network routers must support QoS and QoS must be enabled on these devices. To enable the QoS on the camera, select a Differentiated Services Code Point (DSCP) value. This value is a field in an IP packet that enables different levels of services for the network traffic. When the video stream from the camera reaches a router, the DSCP value will tell the router what service level to be applied, e.g. the bandwidth amount. This value ranges from 0 to 63 in decimal format. The default value is 0, meaning QoS is disabled.

[Network Connection Check Settings] The camera checks for Internet connection, and reboots when it is disconnected from the Internet. This function is enabled by default.

Note: If you do not intend to connect the camera to the network, disable this function to prevent automatic reboot.

4.7.4 HTTPS

Note this function is only supported by face detection camera models.

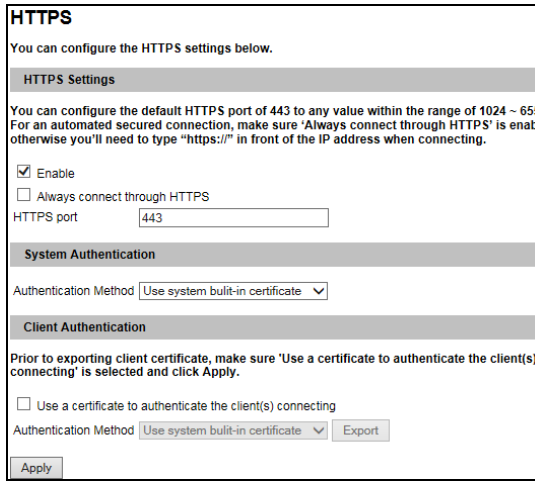


Figure 4-35

[HTTPS Settings] By enabling the HTTPS settings, you can access the camera through a secure protocol. The default HTTPS port is 443.

[System Authentication] You can use the operating system's built-in certificate or import a certificate verified by the SSL authority. To import, select **Import a certificate**, click **Browse** to locate the **Certificate file** and **Certificate Key file**, and type the password if the .pem files are protected by a password.

[Client Authentication] Select to use the certificate to authenticate the client connection.

4.7.5 IEEE 802.1X

IEEE 802.1x is an IEEE standard for port-based Network Access Control. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. Note this function is only supported by **GV-IPCAM H.265 firmware V1.14 or later**. This function is disabled by default.

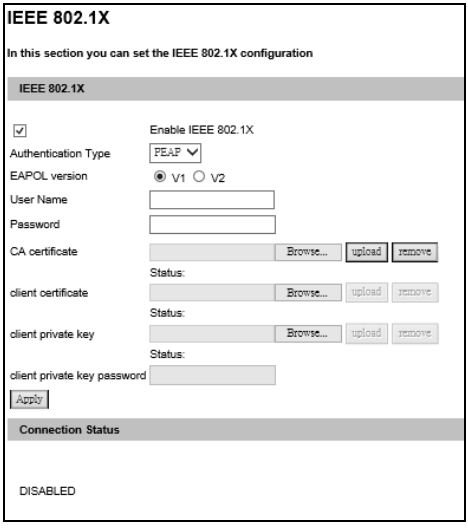


Figure 4-36

1. Enable **IEEE 802.1x**.
2. Select the **Authentication Type** from the dropdown list for your IP devices. If you select **PEAP**, go to Step 3. If you select **TLS**, go to Step 4.
3. Select the **EAPOL version**, type a valid **User Name** and **Password** for the authentication server. Note these options are only available if you select **PEAP**.

4. Click **Browse** to locate the **CA Certificate**, **Client Certificate**, **Client Private Key**, and **Client Private Key Password** at your local computer and click **Upload** to upload the credentials to the authentication server. Note these options are only available if you select **TLS**.
5. Click **Apply**. The **Connection Status** will show **Authentication Success** when the authentication is successful.

4.7.6 UMTS Settings

Not this function is not supported by **GV-IPCAM H.265**.

UMTS stands for Universal Mobile Telephone System. UMTS is a third-generation (3G) broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to 2 megabits per second. UMTS offers a consistent set of services to mobile computer and phone users, no matter where they are located in the world.

With a mobile broadband device (supporting UMTS, HSDPA, etc.) attached to the USB port on the rear panel, and with this UMTS function enabled, GV-Fisheye Camera can be accessed through wireless broadband. For supported mobile broadband devices, see *Appendix C*.

The Virtual Private Network (VPN) over a UMTS connection is also configurable on the setting page.

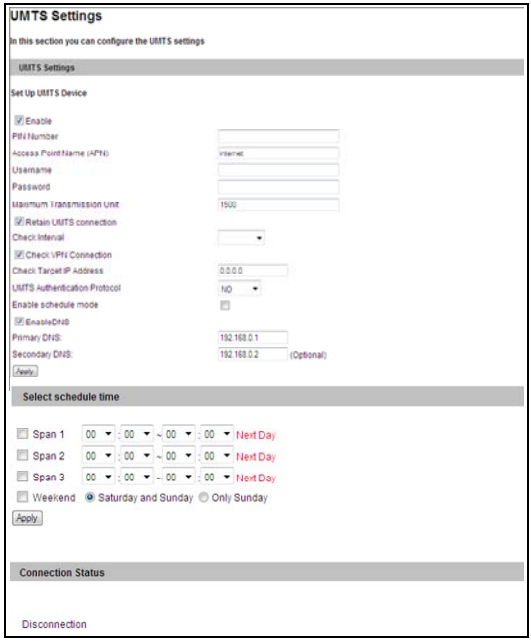


Figure 4-37

- **PIN number:** Type the PIN number that is provided by your network operator.
- **Access Point Name (APN):** Type Access Point Name that is provided by your network operator.
- **Username:** Type a valid username to enable the UMTS service from your network operator.
- **Password:** Type a valid password to enable the UMTS service from your network operator.
- **Maximum Transmission Unit:** Type the Maximum Transfer Unit (MTU). The default value is **1500**.

- **Retain UMTS Connection:** Select this option to check the UMTS connection status and use the drop-down list to specify the desired time length for check frequency. The GV-Video Server will rebuild the connection if disconnection is detected.
- **Enable VPN Connection:** Select this option to enable the VPN (Virtual Private Network) connection. Type the target IP address in the **Check Target IP Address** field.
- **UMTS Authentication Protocol:** Use the drop-down list to select the UMTS Authentication Protocol provided by your network operator.
- **Enable Schedule Mode:** Starts the UMTS connection automatically based on the schedule you set in the **Select Schedule Time** section. Refer to *4.5 Recording Schedule* for the same settings.
- **Enable DNS:** Optional type up to two DNS servers of your network operator.
- **3G Connection Status:** Indicates the connection status of UMTS or VPN.

Note:

1. When both WiFi and 3G signals are detected, the camera will connect to the network through WiFi.
2. UMTS Settings are not supported by GV-EBL2101 / 2111 / 3101 / 5101.

4.7.7 IP Filter Settings

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

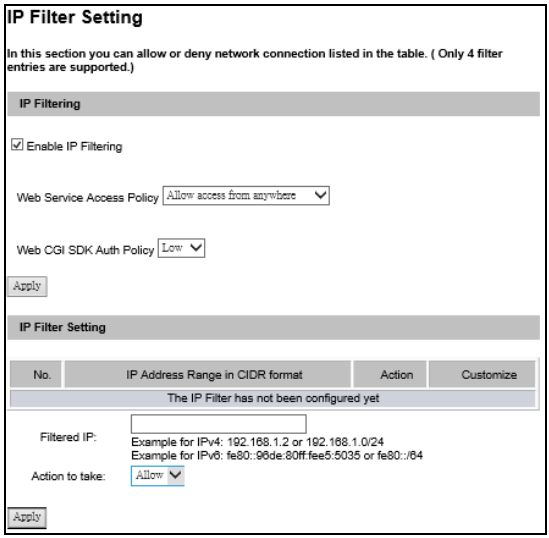


Figure 4-38

To enable the IP Filter function:

1. **Enable IP Filtering:** Enable the IP Filter function.
2. **Web Service Access Policy:** Select **Allow access from anywhere** (Default), **Allow access from local LAN** or **Disallow access from anywhere**.
3. **Web CGI SDK Auth Policy**: Select **Low** (Default) or **High,** which enhances the data transmission security, from the drop-down list. Note this function is designed for customers with the need to develop their own SDK, and is only supported by **GV-IPCAM H.265 firmware V1.14 or later**.

4. Click **Apply**.

Note:

1. Some models do not have the function of Web Service Access Policy.
2. If you select **Disallow access from anywhere**, before clicking Apply, remember to set one IP address for which access to the camera is allowed.

---

5. **Filtered IP:** Type one IP address or a range of IP addresses you want to restrict the access.
6. **Action to take:** Select the action of **Allow** or **Deny** to be taken for the IP address(es) you have specified.
7. Click **Apply**.

4.7.8 SNMP Settings

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

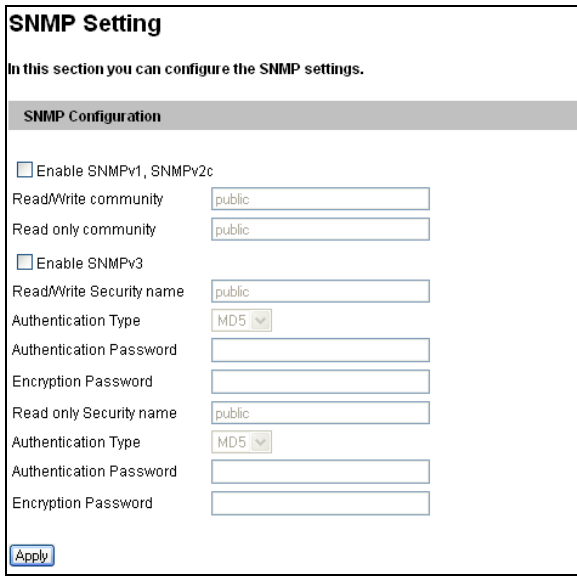


Figure 4-39

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 community string.
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**, follow steps 5 ~ 7.
9. Click **Apply** to save the settings.

4.8 Management

The Management section includes the settings of data and time and user account. You can also view the firmware version and execute certain system operations.

4.8.1 Date & Time Settings

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

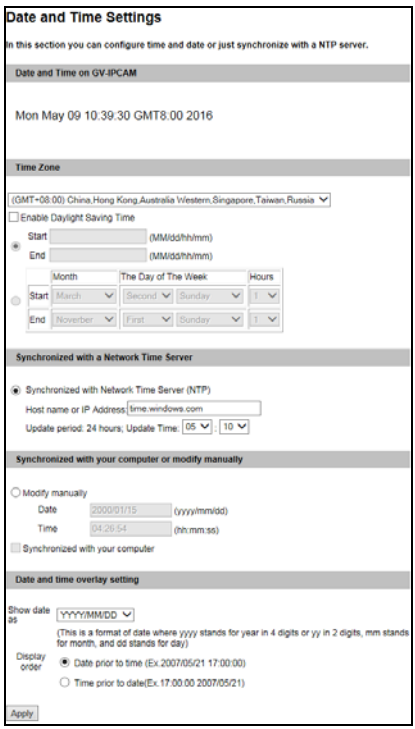


Figure 4-40

[Date & Time on GV-IP Camera] 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. Define the Start Time and End Time to enable the daylight saving function. You can also select which day of a week within a month to apply the DST setting.

To play back, see *5.2.4 Playback of Daylight Saving Time Events*. To automatically synchronize the Daylight Saving Time with the GV-DVR / NVR, see *7.1.1 Customizing IP Camera Settings on GV-DVR / NVR*.

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

[Synchronized with your computer or modify 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 Storage Settings

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

Note: The Target Series does not support memory cards. You can store recordings to a connected NAS server instead. Refer to *Network Neighborhood Settings* below.

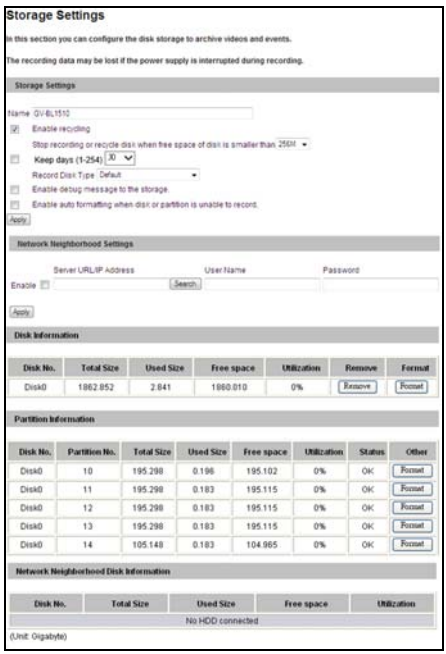


Figure 4-41

[Storage Settings]

- **Name:** Type the name of the storage device. The name can only contain English letters (of upper or lower cases), numerals, slashes, and hyphens.

Note: The setting of the device name is for GV-NAS System only.

- **Enable recycling:** If **Enable recycling** is selected, when the space of the storage device is lower than the specified space, the system will overwrite the oldest recorded files. If **Enable recycling** is not selected, the system will stop recording when the specified space is reached.
- **Keep days (1-254):** Select the number of days to keep the files from **1** day to **254** 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.
- **Enable debug message to the storage:** Note this function is not supported for **Target Series**. Debug message (see *4.8.4 Log Information*) is deleted after reboot. Select this option to store log information to an inserted storage device.
- **Enable auto formatting when disk or partition is enabled to record:** Note this function is not supported for **Target Series**. Select this option for the camera to automatically format the storage device when there is error during recording.

[Network Neighborhood Settings]

You can record to a connected NAS server.

Note:

1. Make sure your camera's video settings adhere to the following:
   - VBR is set to **Good**
   - Maximal Bit Rate is set to the following:

Camera Type	Max. Bit Rate
1.3 M	6 Mbps or lower
2 MP / 3 MP / 4 MP / 5 MP	8 Mbps or lower

2. For optimal performance and compatibility, it is highly recommended to use a GV-NAS System.
3. It is highly recommended to use a NAS server that supports a quota function, with which a separate quota is allocated to each camera.
4. GV-NAS System is not supported by GV-BX12201, GV-EBL2101 / 2111 / 3101 and GV-IPCAM H.265.
5. GV-IP Camera and GV-Target Series do not support recording to shared folders of a Windows-based server.
6. To avoid dropping frame rate, when GV-EFD3101 / GV-EVD3100 , GV-EFD5101 / GV-EVD5100 and GV-EBL5101 are connected to GeoVision software, and recording to NAS with the resolution of 2048 x 1536 and 2592 x 1944 at 30 fps, it is highly recommended to change its Max. Bit Rate to 6 Mbps in VBR setting.

To connect record to GV-NAS Systems, follow the steps below.

1. Under Network Neighborhood Settings, select **Enable** and click the **Search** button to search for available NAS servers.

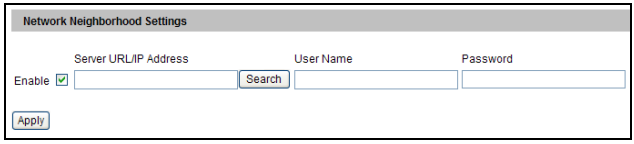


Figure 4-42

2. Type the username and password, and click **Select**.

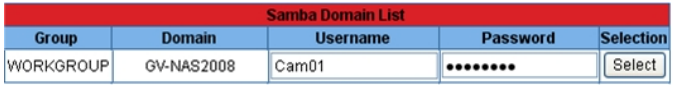


Figure 4-43

Note: Depending on the models of GV-NAS System, up to 16 default user accounts (username: **Cam01** – **Cam16**; password: **12345678**) are available. The storage limitation and recycle is applied on a user basis. It is recommended to use one user account exclusively for recording of one GV-IP Camera to avoid uneven data recycle.

---

3. Select a folder to store recordings, and click **OK**.

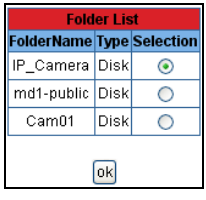


Figure 4-44

4. Click **Apply**. Once connected, the disk status will display.

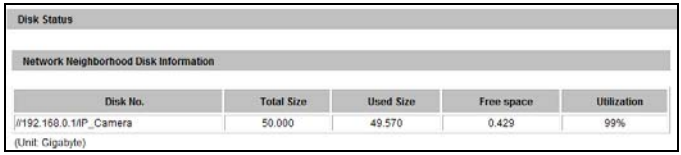


Figure 4-45

Tip: Instead of searching for available NAS servers, you can also type the storage path directly.

1. Type the Server URL/ IP Address in this format: **\\NAS IP Address\Storage Folder**. For example, \\192.168.0.1\IP_Camera. This GV-IP Camera will be recorded to a default shared folder named "IP_Camera" in the GV-NAS System.
2. Type the username and password. For GV-NAS System, you can type any of default usernames **Can01** to **Cam16**, and password is **12345678**.

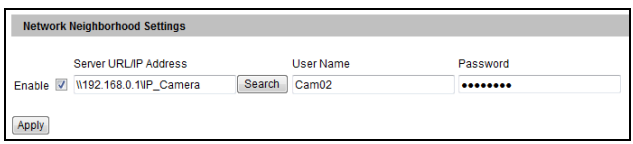


Figure 4-46

For details on GV-NAS System, refer to *GV-NAS System Quick Start Guide*.

[Disk Information]

Note this function is not supported for **Target Series**. This section shows the details of the attached storage device. Use the **Format**/**Remove** button to format or unload a storage device. For detail steps, see *Partition Information* below.

[Partition Information]

Note this function is not supported for **Target Series**. This section shows the partition details of the attached storage device.

To add a storage device:

1. Insert the storage device 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 storage device:

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

The storage device status is indicated in the status column:

Status	Description
Formatting	The storage device is being formatted.
Unknown	The camera can not recognize the format of the storage device or the device can not be found.
OK	Storage formatting is successful.
Try Mount	The camera is attempting to connect to the storage device.
Error File System	There is a recording error in the storage device. All the recording data is inaccessible under the status.

Read Only	The storage device cannot be written due to abnormal power disruption.
Repairing	The system is attempting to repair the recording data.

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. To upgrade the firmware from versions earlier than V2.07 to the latest version, be sure to back up the recordings on the camera’s storage device before the upgrade, and re-format the memory card after the upgrade. If you have not done so, this warning message appears when you view the Monitoring or Storage Settings’ Web interface:

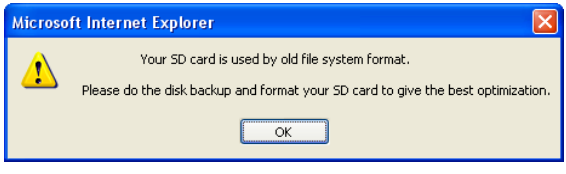


Figure 4-47

4.8.3 User Account

You can change the login name and password of Administrator and Guest. The default Administrator login name and password are **admin**; the default Guest login name and password are **guest**; the default FTP Server login name is **ftpuser** and the password is **123456**. To allow a Guest user log in without entering name and password, select **Disable authentication for guest account**. To prevent automatic logout of an Administrator / Guest account user after reboot, select **Disable auto logout when reboot**.

For **GV-IPCAM H.265 firmware V1.14 or later**, the default Administrator account is no longer supported. To adjust the minimum strength requirement for login password, select **Normal** or **Great** from Minimum Password Strength.

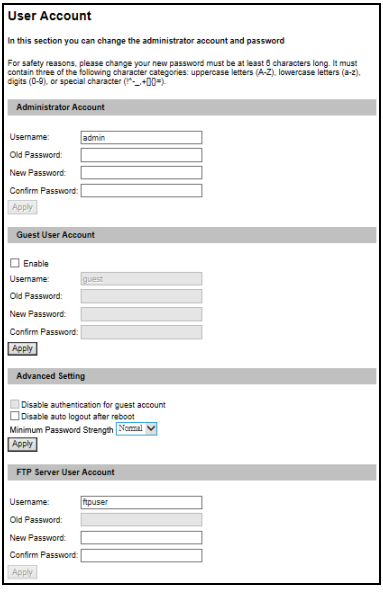


Figure 4-48

4.8.4 Security

Note this function is only supported by cameras with face detection features.

You can change the password security settings with 3 levels: Low, Medium (default value) and High. Each level differs from one another in the password strength required to log into the Web interface.

To customize the password security level based on your specified requirements, select one **Security Level** and configure the relevant user account and logon settings.

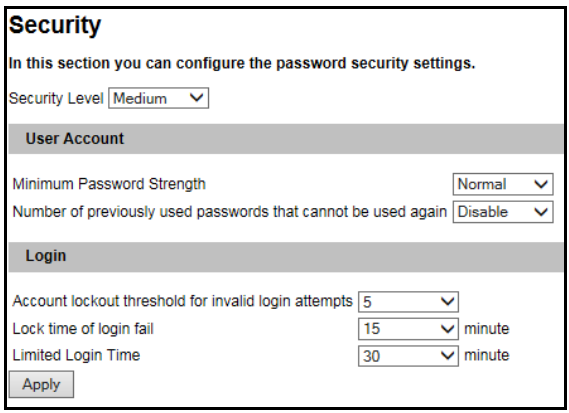


Figure 4-49

4.8.5 Privacy

Note this function is only supported by cameras with face detection features.

In order to provide you with the best user experience and deliver appropriate advertising messages and website content, GV-IP Camera's Web interface uses cookies. Select to agree with our privacy policy or delay in accepting our privacy policies.

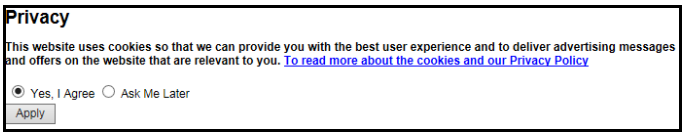


Figure 4-50

4.8.6 Log Information

The log information contains dump data that is used by service personnel for analyzing problems. The logs available may vary depending on the camera model.

4.8.7 Tools

You can execute certain system operations and view the firmware version.

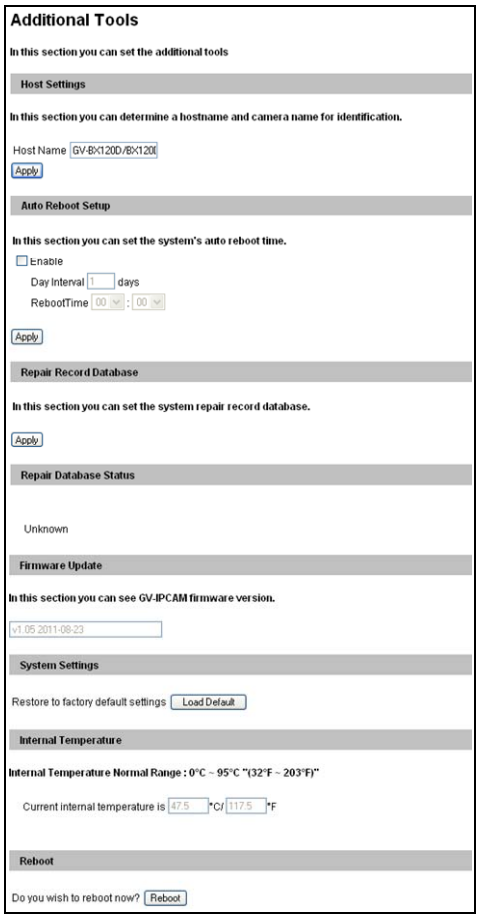


Figure 4-51

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

[Auto Reboot Setup] Select **Enable** to activate automatic reboot and specify the time for reboot in the sub fields.

- **Day Interval:** Type the day interval between each reboot.
- **Reboot Time:** Use the drop-down lists to specify the time for automatic reboot.

[Repair Record Database] Note this function is not available for **Target Series**. Click **Apply** to repair the database when errors occur while playing back the recordings with the Remote ViewLog player. Problems can occur when there are errors in firmware or damages to the micro SD card.

[Database Status] Note this function is not available for **Target Series**. Displays the repairing status of database.

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

[System Settings]

- **Load Default:** Clicking the **Load Default** button to restore factory default settings. After applying the default settings configure the camera's network setting again.
- **Load Default Without Network:** Clicking the **Load Default without Network** button to restore factory default settings without changing the camera's network settings.

[Temperature Status] Note this function is not available for **Target Series** (except for GV-EFD2101/3101/5101, GV-EVD2100/3100/5100 and GV-EBL5101), **Cube Camera** and **Advanced Cube Camera**. Displays the current chipset temperature inside the camera.

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

4.8.8 Language

Note this function is not available in **GV-PTZ010D**.

You can select the language for the Web interface. By default, the language on the Web interface will be the same with the one used for the operating system.

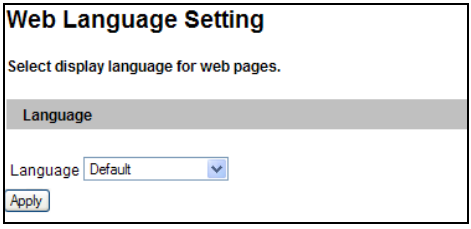


Figure 4-52

Chapter 5 Recording and Playback

Note that Recording and Playback function is not available for **Target Series**.

The camera can record video and audio directly to the memory card. You can play back the recorded files on the GV-DVR / NVR / VMS 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”, *4.8.2 Storage Settings*.
2. If you like to set up the 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 input device. 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 from the memory card by connecting it directly to the GV-DVR / NVR / VMS through a card reader
- Playback by using the Remote ViewLog function over the TCP/IP network
- Playback by using the recorded files downloaded from built-in FTP Server

5.2.1 Playback from the Memory Card

You can play back the files recorded at the GV-IP Camera by connecting the memory card to GV-DVR / NVR / VMS through a card reader. However, the videos on GV-IP devices are recorded in the Linux format and GV-DVR / NVR / VMS runs on a Windows-based computer. For Linux files to be readable and accessible on Windows, we use the Ext2Fsd program. Follow the steps below to download, install and execute the Ext2Fsd program.

IMPORTANT:

1. The Ext2Fsd program only works on Windows 2000, XP, 2003, vista, 7, 8 and Server 2012 (32-bit and 64-bit).
2. The Ext2Fsd program is subject and under term/condition of The GNU General Public License version 2 (GPLv2). Please read http://www.gnu.org/licenses/gpl-2.0.html before installation.

1. Download and install the Ext2Fsd from the company website.

Note: If you are using **Windows 8** or **Windows Server 2012**, change its compatibility before installing the Ext2Fsd program:

A. Right-click the Ext2Fsd program and select **Properties**. This dialog box appears.

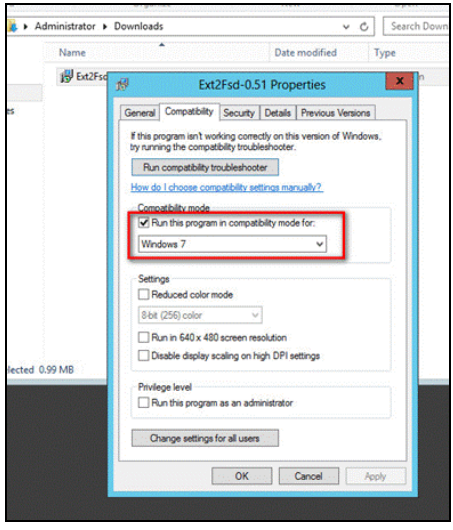


Figure 5-1

B. Select the **Compatibility** tab.

C. Select **Windows 7** using the drop-down list.

---

2. On Your desktop, click **Start**, select **Programs**, locate the **Ext2Fsd** folder and select **Ext2 Volume Manager**. All the connected drives are shown.

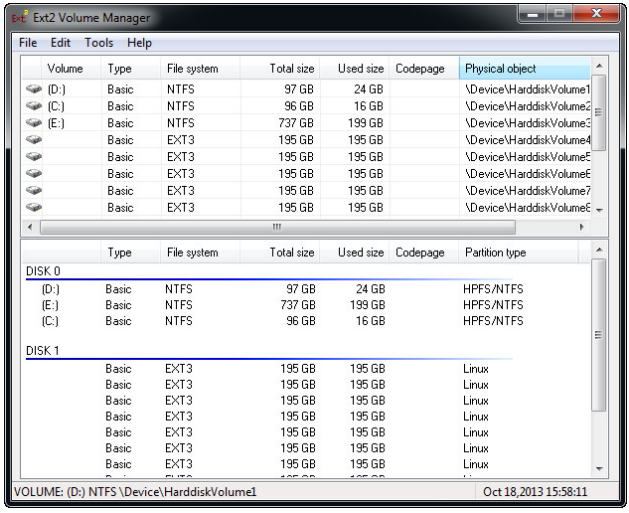


Figure 5-2

3. For the first-installation, execute the Ext2Fsd Service.

   A. From the Ext2 Volume Manager window, select **Tools** and select **Service Management**. This dialog box appears.

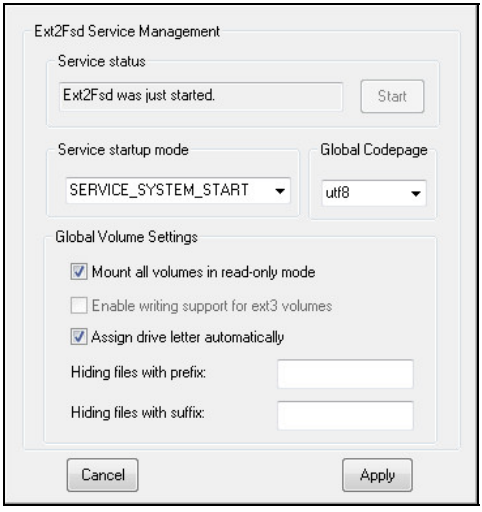


Figure 5-3

   B. Click **Apply**.

4. Mount the storage drive to your computer.

   A. From the Ext2Fsd Volume Manager window, right-click the storage drive and select **Ext2 Management**. This dialog box appears.

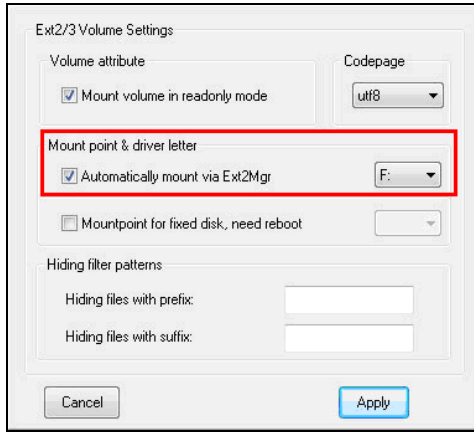


Figure 5-4

   B. Under the Mount point & driver letter section, select **Automatically mount via Ext2Mgr**, specify a disk drive using the drop-down list and click **Apply**.

C. On the Ext2 Volume Manager window, the storage drive is successfully mounted to your computer when it is indicated with the disk drive you specified.

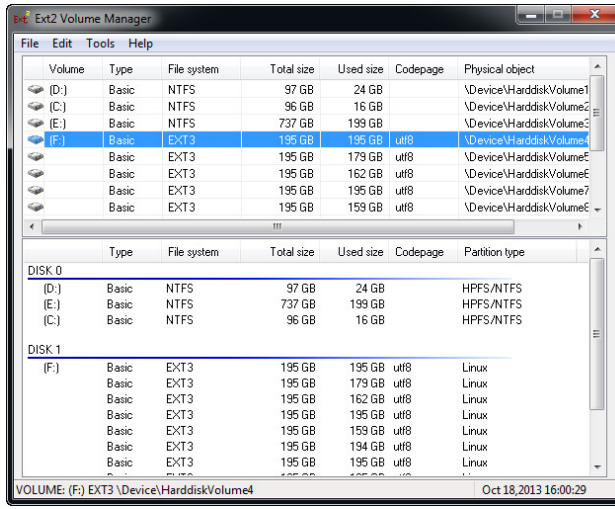


Figure 5-5

5. Access the recording files from the specified drive of your computer.

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. You can also play back the files recorded at the camera over GV-NAS System.

1. The camera needs to allow the remote access with **ViewLog Server** activated. See *4.3.7 ViewLog Server*.
2. For the first-time user, install the **Remote ViewLog** program from the company website. Next time whenever you like to use this remote playback function, access this option from the camera's Web interface.
3. When the Remote ViewLog player is enabled, you will be prompted to select Remote ViewLog Service or Remote Storage System. Select **Remote ViewLog Service**.
4. When this dialog box appears, type the camera's IP address, login ID and password. In the Host Type field, select **GV-IP Device-SD Card**. and the default port is **5552**. To retrieve recordings from GV-NAS System, select **GV-IP Device-NAS** and the default http port is **80**.

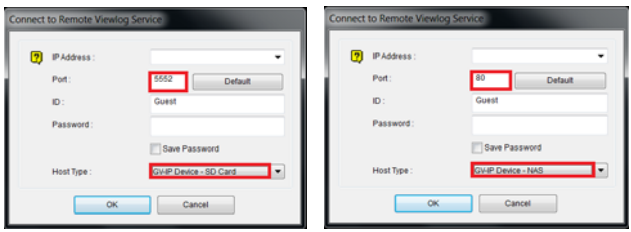


Figure 5-6

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 Media Player. For details to download files, see [Act as FTP Server], *4.3.2 FTP*.

Note: To play back videos, ensure you have installed Geovision codec on the computer. The codec is available on the company website. If you have installed the Remote Playback player on the computer, it is not required to install the codec.

5.2.4 Playback of Daylight Saving Time Events

On GV-DVR / NVR, 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 to GV-DVR / NVR for playback.

The following instructions describe how to retrieve the recorded files from the camera over network. 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 *5.3.7 ViewLog Server*.
2. To remotely connect to the camera from GV-DVR / NVR, 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.

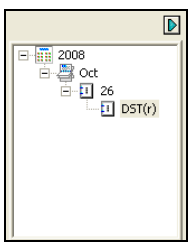


Figure 5-7

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 the GV-DVR / NVR of version 8.3 and 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 periodically releases updated firmware on the website. Simply download the new firmware into the camera using the Web interface or GV-IP Device Utility available on the company website.

Important Notes before You Start

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

1. If you use the IP Device Utility for firmware upgrade, the computer used to upgrade firmware must be under the same network as the camera.
2. Stop monitoring of the camera.
3. Stop all the remote connections, such as GV-VMS.
4. 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).

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

---

5. Do not turn the power off within 10 minutes after the firmware is updated.

If firmware upgrade fails, manually restore the camera to its default settings. For details, see *Loading Factory Default* in the corresponding *Hardware Manual*.

6.1.1 Using the Web Configuration 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.

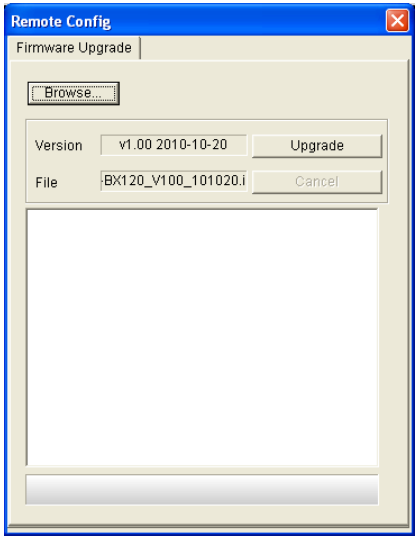


Figure 6-1

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

6.1.2 Using the IP Device Utility

The IP Device Utility provides a direct way to upgrade the firmware to multiple units of the GV-IPCAM. Note the computer used to upgrade firmware must be under the same network as the camera.

1. Download and install the GV-IP Device Utility program from the company website.
2. Double-click the **IP Device Utility** icon created on your desktop. This dialog box appears and lists the IP devices detected on the same LAN. You can click the titles of Mac Address and IP Address to sort the devices in the list.

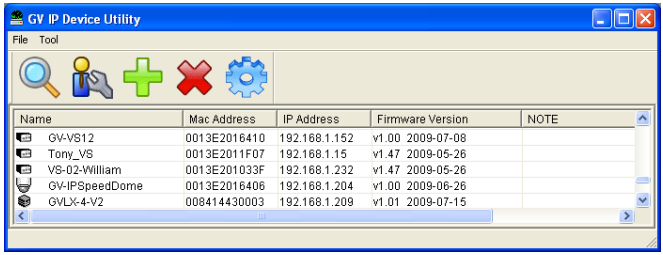


Figure 6-2

3. Double-click one camera in the list, and click the **Firmware Upgrade** tab on the pop-up dialog box.

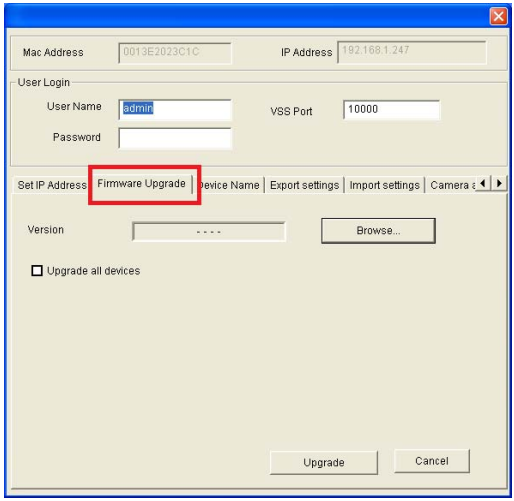


Figure 6-3

4. Click the **Browse** button to locate the firmware file (.img) saved at your local computer.
5. If you like to upgrade all the cameras in the list, select **Upgrade all devices**.
6. Type **Password**, and click **Upgrade** to start the upgrade.

6.2 Backing Up and Restoring Settings

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

To back up the settings:

1. Run **IP Device Utility** and locate the desired camera. See Steps 1-2 in *6.1.2 Using the IP Device Utility*.
2. Double-click the camera in the list, and click the **Export Setting** button on the pop-up dialog box.

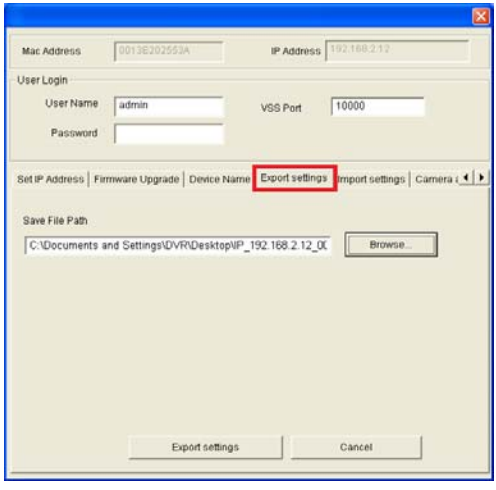


Figure 6-4

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

To restore the settings:

1. In Figure 6-4, click the **Import Settings** tab. This dialog box appears.

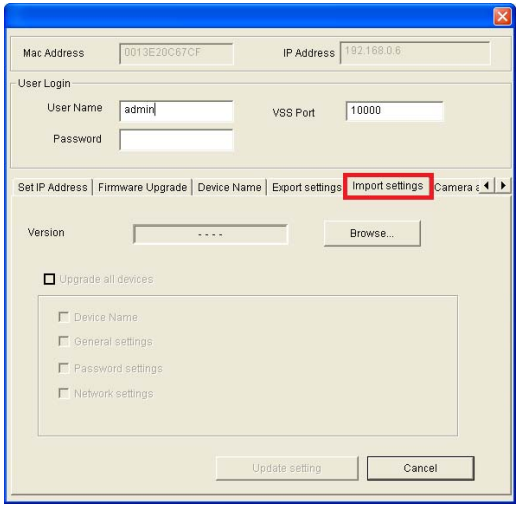


Figure 6-5

2. Click the **Browse** button to locate the backup file (.dat).
3. Select **Upgrade all devices** to import the settings into devices of the same type in the same LAN.
4. To import device name, password settings and/or network settings, select **Device Name**, **Password settings** and/or **Network settings**.
5. Type **Password** and click the **Update settings** button to start restoring.

6.3 Changing Password

You can change the login password of your GV-IP Camera using GV-IP Device Utility.

1. Run **IP Device Utility** and locate the desired camera. See Steps 1-2 in *6.1.2 Using the IP Device Utility*.
2. Double-click the camera in the list, select the **Other Settings** tab on the pop-up window and type **Password** of the camera under User Login.

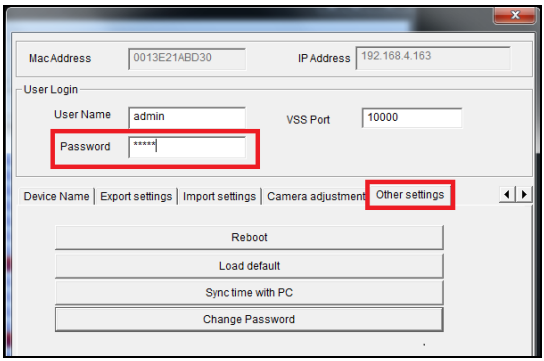


Figure 6-6

3. Select **Change Password** to set up a new password.
4. To change devices of the same type to the same password, select **Sync all devices**.
5. Click **OK** to apply the change.

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 creation. Watermarking ensures that an image is not edited or damaged after it is recorded. To enable the watermark function, see [Watermark Setting], *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 (No.6, 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 **Ext2Fsd program** for Windows-based system to read and access Linux-based files. For the instructions, see *5.2.1 Playback from the Memory Card*.

6.4.2 Running Watermark Proof

1. Install **Watermark Proof** from GeoVision Website. 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 mark will appear in the **Pass** column. On the contrary, if the recording is modified or does not contain watermark during recording, a check mark would appear in the **Failed** column. To review the recording, double-click the listed file on the window.

6.4.3 The Watermark Proof Window

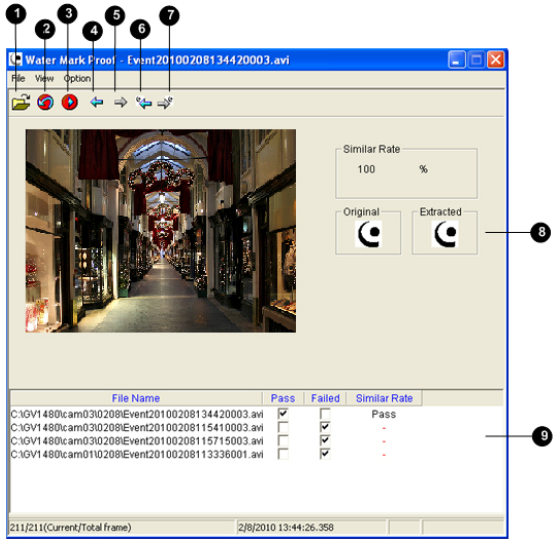


Figure 6-7

The controls in the window:

No.	Name	Description
1	Open File	Opens the recording.
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.

No.	Name	Description
8	Original vs. Extracted	The Extracted icon should be identical with the Original icon. If not, it indicates the recording has been tampered.
9	File List	Displays the proof results.

6.5 Downloading Videos from the Micro SD Card

When connections of GV-IP Cameras to the GV-DVR / NVR / VMS are lost, recordings are automatically saved to the memory cards inserted in the GV-IP Cameras. To automatically synchronize and download recordings from the micro SD cards to a local folder, install and execute the **GV-SDCardSync Utility** program.

Note:

1. GV-SDSyncCard Utility is only supported in GV-DVR / NVR V8.5.4 or later, GV-VMS V14.10 or later and in GV-IPCam H.264 V1.11 or later.
2. Target Series do not support Micro SD Card.

6.5.1 Installing the GV-SDCardSync Utility

1. Download the **GV-SD Card Sync Utility** program.

Note: The GV-SD Card Sync Utility must be installed on the computer installed with GV-DVR / NVR V8.5.4, GV-VMS V14.10 or later software versions.

---

2. Execute the **GV-SDCard Sync Utility** program. The main window and the Setting window appear. The Setting window pops up automatically upon first execution. Otherwise, click the **Setting** button .

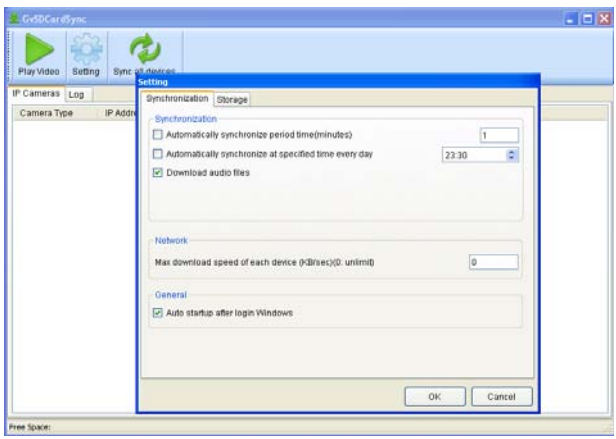


Figure 6-8

3. To configure synchronization, network and startup settings, see the steps below.

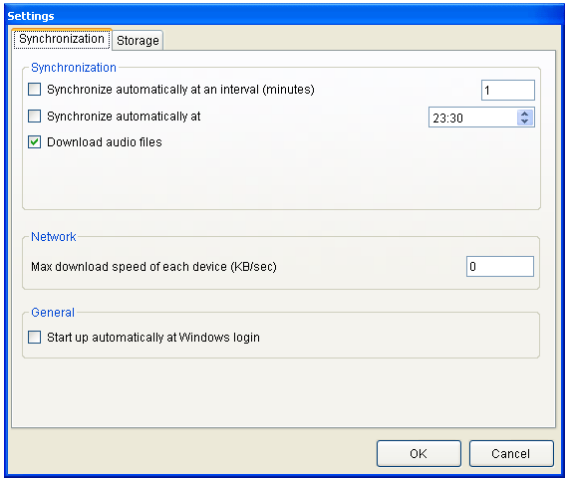


Figure 6-9

[Synchronization]

- **Synchronize automatically at an interval:** Automatically synchronize videos from micro SD cards to a local folder at the specified interval.
- **Synchronize automatically at:** Automatically synchronize videos from micro SD cards to a local folder at the specified time.
- **Download Audio Files:** You may choose to download audio files along with the video files. This option is enabled by default.

[Network]

- **Max. download speed of each device (Kb/sec):** To make sure the bandwidth is not completely taken up while downloading files from the memory card, specify a maximum download speed. If you do not want to set a bandwidth limit, type **0**.

[General]

- **Start up automatically at Windows login:** GV-SDSync Utility launches automatically when Windows starts up.

4. By default, downloads are saved to **:\GvSDCardSync** and are not recycled automatically. To configure the storage and recycling settings, select the **Storage** tab on the Setting window. This page appears.

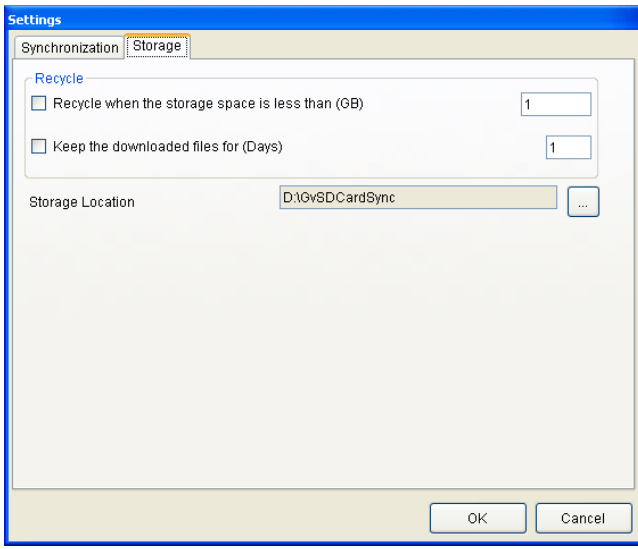


Figure 6-10

[Recycle]

- **Recycle when the storage space is less than (GB):** Specify a minimum free space of your local storage for file recycling.
- **Keep the downloaded files for (Days):** Specify the number of days to keep the download files at the local hard drive.

[Storage Location]

To configure the storage path, click the button next to the location field and specify a storage location.

5. Click **OK** to save the configuration or exit the Setting window.

Note: Keep the GV-SDCardSync Utility running in the background to automatically synchronize and download videos.

6.5.2 The GV-SDCardSync Utility Window

After you have installed the GV-SDCardSync Utility, point to **Start**, select **Programs**, select **GV-SDCardSync** and select GvSDCardSync to launch the program. This window appears.

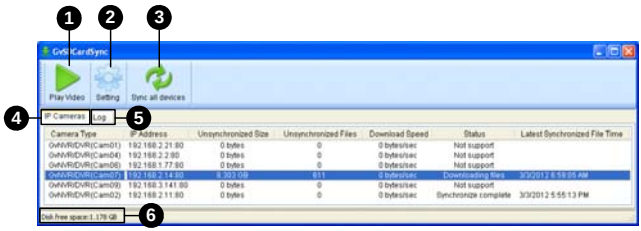


Figure 6-11

No	Name	Description
1	Play Video	Plays downloaded recordings of the selected GV-IP Cameras using the ViewLog player. For details, see Chapter 4, *DVR User's Manual* on GeoVision Website.
2	Setting	Contains settings on synchronization, network, storage location and recycling criteria. See step 4 in *6.6.1 Installing the GV-SDCardSync Utility*.
3	Sync all devices	Manually synchronizes and downloads the recording files stored at GV-IP Cameras.
4	IP Camera Tab	Shows information of GV-IP Cameras connected to the GV-DVR / NVR / VMS, including channel number, IP address, size and number of unsynchronized files, download speed, status and the last synchronization time.

No	Name	Description
5	Log Tab	Displays up to 100 event entries of the GV-SDCardSync Utility. Once the entries are full, recycling will start from the oldest file.
6	Storage Space	Shows the storage space of the designated hard drive.

Note:

1. The synchronization time is recorded according to the system time of the GV-IP Camera.
2. The logs are deleted once the GV-SDCardSync Utility is re-activated.

Chapter 7 DVR / NVR / VMS

The GV-DVR / NVR / VMS provide a total video management solution, with features such as video viewing, recording, playback, alert settings and more. Compatible GV-DVR / NVR / VMS version is required to integrate with your IP camera. For details, see *Appendix G*.

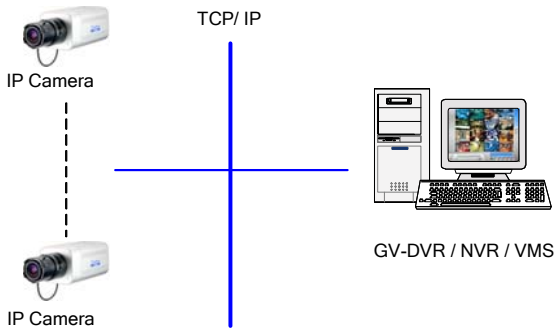


Figure 7-1

- The maximum number of streams which the camera allows varies according to its resolution:

Camera Models	Max. No. of Streams
GV-PTZ010D	3
1.3 M models except GV-PTZ010D	8
2 M models	
3 M models	
5 M models	
8 M models	
12 M models	

- When the camera is connected to IE browser or any other applications, it takes up 1 stream; when the camera is connected to GV-DVR / NVR / VMS, it takes up 2 streams.

Note: By default, the camera is in dual streams and will take up 2 streams when connected to GV-DVR / NVR / VMS.

- The hardware compression and the “Pre-Recording Using RAM” feature cannot work on the videos from the camera.

7.1 Setting up an IP Camera on GV-DVR / NVR

To set up the camera on the GV-DVR / NVR, follow these steps:

1. On the main screen, click the **Configure** button, select **System Configure**, select **Camera Install** and click **IP Camera Install**. This dialog box appears.

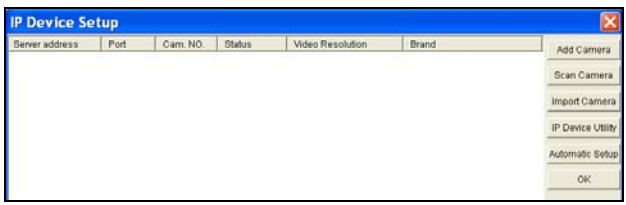


Figure 7-2

- To add an IP camera from a list of the IP cameras on the LAN, click **Scan Camera**.
- To manually set up an IP camera, follow steps 2 to 7

2. Click **Add Camera**. The dialog box appears.

Figure 7-3

3. Type the IP address, username and password of the IP camera. Select the camera brand and device from the drop-down lists. This dialog box appears.

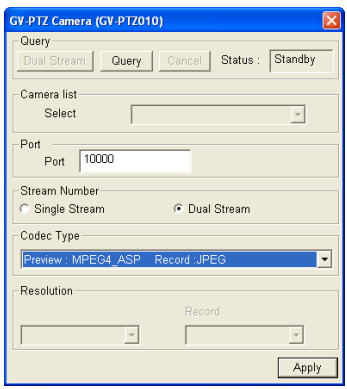


Figure 7-4

4. The GV-DVR / NVR will automatically query for the IP camera, and the status will be indicated as “Standby”. If not, modify the HTTP port (Figure 7-3) and streaming port (Figure 7-4) to match those of the IP camera, and click the **Query** button to detect the IP camera again.

5. The options in the setup dialog box may vary depending on the camera model.
   - **Dual Stream:** Click this button to set the codec type to H.264 in the main stream and to MJPEG in the sub stream, and each stream with a different resolution.
   - **Port:** Video streaming port number.
   - **Stream Number:** You have the option of single streaming only or both single and dual streaming.
   - **Codec type:** You have the options of JPEG and H.264. If the selected camera supports dual streaming, the preview codec and recording codec can be set differently.
   - **Resolution:** Select resolutions for preview and recording.
6. Click **Apply**. The IP camera is added to the list.
7. Click the listed camera, and select **Display position** to map the IP camera to a channel on the GV-DVR / NVR.

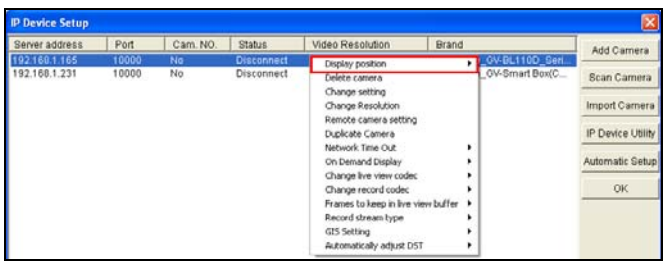


Figure 7-5

8. The Status column now should display "**Connected**". Click **OK**.

7.1.1 Customizing IP Camera Settings on GV-DVR / NVR

After the IP camera is connected and assigned with a display position, you can configure the camera's settings such as frame rate, codec type and resolution. Right-click the desired camera to see the following list of options:

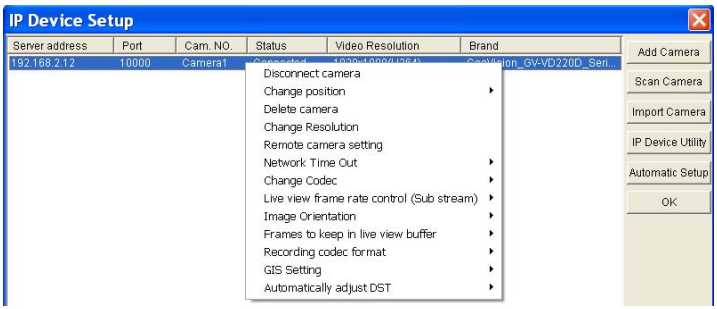


Figure 7-6

- **Change Resolution:** Changes the display ratio, live view resolution and record resolution
- **Network Time Out:** When network disconnection exceeds the specified time period, the camera status will be displayed as Connection Lost.
- **Change Live View Codec:** Changes the live view codec.
- **Change Record Codec:** Changes the recording codec.
- **Live-view frame rate control (Sub stream):** Sets the live view frame rate of the sub stream to help reduce the CPU usage. If you have set the live view codec to be **JPEG**, select the number of frames to allow in a second. If you chose the **H.264** codec, select one of the following options:
  - **Maximum Live-view Frame Rate:** View the video at the maximum frame rate possible.

- **Live-view Key Frame only:** You can choose to view the key frames of the videos only instead of all frames on the live view. 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.

- **Live-view frame rate control (Main stream):** Sets the live view frame rate of the main stream with higher resolution when On Demand function is enabled. Refer to Live-view frame rate control above to see the options available.
- **Image Orientation:** You can adjust the image orientation by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip** or **Rotate 180**.
- **Frames to keep in live view buffer:** Specifies the number of frames to keep in the live view buffer.
- **Recording Codec Format:** Specifies whether to record in standard or GeoVision type of JPEG or H.264 codec.
- **GIS Setting:** Records the video with the GPS data. To record the GPS data, remember to also enable the GIS function of the GV-DVR / NVR (Configure button < Accessories < Enable Local GIS).
- **Automatically Adjust DST:** If enabled, the time on the GV-IP device Web interface will be synchronized with the time of the GV-DVR / NVR when DST period starts or ends on the GV-DVR / NVR.

7.2 Setting Up IP Cameras on GV-VMS

Follow the steps below to manually connect your GV-IP Camera to GV-VMS.

Note: The following instructions are based on V14.10 software and user interfaces.

1. To access the IP Device Setup page, click **Home**, select **Toolbar**, click **Configure** and select **Camera Install**.

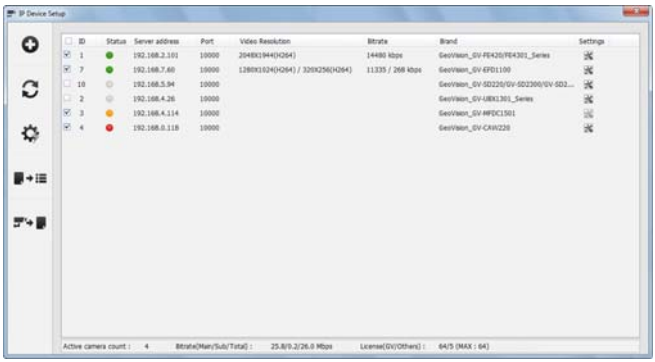


Figure 7-7

2. Click **Add Camera** . This dialog box appears.

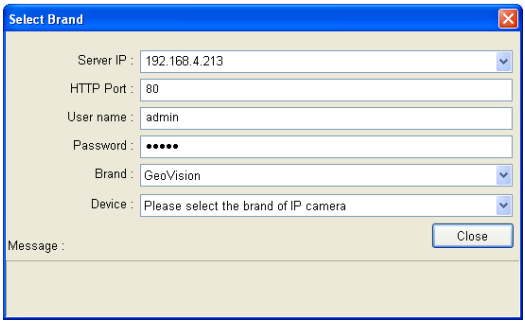


Figure 7-8

3. Type the IP address, username and password of the GV-IP Camera. Modify the default HTTP port **80** if necessary.
4. Select **GeoVision** and model name from the **Brand** drop-down list and select the GV-IP Camera from the **Device** drop-down lists. This dialog box appears.

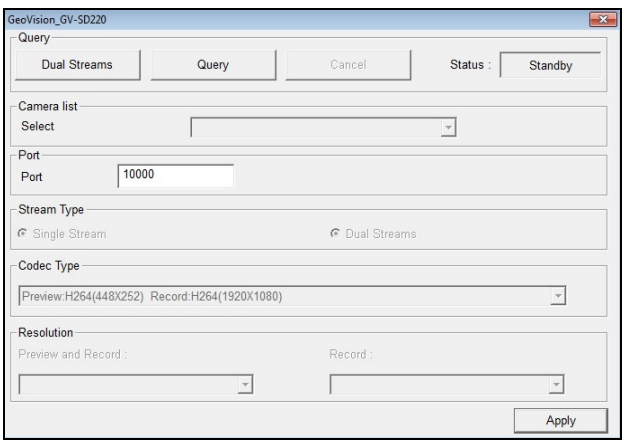


Figure 7-9

5. In the dialog box, configure the options which may vary depending on camera brands.
   - **Dual Streams:** It is set to dual streams by default. Select this option to apply the dual-streaming settings (lower resolution for live view and higher resolution for recording) if the camera supports dual streams.
   - **Query:** Detect and apply the current codec and resolution setting on the camera. This function may not be available for some third-party cameras.
   - **Camera list**: Select a camera number.
   - **Port:** Modify the video streaming port number if necessary.
   - **Stream Type:** You may have the option of **Single Stream** or **Dual Streams** depending on camera models.
   - **Codec Type:** You may have different codec options depending on camera models. If the selected camera supports dual streaming, the live view codec and recording codec can be set differently.
   - **Resolution:** You may select the different resolutions for live view and recording.
6. Click **Apply** to add the GV-IP Camera to the list.
7. To connect the added camera, click the box besides the **ID** column. Upon successful connection, the **Status** icon shows green, with the video resolution and bit rate being displayed in the correspondent columns.

Figure 7-10

7.3 Remote Monitoring with Multi View

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

Note: Multi View is not supported by GV-VMS.

7.3.1 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.

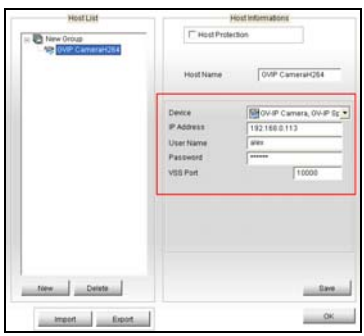


Figure 7-11

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

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

7.4 Remote Monitoring with E-Map

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

7.4.1 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
4. To create a host, click the **Add Host** button on the toolbar and select **Add IPCam**.
5. Right-click the created New Host in the Host View, and select **Host Settings**. This dialog box appears.

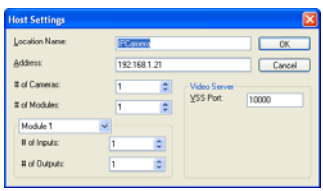


Figure 7-12

6. Give the camera a location name, and type its IP address (or domain name). Modify the default VSS port **10000** if necessary.

7. Click **OK** to save the settings.
8. Expand the created host folder. Drag and drop the icons of camera and I/O devices onto the imported E-Map.
9. 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 Applications”, *GV-DVR User’s Manual* or *GV-VMS User’s Manual.*

7.4.2 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 “E-Map Applications”, *GV-DVR User’s Manual* or *GV-VMS User’s Manual*.

Chapter 8 CMS Configurations

This section introduces the related settings to enable connecting to the camera in the central monitoring stations Center V2, Vital Sign Monitor and Dispatch Server.

8.1 Center V2

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

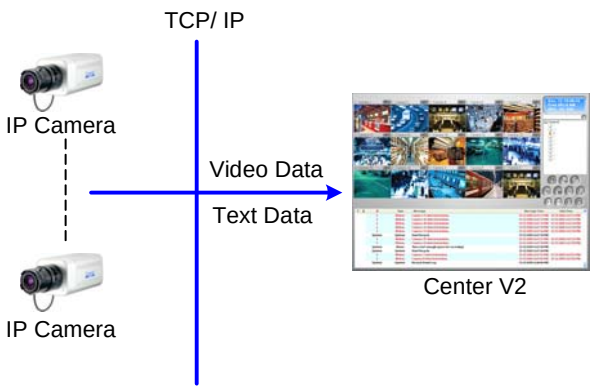


Figure 8-1

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

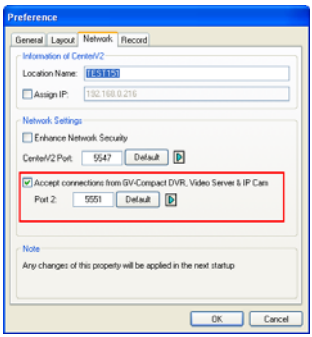


Figure 8-2

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

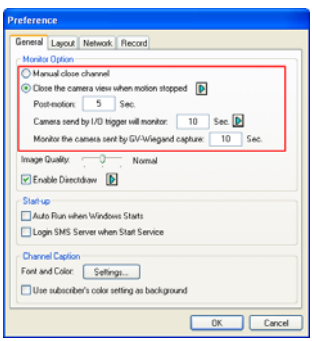


Figure 8-3

- **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 a 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 remain on the monitoring window for the specified time. For example, if the alarm is triggered for 5 minutes and you set 10 minutes, the camera view will be displayed for 15 minutes.

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

8.2 Vital Sign Monitor

The Vital Sign Monitor is designed to monitor and manage the camera and I/O devices connected to the camera under low bandwidth network.

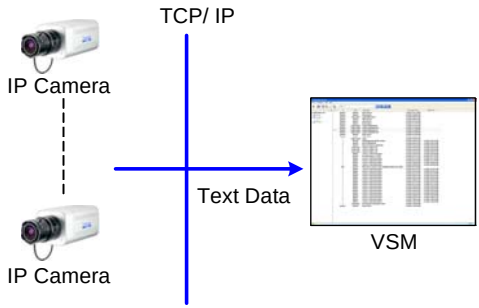


Figure 8-4

- To set the appropriate port connecting to the IP camera, click **Configure** on the window menu, and select **System Configure** to display this dialog box. In the Connective Port field, keep the default port **5609**, or modify it to match the Vital Sign Monitor port on the IP camera.

Figure 8-5

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

8.3 Dispatch Server

The Dispatch Server minimizes overloading of Center V2 Servers by re-distributing the GV-IPCAM subscribers to the least busy Center V2 Server.

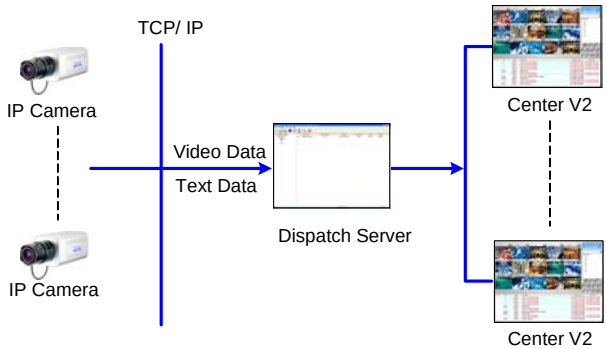


Figure 8-6

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

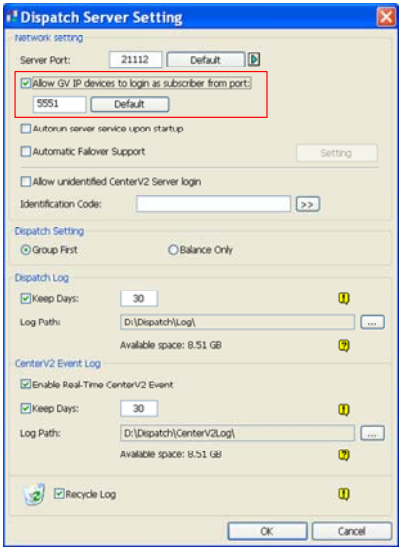


Figure 8-7

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

Chapter 9 Smart Device Connection

You can access the live view and play back recordings on your mobile devices using the mobile application **GV-Eye**. Android Smartphone, tablet, iPad, iPhone and iPod Touch are supported.

For details on system requirements, installation and setup, visit the company website.

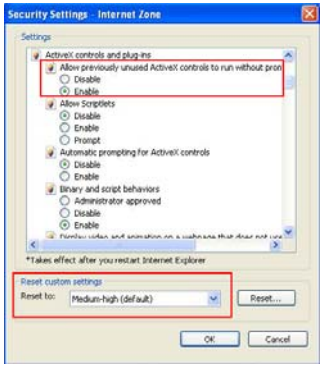
Note: To receive the live video from the camera, enter the TCP/IP port on your mobile phone. To play video back, enable **ViewLog Server** on the camera and enter the RPB Port on your mobile phone.

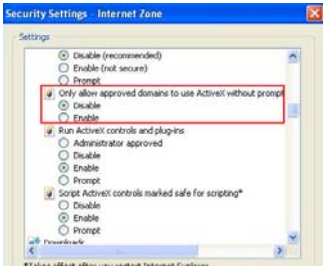
Appendix

A. Settings for Internet Explorer 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 Command

The GV-IPCAM H.264 can support RTSP protocol for both audio and video streaming.

- If you use the QuickTime player, enter:

rtsp://<IP of the GV-IPCAM H.264:8554/<CH No.>.sdp

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

- If you use the VLC, and if authentication is required, enter:

rtsp://username:password@<IP of the GV-IPCAM H.264:8554/<CH No.>.sdp

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

- If you use the VLC, and if authentication is *not* required, enter:

rtsp://@<IP of the GV-IPCAM H.264:8554/<CH No.>.sdp

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

- For RTSP Multicast, add “M” after the channel number.

For example, rtsp://@192.168.3.111:8554/CH001M.sdp or

rtsp://admin: admin@192.168.3.111:8554/CH001M.sdp

Note:

1. The RTSP streaming is supported over HTTP, UTP and TCP port.
2. The RTSP server must be enabled on the Web interface. See Figure 21-20.
3. Only VLC and QuickTime players are supported for streaming video via RTSP protocol.
4. For GV-PTZ010D, the RTSP streaming provides source video images of 352 x 240 / 352 x 288 only.

C. Supported UMTS Protocol (3G Modem)

Brand	Model
Huawei	E220, E392
	E169, E1692, E156, EC189, E1752, E1756, E1756C, E169C
Novatel	MC998D
	USB760, USB727, MC950D
ONDA	MSA523HS
ZTE	MF100

D. The CGI Command

You can use the CGI command to obtain a snapshot of the live view or access the User Account Web interface. For a GV-IPCAM H.264 with the following details:

IP address: 192.168.2.11

Username: admin

Password: admin

Desired stream: 1

- To obtain a snapshot of the live view, type the following into your Web browser:

http://192.168.2.11/PictureCatch.cgi?username=admin&password=admin&channel=1

- To access the User Account Web interface, type the following into your Web browser:

http://192.168.2.11/ConfigPage.cgi?username=admin&password=admin&page=UserSetting

Note: For GV-BX12201, if you use the CGI command to obtain a snapshot, the images stem from the live view of Stream 2 with the maximum resolution of 1 MP.

E. Power Supply Support List

The supported power type is indicated with a tick (✓) and the unsupported power type with a cross (✗).

GV-IP Camera		DC Power	AC Power	PoE
Box Camera (H.264 and H.265)		✓	✗	✓
Ultra Box Camera		✓	✗	✓
Target Box Camera		✓	✗	✓
IR Arctic Box Camera	GV-BX1500-E GV-BX2400-E GV-BX3400-E GV-BX5300-E	✗	✗	✓
	GV-BX2510-E GV-BX5310-E	✓	✓	✓
Mini Fixed Dome		✓	✗	✓
Mini Fixed Rugged Dome		✗	✗	✓
Target Mini Fixed Dome		✓	✗	✓
Target Mini Fixed Rugged Dome		✓	✗	✓

GV-IP Camera		DC Power	AC Power	PoE
Bullet Camera	All except GV-BL2510-E GV-BL5310-E	✓	✓	✓
	GV-BL2510-E GV-BL5310-E	✓	✓	✗
Bullet Camera (H.265)		✓	✗	✓
Ultra Bullet Camera		✓	✗	✓
Target Bullet Camera		✓	✗	✓
PTZ Camera		✓	✓	✓
PT Camera		✓	✓	✓
Vandal Proof IP Dome		✓	✓	✓
Vandal Proof IP Dome (H.265)		✓	✗	✓
Fixed IP Dome		✓	✓	✓
Cube Camera		✓	✗	✗
Advanced Cube Camera	GV-CA120/220	✓	✗	✓
	GV-CAW120/220	✓	✗	✗
Uni Pinhole Camera		✗	✗	✓

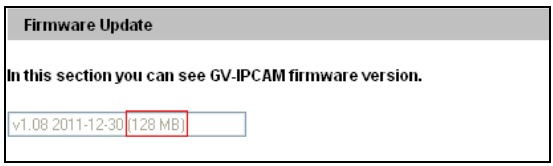
F. Supported Firmware for Flash Memory

The 128 MB flash memory is supported in **V1.09 or later** in all models of GV-IPCam H.264 Series except GV-PTZ010D.

To look up if the camera contains a 128 MB type flash memory, access the Web interface or the GV IP Device Utility:

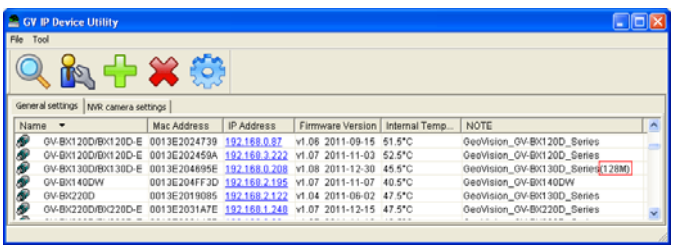
- **Web Interface**

  Click **Management** and click **Tools**. The “128 MB” should be noted after the firmware version.



- **GV IP Device Utility**

  The “128 M” should appear under the NOTE column.



G. Compatible Version of GV-DVR / NVR / GV-VMS for Each Camera Model

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Box Camera	GV-BX2400-1F ~ 2F	V8.5.5 or later / V14.10 or later
	GV-BX2700 Series	V8.7.1.0 (with patch files) or later / V15.11.1.0 (with patch files) or later
	GV-BX4700 Series / 5700 Series	V8.7.0 (with patch files) or later / V15.11 (with patch files) or later
	*Video Analysis only works with GV-VMS V15.10 or later	

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Box Camera	GV-BX12201	V8.6.2 (with patch files) or later / V14.10.1 (with patch files) or later
	GV-BX2700-FD GV-BX4700-FD GV-BX8700-FD	V8.7.6.0 or later (with patch files) / V18.1 or later (with patch files)
	GV-BX2600-FD GV-BX8700	V8.8.0 or alter (with patch files) / V17.2.1 or later
Ultra Box Camera	GV-UBX1301 Series GV-UBX2301 Series GV-UBX3301 Series	V8.5.6 or later / V14.10 or later
Target Box Camera	GV-EBX1100 Series GV-EBX2100 Series	V8.5.9 or later / V14.10 or later
Target Fixed Dome	GV-EFD2101 GV-EFD3101	V8.6.2 (with patch files) or later / V14.10.1 (with patch files) or later
	GV-EFD5101	V8.6.2.0 (with patch files) or later / V15.10.1.0 or later
IR Arctic Camera	GV-BX1500-E	V8.5.8 or later / V14.10 or later
	GV-BX2400-E GV-BX3400-E GV-BX5300-E	V8.5.7 or later / V14.10 or later
	GV-BX2510-E GV-BX5310-E	V8.5.9 (with patch files) / V14.10 or later
	GV-BX4700-E	V8.7.1.0 (with patch files) or later / V15.11.1.0 (with patch files) or later

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Mini Fixed Dome	GV-MFD3401 Series GV-MFD5301 Series	V8.5.8 or later / V14.10 or later
	GV-MFD2700 Series GV-MFD4700 Series	V8.7.1.0 (with patch files) or later / V15.11.3.0 (with patch files) or later
Mini Fixed Rugged Dome	GV-MDR320 GV-MDR520	V8.5 or later / V14.10 or later
	GV-MDR1500 Series GV-MDR3400 Series	V8.5.9 or later / V14.10 or later
Target Mini Fixed Dome	GV-EFD1100 Series	V8.5.9 or later / V14.10 or later
	GV-EFD4700 Series	V8.7.1.0 (with patch files) or later / V15.11.1.0 (with patch files) or later
	GV-EFD2700 Series	V8.7.3.0 (with patch files) or later / V16.11.0.0 (with patch files) or later
Target Mini Fixed Rugged Dome	GV-EDR1100 Series GV-EDR2100 Series	V8.5.9 or later / V14.10 or later
	GV-EDR4700 Series	V8.7.1.0 (with patch files) or later / V15.11.3.0 (with patch files) or later
	GV-EDR2700 Series	V8.7.3.0 (with patch files) or later / V16.11.0.0 (with patch files) or later

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Bullet Camera	GV-BL2400 GV-BL3400 GV-BL1210 GV-BL2410 GV-BL3410 GV-BL5310	V8.5.6 or later / V14.10 or later
	GV-BL3700 GV-BL5700	V8.7.0 (with patch files) or later / V15.10.1 (with patch files) or later
	GV-BL1500	V8.5.7 (with patch files) or later / V14.10 or later
	GV-BL2500 GV-BL2510-E GV-BL5310-E	V8.7.4.0 or later / V16.11.0.0 or later
	GV-BL2702 GV-BL4702 GV-BL4713 GV-BL5713	V8.7.4.0 (with patch files) or later / V16.11.0.0 (with patch files) or later
	GV-BL8714	V8.8.0 (with patch files) or later / V17.2.1 or later
Ultra Bullet Camera	GV-UBL1211 GV-UBL2411 GV-UBL3411 GV-UBL1301 Series GV-UBL2401 Series GV-UBL3401 Series	V8.5.6 or later / V14.10 or later
	GV-UBL1511	V8.5.8 or later / V14.10 or later
	GV-UBL2511	V8.5.9 or later / V14.10 or later

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Target Bullet Camera	GV-EBL1100 Series GV-EBL2100 Series	V8.5.9 or later / V14.10 or later
	GV-EBL2101	V8.6.2.0 or later / V14.10.1 or later
	GV-EBL2111 GV-EBL3101	V8.7.0.0 (with patch files) or later / V15.10.1.0 (with patch files) or later
	GV-EBL5101	V8.7.3.0 (with patch files) or later / V16.10.3.0 (with patch files) or later
	GV-EBL4702	V8.7.3.0 (with patch files) or later / V16.10.3.0 (with patch files) or later
	GV-EBL2702 Series	V8.7.3.0 (with patch files) or later / V16.11.0.0 (with patch files) or later
	GV-EBL4711	V8.7.4.0 (with patch files) or later / V16.11.0.0 (with patch files) or later
PTZ Camera	GV-PTZ010D	V8.4 or later / V14.10 or later
PT Camera	GV-PT130D GV-PT220D GV-PT320D	V8.5.7 or later / V14.10 or later

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Target Vandal Proof IP Dome	GV-EVD2100 GV-EVD3100	V8.6.2 (with patch files) or later / V14.10.1 (with patch files) or later
	GV-EVD5100	V8.6.2.0 (with patch files) or later / V15.10.1.0 or later
Vandal Proof IP Dome	GV-VD120D Series GV-VD220D Series GV-VD320D Series	V8.4 (with patch files) or later / V14.10 or later
	GV-VD1500	V8.5.8 or later / V14.10 or later
	GV-VD2400 GV-VD3400	V8.5.6 or later / V14.10 or later
	GV-VD1530/1540 GV-VD2430/2440 GV-VD2500/2530/2540 GV-VD2540-E GV-VD3430/3440 GV-VD5340 GV-VD5340-E	V8.5.9 or later / V14.10 or later
	GV-VD2702/2712	V8.7.1.0 (with patch files) or later / V15.11.3.0 (with patch files) or later
	GV-VD4702/5702	V8.7.3.0 (with patch files) or later / V16.10.3.0 (with patch files) or later
	GV-VD4712	V8.7.4.0 (with patch files) or later / V16.11.0.0 (with patch files) or later

Camera	Models	Compatible version of GV-DVR / NVR / GV-VMS
Vandal Proof IP Dome	GV-VD4711 GV-VD5711	V8.7.1.0 (with patch files) or later / V15.11.1.0 (with patch files) or later
	GV-VD3700 GV-VD5700	V8.7.0 (with patch files) or later / V15.10.1 (with patch files) or later
Motorized IP Dome	GV-MD8710-FD	V8.7.6.0 or later (with patch files) / V18.1 or later (with patch files)
	GV-MD8710	V8.8.0 (with patch files) or later / V17.2.1 or later
Cube Camera	GV-CB120 GV-CB220	V8.4.3 (with patch files) or later / V14.10 or later
Advanced Cube Camera	GV-CA120 GV-CA220 GV-CAW120 GV-CAW220	V8.5.5 or later / V14.10 or later
Pinhole Camera	GV-UNP2500	V8.6.0 or later / V14.10.1 (with patch files) or later

H. Notice for Using the IR Arctic Box Camera

Make sure sure that you:

- enable IR LED function on the Web interface after loading the default settings.
- disable the status LED to reduce reflection when a green light spot appears on the live view.

Enabling IR LED after Loading Default

Each GV-IR Arctic Box Camera is equipped with 4 IR LEDs to provide infrared illumination at night. The factory-loaded setting for the IR LED function is **enabled**. If you have restored the camera to default settings, please follow the steps below to enable the IR LED function.

1. In the left menu of Web interface, select **Video Settings** and then **Streaming 1**.
2. Enable **Trigger IR by D/N** in IR Check Function. Click **Apply**.

Disabling Status LED under Low Light Conditions

A green light spot on the live view is likely caused by the insufficient light at the installation site, which leads to the status LED to reflect on the camera cover. Disable the status LED to prevent this.

1. In the left menu of Web interface, select **Video Settings** and then **Streaming 1**.
2. Select **Disable** in LED Control. Click **Apply**.