

# GV-IP LPR-DL

*User's Manual*



- GV-LPR2800-DL
- GV-LPR2811-DL

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

IPLPR-DL-UM-A



© 2020 GeoVision, Inc. All rights reserved.

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

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

**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>

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

November 2020

## Preface

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

GV-IP LPR Camera is an IP camera designed for instantaneous license plate recognition under various surveillance scenarios. This manual consists of the following models:

<b>Models</b>
GV-LPR2800-DL
GV-LPR2811-DL

# Contents

<b>Naming Definition</b> .....	<b>v</b>
<b>Options</b> .....	<b>vi</b>
<b>Note for Connecting to GV-DVR / NVR / VMS</b> .....	<b>viii</b>
<b>Note for Installing Camera Outdoor</b> .....	<b>viii</b>
<b>Note for Silica Gel Bags</b> .....	<b>viii</b>
<b>Chapter 1 Introduction</b> .....	<b>1</b>
1.1 System Requirements .....	1
1.2 Key Features .....	2
1.3 GV-LPR2800-DL .....	3
1.3.1 Packing List .....	3
1.3.2 Installing the Camera .....	4
1.3.3 Overview & Wiring .....	7
1.3.4 Disconnecting Built-in IR Lights and Connecting to External IR Lights .....	9
1.4 GV-LPR2811-DL .....	10
1.4.1 Packing List .....	10
1.4.2 Installing the Camera .....	11
1.4.3 Wire Definition .....	13
1.5 Connecting the Camera .....	14
1.5.1 I/O Device Connection .....	15
1.5.2 UHF RFID Reader Connection .....	16
<b>Chapter 2 Getting Started</b> .....	<b>17</b>
2.1 Looking Up the IP Address .....	17
2.2 Changing the IP Address .....	18
2.3 Accessing Live View .....	20
2.3.1 Saving Snapshots .....	21
2.3.2 Video Recording .....	21
2.3.3 Control Panel of the Live View .....	22
2.4 Picture-in-Picture and Picture-and-Picture View .....	25
2.5 Alarm Notification .....	27
2.6 Video and Audio Configuration .....	28
2.7 Remote Configuration .....	29
2.8 Camera Name Display .....	29
2.9 Image Enhancement .....	29
2.10 Digital PTZ .....	30
2.11 I/O Control .....	31

2.12	Visual Automation .....	32
------	-------------------------	----

**Chapter 3 Administrator Mode..... 33**

3.1	System .....	35
3.1.1	General Settings.....	35
3.1.2	Maintenance.....	37
3.1.3	Security .....	38
3.1.4	Account Management.....	39
3.1.5	V/A License Management.....	41
3.2	Network .....	42
3.2.1	Basic Settings.....	42
3.2.2	SNMP .....	44
3.2.3	FTP Settings.....	45
3.2.4	E-mail .....	47
3.2.5	HTTPS .....	49
3.2.6	802.1x .....	50
3.2.7	RTSP.....	51
3.2.8	QoS, UPnP & ONVIF.....	52
3.3	Video and Audio .....	54
3.3.1	Video Settings .....	54
3.3.2	Audio Settings .....	55
3.3.3	ROI.....	56
3.3.4	AES Encryption .....	56
3.4	Image .....	57
3.4.1	OSD & Text Overlay.....	57
3.4.2	Privacy Mask .....	59
3.4.3	Visual Automation.....	60
3.5	Events and Alerts.....	61
3.5.1	Input Settings .....	61
3.5.2	Output Settings.....	62
3.5.3	I/O Schedule.....	63
3.5.4	Tampering Alarm.....	63
3.5.5	LPR.....	65
3.6	Storage.....	76
3.6.1	Storage Settings .....	76
3.6.2	Disk Management.....	77
3.7	Monitoring.....	78
3.8	Back-end System .....	79
3.8.1	Center V2.....	79

3.8.2	VSM (Vital Sign Monitor) .....	81
3.8.2	GV-Video Gateway / GV-Recording Server.....	83
<b>Chapter 4</b>	<b>Advanced Applications .....</b>	<b>85</b>
4.1	Upgrading System Firmware .....	85
4.1.1	Using the Web Interface .....	86
4.1.2	Using the GV-IP Device Utility .....	87
4.2	Backing up and Restoring Settings .....	89
4.3	Restoring to Factory Default Settings .....	91
4.3.1	Using the Web Interface .....	91
4.3.2	Directly on the Camera .....	91
4.4	Verifying Watermark .....	92
4.4.1	Accessing AVI Files .....	92
4.4.2	Running Watermark Proof .....	92
4.4.3	The Watermark Proof Window .....	93
<b>Chapter 5</b>	<b>DVR / NVR / VMS Configurations .....</b>	<b>94</b>
5.1	Setting up IP Cameras on GV-DVR / NVR.....	95
5.1.1	Customizing Camera Settings .....	98
5.2	Setting up IP Cameras on GV-VMS .....	99
5.3	Remote Monitoring with E-Map.....	101
<b>Chapter 6</b>	<b>CMS Configurations .....</b>	<b>103</b>
6.1	Center V2 .....	103
6.2	Vital Sign Monitor .....	105
6.3	Dispatch Server .....	106
<b>Chapter 7</b>	<b>Smart Device Connection .....</b>	<b>107</b>
<b>Chapter 8</b>	<b>GV-ASManager Connection.....</b>	<b>108</b>
<b>Appendix</b> .....		<b>111</b>
A.	The CGI Command.....	111
B.	Settings for Internet Explorer 8 or later .....	112

## Naming Definition

<b>GV-DVR / NVR</b>	GeoVision Analog and Digital Video Recording Software. The GV-DVR / NVR also refers to <b>Multicam System</b> , <b>GV-NVR</b> system, <b>GV-DVR</b> system and <b>GV-Hybrid DVR</b> system at the same time.
<b>GV-VMS</b>	GeoVision Video Management System for IP cameras.
<b>PC LPR</b>	PC LPR refers to GV-DVR LPR and GV-VMS LPR. A GV-DVR / NVR / VMS can be turned into a GV-DVR LPR / GV-VMS LPR simply by installing the LPR Plugin and inserting an LPR Dongle. PC LPRs are capable of comparing captured license plates with the database from GV-ASManager.

## Options

Optional devices can expand the capabilities and versatility of your camera. Contact your dealer for more information.

Device	Description
<b>GV-PA191 (for LPR2811-DL)</b>	GV-PA191 is an IEEE802.3af/at PoE adapter, with a maximum power output of 19 W, that can be used to power GV-IP devices while providing Internet connection via an Ethernet cable.
<b>GV-PA902BT (for LPR2800-DL)</b>	GV-PA902BT is an IEEE802.3af/at/bt PoE adapter, with a maximum power output of 95 W, that can be used to power GV-IP devices while providing Internet connection via an Ethernet cable.
<b>GV-Relay V2</b>	With GV-Relay V2, the camera is capable of driving loads of relay outputs over 5 volts. It provides 4 relay outputs, and each can be set as normally open (NO) or normally closed (NC) independently as desired.
<b>Power Adapter</b>	Contact our sales representatives for the countries and areas supported.



## **Note for Connecting to GV-DVR / NVR / VMS**

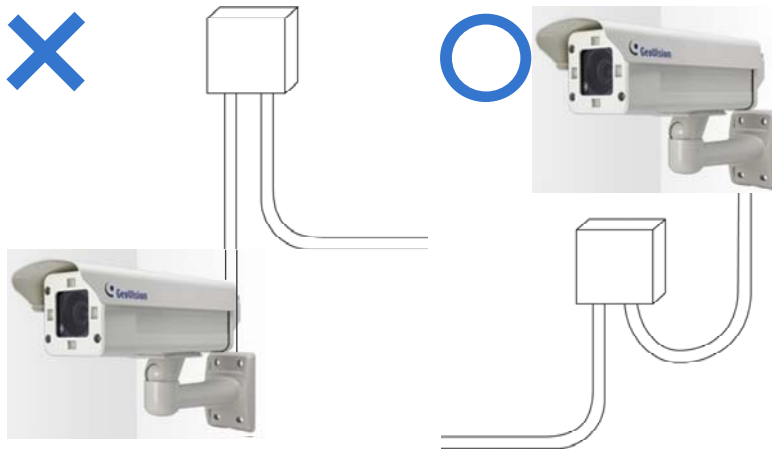
The GV-IP LPR-DL Camera is designed to work with and record on GV-DVR / NVR / VMS, a video management system.

Once the camera is connected to a 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.

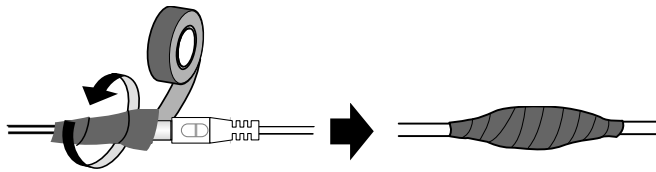
## Note for Installing Camera Outdoor

When installing the GV-IP LPR-DL Camera outdoor, mind the following:

1. Set the camera above the junction box to prevent water from entering the camera along the cables.



2. Waterproof the PoE, power and any other cables with waterproof silicon rubber or the like.



3. The camera casing may be hot due to its IR LED. Make sure you unplug the power cable and allow the camera casing to cool before handling the camera.

## Note for Silica Gel Bags

The silica gel loses its effectiveness whenever the camera is opened. To prevent the lens from fogging up, replace the silica gel bag every time you open the camera and conceal the gel bag in the camera within two minutes of exposing it to open air.

# Chapter 1 Introduction

## 1.1 System Requirements

To access the camera functions and settings through Web browser, ensure your PC is in good network connection and use one of the following Web browsers:

- Microsoft Internet Explorer 11.0 or later
- Google Chrome
- Mozilla Firefox
- Safari
- Microsoft Edge

---

**Note:** With non-IE browsers, the following functions are not supported: motion detection, text overlay and two-way audio.

---

### Compatible Software Version

Model	Firmware Version	GV-DVR / NVR	GV-VMS	GV-ASManager
GV-LPR2800-DL	V1.00	V8.8.0 or later	V17.4.0 / V18.2.0 or later	V5.3.1 or later
GV-LPR2811-DL	V1.00	V8.8.0 or later	V17.4.0 / V18.2.0 or later	V5.3.1 or later

**Note:** For GV-DVR / NVR and GV-VMS turned into GV-DVR LPR and GV-VMS LPR capable of comparing license plates captured with the database from access control system GV-ASManager, an LPR Dongle is required.

## 1.2 Key Features

- Built-in deep learning LPR processor for license plate recognition
- 1/2.8" progressive scan super low lux CMOS
- Min. illumination at 0.04 lux
- Triple streams from H.265, H.264 and MJPEG
- Up to 60 fps at 1920 x 1080
- Motorized varifocal lens for remote zoom / focus adjustment for GV-LPR2811-DL only
- Intelligent IR
- IR distance up to 30 m (100 ft) for GV-LPR2800-DL / up to 22 m (70 ft) for GV-LPR2811-DL
- Day and Night function (with removal IR-cut filter)
- Wide Dynamic Range Pro (WDR Pro)
- DC 12 V / PoE (IEEE 802.3bt for GV-LPR2800-DL / IEEE 802.3af for GV-LPR2811-DL)
- Ingress protection (IP68 for GV-LPR2800-DL / IP67 for LPR2811-DL)
- Vandal resistance (IK10 for metal casing)
- Two-way audio
- Built-in micro SD card slot (SD/SDHC/SDXC/UHS-I, Class 10) for local storage
- Digital I/O (2 in / 2 out)
- Built-in heater and fan for GV-LPR2800-DL only
- Recognize vehicles with speeds up to 100 km/h (62 mph)
- Standalone database
- Recognized plate numbers export
- Defog
- Motion detection
- Privacy mask
- Text overlay
- IP address filtering
- Supports iPhone, iPad, Android and 3GPP
- 31 languages on Web interface
- ONVIF (Profile S) compliant
- CE, FCC, LVD, RoHS compliant

## 1.3 GV-LPR2800-DL



Ideal for parking lot and roadside installation, GV-LPR2800-DL is a 2 MP color network camera designed for recognition of non-reflective license plates on vehicles traveling at up to 100 km/h (62 mph). With its multiple high-power LEDs and intelligent IR, the camera is able to automatically adjust its shutter speed to the scene and capture clear license plate images for single- and/or dual-lane scenarios under low-light conditions. It adheres to IP68 and IK10 standards and is able to operate within a temperature range of -40°C (-40°F) to 50°C (122°F).

GV-LPR2800-DL is capable of recognizing license plate numbers with its built-in deep learning LPR processor. GV-LPR2800-DL can compare captured license plates either with its on-the-edge standalone database, or the database stored at GV-ASManager, an access control system. When there is a match, GV-LPR2800-DL can grant access for the vehicle by opening a gate or barrier.

### 1.3.1 Packing List

- GV-LPR2800-DL Camera
- Sun Shield Cover
- Sun Shield Cover Short Screws x 2
- Screw Anchor x 4
- 1/4"-10 Screw (32 mm) x 4
- M4 Screw (5 mm) x 2
- Washer x 4
- Hex Wrench
- Silica Gel Bag
- Adhesive Tape for Silica Gel Bag
- micro SD card (already inserted and formatted)
- Installation Guide
- Download Guide
- Warranty Card

## 1.3.2 Installing the Camera

---

**IMPORTANT:** To produce quality image and to avoid software recognition errors, make sure you adhere to the guidelines as specified in *GV-LPR2800-DL Camera Installation Guide*.

---

After you have read through the installation guides and chosen an installation site, follow the steps below to install the camera.

1. Slide the sun shield cover onto the top of the camera. Adjust the position of the cover before fully securing it with the 2 supplied short screws.



2. Mark the installation site and drill four holes for the screw anchors.
3. Insert the supplied screw anchors.
4. Secure the camera to the wall using the supplied screws.



5. Connect the camera for power and network connection. See *1.5 Connecting the Camera*.
6. Access the live view. See *Chapter 2 Accessing the Camera*.
7. Based on the live view, adjust the tilt and pan angle of the camera by loosening the screw as indicated with the supplied hex wrench.

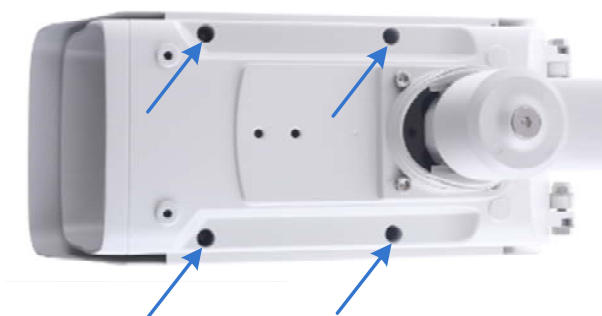
A. Tilt Adjustment



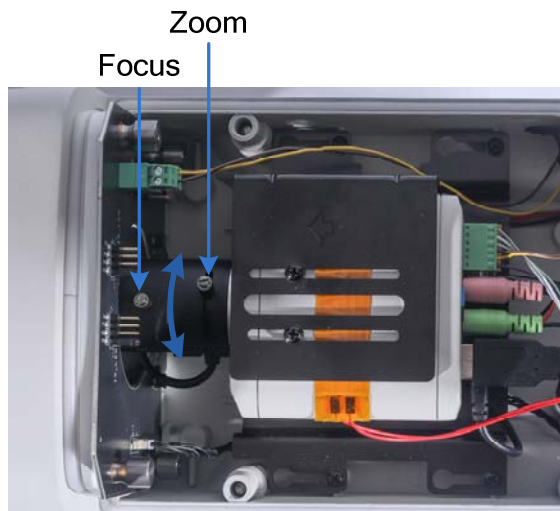
B. Pan Adjustment



8. Open the camera's lid by loosening the 4 screws indicated.



9. Based on the live view, adjust the zoom and focus of the camera using the zoom and focus screws.



10. Before closing the camera's lid, make sure to replace the original silica gel bag with a new one, which must be done every time you open the camera.
  - A. Remove the silica gel bag attached to the interior of the lid and place a new one to the same position using the supplied adhesive tape.
  - B. Close and tighten the camera's lid within 2 minutes of replacing the silica gel bag.



---

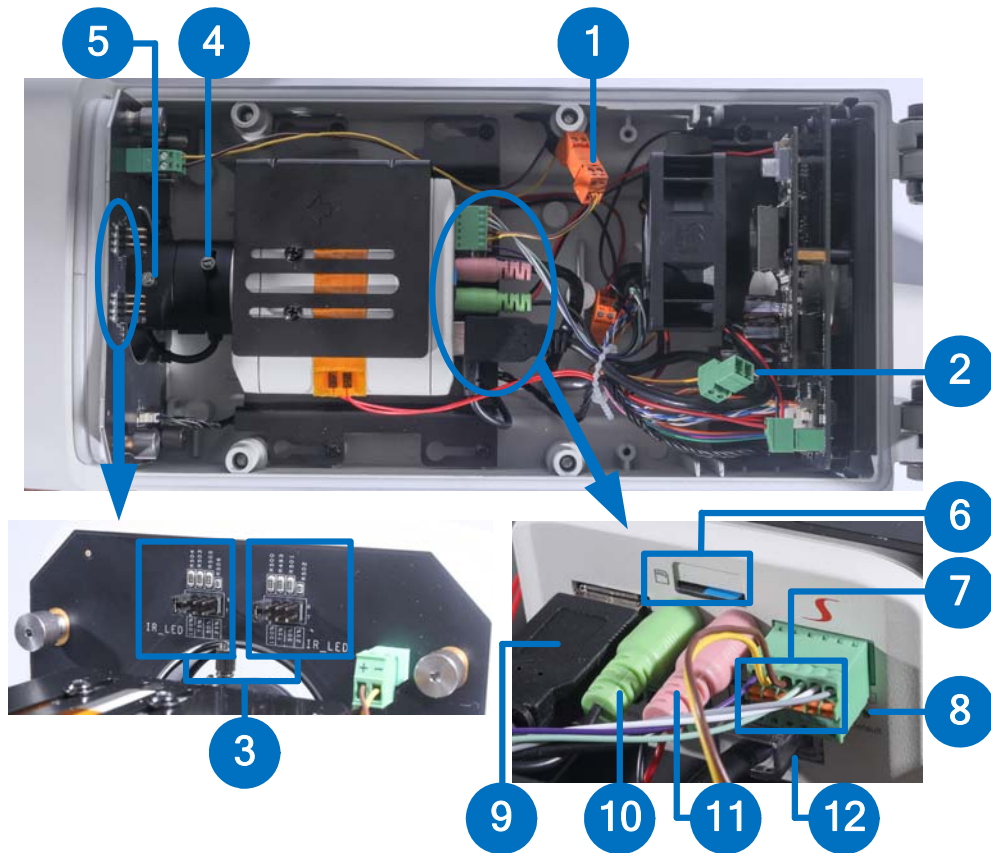
**IMPORTANT:** See the Note for Silica Gel Bags at the beginning of the manual.

---



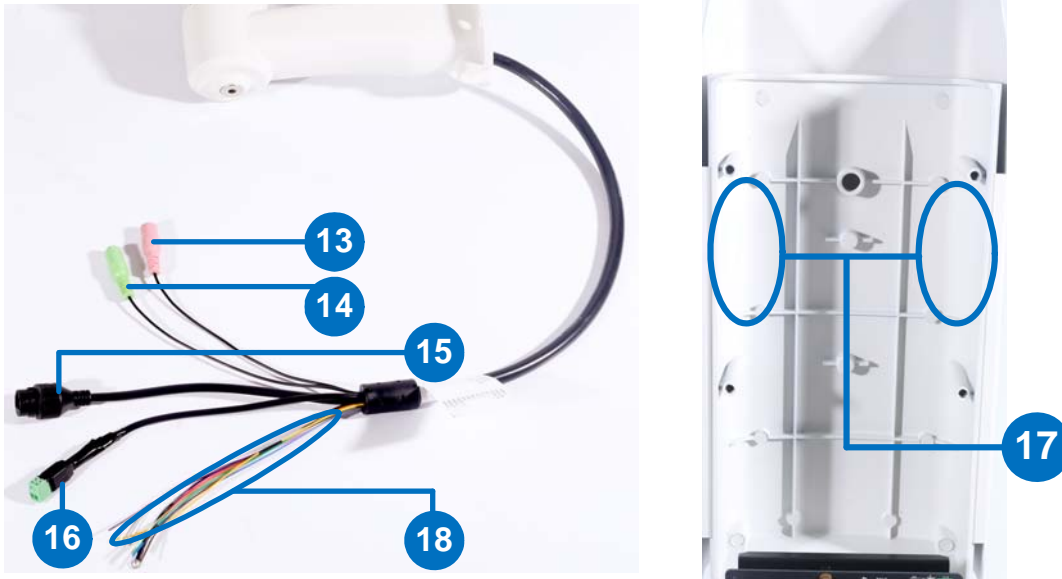
### 1.3.3 Overview & Wiring

#### Internal Wiring



No.	Name	Description
1.	Built-in IR Light Wiring	Connects to the built-in IR lights.
2.	External IR Wiring Pin	Optionally disconnect the wiring from the built-in IR lights to connect it to user-supplied external IR lights.
3.	L/R IR Intensity	Adjusts the maximum intensity of the left and right built-in IR lights
4.	Zoom Screw	Adjusts the zoom of the camera.
5.	Focus Screw	Adjusts the focus of the camera.
6.	SD Card Slot	By default, a 32GB Micro SD card is already inserted and formatted. When replacing the SD card, make sure the newly-inserted SD card is formatted, see <i>3.6.2 Disk Management</i> .
7.	Internal I/O Wiring	Connects to the external I/O wiring of GV-LPR2800-DL.
8.	Default Button	Resets the camera to factory default settings.
9.	RS-485 USB	Connects to the external RS-485 wires.
10.	Internal Audio-out	Connects to the external audio-out wire.
11.	Internal Audio-In	Connects to the external audio-in wire.
12.	Internal PoE / Ethernet port	Connects to the external Ethernet / PoE connector.

## External Wiring



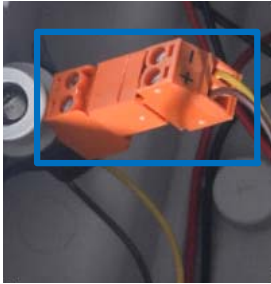
No.	Name	Description	
13.	External Audio-In	Connects to a microphone.	
14.	External Audio-Out	Connects to a speaker.	
15.	External Ethernet / PoE Connector	Connects the camera to a network and PoE power supply via Ethernet.	
16.	2-Pin Terminal Block	Optionally connect to a user-supplied power adapter.	
17.	Silica Gel Bag placement	<b>Must replace the original silica gel bag and attach a new one to one of the locations indicated every time after opening the camera.</b>	
18.	I/O Wires	Bright Green	DI 1
		Purple	DI 2
		Gray	DO 1
		Brown	DO 2 [External IR Light Wiring]
		White	GND
		Yellow	GND
		Orange	RS-485 1+
		Pink	RS-485 1-
		Blue	RS-485 2+
Green	RS-485 2-		

**IMPORTANT:** By default, all the internal wiring, including Internal I/O, Fan USB, Internal Audio-out, Audio-In and PoE / Ethernet port (No. 7, 9, 10, 11 & 12), are already connected when supplied. Do not fiddle with them as it may hinder certain functions of the camera.

### 1.3.4 Disconnecting Built-in IR Lights and Connecting to External IR Lights

Follow the steps below to connect to any user-supplied external IR lights in place of the camera's built-in IR lights:

1. First, turn off the camera.
2. Disconnect **Built-in IR Light Wiring** (see No. 1, *1.3.3 Overview & Wiring*).



3. Then connect it to **External IR Wiring Pin** (see No. 2, *1.3.3 Overview & Wiring*), as illustrated below.
4. Connect the user-supplied external IR lights to **DO2 [External IR Light Wiring]** (see No. 18 — Brown wire, *1.3.3 Overview & Wiring*) of the camera.

---

**Note:** For IR light to work, both internal and external, make sure **Digital Output 2** is enabled to control the IR light, see *3.5.2 Output Settings*.

---

## 1.4 GV-LPR2811-DL



GV-LPR2811-DL is a 2 MP, 2.5x zoom color network camera designed for recognition of non-reflective license plates on vehicles traveling at up to 100 km/h (62 mph). With its motorized lens, and intelligent IR, the camera's zoom and focus can be adjusted remotely and can also automatically adjust its shutter speed to the scene to capture clear license plate images for single- or dual-lane scenarios under low-light conditions. It adheres to IP67 and IK10 standards and is able to operate within a temperature range of -30°C (-22°F) to 50°C (122°F).

GV-LPR2811-DL is capable of recognizing license plate numbers with its built-in deep learning LPR processor. GV-LPR2811-DL can compare captured license plates either with its on-the-edge standalone database, or the database stored at GV-ASManager, an access control system. When there is a match, GV-LPR2811-DL can grant access for the vehicle by opening a gate or barrier.

### 1.4.1 Packing List

- GV-LPR2811-DL Camera
- Sun Shield Cover
- Sun Shield Cover Short Screw x 2
- Supporting Rack Screw x 3
- Mounting Kit Screw x 3
- Mounting Kit Screw x 3
- Screw Anchor x 3
- Washer x 2
- Hex Wrench
- Silica Gel Bag x 2
- micro SD card (already inserted and formatted)
- Download Guide
- Warranty Card

## 1.4.2 Installing the Camera

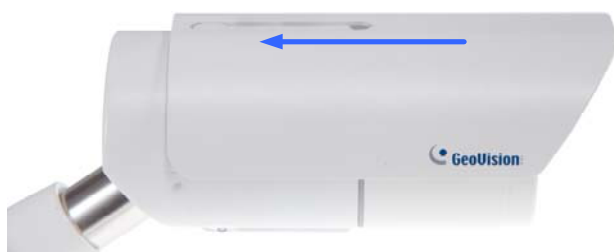
---

**IMPORTANT:** To produce quality image and to avoid software recognition errors, make sure you adhere to the guidelines as specified in *GV-LPR2811-DL Camera Installation Guide*.

---

After you have read through the installation guides and chosen an installation site, follow the steps below to install the camera.

1. Slide the sun shield cover onto the top of the camera. Adjust the position of the cover before fully securing it with the 2 supplied short screws.

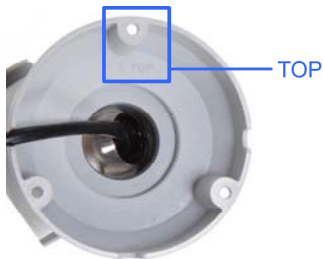


2. Mark the installation site and drill three holes for the screw anchors.
3. Insert the supplied screw anchors.
4. Secure the camera to the wall using the supplied screws.



**IMPORTANT:** To avoid waterproofing failures, make sure of the following:

1. Do not open the camera cover under any circumstances.
2. The top of the camera must be facing upward for wall mount.



5. Connect the camera for power and network connection. See *1.5 Connecting the Camera*.
6. Access the live view. See *Chapter 2 Accessing the Camera*.
7. Based on the live view, adjust the angle of the camera by loosening the screws, for the first and second shafts, as indicated with the supplied hex wrench.

A. First Shaft



B. Second Shaft



### 1.4.3 Wire Definition

The data cable provides connection for power, ground and network access. The wires are defined as below:



No.	Wire	Definition	
1.	RJ-45	Ethernet / PoE (IEEE 802.3af)	
2.	2-pin terminal block	DC 12V	
3.	Pink RCA	Audio Input	
4.	Green RCA	Audio Output	
5.	Digital I/O	Blue	DI 1
		Green	DI 2
		Yellow	DO 1
		Orange	DO 2
		Brown	GND
		Gray	RS-485 1+
		Purple	RS-485 1-
		Bright Green	RS-485 2+
		White	RS-485 2-

## 1.5 Connecting the Camera

Use optional accessory GV-PA902BT or GV-PA191 PoE Adapter to respectively connect the GV-LPR2800-DL / GV-LPR2811-DL to power and network at the same time. The following procedures are exemplified using GV-LPR2800-DL and GV-PA902BT.

1. Insert one end of an Ethernet cable into **PoE Out** on the PoE Adapter.
2. Connect the other end of the cable to your camera through the conduit connector.
  - A. Remove the plug from the conduit connector.



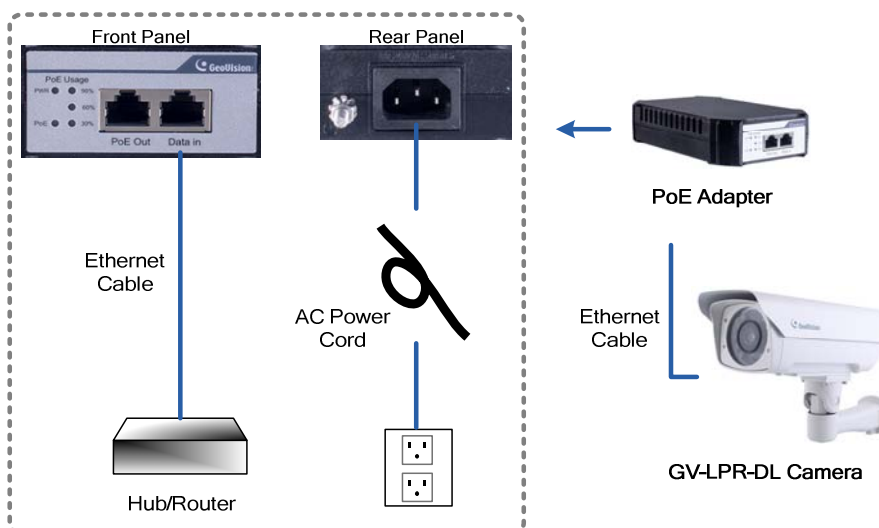
- B. Disintegrate the conduit connector and thread the Ethernet cable through its 3 parts.



- C. Assemble the conduit connector.



3. Insert one end of a second Ethernet cable into the **Data In** port on the PoE Adapter and connect the other end of the cable to your network's hub or router.



4. Attach the AC power cord to the rear panel of the PoE Adapter.
5. Connect the AC power cord to the power outlet.
6. When the Power LED on the PoE Adapter turns green, you are ready to access the live view. See *Chapter 2 Accessing the Camera*.





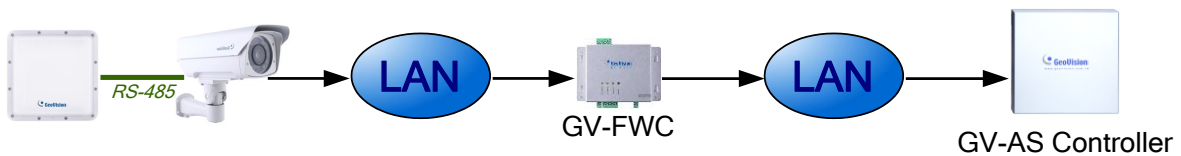
### 1.5.2 UHF RFID Reader Connection

Users can connect GV-LPR2800-DL / GV-LPR2811-DL to GV-RU9003 UHF RFID Readers through its RS-485 interface for license plate recognition + RFID tag access management. When registered license plates are recognized, the GV-RU9003 reads the corresponding RFID tags to open a gate or barrier, and/or trigger an alarm output. The following figure is exemplified using GV-LPR2800-DL.



GV-RU9003	GV-LPR2800-DL	GV-LPR2811-DL
D485+ (Orange-White)	RS-485+ (Orange / Blue)	RS-485+ (Gray / Bright Green)
D485- (Orange)	RS-485- (Pink / Green)	RS-485- (Purple / White)

### License Plate + RFID Tag Access Management Integration



**Note:** For this integration to work, it is required to enable **RS-485-B** to accept data from the GV-RU9003 and configure network connection to GV-FWC, see [3.5.5.3 GPS & RS-485](#) and [3.5.5.6 Push Notification](#), respectively.

## Chapter 2 Accessing the Camera

### 2.1 Checking the Dynamic IP Address

By default, your camera is assigned with an unused IP address by the DHCP server when the camera is connected to the network. This IP address remains unchanged unless you unplug or disconnect your camera from the network.

---

**Note:** If your router does not support DHCP, the default IP address will be **192.168.0.10**. In this case, it is strongly recommended to modify the IP address to avoid IP address conflict with other GeoVision IP devices within the same LAN. To change the IP address, see 2.2 *Configuring the IP Address*.

---


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

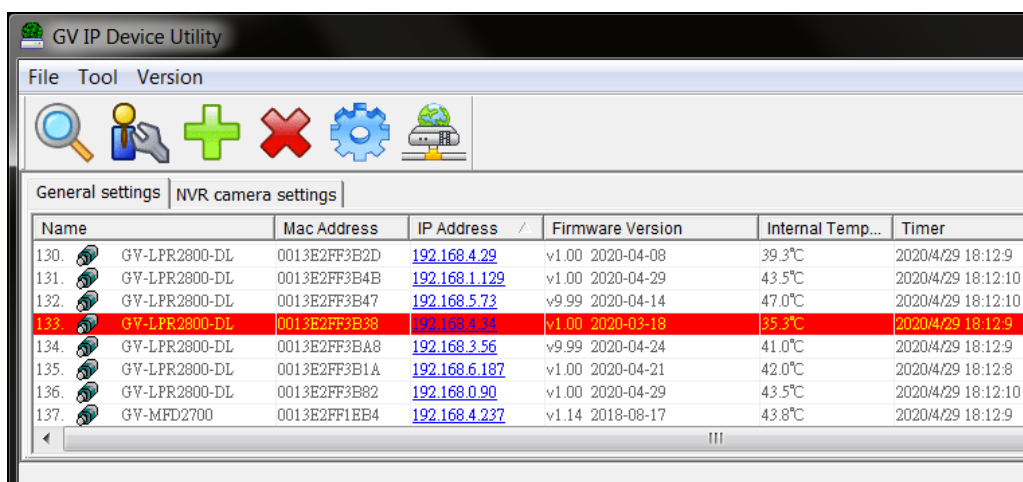
1. Install the GV-IP Device Utility program from the [GeoVision website](#).

---

**Note:** The PC installed with GV-IP Device Utility must be under the same LAN as 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**.



- The login page appears. Upon first-time login, the user must create a **Username** and **Password** for the Administrator account.



- Type the Username and Password set and click **Login**.

---

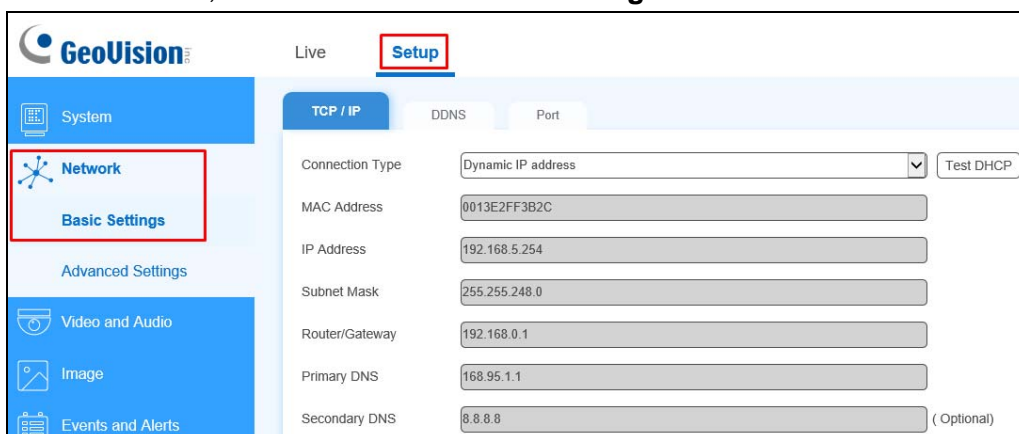
**Note:** To enable image updates, i.e. streaming live view, on Microsoft Internet Explorer, you must allow ActiveX Control and perform a one-time installation of the ActiveX component upon your first-time login.

---

## 2.2 Configuring the IP Address

To modify the static IP address 192.168.0.10 or set the camera to a public dynamic IP address, log into the Web interface to access the network setting page.

- Log into the camera using GV-IP Device Utility as described in section 2.1 or type the default IP address [192.168.0.10](http://192.168.0.10).
- Define a *Username* and *Password* for the Administrator account, log in and click **Setup**.
- In the left menu, select **Network > Basic Settings > TCP / IP**.



4. Select **Static IP address** or **PPPoE** from the Connection Type dropdown list.
5. Type the required network information and click **Apply**.

---

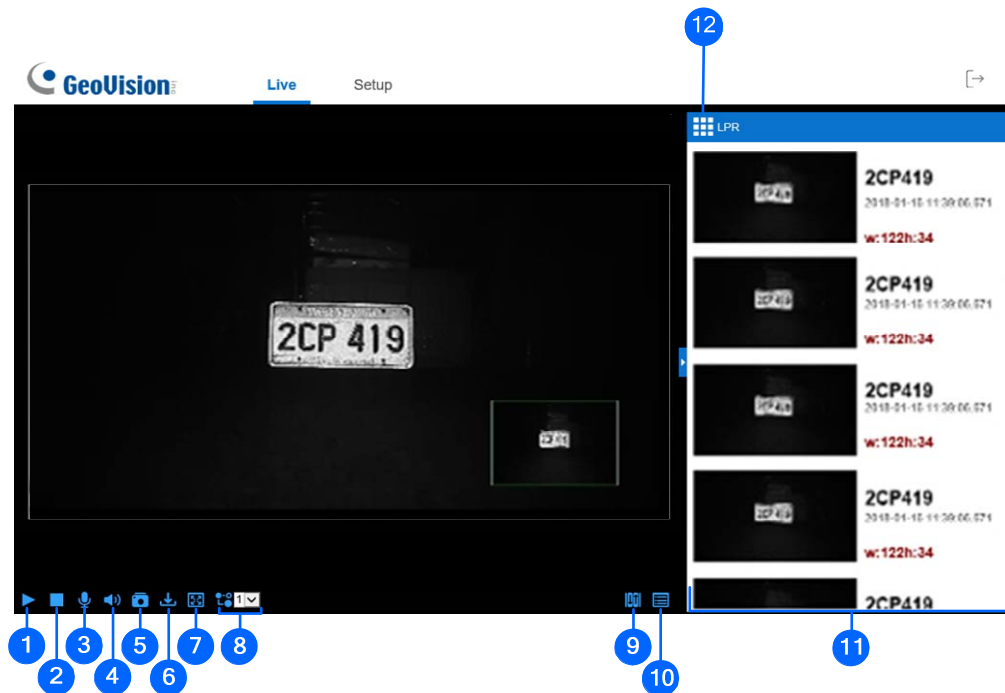
**IMPORTANT:**

1. To set the camera to use a public dynamic IP address via PPPoE, you must first use the dynamic DNS Service to obtain a domain name linked to the camera's changing IP address. For details, see *3.2.1 Basic Network Settings*.
  2. If **PPPoE** is enabled and you cannot access the camera, you may have to reset it to factory default settings and reconfigure the network settings. To restore to factory default settings, see *4.3 Restoring to Factory Default Settings*.
-

## 2.3 Accessing Live View

After logging into the camera, click **Live** to see the live video.

**Note:** Certain features may not be available on non-IE browsers.



No.	Name	Function
1	Play	Plays live video.
2	Stop	Stops playing video.
3	Microphone	Talks to the surveillance area from the local computer.
4	Speaker	Listens to the audio around the camera.
5	Snapshot	Takes a snapshot of live video. --- See 2.3.1 <i>Saving Snapshots</i> .
6	File Save	Records live video to the local PC. --- See 2.3.2 <i>Video Recording</i> .
7	Full Screen	Switches to full screen view. Right-click the image to have these options: <b>Snapshot, Full Screen, Resolution, Visual Automation, Digital PTZ, PIP</b> and <b>PAP</b> . --- See 2.12 <i>Visual Automation</i> , 2.10 <i>Digital PTZ</i> and 2.4 <i>Picture-in-Picture and Picture-and-Picture View</i> , respectively.
8	Stream	Switches between Streams 1, 2 and 3.
9	I/O Control	Enables the I/O Control Panel or Visual Automation. --- See 2.11 <i>I/O Control</i> .

No.	Name	Function
10	More Functions	Brings up these functions: <b>Alarm Notify, Video and Audio Configuration, Remote Config, Show Camera Name and Image Enhance</b> . --- See 2.5 Alarm Notification, 2.6 Video and Audio Configuration, 2.7 Remote Configuration, 2.8 Camera Name Display and 2.9 Image Enhancement respectively.
11	Recognition Result	Displays the snapshots of the recognition results when the camera recognizes a license plate.
12	Options	Accesses the <b>Control Panel</b> of the live view. --- See 2.3.3 Control Panel of the Live View.


### 2.3.1 Saving Snapshots

1. Click **Snapshot** button (No. 5, 2.3 Accessing Live View). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and select a format, **JPEG** or **BMP**. You may also choose to display the camera name and/or the date, the text color and image quality.
3. Click **Save** to save the image in your PC.

### 2.3.2 Video Recording

1. Click the **File Save** button (No. 6, 2.3 Accessing Live View). The Save As dialog box appears.
2. Specify **Save in**, type the **File name**, and move the **Time Period** scroll bar to specify the maximum time length of each individual video file, from 1 to 5 minutes.
3. Click **Save** to start recording.
4. To stop recording, click the **Stop** button (No. 2, 2.3 Accessing Live View).

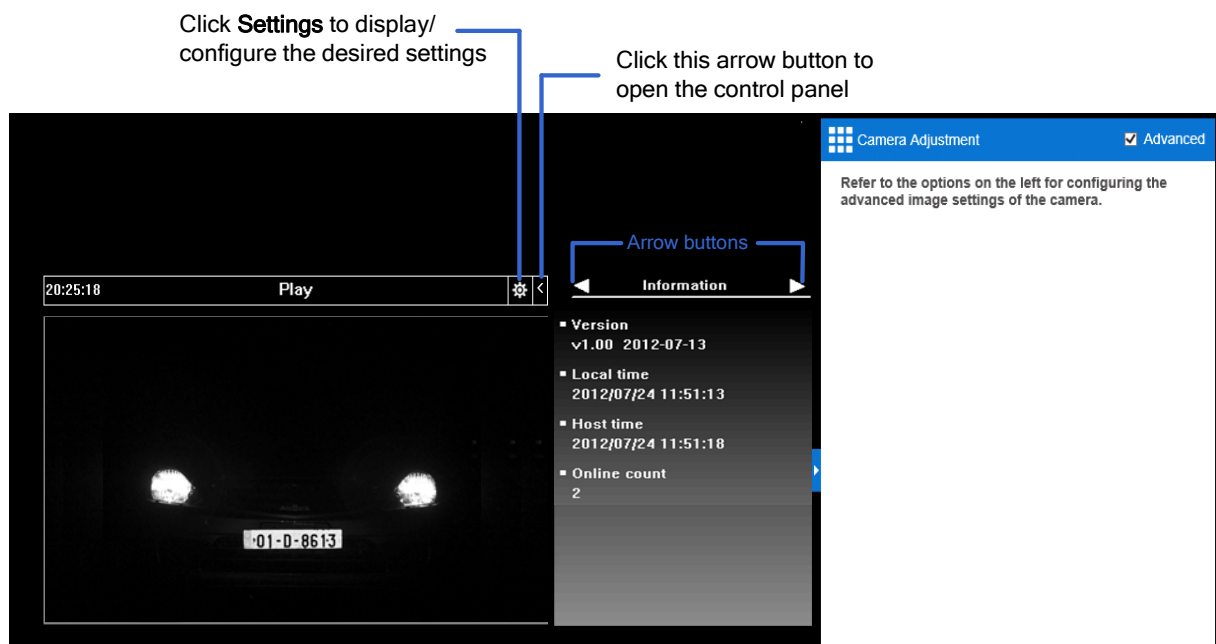
### 2.3.3 Control Panel of the Live View

To open the control panel of the Live View window, click **Options > Camera Adjustment**, select **Advanced** and click **Settings**  to display/adjust one of the following: **Information**, **Video**, **Audio**, **I/O Control**, **Alarm Notify**, **Camera Adjustment** and **Internal Temperature**.

---

**Note:** The Advanced functions within Camera Adjustment are only accessible on Internet Explorer.

---



**[Information]** Displays the version of the camera, local time of the PC, time of the camera, and the number of users currently logged in.

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

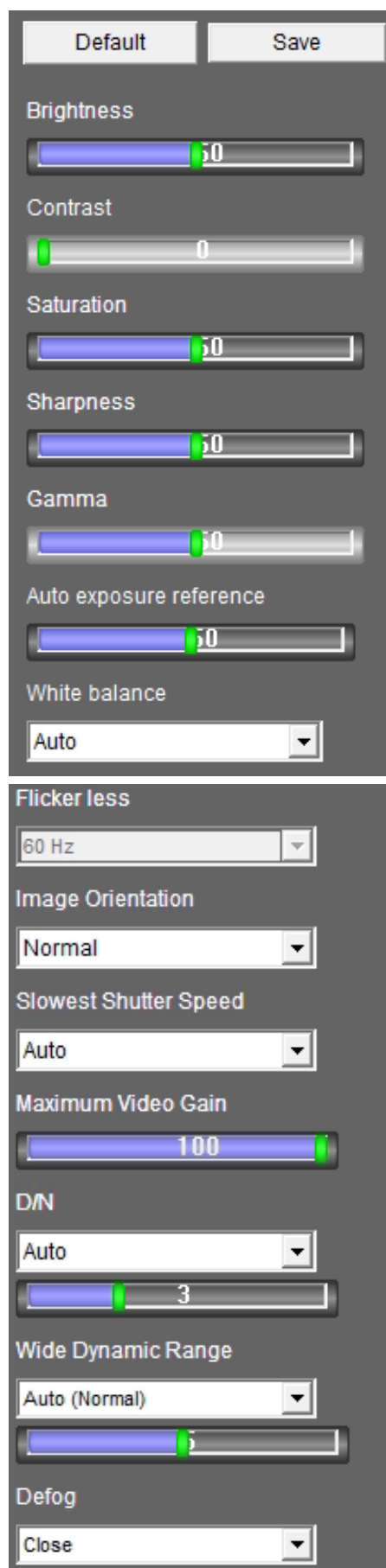
**[Audio]** Displays the audio data rates when the microphone and speaker are enabled.

**[I/O Control]** Displays the realtime status of the camera's digital inputs and outputs. You can manually trigger the outputs by double-clicking their icons.

**[Alarm Notify]** Displays the snapshots captured during an alarm event. For this function to work, you must configure the Alarm Notify settings first. See *2.5 Alarm Notification*.

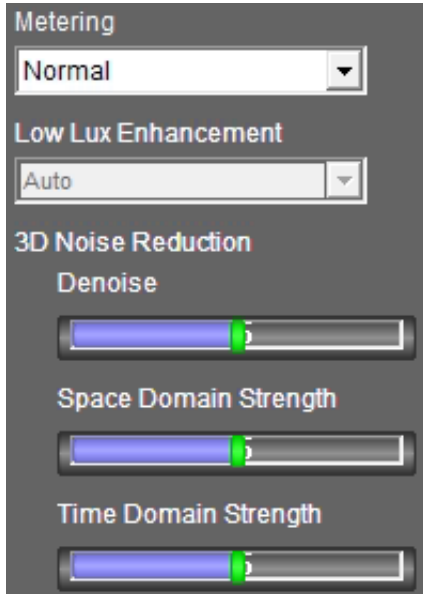
**[Internal Temperature]** Shows the current internal temperature of the camera and the normal temperature range.





**[Camera Adjustment]** Adjusts the image quality settings. Click **Save** to store the changes to the settings.

- **Brightness:** Adjusts the brightness of the image.
- **Contrast:** Adjusts the relative differences between one pixel to 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 within the image.
- **Auto Exposure Reference:** Adjusts the exposure of the image.
- **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**, **Indoor**, and **Fluorescent**. You can also choose **Manual** to adjust the white balance manually.
- **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.
- **Image Orientation:** Adjusts the orientation of image by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip** or **Rotate 180**.
- **Slowest Shutter Speed:** Sets the shutter speed. A slower 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 1/16,000 to 1/120 second.



- **Maximum Video Gain:** Changes the maximum gain level.
- **D/N:** Select **Auto** for automatically switching 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. Select **Triggered by Input** to switch between day and night modes upon input trigger. Select **Triggered by Schedule** to have the camera switch between day and night modes according to a schedule, see 3.5.3 I/O Schedule. The value 10 is the most light-sensitive.

- **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 in the dark areas of the scene 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.
- **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 to the specified zones. Draw directly on the live view and a rectangular box appears. You can establish up to 4 zones. To remove a box, right-click on it 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
- **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.

## 2.4 Picture-in-Picture and Picture-and-Picture View

The Live View window 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.



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.



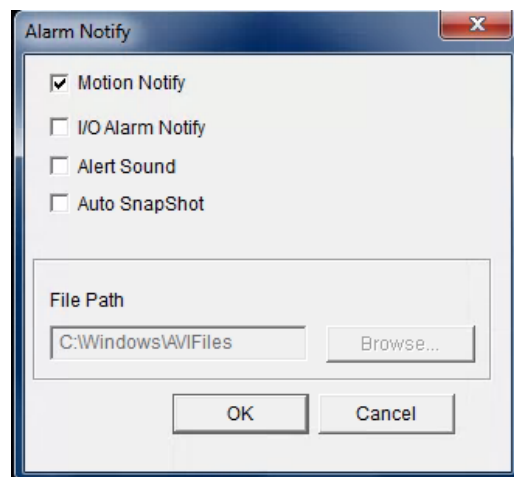
1. Right-click the live view and select **PAP**. A row of three inset windows appears at the bottom.
2. Draw a navigation box on the image, and this selected area is immediately reflected in one inset window. Up to seven navigation boxes can be drawn on the image.
3. To adjust a navigation box size, 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, display/hide or to change the frame color of the navigation boxes, right-click the live view, select **Mega Pixel Setting** and click one of these options:
  - **Enable Add-Focus-Area Mode:** Allows the user to add navigation boxes to the image.
  - **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.

## 2.5 Alarm Notification

Users can be alerted by a pop-up live video and view up to four captured images upon motion detection and/or input trigger events.



To configure this function, click the **More Functions** button (No. 10, 2.3 *Accessing Live View*), and select **Alarm Notify**. This dialog box appears.



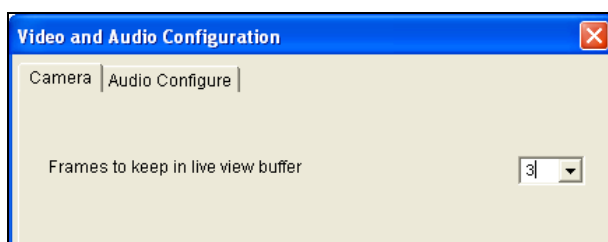
- **Motion Notify:** When motion is detected, the captured images are displayed on the control panel of the Live View window.
- **I/O Alarm Notify:** When an input device is triggered, the captured images are displayed on the control panel of the Live View window. For this function to work, the required input devices must be installed and configured properly. See 3.5.1 *Input Setting*.
- **Alert Sound:** Activates the computer alarm upon an alert event.
- **Auto Snapshot:** Automatically captures snapshots for every 5 seconds during an alert event.
- **File Path:** Assigns a file path to save the snapshots.

## 2.6 Video and Audio Configuration

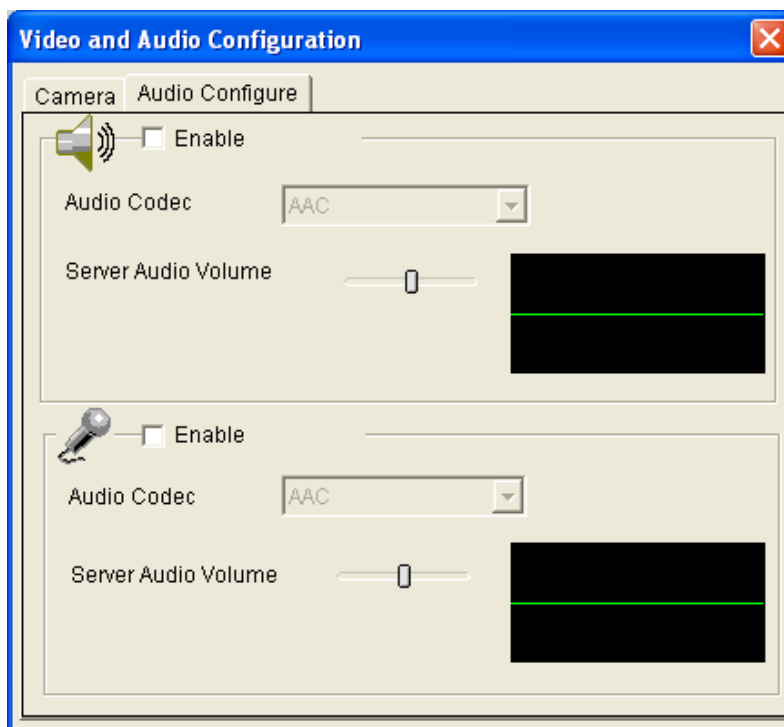
You can enable the microphone and speaker for two-way audio communication and adjust the number of frames to keep for live view buffer.

Click the **More Functions** button (No. 10, 2.3 *Accessing Live View*), 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 smoother live view, but the live view will be delayed for the number of seconds specified.



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



## 2.7 Remote Configuration

You can upgrade the device firmware over the network. Click the **More Functions** button (No. 10, 2.3 *Accessing Live View*), and select **Remote Config**. The Remote Config dialog box appears.

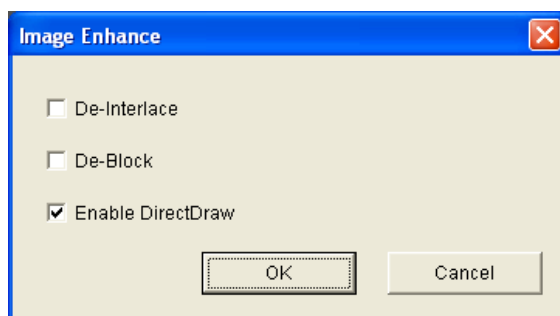
**[Firmware Upgrade]** In this tab, you can upgrade the firmware of your camera over the network. For details, see *Chapter 4 Advanced Applications*.

## 2.8 Camera Name Display

To display the camera name on the image, click the **More Functions** button (No. 10, 2.3 *Accessing Live View*), and select **Show Camera Name**.

## 2.9 Image Enhancement

To enhance the image quality of live video, click the **More Functions** button (No. 10, 2.3 *Accessing Live View*), and select **Image Enhance**. This dialog box appears.

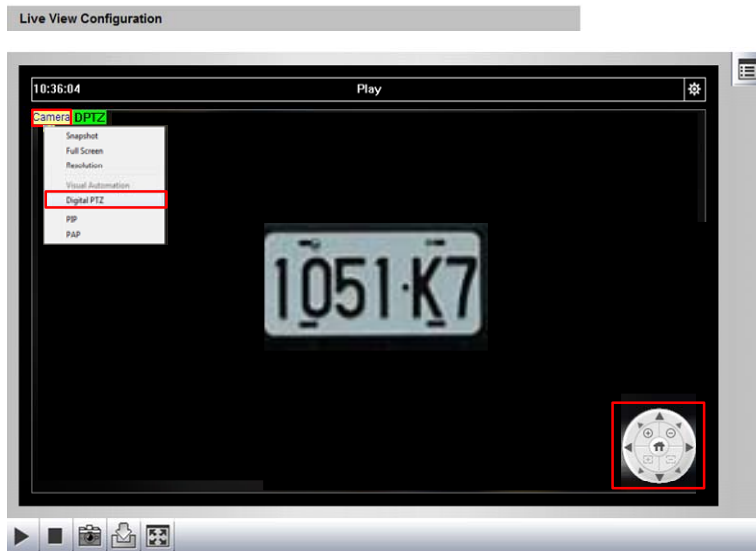



- **De-Interlace:** Covert interlaced video into non-interlaced video.
- **De-Block:** Remove the block-like artifacts from low-quality and highly compressed video.
- **Enable DirectDraw:** Activate the DirectDraw function.

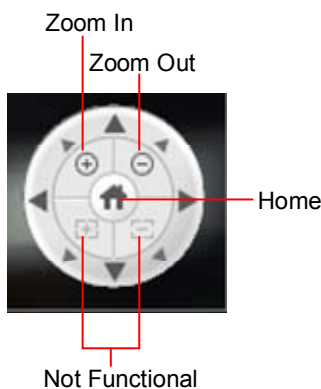
## 2.10 Digital PTZ

Digital PTZ allows non-PTZ cameras to simulate PTZ movements on the live view.

1. Right-click on the live view and select **Digital PTZ**.



2. To zoom in / out, move the cursor to the control panel at the bottom-right corner and click the corresponding buttons. To bring the view back to its default image, click **Home**.
3. To adjust the view, zoom the image first and then click the arrow buttons  to move your camera up, down, left, right, left-up, left-down, right-up or right-down.




---

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

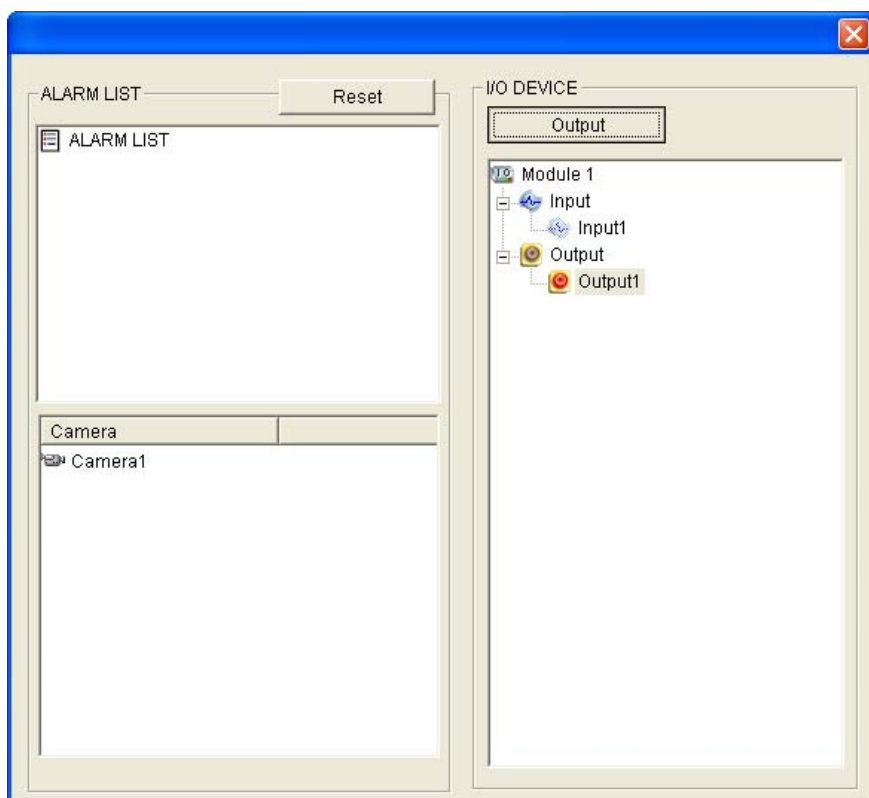
---



## 2.11 I/O Control

The I/O Control window displays the realtime status of the camera's digital inputs and outputs. You can also manually trigger the outputs by double-clicking their icons.

To display the I/O Control window, click the **I/O Control** button (No. 9, 2.3 *Accessing Live View*) and select **I/O Control**.



The Alarm List is displayed in three levels. The first level indicates the date, the second indicates the time, and the third indicates the alarm ID. Clicking the **Reset** button will clear the list.

## 2.12 Visual Automation

The Visual Automation features allows you to change the current state of a connected electronic device by simply clicking on its image, e.g. turning the light ON. For this function to work, the necessary Visual Automation settings must be set, see [3.4.3 Visual Automation](#).

To access this feature, click the **I/O Control** button (No. 9, [2.3 Accessing Live View](#)) and select **Visual Automation**.



To change the style of the areas, click the green **I/O** button at the upper-left corner to access the following options:

- **Show All:** Displays all set areas.
- **Rect Float:** Embosses all set areas.
- **Set Color:** Changes the frame color of all set areas.

## Chapter 3 Administrator Mode

The Administrator can access and configure the camera over the network through its Web interface, with settings including: **System, Network, Video and Audio, Image, Events and Alerts, Storage, Monitoring** and **Back-end System**.

The screenshot displays the GeoVision web interface. On the left is a navigation menu with icons and labels for System, Network, Video and Audio (highlighted), Image, Events and Alerts, Storage, Monitoring, and Back-end System. The main content area is titled 'Setup' and has tabs for Video, Audio, ROI, and Advanced Settings. The 'Video' tab is active, showing a list of settings with dropdown menus:

Setting	Value	Unit
Stream	Stream1	
Video Encoding	H264	
Flicker Hz	60HZ	
Resolution	1920*1080 (16:9)	
Frames per second	30	
Group of Picture (GOP) Size	1.0	seconds
Bandwidth management	VBR	
Quality	Good	
Maximal Bit Rate	8	Mbps

An 'Apply' button is located at the bottom of the settings list.

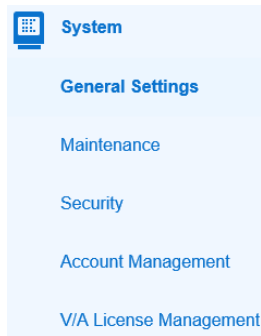
## Corresponding Section for Configuration Menu

Find the topic of interest by referring to the sections below.

3.1 System	<ul style="list-style-type: none"> <li>3.1.1 General Settings</li> <li>3.1.2 Maintenance</li> <li>3.1.3 Security</li> <li>3.1.4 Account Management</li> <li>3.1.5 V/A License Management</li> </ul>
3.2 Network	<ul style="list-style-type: none"> <li>3.2.1 Basic Settings</li> <li>3.2.2 SNMP</li> <li>3.2.3 FTP Settings</li> <li>3.2.4 E-mail</li> <li>3.2.5 HTTPS</li> <li>3.2.6 802.1x</li> <li>3.2.7 RTSP</li> <li>3.2.8 QoS, UPnP &amp; ONVIF</li> </ul>
3.3 Video and Audio	<ul style="list-style-type: none"> <li>3.3.1 Video Settings</li> <li>3.3.2 Audio Settings</li> <li>3.3.3 ROI</li> <li>3.3.4 AES Encryption</li> </ul>
3.4 Image	<ul style="list-style-type: none"> <li>3.4.1 OSD &amp; Text Overlay</li> <li>3.4.2 Privacy Mask</li> <li>3.4.3 Visual Automation</li> </ul>
3.5 Events and Alerts	<ul style="list-style-type: none"> <li>3.5.1 Input Settings</li> <li>3.5.2 Output Settings</li> <li>3.5.3 I/O Schedule</li> <li>3.5.4 Tampering Alarm</li> <li>3.5.5 LPR</li> </ul>
3.6 Storage	<ul style="list-style-type: none"> <li>3.6.1 Storage Settings</li> <li>3.6.2 Disk Management</li> </ul>
3.7 Monitoring	
3.8 Back-end System	<ul style="list-style-type: none"> <li>3.8.1 Center V2</li> <li>3.8.2 VSM</li> <li>3.8.3 Recording Server / Video Gateway</li> </ul>

## 3.1 System

This section covers system settings of the camera, including **General Settings**, **Maintenance**, **Security**, **Account Management** and **V/A License Management**.



### 3.1.1 System Settings

#### [Basic Information]

Basic Information	Date And Time	Daylight Saving	Language	LED
Host Name	<input type="text" value="GV-LPR2800-DL"/>			
firmware version	<input type="text" value="v1.00 2020-03-18 (1024 MB)"/>			
CPU Temperature	<input type="text" value="35"/> °C /	<input type="text" value="95"/> °F		
<input type="button" value="Apply"/>				

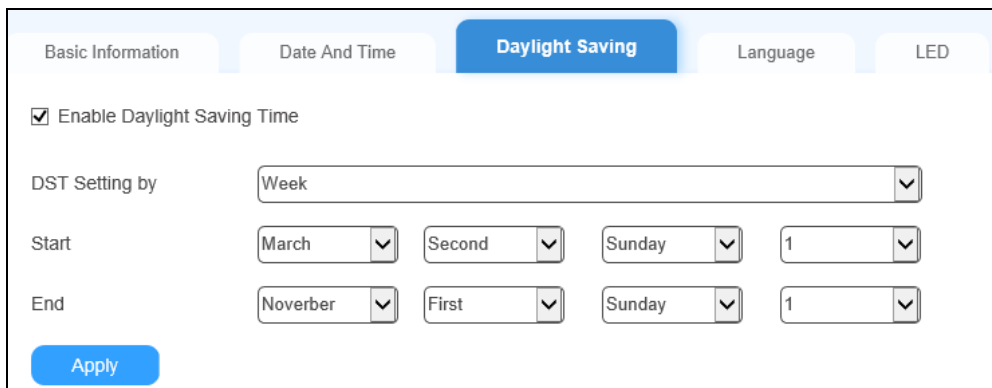
This page displays the basic information of the camera and allows users to change the name of the device.

#### [Date and Time]

Basic Information	Date and Time	Daylight Saving	Language	LED	About
Date and Time on IPCAM	<input type="text" value="Thu Aug 27 14:07:00 GMT8:00 2020"/>				
Time Zone	<input type="text" value="(GMT+08:00) China,Hong Kong,Australia Western,Singapore,Taiwan,Russia"/> ▼				
Time Synchronization by	<input type="text" value="Synchronize with Network Time Server (NTP)"/> ▼				
Host name or IP Address:	<input type="text" value="time.windows.com"/>				
Update Time:	<input type="text" value="05"/> ▼	:	<input type="text" value="10"/> ▼		
<input type="button" value="Apply"/>					

- **Date and Time on IPCAM** Displays the current date and time of the camera.
- **Time Zone:** Sets the time zone of the camera.
- **Time Synchronization by:** Select one of the following to synchronize the camera's date and time by.
  - **Synchronize with Network Time Server (NTP):** By default, the camera uses timeserver [time.windows.com](http://time.windows.com) to automatically update its internal clock every 24 hours. You can change the host name or IP setting to the timeserver of interest.
  - **Synchronize with the local PC or modify manually:** Select to manually set the date and time of the camera or synchronize with the time of the PC.

**[Daylight Saving]** Select **Enable Daylight Saving Time** to automatically adjust the camera for daylight saving.



- **DST Setting By:** Select **Time** to specify a *Start* and *End Time* to enable the daylight saving. Or select **Week** to set specific days of certain weeks as the Start and End Time.

**[Language]** Change the language of the Web interface.

**[LED]** The **Ready LED** is enabled by default. Optionally disable the Ready LED of the camera if necessary.

**[About]** Displays the open source licenses, if any, used by the firmware.

### 3.1.2 Maintenance

#### [Maintenance]

The screenshot shows the Maintenance configuration interface. It features two tabs: 'Maintenance' and 'Log'. The 'Maintenance' tab is active and contains three sections:

- Reset To Default:** Contains two buttons labeled 'Load Default'. The first button is associated with the text 'Restore to factory default settings'. The second button is associated with the text 'Restore to factory default settings (except network)'.
- Reboot:** Contains a button labeled 'Reboot' and the text 'Do you wish to reboot now?'.
- Auto Reboot:** Contains an 'Enable' checkbox, a 'Day Interval' field with a value of '1' and the unit 'days', and a 'Reboot Time' field with two dropdown menus showing '00' and '00'.

An 'Apply' button is located at the bottom of the configuration area.

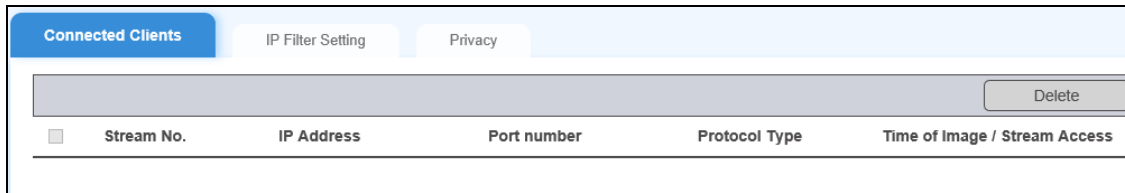
- **Load Default:** Restores the camera back to factory default settings.
- **Load Default (Except Network):** Restores the camera, except for its network configurations, back to factory default settings.
- **Reboot:** Reboots the camera.
- **Auto Reboot:** Automatically reboots the camera at specified time for every specified number of days.

**[Log]** The log contains dump data that is used by service personnel for analyzing problems.

Optionally **Enable Debug Messages** to send the camera's logs to a designated remote server.

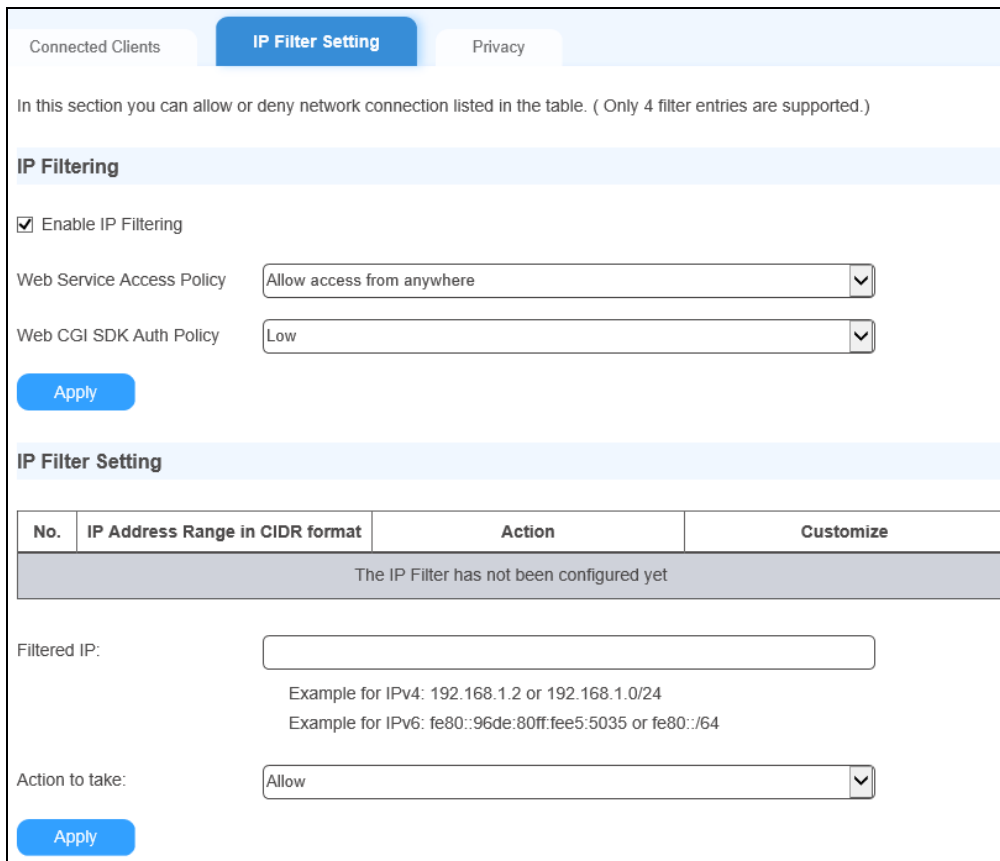
### 3.1.3 Security

#### [Connected Clients]



Displays and manages all clients currently connected to the camera.

**[IP Filter Settings]** The Administrator can set IP filtering to restrict or grant access to the camera for specific IP addresses.



1. To enable IP Filter, select **Enable IP Filtering**.
2. Type specific IP addresses that you want to access or deny access for within **Filtered IP**.
3. Select *Allow* or *Deny* in **Action to Take** to allow or deny access for the IP address(es) specified.
4. Click **Apply**.


**[Privacy]** Displays *Privacy Policy* and requests permissions for the use of cookies.



### 3.1.4 Account Management

#### [Account Management]

Account Management			
No	Username	Account Type	Status
1	admin	Administrator	Enable
2	guest	Guest	Disable

Click **Edit**  next to either the *Administrator* or *Guest* account to change its login Username and Password.

#### [Advanced Setting]

- **Disable authentication for guest account:** Select to restrict access to the camera by the Guest account.

#### [Security]

User Management    Advanced Setting    **Security**

**In this section you can configure the password security settings.**

Security Level Medium ▼

**User Account**

Minimum Password Strength Normal ▼

Number of previously used passwords that cannot be used again Disable ▼

**Login**

Account lockout threshold for invalid login attempts 5 ▼

Lock time of login fail 15 ▼ minute

Limited Login Time 30 ▼ minute

**Apply**

- **Security Level:** Select from **Low**, **Medium** or **Hight** to automatically define all of the setting parameters on the Login Protection tab accordingly.

- **Minimum Password Strength:** Select the required password strength for setting login passwords.
  - ⊙ **Normal:** Requires login passwords to be at least 6 characters in length and containing 3 of the following 4 types of characters: uppercase letters, lowercase letters, 0-9, and special characters (!^\_+,[]{}=).
  - ⊙ **Great:** Requires login passwords to be at least 9 characters in length and containing 1 or more special characters (!^\_+,[]{}=) plus 2 of the following 3 types of characters: uppercase letters, lowercase letters, and 0-9.
- **Number of previously used passwords that cannot be used again:** Specifies the number of previously used passwords that cannot be set as the new password.
- **Account lockout threshold for invalid login attempts:** The number of failed login attempts allowed before the Web interface becomes locked.
- **Lock time of login fail:** The amount of time the camera is locked for after failing to log in and exceeding the maximum number of failed login attempts allowed.
- **Limited Login Time:** The system automatically logs out of the Web interface after it's been idled for the time set.

### 3.1.5 V/A License Management

The V/A License Management page displays the country and version of the recognition engine currently installed. The camera can only have the recognition engine of one country at any given time.

DB Record Limit	Engine	Version	Country / Region	Channels Licensed	Status
--	LPR	1	Taiwan	--	Valid

#### Changing the Country of the Recognition Engine

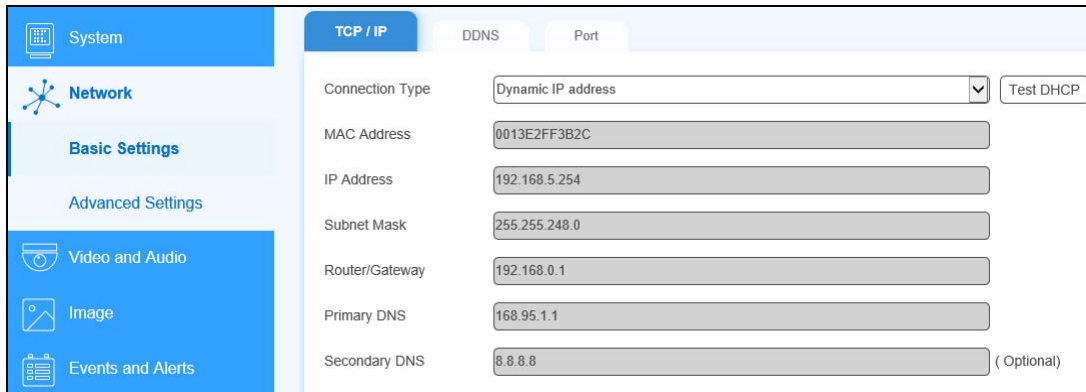
1. Contact our representatives to request for changing the recognition engine of your camera to a different country.
2. Click **Download** under **Export License** to save the required *License* file.
3. Send the *License* file to our representatives and they'll provide you with a new one.
4. Click **Upload** under **Import License** to locate and upload the newly provided *License* file.
5. Follow the procedures in *4.1 Upgrading System Firmware* to update the recognition engine file (.img) corresponding to the country you changed to.

## 3.2 Network

This section covers all of the network settings of the camera, such as **TCP/IP**, **DDNS**, **FTP**, **E-mail**, **HTTPS**, **SNMP**, **QoS**, **802.1x**, **UPnP**, **RTSP** and **ONVIF**.

### 3.2.1 Basic Settings

The Basic Settings page includes the **TCP/IP**, **IPv6**, **DDNS** and **Port** settings of the camera.



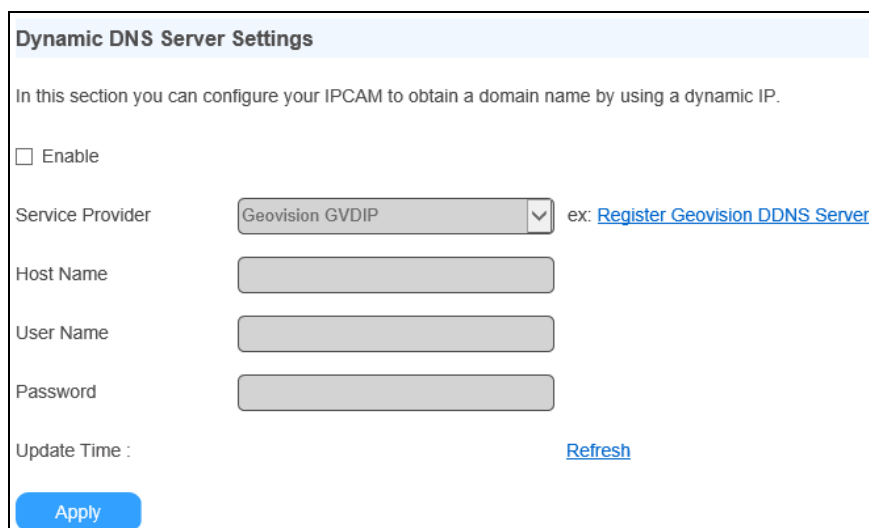
The screenshot shows the 'Basic Settings' page with the 'TCP / IP' tab selected. The settings are as follows:

Field	Value
Connection Type	Dynamic IP address (with Test DHCP button)
MAC Address	0013E2FF3B2C
IP Address	192.168.5.254
Subnet Mask	255.255.248.0
Router/Gateway	192.168.0.1
Primary DNS	168.95.1.1
Secondary DNS	8.8.8.8 (Optional)

**[TCP/IP]** For assigning a static IP address for the camera, see *2.2 Changing the Static IP Address*.

**[IPv6]** Optionally **Enable IPv6**, select *Dynamic* or *Static IP Address* from the **Connection Type** dropdown list, type the required network information and click **Apply** to use the function.

**[DDNS]** DDNS (Dynamic Domain Name System) provides a convenient way of accessing the camera when it uses a dynamic IP address. DDNS assigns a domain name to the camera, which always automatically points to the changing IP assigned by the DHCP Server or ISP (in xDSL connection).



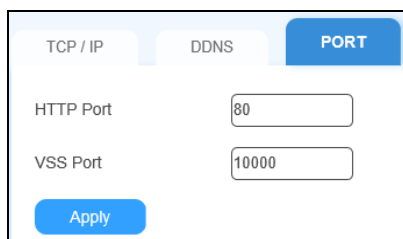
The screenshot shows the 'Dynamic DNS Server Settings' page with the following configuration:

- Enable
- Service Provider: Geovision GVDIP (with ex: [Register Geovision DDNS Server](#))
- Host Name: [Text Input Field]
- User Name: [Text Input Field]
- Password: [Text Input Field]
- Update Time: [Text Input Field] [Refresh](#)
- Apply** button

1. To start, select **Enable** which enables 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 your camera. For the users of GeoVision DDNS Server, it is unnecessary to fill the field because the system will detect the host name automatically.
4. **User Name:** Type the user name used to enable the service from the DDNS.
5. **Password:** Type the password used to enable the service from the DDNS.
6. Click **Apply**.

**[Port]** Users can optionally modify the default port values of the camera if necessary.

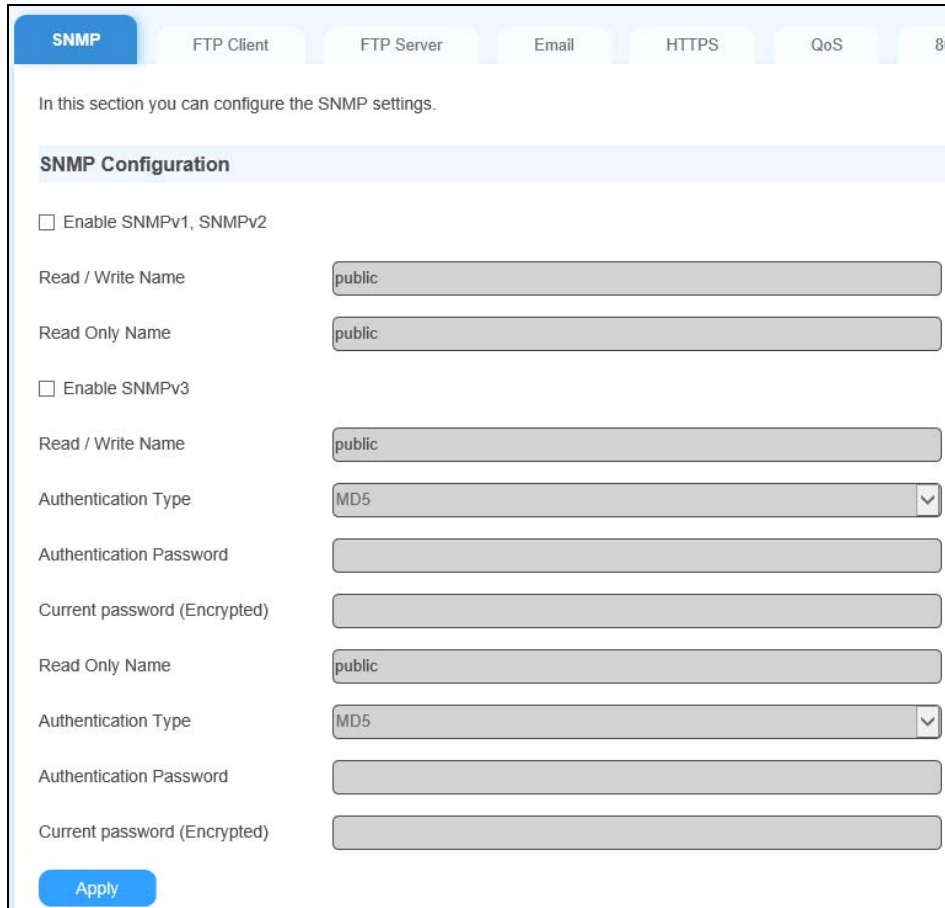


The screenshot shows a web interface with three tabs: 'TCP / IP', 'DDNS', and 'PORT'. The 'PORT' tab is selected and highlighted in blue. Below the tabs, there are two input fields: 'HTTP Port' with the value '80' and 'VSS Port' with the value '10000'. At the bottom left of the form is a blue 'Apply' button.

- **HTTP Port:** Enables connecting your camera to the Web. For security integration, the Administrator can hide the server from the general HTTP port by changing the default HTTP port **80** to a different port, within the range of **1** to **65535**.
- **VSS Port:** Enables connecting the camera to GV-Software.

## 3.2.2 SNMP

Simple Network Management Protocol (SNMP) allows users to monitor the status of the camera through SNMP software. To access, select **Network > Advanced Settings**.



The screenshot shows the 'SNMP' configuration page. At the top, there are tabs for 'SNMP', 'FTP Client', 'FTP Server', 'Email', 'HTTPS', 'QoS', and '80'. Below the tabs, a message states: 'In this section you can configure the SNMP settings.' The main content is titled 'SNMP Configuration' and contains two sections:

- SNMPv2 Configuration:**
  - Enable SNMPv1, SNMPv2
  - Read / Write Name: public
  - Read Only Name: public
- SNMPv3 Configuration:**
  - Enable SNMPv3
  - Read / Write Name: public
  - Authentication Type: MD5
  - Authentication Password: [Empty field]
  - Current password (Encrypted): [Empty field]
  - Read Only Name: public
  - Authentication Type: MD5
  - Authentication Password: [Empty field]
  - Current password (Encrypted): [Empty field]

An 'Apply' button is located at the bottom left of the configuration area.

1. Select **Enable SNMPv1 SNMPv2c** to enable the function.
2. To enable access to **Read / Write Name**, 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 Name**, 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 **Read / Write Name**, type a community string.
6. Select an **Authentication Type** to be used for SNMP requests.
7. Type the **Authentication Password** and **Current Password (Encrypted)**. You will need to type these passwords in the SNMP software to be able to access the camera.
8. To enable access to **Read Only Name**, type a community string to allows read-only access to the camera, and set up the **Authentication Type**, **Authentication Password** and the **Current Password (Encrypted)**.
9. Click **Apply** to save the settings.

### 3.2.3 FTP Settings

**[Upload to FTP Server]** Users can set the camera to send captured images to a remote FTP server upon alert events.

1. Select **Enable** to set up the FTP function.
2. Select **Active Mode** or **Passive Mode**, depending on the setting of your FTP server.
3. **Server URL/IP Address:** Type the URL address or IP address of the FTP Server.
4. **Server Port:** Type the port number of the FTP Server or keep the default value **21**.
5. Type the **Username** and **Password** of the FTP Server.
6. **Remote Directory:** Type the name of the storage folder on the FTP Server.
7. **Alerts interval time in minute:** Specify the interval between FTP alerts. The interval can be between 0 and 60 minutes. The option is useful for frequent event occurrence. Any event triggers during the interval period will be ignored.

**[FTP – Alert Settings]** Configures the type of alerts to be sent to the FTP server.

- **Motion Detection:** Select to automatically send a snapshot to the FTP Server upon motion detection. Select **Continuously send images upon trigger events (Motion)** to upload a series of snapshots to the FTP Server upon motion detection.
- **Digital Input:** Select to automatically send a snapshot to the FTP Server when a digital input is triggered. Select **Continuously send images upon trigger events (Input)** to upload a series of snapshots to the FTP Server upon input trigger events.
- **Continuously Send Images:** Sends images to the FTP server at the specified interval.
  - ⊙ **Interval:** Use the dropdown list to specify how frequent the images are sent to the FTP server.
  - ⊙ **FTP Schedule:** Enable and click **Set** to specify a schedule for which images are sent to the FTP server.

<input type="checkbox"/> Span 1	1	minutes	00	:	00	~	00	:	00	Next Day	
<input type="checkbox"/> Span 2	1	minutes	00	:	00	~	00	:	00	Next Day	
<input type="checkbox"/> Span 3	1	minutes	00	:	00	~	00	:	00	Next Day	
<input type="checkbox"/> Weekend	1	minutes	<input checked="" type="radio"/> Saturday and Sunday <input type="radio"/> Only Sunday								
<input type="checkbox"/> Special Day	1	minutes	(MM/DD)								
01.	<input type="text"/>	02.	<input type="text"/>	03.	<input type="text"/>	04.	<input type="text"/>				
05.	<input type="text"/>	06.	<input type="text"/>	07.	<input type="text"/>	08.	<input type="text"/>				
09.	<input type="text"/>	10.	<input type="text"/>	11.	<input type="text"/>	12.	<input type="text"/>				

- **Span 1- Span 3:** Set different time frames during the day for the images to be sent to the FTP server. Each day can be divided into 3 time spans, represented by Span 1 to Span 3.
- **Weekend:** Enable this option to send images to the FTP server all day on the weekend and define whether your weekend includes **Saturday and Sunday** or **Only Sunday**.
- **Special Day:** Send images to FTP server for specific dates.

---

**Note:** If the settings for Special Day conflict with those of Span 1-3 or Weekend, the Special Day settings have priority.

---

- ⊙ **Enable Recycling / Keep Days:** Select this option to recycle the FTP storage for data that've been stored after the specified Keep Days.



**[FTP Server]** Sets the camera as an FTP server, and define a desired Username and Password to allow users to download its image files. The default username is *ftpuser*.

The screenshot shows the 'FTP Server' configuration page. At the top, there are tabs for 'SNMP', 'FTP Client', 'FTP Server' (selected), 'Email', 'HTTPS', and 'QoS'. Below the tabs is the 'FTP Server User Account' section. A yellow warning box contains the text: 'For safety reasons, the password must be at least 8 characters long. It must contain three character categories among the following: uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), and special characters (!@\_~+[])='. Below the warning is a checkbox labeled 'Enable ftp access to IPCAM'. There are four text input fields: 'Username' (containing 'ftpuser'), 'Old Password', 'New Password', and 'Confirm Password'. There is also a 'Use alternative Port' field with the value '21'. An 'Apply' button is at the bottom left.

To access the internal FTP server of the camera, type the IP address or the domain name of the camera on an Internet browser, e.g. `ftp://192.168.0.10`.

### 3.2.4 E-mail

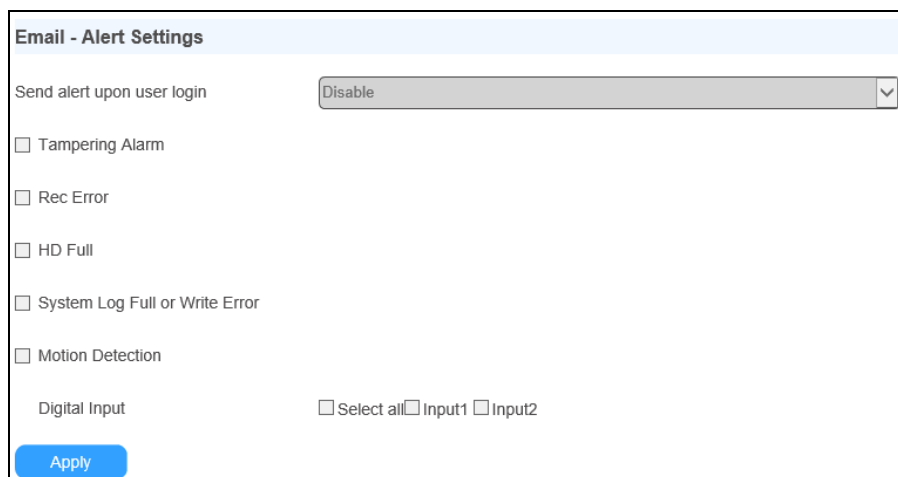
Users can set the camera to send out e-mail alerts upon motion and/or input trigger events.

The screenshot shows the 'Email' configuration page. At the top, there are tabs for 'SNMP', 'FTP Client', 'FTP Server', 'Email' (selected), 'HTTPS', 'QoS', '802.1x', 'UPnP', and 'RTSP'. Below the tabs is the 'Email' section. It contains several fields: 'Server URL/IP Address' with a 'Test Email' button, 'Server Port' (25), 'From email address', 'Send to' (with a note: '( Please use ";" to seperate recipients' addresses)'), 'Alerts Interval time in minute (0 to 60)' (0), a checkbox 'Need authentication to login', 'User Name', and 'Password'. There is also a checkbox 'This server requires a secure connection'. Below this is the 'Email - Mail Content' section, which has a 'Subject' field (GV-LPR2800-DL) and a 'Note' field (a large text area).

1. Select **Enable** to set up e-mail notifications.

2. **Server URL/IP Address:** Type the SMTP Server's URL address or IP address.
3. **Server Port:** Type the SMTP Server's port number or keep the default value **25**.
4. **From email address:** Type the sender's e-mail address.
5. **Send to:** Type the e-mail address(s) you want to send alerts to.
6. **Alerts interval time in minute:** Specify the interval between e-mail alerts, from 0 to 60 minutes. This option is useful for frequent event occurrence. Any event detected during the interval period will be ignored.
7. If the SMTP Server needs authentication, select **Need authentication to login** and type a valid **Username** and **Password** to log in the SMTP server. If the SMTP Server needs a secure connection (SSL), select **This server requires a secure connection**.

**[E-mail – Alert Settings]** Configures the events that e-mail alerts shall be sent for.



- **Tampering Alarm:** Sends an e-mail alert when a tampering event occurs.
- **Rec Error:** Sends an e-mail alert upon a memory card recording error.
- **HD Full:** Sends an e-mail alert when the memory card is full.
- **System Log Full or Write Error:** Send an e-mail alert when the system alert is full or when the device is unable to write into the memory card.
- **Motion Detection:** Sends an e-mail alert when the camera detects a motion.
- **Digital Input:** Sends an e-mail alert upon a triggered input event.

### 3.2.5 HTTPS

By enabling the Hypertext Transfer Protocol Secure (HTTPS) settings, you can access the camera through a secure protocol.

The screenshot displays the configuration page for HTTPS. At the top, there are navigation tabs: SNMP, FTP Client, FTP Server, Email, **HTTPS**, QoS, and 802.1x. Below these are sub-tabs: UPnP, RTSP, Onvif, and Others. The main content area starts with the text: "You can configure the HTTPS settings below." This is followed by a section titled "HTTPS Settings" with a light blue header. Below this header, there is explanatory text: "You can configure the default HTTPS port of 443 to any value within the range of 1 ~ 65534. For an automated secured connection, make sure 'Always connect through HTTPS' is enabled, otherwise you'll need to type 'https://' in front of the IP address when connecting." The settings include:
 

- Enable
- Always connect through HTTPS
- HTTPS port:

 The next section is "System Authentication" with a light blue header. It contains:
 

- Authentication Method:

 The final section is "Client Authentication" with a light blue header. It includes:
 

- Text: "Prior to exporting client certificate, make sure 'Use a certificate to authenticate the client(s) connecting' is selected and click Apply."
- Use a certificate to authenticate the client(s) connecting
- Authentication Method:

 At the bottom of the form is a blue "Apply" button.

**[HTTPS Settings]** By enabling the HTTPS settings, you can allow or require all users to 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** from the Authentication Method dropdown list, click **Browse** to locate the **Certificate** and **Certificate Key Files** and type the password if the *.pem* files are protected by a password.

**[Client Authentication]** Select to use the certificate to authenticate all client connections.

### 3.2.6 802.1x

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.

IEEE 802.1X

Enable IEEE 802.1X

Authentication Type:

EAPOL version:  V1  V2

User Name:

Password:

CA certificate:     
  
 Status:

client certificate:     
  
 Status:

client private key:     
  
 Status:

client private key password:

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.

### 3.2.7 RTSP

The RTSP Server enables video and audio streaming to mobile devices.

- **Activate Link:** Enable the RTSP / 3GPP service.
- **RTSP/TCP Port:** Keep the default value **8554**, or modify it if necessary.
- **RTP/UDP Port:** Keep the default range from **17300** to **17315**, or modify it if necessary. The number of ports for use is limited to 16.
- **Max Connection:** Set the maximum number of RTSP and 3GPP connections to your camera. The maximum value is **8**.
- **Enable Audio:** Select to enable audio streaming through RTSP.
- **Disable Authentication:** Authentication is disabled by default, with which the ID and password of your camera are not required when accessing live view through the RTSP command.

- For RTSP command, enter:

```
rtsp://<username>.<password>@<IP of the camera>:8554/<CH No.>.sdp
```

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

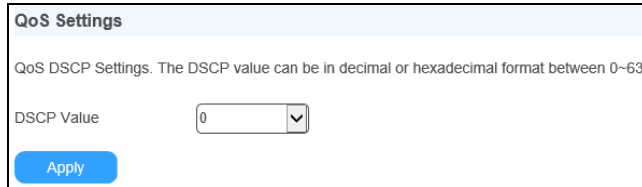
- For RTSP Multicast, add “M” after the channel number:

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

For remote monitoring with mobile phones, see *Chapter 7 Smart Device Connection*.

### 3.2.8 QoS, UPnP & ONVIF

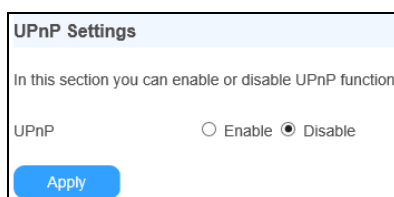
**[QoS]** The Quality of Service (QoS) is a bandwidth control mechanism that guarantees delay-sensitive data flows, such as voice and video streams, to achieve a certain amount of bandwidth in keeping the streaming smooth.



The screenshot shows a web interface titled "QoS Settings". Below the title, there is a descriptive text: "QoS DSCP Settings. The DSCP value can be in decimal or hexadecimal format between 0~63". Below this text, there is a label "DSCP Value" followed by a text input field containing the number "0" and a small downward arrow icon. At the bottom left of the form, there is a blue button labeled "Apply".

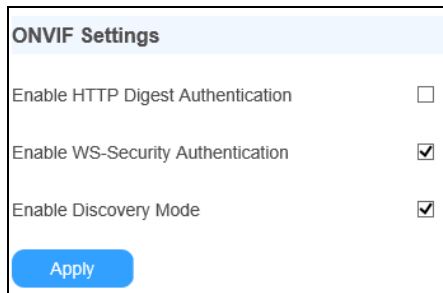
To apply QoS to the camera, all network routers used must support and have QoS enabled. To enable the QoS on the camera, enter a Differentiated Services Code Point (DSCP) value. This value is a field in an IP packet that enables different levels of services for the network traffic. When the video stream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

**[UPnP]** 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 systems (such as Windows XP) supported by this function. Enabling this function, you can connect to the camera directly by clicking on the camera listed in the network devices table.



The screenshot shows a web interface titled "UPnP Settings". Below the title, there is a descriptive text: "In this section you can enable or disable UPnP function.". Below this text, there is a label "UPnP" followed by two radio buttons: "Enable" (which is unselected) and "Disable" (which is selected). At the bottom left of the form, there is a blue button labeled "Apply".

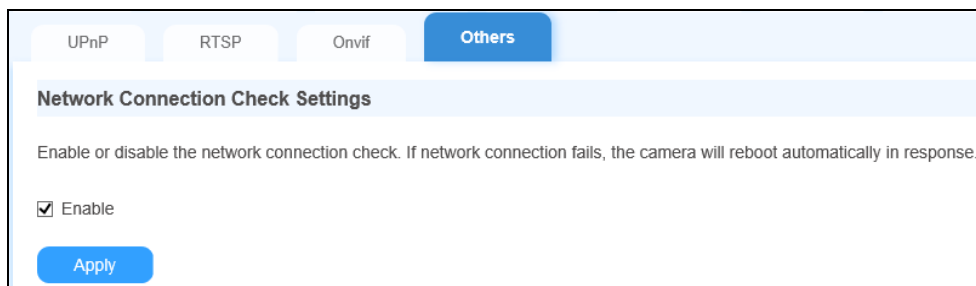
**[ONVIF]** Enable ONVIF to allow connections to third-party video management systems.



The screenshot shows the 'ONVIF Settings' section of a web interface. It contains three settings: 'Enable HTTP Digest Authentication' with an unchecked checkbox, 'Enable WS-Security Authentication' with a checked checkbox, and 'Enable Discovery Mode' with a checked checkbox. A blue 'Apply' button is located at the bottom left of the settings area.

- **Enable HTTP Digest Authentication:** The compatibility with HTTP Digest Authentication is required to access the camera by a 3<sup>rd</sup>-party software through ONVIF.
- **Enable WS-Security Authentication:** Requires 3<sup>rd</sup>-party software to type the login credentials of the cameras upon connecting.
- **Enable Discovery Mode:** Allows third-party software to detect for the camera. This function is enabled by default.

**[Network Connection Check Settings]** When the network connection check is enabled, the camera will check for Internet connection and reboots automatically when it is disconnected from the Internet. This function is enabled by default.

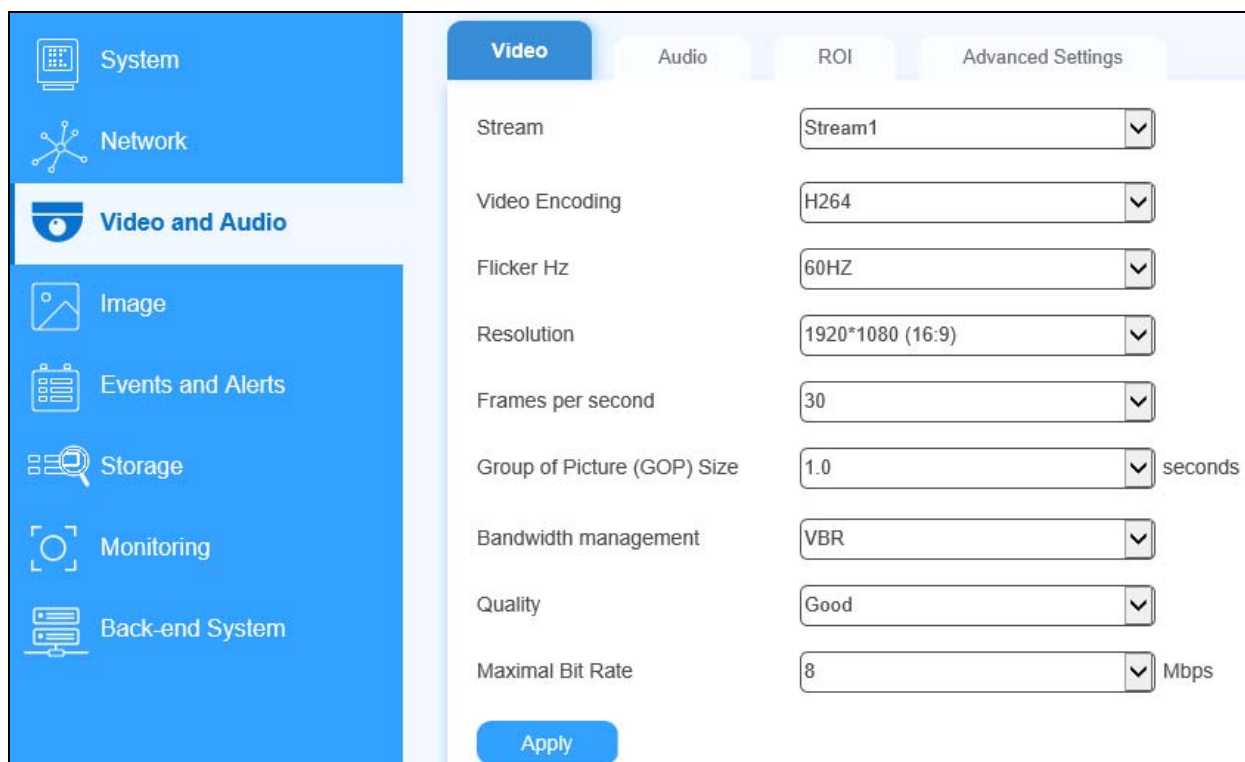


The screenshot shows the 'Network Connection Check Settings' section under the 'Others' tab. It includes a description: 'Enable or disable the network connection check. If network connection fails, the camera will reboot automatically in response.' Below this, the 'Enable' checkbox is checked. A blue 'Apply' button is at the bottom.

## 3.3 Video and Audio

The camera supports triple streams, Stream 1, 2 and 3, which allow 3 separate sets of codec and resolutions settings to be transmitted through a single video transmission. This triple-stream feature allows users to view and record live video differently under various network and surveillance scenarios.

### 3.3.1 Video Settings



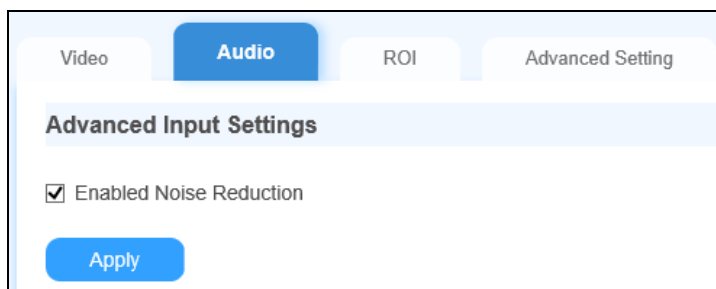
Setting	Value	Unit
Stream	Stream1	
Video Encoding	H264	
Flicker Hz	60HZ	
Resolution	1920*1080 (16:9)	
Frames per second	30	
Group of Picture (GOP) Size	1.0	seconds
Bandwidth management	VBR	
Quality	Good	
Maximal Bit Rate	8	Mbps

- **Stream:** Select the stream you want to configure.
- **Video Encoding:** Select the video codec for the current stream, from H.265, H.264 or MJPEG.
- **Flicker HZ:** Only for Stream 1, select the flicker frequency for the video image. Streams 2 & 3 will follow the same flicker frequency as that of Stream 1.
- **Resolution:** Select the resolution for the current stream.
- **Frames per second:** Select the FPS for the current stream, from 1 to 30.
- **Group of Picture (GOP) Size:** Set the maximum number of seconds between each key frame.



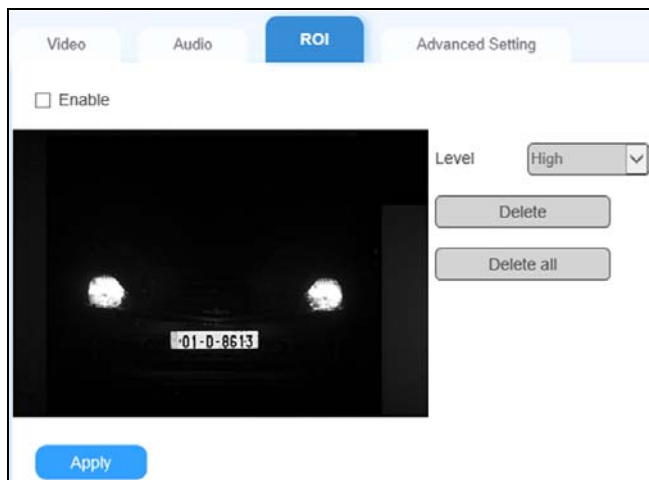
**[Bandwidth Management]**

- **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 following: *Standard, Fair, Good, Great* and *Excellent*. And set the **Maximal Bitrate** between 1 and 20 Mbps.
- **CBR (Constant Bitrate):** CBR is used to achieve a specific bitrate by varying the quality of the stream. The bitrates available for selection depend on the image resolution.
- **Smart Streaming:** When selected, the bitrates and frame rates will be automatically reduced in static scenes, significantly maximizing bandwidth and lowering file size.
  - ⊙ **Bitrate Reduction Level:** The default value is 300. The bigger the value, the more bitrates can be reduced in static scenes, thus saving the recording size.
  - ⊙ **Framerate Reduction Level:** The default value is 30. The bigger the value, the more fps can be reduced in static scenes, thus saving the recording size.
- **Maximal Bitrate:** When the system bitrate reaches the value specified, the system will automatically reduce its bitrate to prevent from exceeding it. Select one of the bitrates from the dropdown list.

**3.3.2 Audio Settings**

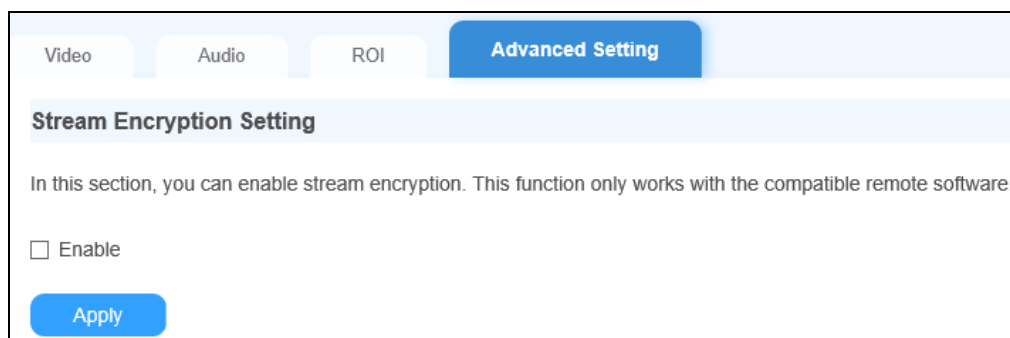
- **Enable Noise Reduction:** Reduces the background noise in the audio recorded.

### 3.3.3 ROI



The **ROI (Region of Interest)** allows you to enhance the image clarity, high or low, for up to 5 defined regions by clicking and dragging on the image.

### 3.3.4 AES Encryption



To access AES Encryption function, select **Video and Audio > Advanced Settings**.

Enable to add **AES Encryption** to all images sent to the connected software for enhanced security, such as GV-DVR / NVR / VMS.

## 3.4 Image

This section covers all settings that can be applied to the live and recorded video images, including **OSD & Text Overlay**, **Watermark Setting**, **Privacy Mask** and **Visual Automation**.

### 3.4.1 OSD & Text Overlay

The screenshot shows the 'OSD And Text Overlay' configuration page. On the left is a blue sidebar with menu items: System, Network, Video and Audio, Image (highlighted), Events and Alerts, Storage, Monitoring, and Back-end System. The main content area has a top navigation bar with tabs: OSD And Text Overlay (selected), Text Overlay OCX, Privacy Mask, Visual Automation, and Watermark Setting. Below the tabs, the 'Video Type' is set to 'Stream1'. The 'Text Overlay Settings' section includes a 'Camera Name' field with 'Camera' entered, and an 'Overlay with:' section with checkboxes for 'Camera Name', 'Date', 'System Time', and 'Name of the associated digital input' (with sub-options for 'Input 1' and 'Input 2'). The 'Text Overlay Settings (OSD)' section includes a 'Camera Name' field with 'Camera' entered, a 'Font Size' dropdown set to '1x', and an 'Overlay with:' section with checkboxes for 'Camera Name', 'Date', and 'System Time', each with a dropdown menu set to 'Lower Right'.

#### [Text Overlay Settings]

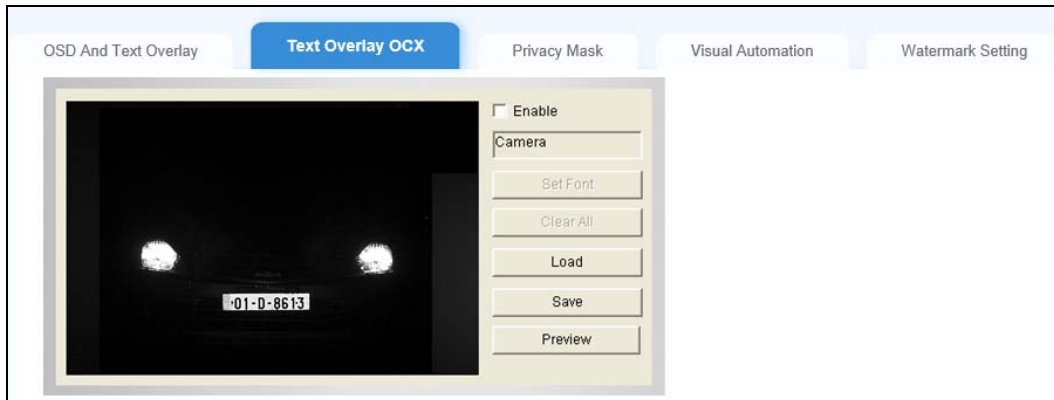
- **Camera Name:** Give a name for the camera, which can be displayed on the video image.
- **Overlay with:** Select to overlay any of the following on the live and recorded videos.
  - ⊙ **Camera Name:** Displays the name of the camera.
  - ⊙ **Date:** Displays the date.
  - ⊙ **System Time:** Displays the local time of the camera.
  - ⊙ **Name of the associated digital input:** Select to display one of or both Input 1 and 2.

**[Text Overlay Settings (OSD)]** Displays the 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.

- **Camera Name:** Type the camera name.

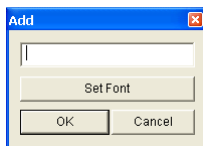
- **Font Size:** Select the font size using the dropdown list.
- **Date:** Displays the date.
- **System Time:** Displays the local time of the camera.
  - Select a position for each of the information to be displayed on the video image, from *Upper Left, Upper Right, Lower Left and Lower Right*.

### [Text Overlay OCX]



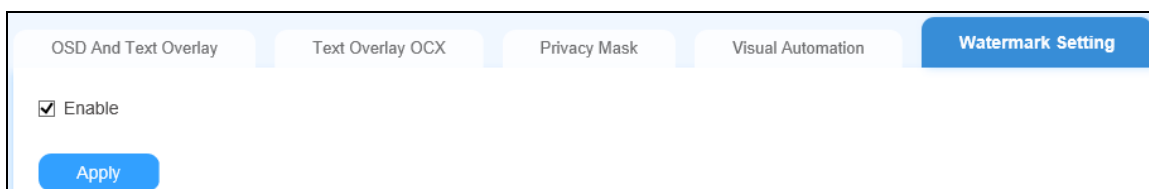
The Text Overlay OCX function allows you to overlay any text in any place on the live and recorded videos. Up to 16 text messages can be created.

1. To create overlay text, select **Enable** and click on the image. This dialog box appears.



2. Type the desired text and click **OK**. Then drag the overlaid text to any place on the image.
3. Click **Save** to apply the settings, or click **Load** (Undo) to revert to the last saved setting.
4. Optionally click **Preview** to see how the texts will appear on the image.

### [Watermark Setting]



Enable this option to watermark all recordings. The watermark allows you to verify whether the video has been tampered with. See *4.4 Verifying Watermark*.

### 3.4.2 Privacy Mask

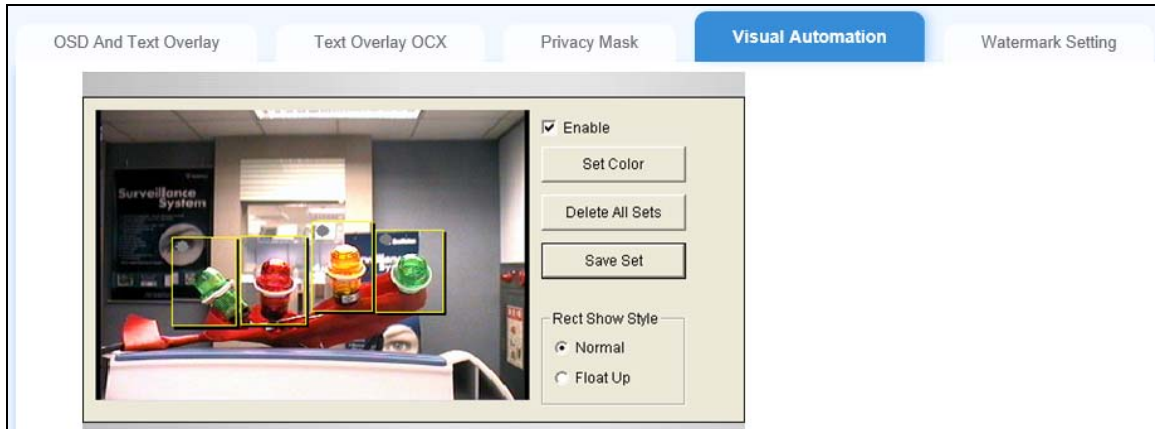
The Privacy Mask can block out sensitive areas to be viewed, in both live view and recorded videos. This feature is ideal for privacy protection on locations with private information, such as keyboard sequences (e.g. passwords), and any place you would like to keep inaccessible to view.



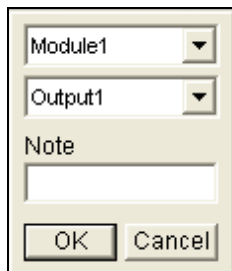
1. Select **Enable** and click-and-drag to draw area(s) where you want to block out on the image. Click **Add** when you are prompted to confirm the setting.
2. Click **Save** to save the settings.

### 3.4.3 Visual Automation

This intuitive feature helps you automate any electronic device by triggering the connected output device. When set, you can change the current stage of the electronic device, e.g. light ON, by simply clicking on the image.



1. Select **Enable** and click-and-drag on an area on the image of the electronic device. This dialog box appears.



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

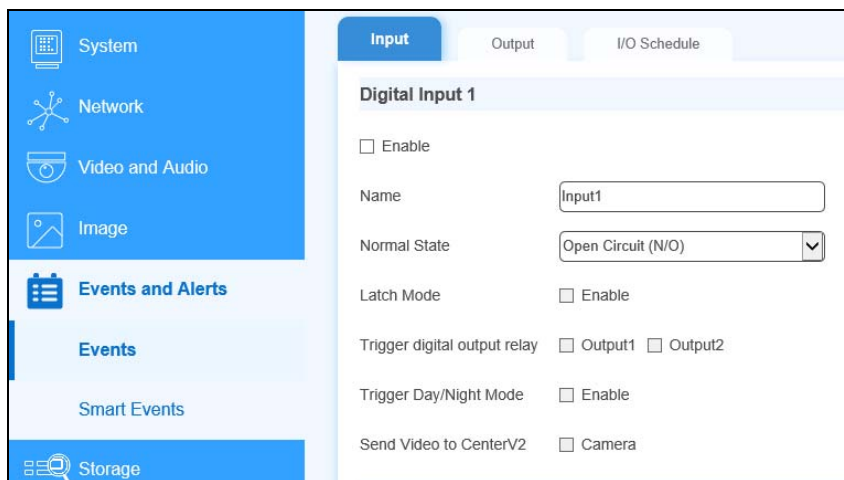
To access and use the function of Visual Automation, see *2.12 Visual Automation*.

## 3.5 Events and Alerts

This section covers the event and alert settings of the camera, including **I/O Settings**, **Tampering Alarm** and **LPR Settings**.

### 3.5.1 Input Settings

**[Digital Input 1/2]** Before configuring, make sure the desired input device has been properly connected to the digital input of the camera, see [1.6.2 External Wiring](#).



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

- **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 to switch between day/night mode when the input is triggered.
- **Send Video to Center V2:** Enable this option to send the images to Center V2 when the input is triggered.

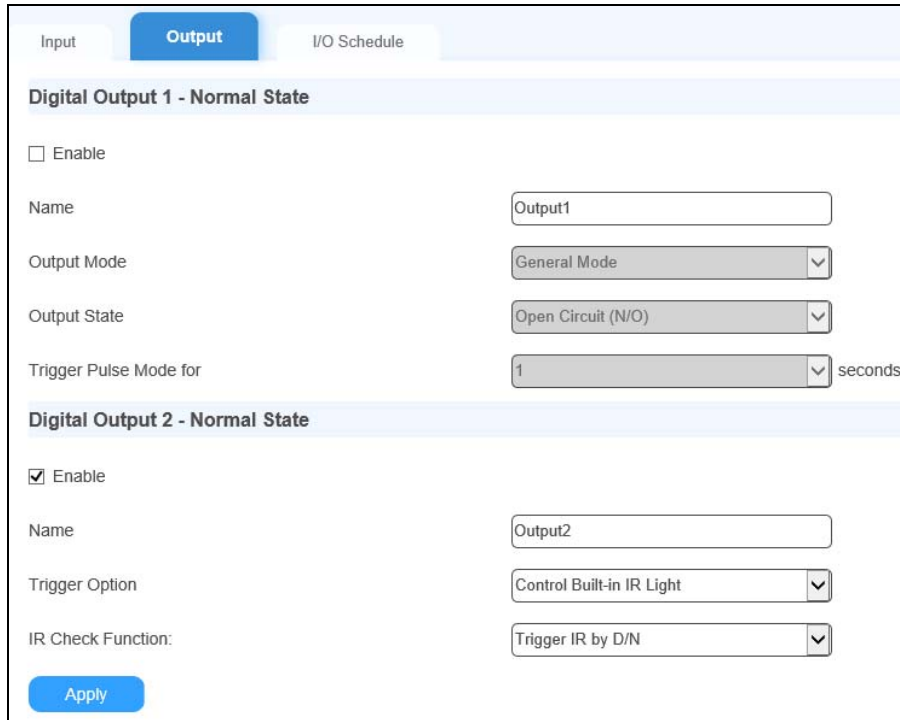
---

**Note:** For input triggers to work, I/O monitoring must be enabled, either manually or by schedule. See [3.7 Monitoring](#) and [3.5.3 I/O Schedule](#) for details.

---

### 3.5.2 Output Settings

**[Digital Output 1 – Normal State]** Before configuring, make sure the desired output device, e.g. the required gate or barrier for access control, has been properly connected to Output 1 of the camera, see *1.6.2 External Wiring*.



The screenshot shows a web interface for configuring camera outputs. At the top, there are three tabs: 'Input', 'Output' (which is active), and 'I/O Schedule'. Below the tabs, there are two sections for digital outputs. The first section is titled 'Digital Output 1 - Normal State' and includes an 'Enable' checkbox (unchecked), a 'Name' field with 'Output1', an 'Output Mode' dropdown menu (set to 'General Mode'), an 'Output State' dropdown menu (set to 'Open Circuit (N/O)'), and a 'Trigger Pulse Mode for' dropdown menu (set to '1') followed by the text 'seconds'. The second section is titled 'Digital Output 2 - Normal State' and includes an 'Enable' checkbox (checked), a 'Name' field with 'Output2', a 'Trigger Option' dropdown menu (set to 'Control Built-in IR Light'), and an 'IR Check Function' dropdown menu (set to 'Trigger IR by D/N'). At the bottom of the form is a blue 'Apply' button.

- **Output Mode:** Choose the output mode that mostly suits your scenario, from **General**, **Toggle** or **Pulse Mode**.
  - ⊙ **General Mode:** Triggers the output once.
  - ⊙ **Toggle Mode:** The output continues to be triggered until a new input trigger ends the output.
  - ⊙ **Pulse Mode:** The output is triggered for the amount of time you specify in the **Trigger Pulse Mode for x Seconds** field.
- **Output State:** Choose the output signal that mostly suits the device you are using: **Open Circuit (N/O)** or **Grounded Circuit (N/C)**.



### [Digital Output 2 – Normal State]

- **Trigger Option:** Select a trigger option from **Control Built-in IR Light**, **Control External IR Light** or **As Configured by Digital Output Alerts**.
  - ⊙ **Control Built-in IR Light:** Select to turn on/off the built-in IR light upon trigger.
  - ⊙ **Control External IR Light:** Select to turn on/off the external IR light upon trigger.
  - ⊙ **As Configured by Digital Output Alerts:** Select to set Output 2 with settings similar to that of Output 1.
- **IR Check Function:** By default, **Trigger IR by D/N** is selected to automatically turn the IR light on or off based on the amount of light detected. Optionally select **On** or **Off** to always keep the IR light on or off, respectively.

### 3.5.3 I/O Schedule

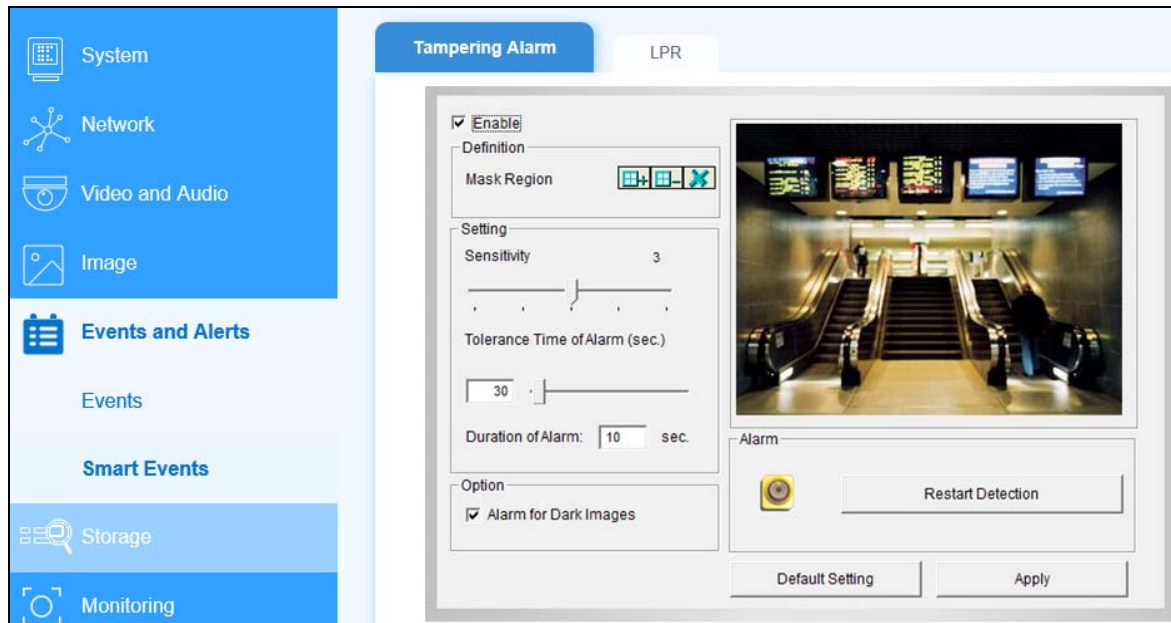
Users can set the schedule for which the I/O to operate.


For details of setting schedules, see *FTP Schedule*, *3.2.3 FTP Settings*.

### 3.5.4 Tampering Alarm

Tampering Alarm is used to detect and alert for when the camera is being physically tampered with. An alarm can be generated when the camera is moved, covered up, or out of focus. The alarm types include triggering connected output device(s), sending e-mail alert and notifying the connected GV-Software. For this function to work, set up at least one of the following:

- To trigger an output device when a tampering event occurs, enable the output setting and select **Tampering Alarm**. See *3.5.2 Output Settings*.
- To trigger the e-mail alert when a tampering event occurs, enable the e-mail setting and select **Tampering Alarm**. See *3.2.4 E-Mail*.
- To notify the desired GV-Software when a tampering event occurs, enable the connection accordingly. See *3.8.1 Center V2*, *3.8.2 VSM (Vital Sign Monitor)* and, *5.1 Setting up IP Cameras on GV-DVR / NVR*, and *5.2 Setting up IP Cameras on GV-VMS*.



1. To configure the tampering alarm, select the **Enable**.
2. If you want the camera to ignore any movement or scene change in certain areas, click  to draw the areas to be ignored 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.
7. Click **Apply** to save all the settings.

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

## 3.5.5 LPR

This section covers the LPR-related settings of the camera.

### 3.5.5.1 Recognition Result

This function allows you to display the recognized plate number capture, along with the date and time of the recognition, and/or a desired text on the images of the recognition results.

The screenshot shows the 'LPR' configuration page with the 'Recognition Result' tab selected. The page includes a navigation bar with 'LPR' and 'Tampering Alarm' tabs, and a sub-menu with 'Recognition Result', 'LPR Detection', 'GPS & RS485', 'Inquire Recognized Database', 'Registry Database', and 'Push Notification'. The 'Recognition Result' section is titled 'Recognizing Schedule' and contains the following settings:

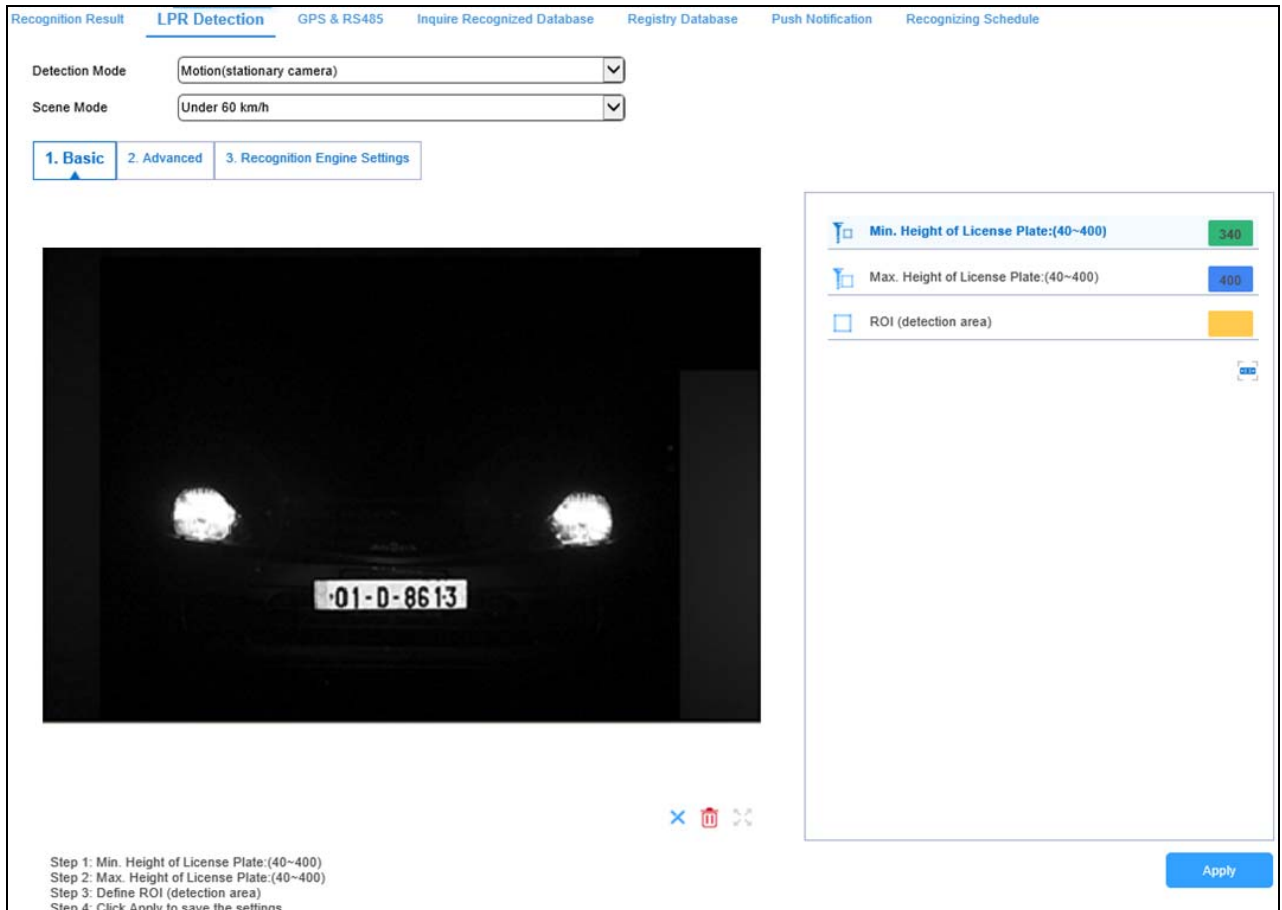
- Overlay Text on Recognition Results: GEOVISION
- Overlay Time on Recognition Results
- Overlay LPR Result on Recognition Results
- Overlay Text Position: Down-Left
- Snapshot Size: Original
- JPEG Quality: 80%

An 'Apply' button is located at the bottom left of the configuration area.

- **Overlay Text on Recognition Results:** Includes a desired text or description on the images of the recognition results.
- **Overlay Time on Recognitions Results:** Includes date and time stamps on the images of the recognition results.
- **Overlay LPR Result on Recognition Results:** Includes the recognized plate number on the images of the recognition results.
- **Overlay Text Position:** Select a position for which to display the overlay texts on the images of the recognition results.
- **Snapshot Size:** Select the size of the recognition event snapshots, between *Small* and *Original*.
- **JPEG Quality:** Select the quality of the snapshot, from 50 ~ 80%.

### 3.5.5.2 LPR Detection

Users can set the camera to perform LPR upon motion detection or input trigger. Up to 8 detection areas can be defined for motion detection and plate recognition.



- **Detection Mode:** Sets the detection for which LPR shall be activated.
  - ⊙ **Disable:** Deactivate recognition.
  - ⊙ **Motion (Stationary Camera):** Activate recognition by motion detection. Select this mode if your camera is fixed at one place.
  - ⊙ **Motion (Mobile Camera):** Activate recognition by motion detection. Select this option if your camera is not fixed at one place or is installed on a vehicle.
  - ⊙ **Motion (Continuous Recognition):** Activate for round-the-clock nonstop recognition.
  - ⊙ **Parking (I/O):** This option is designed for parking areas. The recognition is activated by input triggers and records all vehicle entries within its detection and recognition range. Select which input(s) will trigger recognition, as mentioned in the **2. Advanced** section below.
  - ⊙ **Parking (Motion):** This option is designed for parking areas. The recognition is activated by motion detection at the parking area. Select this option if the parking area is without a gate installed to trigger the recognition.

- **Parking (I/O) 2/3:** This option is designed for parking areas. The recognition is activated by input triggers and records only the first vehicle entry, while ignoring others, within its detection and recognition range. Select which input(s) will trigger recognition, as mentioned in the **2. Advanced** section below.
- **Scene Mode:** Select the speed of the recognition targets, from **Under 60 km/h** or **Over 60 km/h**.

**[1. Basic]** Sets the minimum and maximum height of the license plates to be detected and the area of detection.

1. Select **Min. Height of License Plate: (40~400)** and click and drag on the image to define the minimum height of the license plates to be detected, from 40 to 400 pixels.
2. Select **Max. Height of License Plate: (40~400)** and click and drag on the image to define the maximum height of the license plates to be detected, from 40 to 400 pixels.
3. Select **ROI (detection area)** and click and drag on the image to draw the desired areas for license plate detection. Up to 8 ROIs can be defined.
4. Click **Apply**.

**[2. Advanced]** Sets the parameters for license plate detection.

- **If the recognition is still repeating, it will notify after X seconds (0~300):** Specify the amount of time recognition is activated for upon motion detection or input trigger events.
- **Parking Mode (Controlled by ASM, SD storage is necessary):** Performs license plate recognition only when the inputs at a GV-ASManager-controlled parking lot are triggered.
- **Output recognition result quickly (It will increase error rate of recognition system):** Select this option if you want to have a faster recognition result at the cost of accuracy. This option is suitable for a large amount of traffic and the frames received will go through a faster recognition process (approximately at a processing rate of 1 frame per second).
- **Detected Sensitivity:** Select the sensitivity level of motion detection from the dropdown list, from 1 to 10. The higher the value, the more sensitive the system is to the motion.
- **Detected Object Size:** Select the value of the targeted object's normal size, from 1 to 5. The higher the value, the bigger the size of the object.
- **Trigger Input:** Select to trigger **Input 1** or **Input 2**.
- **Force Export (Used in I/O Mode):** Select to display the symbol \*\*\*\*\* to represent unknown license plates even when the recognition fails. If the option is not selected, invalid (failed) recognition results will not be recorded.

- **Capture Frame Number in Each Triggered (1~5):** Select the number of image frames, from 1 to 5, to be captured when the recognition is activated by input trigger.
- **Repeat Recognition when Recognition Failed (0~3):** Select the number of recognitions attempts, from 1 to 3, to be performed when an input-triggered recognition fails.

**[3. Recognition Engine Settings]** Sets the parameters for license plate recognition.

- **Maximum Number of Characters (1~16):** Set the maximum number of characters allowed on the license plate to activate the recognition process. If the number of characters exceeds the limit, the system will not perform recognition.
- **Minimum Number of Characters (1~16):** Set the minimum number of characters allowed on the license plate to activate the recognition process. If the number of characters does not reach the minimum requirement, the system will not perform recognition.
- **Maximum Number of Plates (1~8):** Sets the maximum number of plates to be recognized simultaneously.
- **LPR Confidence Level:** The higher the value, the stricter the LPR engine is to filtering out blurred license plates and only capturing license plates deemed as clear. The default value is 3.

Click **Apply** to save the settings.

## 3.5.5.3 GPS &amp; RS-485

Tampering Alarm **LPR**

Recognition Result Detection Mode Recognition Engine Settings **GPS & RS485** Inquire Recognized Database

Registry Database Push Notification Recognizing Schedule

Enable

**GPS**

Enable GPS

User-defined GPS  Example: (25.082080, 121.566178)

**RS-485-A**

Enable

Output Format

**RS-485-B**

Enable

Input From

Apply

**[GPS]** Enable to type the longitude and latitude location of the device for its location to be displayed on the E-Map, using Google Maps, of the connected GV-ASManager.

**[RS-485 A/B]** Users can enable to send or receive data through RS-485.

- **Output Format:** Select the desired recognition results from the dropdown list to export, including *License Plate Only*, *License Plate and Time*, and *License Plate File Name*.

---

**Note:** RS-485 B can only be used to connect to GV-RU9003.

---

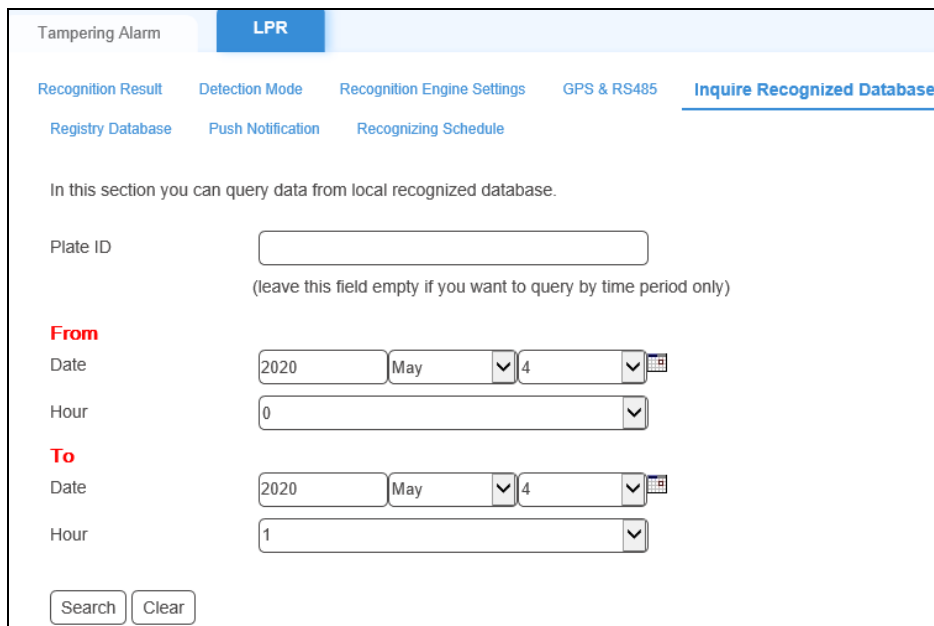
### 3.5.5.4 Inquire Recognized Database

Users can enquire the history of a plate number from the database stored in the memory card.

---

**Note:** Make sure you have inserted a memory card that contains the database of recognized license plate numbers.

---



Tampering Alarm | **LPR**

Recognition Result | Detection Mode | Recognition Engine Settings | GPS & RS485 | **Inquire Recognized Database**

Registry Database | Push Notification | Recognizing Schedule

In this section you can query data from local recognized database.

Plate ID

(leave this field empty if you want to query by time period only)

**From**

Date: 2020 | May | 4

Hour: 0

**To**

Date: 2020 | May | 4

Hour: 1

1. Type a license plate number in the Plate ID field. The entries are case-sensitive.
2. Specify a start and end time by typing the year and using the dropdown lists.
3. Click **Search** to start searching for the license plate within the memory card.

---

**Tip:** To list all license plates captured during a certain period, leave the **Plate ID** field blank and only specify the time period.

---



### 3.5.5.5 Registry Database

Users can automatically activate an output, for example, opening a gate when a captured license plate matches a registered license plate in the database based on the configurations set.

You can create a standalone database on the camera or obtain the database from GV-ASManager, an access control and license plate recognition management software.

For the integration of the camera to GV-ASManager, the vehicle database is transmitted from GV-ASManager and saved on the memory card. To set up the connection with the GV-ASManager for database download, see *Chapter 8 GV-ASManager Connection*.



To access the database from GV-ASManager:

- Make sure a memory card is inserted to the camera and the storage settings are configured. For detail, see *3.6.1 Storage Settings*.
- Make sure the camera is connected with GV-ASManager to download the vehicle database.
- Make sure the output settings of the gate or barrier are configured and enabled. The gate or barrier must be connected to **output 1** of the camera. For detail, see *3.5.2 Output Settings*.

---

**Note:** This function is only supported by GV-ASManager V5.3.1 or later.

---

Tampering Alarm
LPR

Recognition Result
Detection Mode
Recognition Engine Settings
GPS & RS485
Inquire Recognized Database

Registry Database
Push Notification
Recognizing Schedule

Registry Database

**In this section you can set registry database and compared mode.**

Enable Registry Database(SD storage is necessary)

Database Control by AS Manager

Registry Database Comparison Complete (All Characters Match)

Plate Only

Apply

**Standalone Database( Support White List only)**

Plate Number

Card Number  (Format:xxxx xxxx xxxx xxx)

Add
Query
Query All
Delete
Delete All

## [Registry Database]

1. Select **Enable Registry Database**.
2. Select a type of database for **Database Control** to specify the source of database.
  - ⊙ **AS Manager:** Select to allow the vehicle database to be transmitted from GV-ASManager and saved onto the memory card. To set up the connection with the GV-ASManager for database download, see *Chapter 8 GV-ASManager Connection*.
  - ⊙ **Standalone:** Select to activate the function of **Standalone Database**. You can manually register license plates on the camera. See *Standalone Database, Support White List only* below.

---

**Note:** When you activate **Standalone Database**, do not connect the camera to GV-ASManager.

---

3. Select one comparison type for **Registry Database Comparison** using the dropdown list. The detected license plate will trigger the output under the selected condition:
  - ⊙ **Complete (All Characters Match):** The detected license plate matches every character of a license plate in the database.

- ⊙ **Like (One Character Mismatch):** The detected license plate matches all except one character of a license plate in the database. The first and last characters of that license plate must be the same.
- ⊙ **Somewhat Like (Two Characters Mismatch):** The detected license plate matches all except two characters of a license plate in the database. The first and last characters of that license plate must be the same.

4. Click **Apply**.

**[Standalone Database, Support White List only]** You must select **Standalone Database** to activate this function.

- **Plate Number:** Type license plates and click **Add** to create your database. Click **Query/Query All** to search for certain/all license plates. Click **Delete/Delete All** to remove certain/all license plates.

To set the Recognition Engine, recognition conditions and recognition sensitivity, see 3.5.5.2 *LPR Detection*.

To open a gate when the detected license plate is recognized as a registered vehicle, see 3.5.2 *Output Settings*.

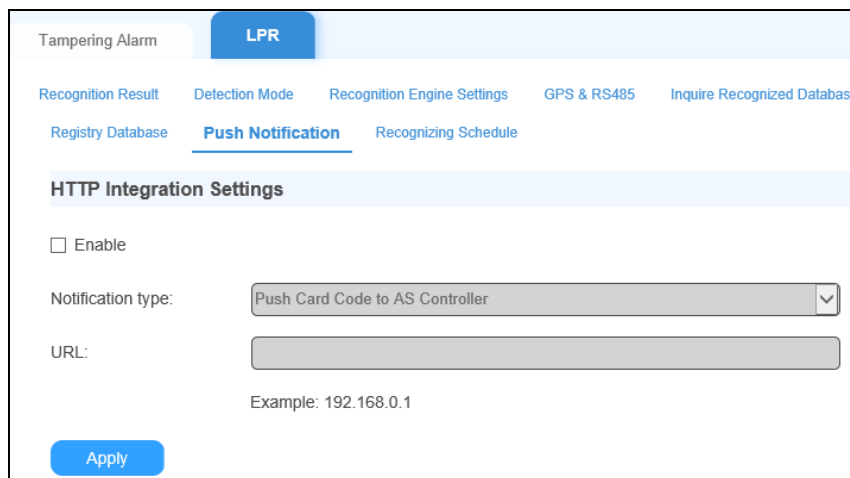
### 3.5.5.6 Push Notification

The **Push Notification** function allows users to send the captured license along with RFID tag data to a desired JSON server or Controllers via GV-FWC for license plate + RFID tag access management.

---

**Note:** For sending the captured license data along with RFID tag numbers, the camera must be connected to a GV-RU9003, see [1.6.2.2 UHF RFID Reader Connection](#).

---



The screenshot shows the 'LPR' configuration page with the 'Push Notification' tab selected. Under 'HTTP Integration Settings', there is an 'Enable' checkbox (unchecked), a 'Notification type' dropdown menu set to 'Push Card Code to AS Controller', and a 'URL' text input field. Below the URL field is an example: 'Example: 192.168.0.1'. An 'Apply' button is located at the bottom left of the settings area.

To set up LPR + RFID tag access management, follow the steps below:

- **Step 1: Connect to GV-RU9003 and Enable RS-485-B**  
See [1.6.2.2 UHF RFID Reader Connection](#) and [3.5.5.3 GPS & RS-485](#).
- **Step 2: Connect to GV-FWC via LAN**
  - A. On the Push Notification page, select **Enable**, select **Push Card Code to AS Controller** from the Notification type dropdown list.
  - B. Type the IP address of the GV-FWC in **URL**
- **Step 3: Connect the GV-FWC to GV-AS Controller via LAN or to 3<sup>rd</sup>-Party Controller via Wiegand**  
See [3.3 Receiving Access Card Data by Controller](#) in [GV-FWC Installation Guide](#).

#### Sending Access Data to JSON Server

To send access card data to a desired JSON server, select **HTTP – POST** from the Notification type dropdown list and type its URL along with its port value within **URL**.

### 3.5.5.7 Recognizing Schedules

Users can set a recognizing schedule for LPR to operate by.

Tampering Alarm | **LPR**

Recognition Result | Detection Mode | Recognition Engine Settings | GPS & RS485 | Inquire Recognized Database

Registry Database | Push Notification | Recognizing Schedule

In this section you can configure schedule time.

Span 1    Motion(stationary camera)    00 : 00 ~ 00 : 00

Span 2    Motion(stationary camera)    00 : 00 ~ 00 : 00

Span 3    Motion(stationary camera)    00 : 00 ~ 00 : 00

Weekend    Motion(stationary camera)     Saturday and Sunday  Only Sunday

Special Day    Motion(stationary camera)    (MM/DD)

01.     02.     03.     04.

05.     06.     07.     08.

09.     10.     11.     12.

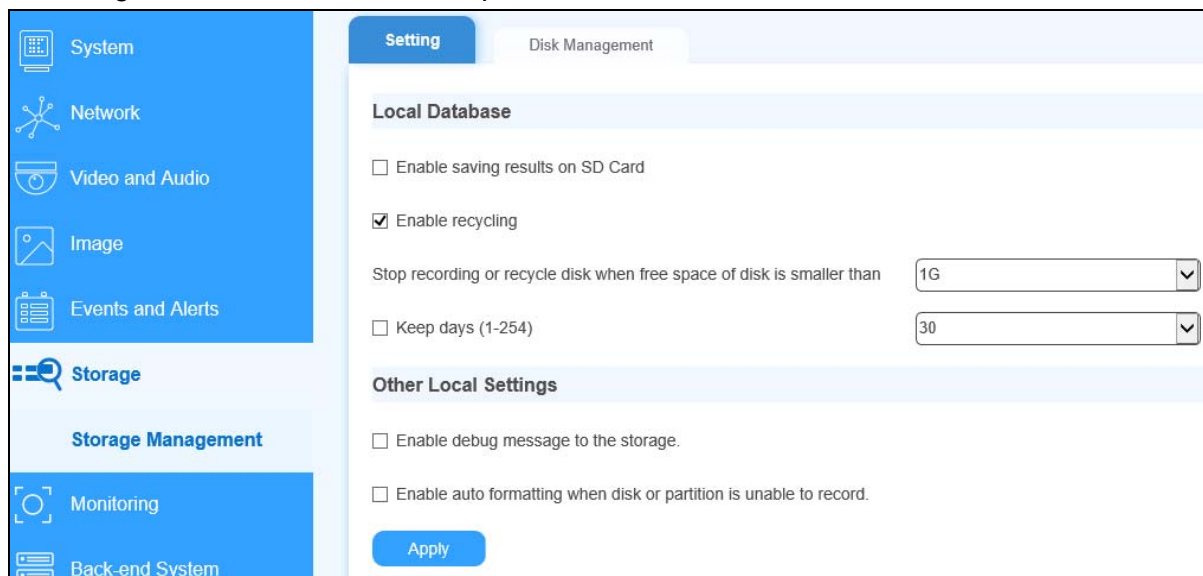
Select a method for license plate recognition from the dropdown list and define the recognition schedule for each.

For details of setting schedules, see *FTP Schedule, 3.2.3 FTP Settings*.

## 3.6 Storage

### 3.6.1 Storage Settings

You can store the recognition results or images to the inserted memory card on the camera. The images are stored in JPEG compressed formats.



#### [Local Database]

- **Enable saving results on a memory Card:** Enable this option to save the recognition results or images to the memory card.
- **Enable recycling:** If this option is checked, the system will overwrite the oldest stored files when the space of the memory card is lower than the specified space. If this option is not checked, the system will stop recording when the specified space is reached.
- **Keep days (1~254):** Specify the number of days to keep the files. 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.
- **Password:** Set a desired password for adjusting storage settings.

#### [Other Local Settings]

- **Enable debug message to the storage:** Debug message (see 3.1.2 *System Maintenance*) is deleted after reboot. Select this option to store log information to the memory card.

- Enable auto formatting when disk or partition is enabled to record:** Select this option for the camera to automatically format the memory card when an error occurs during saving recognition results or images.

### 3.6.2 Disk Management

The Disk Management page allows users to view the status of the memory card inserted, including the total and amount of space used, its Health Check Value and partition status, as well as remove or format the SD card.

Setting
Disk Management

**Disk Information**

Disk No.	Total Size	Used Size	Free space	Utilization	Health Check Value	Remove	Format
Disk11	29.131	28.118	1.012	96%	96	<input type="button" value="Remove"/>	<input type="button" value="Format"/>

If the Health Check Value of an SD card drops below 20, it is recommended to be replaced with a new one immediately.

**Partition Information**

Disk No.	Partition No.	Total Size	Used Size	Free space	Utilization	Status	Other
Disk11	1	29.131	28.118	1.012	96%	OK	<input type="button" value="Format"/>

( Unit: Gigabyte)

**[Partition Status]** The partition status of the SD card is displayed in the **Status** column.

Status	Description
Formatting	The memory card is being formatted.
Unknown	The camera cannot recognize the format of the storage device or the device cannot be found.
OK	Storage has been formatted and is ready to record.
Try Mount	The camera is attempting to connect to the storage device.
Error File System	There is a recording error and all recording data is inaccessible.
Read Only	The storage device cannot be written due to abnormal power disruption.
Repairing	The system is attempting to repair the recording data.

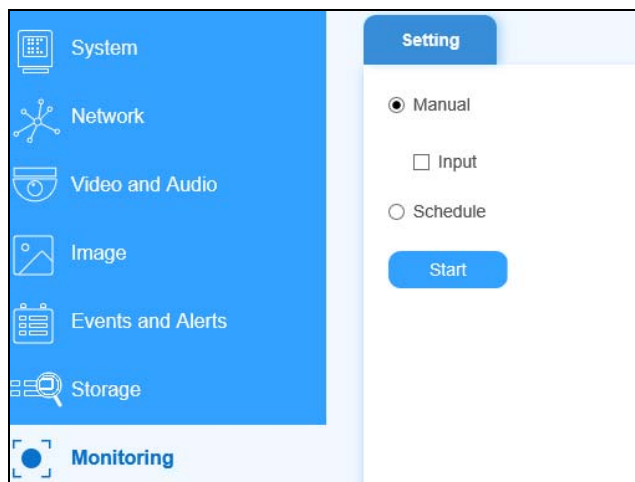
---

**Note:**

1. To prevent data loss, it is recommended to click **Remove** to stop all reading/writing activities of the memory card prior to removing it from the camera.
  2. 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 recorded.
- 

## 3.7 Monitoring

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



**[Manual]** Manually activates motion detection and I/O monitoring.

- **Input:** Select to manually start I/O monitoring. When the sensor input is triggered, its associated camera and output will be activated for alerting and sending video to Center V2.

**[Schedule]** The camera shall start motion detection and I/O monitoring according to the schedules set.



## 3.8 Back-end System

This section covers the GV-Software that can be directly connected by the camera through its Web interface, which includes GV-Center V2, GV-VSM and GV-Video Gateway / Recording Server.

### 3.8.1 Center V2

The central monitoring station Center V2 can be notified of LPR events by live videos and text alerts. Up to **two** Center V2 servers can be connected. For live monitoring through Center V2, you must already have a subscriber account on each of the Center V2 server.

---

**Note:** To notify the Center V2 Server upon LPR events, be sure to set up the LPR Settings. For details, see [3.5.5 LPR](#) and [6.1 Center V2](#).

---

Center V2
VSM
Video Gateway / Recording Server

In this section you can configure the connection to Center V2 and tasks to perform.  
To notify the Center V2 Server upon motions, be sure to set up the detection area on the Motion Detection page.

Connection 1 ▾

**Center V2 server**

Activate Link

Host name or IP Address:

Port number:

User Name:

Password:

Cease motion detection messages from  Camera

Cease input trigger message from  Select all  Input 1  Input 2

Enable schedule mode

Apply

**Recording Schedule Settings**

In this section you can configure schedule time.

Span 1  :  :  ~  :  Next Day

Span 2  :  :  ~  :  Next Day

Span 3  :  :  ~  :  Next Day

Weekend  Saturday and Sunday  Only Sunday

Apply

**Connection Status**

Status: Disconnected

1. To connect to GV-Center V2, select **Activate Link**.

2. **Host Name or IP Address:** Type the host name or IP address of Center V2.
3. **Port Number:** Match the port to **Port 2** on Center V2. Or keep the default value **5551**. For details, see *6.1 Center V2*.
4. **User Name:** Type a valid user name to log in to Center V2.
5. **Password:** Type a valid password to log in to Center V2.
6. Click **Apply**. The Connection Status should display “Connected” and the time of connection.
7. To establish connection to a second Center V2, select **2** from the **Connection** dropdown list and repeat the above steps.

Other optional settings:

- **Cease motion detection messages from:** Stops notifying Center V2 of motion detection.
- **Enable schedule mode:** Starts the monitoring through Center V2 based on the schedule you set in the **Select Schedule Time** section.

### 3.8.2 VSM (Vital Sign Monitor)

The central monitoring station VSM can be notified of a motion event by text alerts. Up to **two** Vital Sign Monitor servers can be connected. For live monitoring through VSM, you must already have a subscriber account on each of the VSM server.

---

**IMPORTANT:** To notify the Vital Sign Monitor upon LPR events, be sure to set up LPR settings. For details, see [3.5.5 LPR](#) and [6.2 Vital Sign Monitor](#).

---

Center V2
VSM
Video Gateway / Recording Server

In this section you can configure the connection to VSM Server and tasks to perform.  
To notify the VSM upon motions, be sure to set up the detection area on the Motion Detection page.

Connection 1 ▾

**Vital Sign Monitor Server**

Activate Link

Host name or IP Address:

Port number:

User Name:

Password:

Cease motion detection messages from  Camera

Cease input trigger message from  Select all  Input 1  Input 2

Enable schedule mode

Apply

**Recording Schedule Settings**

In this section you can configure schedule time.

Span 1  :  :  ~  :  Next Day

Span 2  :  :  ~  :  Next Day

Span 3  :  :  ~  :  Next Day

Weekend  Saturday and Sunday  Only Sunday

Apply

**Connection Status**

Status: Disconnected

1. To connect to GV-VSM, select **Activate Link**.
2. **Host Name or IP Address:** Type the host name or IP address of VSM.
3. **Port Number:** Match the port to **Port 2** on VSM or keep the default value **5609**. For details, see [6.2 Vital Sign Monitor](#).

4. **User Name:** Type a valid user name to log into VSM.
5. **Password:** Type a valid password to log into VSM.
6. Click **Apply**. The Connection Status should display “Connected” and connected time.
7. To establish connection to a second VSM, select **2** from the **Connection** dropdown list and repeat the above steps.

Other optional settings:

- **Cease motion detection messages from:** Stops notifying VSM of motion detection.
- **Enable schedule mode:** Starts the monitoring through VSM based on the schedule you set in the **Select Schedule Time** section.

### 3.8.3 GV-Video Gateway / GV-Recording Server

The GV-Video Gateway and GV-Recording Server are video streaming servers designed for large-scale video surveillance deployments. The GV-Video Gateway / GV-Recording Server (with recording capability) can receive up to 256 channels from various IP video devices, and distribute up to 600 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.

The camera can be connected with up to **two** GV-Video Gateway / GV-Recording Server. To send the video images to the GV-Video Gateway or GV-Recording Server, you must already have an account on each of the GV-Video Gateway / GV-Recording Server with the user name and password specified below.

Center V2 VSM **Video Gateway / Recording Server**

In this section you can configure the connection to Video Gateway / Recording Server.  
To notify the Video Gateway/Recording Server upon motions, be sure to set up the detection area on the Motion Detection page.

Connection: 1

**Video Gateway / Recording Server**

Activate Link:

Host name or IP Address:

Port number: 50000

User Name:

Password:

Enable schedule mode:

Apply

**Recording Schedule Settings**

In this section you can configure schedule time.

Span 1: 00:00 ~ 00:00 Next Day

Span 2: 00:00 ~ 00:00 Next Day

Span 3: 00:00 ~ 00:00 Next Day

Weekend:  Saturday and Sunday  Only Sunday

Apply

1. To connect to GV-Video Gateway / Recording Server, select **Activate Link**.
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 specified on GV-Video Gateway / GV-Recording Server. Or keep the default value **50000**.
4. **User Name:** Type a valid user name to log into GV-Video Gateway / GV-Recording Server.
5. **Password:** Type a valid password to log into GV-Video Gateway / GV-Recording Server.
6. Click **Apply**. The Connection Status should display “Connected” and connected time.
7. To establish connection to a second GV-Video Gateway / GV-Recording Server, select **2** from the **Connection** dropdown list and repeat the above steps.

Other optional settings:

- **Enable schedule mode:** Starts the monitoring through GV-Video Gateway / GV-Recording Server based on the schedule you set in the **Select Schedule Time** section.

## Chapter 4 Advanced Applications

This chapter introduces more advanced applications.

### 4.1 Upgrading System Firmware

GeoVision periodically updates the latest firmware to the company website. You can update your camera firmware, along with its recognition engine, through the Web interface or GV-IP Device Utility from the [website](#).

#### Important Notes before You Start

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

1. While the firmware is being updated, the power supply must not be interrupted.

---

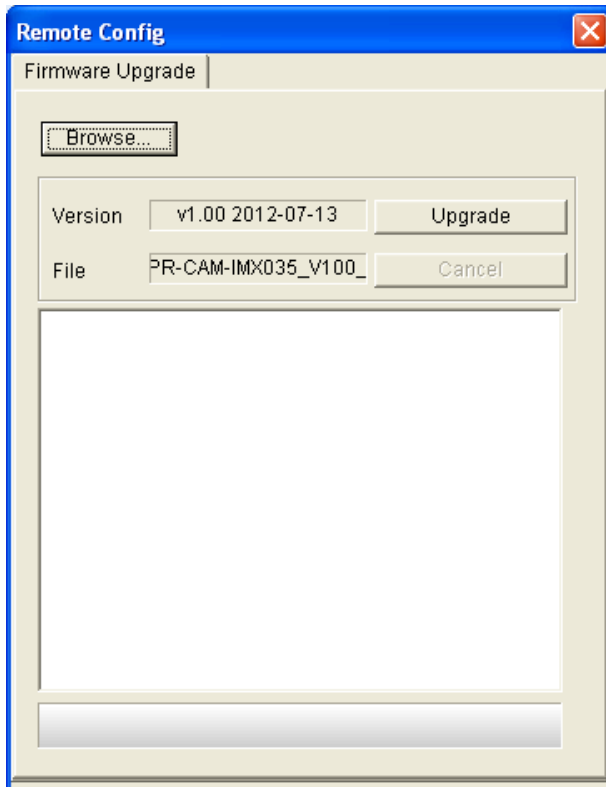
**WARNING:** The interruption of power supply during updating causes not only update failures but also damages to your camera. In this case, please contact your sales representative and send your device back to GeoVision for repair.

---

2. If you use GV-IP Device Utility for firmware upgrade, the computer used to upgrade firmware must be under the same network as the camera.
3. Stop monitoring the camera.
4. Stop all the remote connections including Center V2, VSM (Vital Sign Monitor), ViewLog Server and 3GPP/RTSP.
5. Stop the connection to GV-DVR / NVR / VMS.
6. If firmware upgrade fails, you will need to restore the camera to its default settings. For details, see *4.3 Restoring to Factory Default Settings*.

### 4.1.1 Using the Web Interface

1. In the Live View window, click **More Functions** (No. 10, 2.3 *Accessing Live View*) and select **Remote Config**. This dialog box appears.



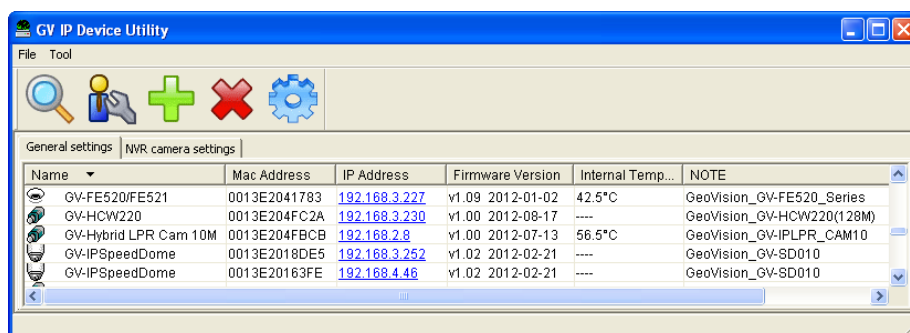
2. Click the **Browser** button to locate the firmware and/or recognition engine files (.img) saved at your local computer.
3. Click the **Upgrade** button to start upgrading.



### 4.1.2 Using the GV-IP Device Utility

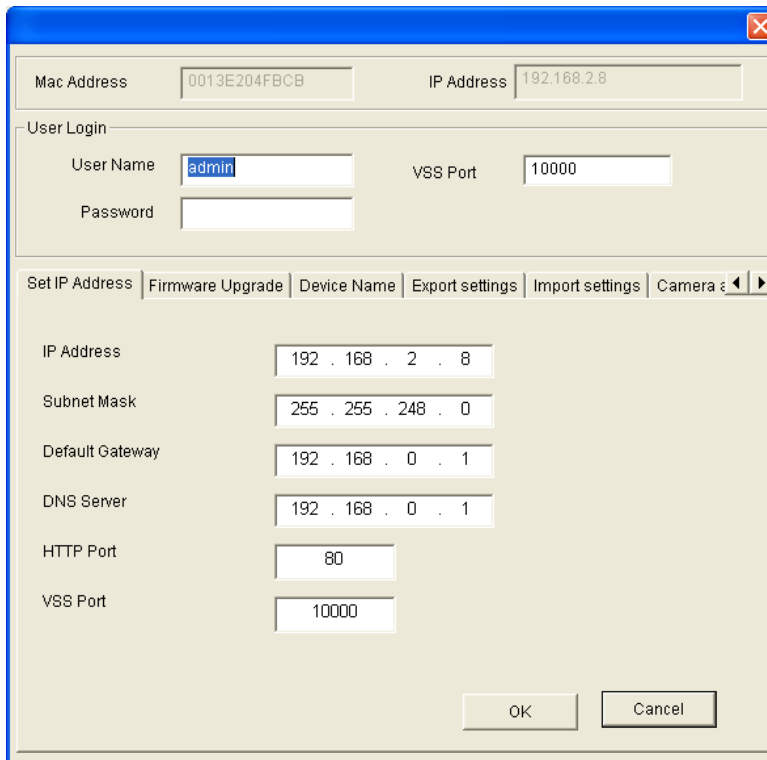
The GV-IP Device Utility provides a direct way to upgrade the firmware to multiple cameras. Note the computer used to upgrade firmware must be under the same network with the cameras.

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

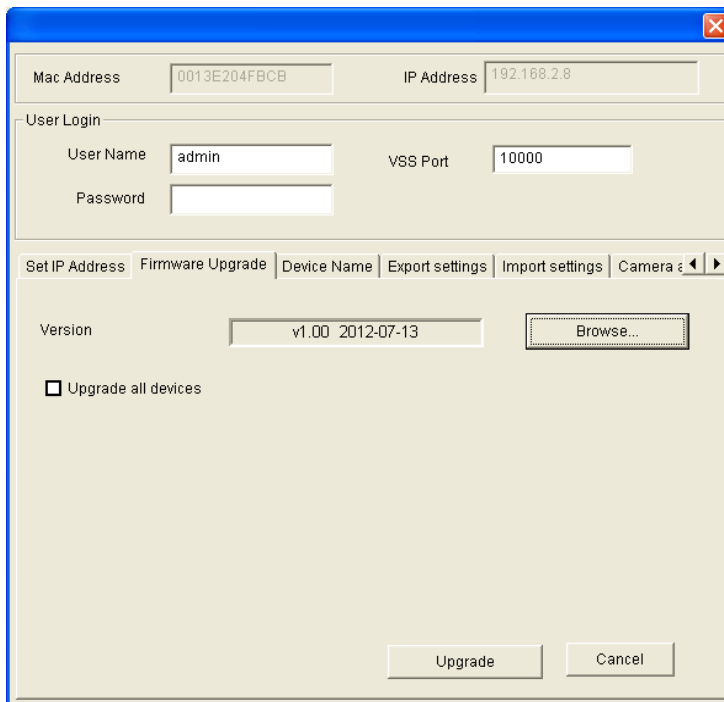


3. Click the **Search** button to locate the IP devices on the LAN or click the **New** button and assign the IP address to locate a camera on the network. Or highlight one IP device in the list and click the **Delete** button to remove it.

- Click on the IP address of the camera and select **Configure**. This dialog box appears.



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



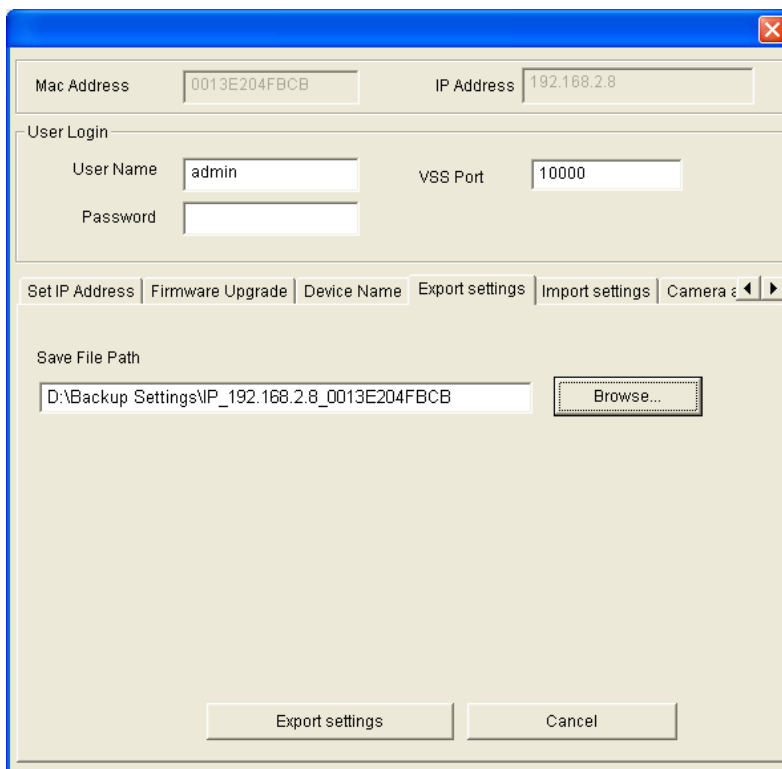
- Click the **Browse** button to locate the firmware and/or recognition engine files (.img) saved at your local computer.
- If you like to upgrade all the cameras in the list, check **Upgrade all devices**.
- Type **Password**, and click **Upgrade** to start the upgrade.

## 4.2 Backing Up and Restoring Settings

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

### To back up the settings

1. Run **GV IP Device Utility** and locate the desired camera. See Step 1 – 3 in *4.1.2 Using the GV-IP Device Utility*.
2. Double-click the camera in the list and select the **Export Settings** tab. This dialog box appears.



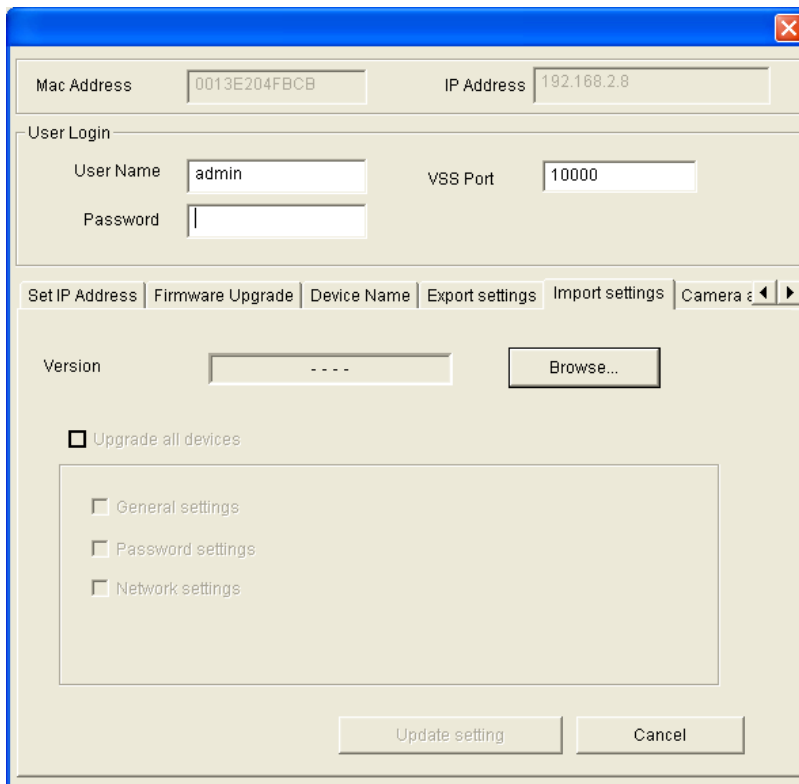
The screenshot shows a dialog box titled "GV IP Device Utility" with a blue header bar and a close button in the top right corner. The dialog is divided into several sections:

- Mac Address:** 0013E204FBCB
- IP Address:** 192.168.2.8
- User Login:**
  - User Name:** admin
  - Password:** (empty field)
  - VSS Port:** 10000
- Navigation Tabs:** Set IP Address | Firmware Upgrade | Device Name | **Export settings** | Import settings | Camera < >
- Save File Path:** D:\Backup Settings\IP\_192.168.2.8\_0013E204FBCB
- Buttons:** Browse... (next to the file path), Export settings, and Cancel.

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

## To restore the settings

1. Select the **Import Settings** tab.



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

## 4.3 Restoring to Factory Default Settings

To restore the factory default settings, you can use the camera's Web interface or operate directly on the camera.

### 4.3.1 Using the Web Interface

Follow the steps below to restore the factory default settings through the camera's Web interface.

1. Click **Setup > System > System Maintenance**.
2. Under **Reset to Default**, click **Load Default** to restore the camera to its factory default settings, while resetting its network settings or not.

### 4.3.2 Directly on the Camera

For GV-LPR2800-DL only, users can alternatively press the default button inside the camera.

1. Keep the power and network cables connected to the camera.
2. Loosen the camera's cover.
3. Press and hold the default button for 8 seconds.



4. Release the default button. When the process of loading default settings is completed, the camera reboots automatically.
5. Insert a new Silica Gel bag and fasten the camera's cover immediately. For details, see *Replacing Silica Gel Bag* in the respective camera section in Chapter 1.

## 4.4 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, 3.4.1 OSD & Text Overlay*.

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

### 4.4.1 Accessing AVI Files

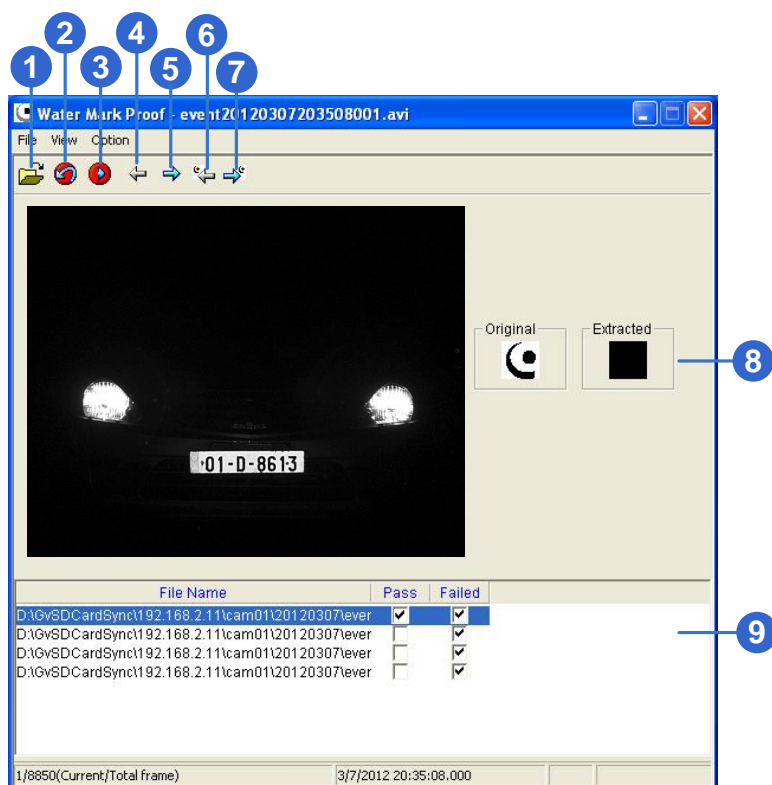
To verify watermark, access the recorded AVI files by one of the following methods:

1. Use the **File Save** function (No. 6, *2.3 Accessing Live View*) to start recording on the local computer.
2. Locate recorded files on the GV-DVR / NVR / VMS.

### 4.4.2 Running Watermark Proof

1. Go to the GV-DVR / NVR / VMS software folder and run WMPProof.exe. After installation, a **WMPProof** 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.

## 4.4.3 The Watermark Proof Window



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.
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.

## Chapter 5 DVR / NVR / VMS Configurations

The GV-IP LPR Camera can deliver live view images, date and time or even recognized plate numbers to the GV-DVR / NVR / VMS for security surveillance. The following is the integration specifications:

- Regarding the compatible GV-DVR / NVR / VMS versions for your camera, refer to *System Requirements* in Chapter 1 for respective cameras.
- The camera allows for up to **8** streams of connection.
- When a camera is connected to a Web browser or any other applications, it takes up **1** stream; when it is connected to GV-DVR / NVR, it takes up **2** streams. When GV-LPR2800-DL / LPR2811-DL is connected to GV-ASManager, it takes up **2** streams.

---

### Note:

1. By default, the camera is in dual streams and will take up 2 streams when connected to GV-DVR / NVR / VMS.
2. GV-DVR / NVR / VMS can turn out to be a license plate recognition system PC LPR when installed with LPR Plugin program and GV-LPR Capture Dongle.

- 
- The hardware compression and the “Pre-Recording Using RAM” feature cannot work on the videos from the camera. For details about the “Pre-Recording Using RAM” feature, see *System Configuration*, Chapter 1, *DVR User’s Manual*.



## 5.1 Setting up IP Cameras on GV-DVR / NVR

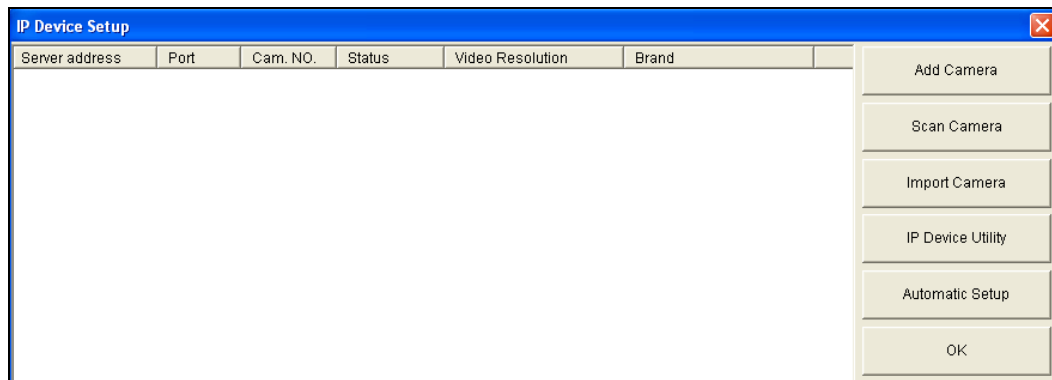
Follow the steps below to manually connect your camera to GV-DVR / NVR.

---

**Note:** The following instructions are based on V8.5.7.0 software and user interfaces.

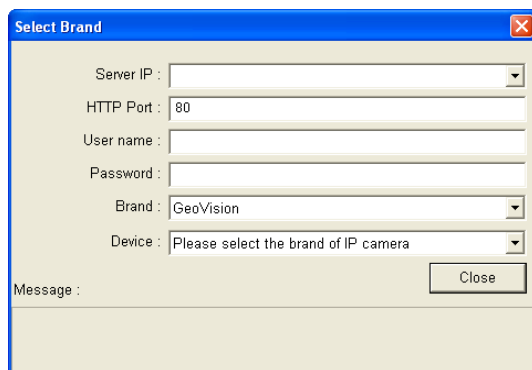
---

1. On the main screen of GV-DVR / NVR, click the **Configure** button, select **System Configure**, select **Camera Install** and click **IP Camera Install**. This dialog box appears.

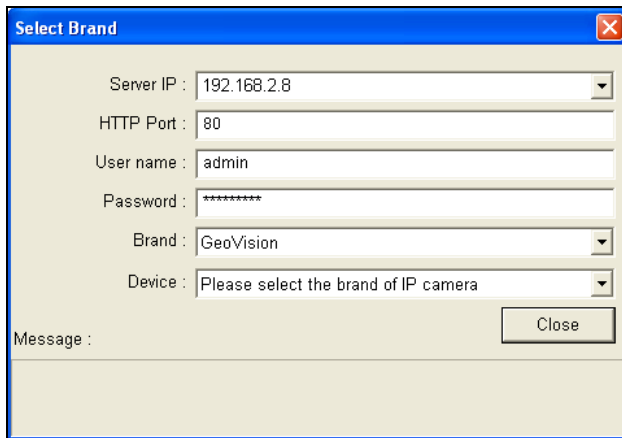


- To automatically set up an IP camera, click **Scan Camera** to detect any IP cameras on the same LAN.
- To manually set up an IP camera, click **Add Camera**.
- To import IP cameras from the GV-IP Device Utility, click **Import Camera**.
- To map IP devices through the GV-IP Device Utility program, click **IP Device Utility**.
- To add all IP cameras within the IP address range, click **Automatic Setup**.

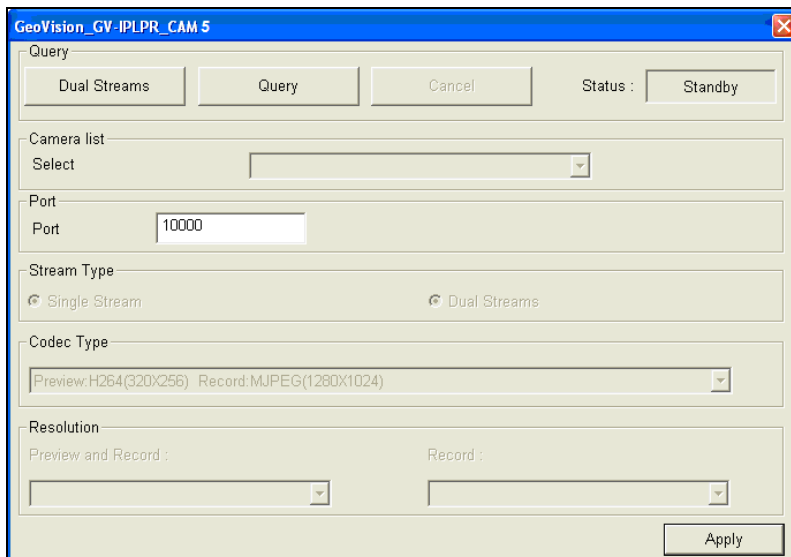
2. Click **Add Camera**. This dialog box appears.



3. Type the IP address, username and password of the camera. Modify the default HTTP port if necessary.

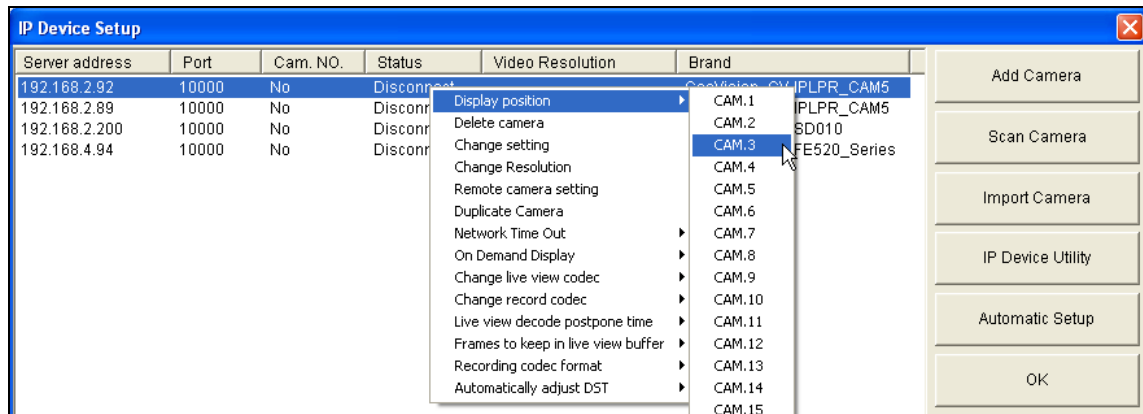


4. Select **GeoVision** from the Brand drop-down list and select your camera from the Device drop-down list. This dialog box appears.



- **Dual Streams:** Click this button to set the codec type to MJPEG in the main stream and to H.264 in the sub stream with the resolutions listed below.
  - **Port:** Modify the video streaming port number if necessary.
  - **Stream Number:** Click the **Query** button and select **Single Stream** or **Dual Streams**.
  - **Codec type:** The live view codec and resolution settings are displayed here.
  - **Resolution:** Select resolutions for preview and recording.
5. Click **Apply**. The camera is added to the list.

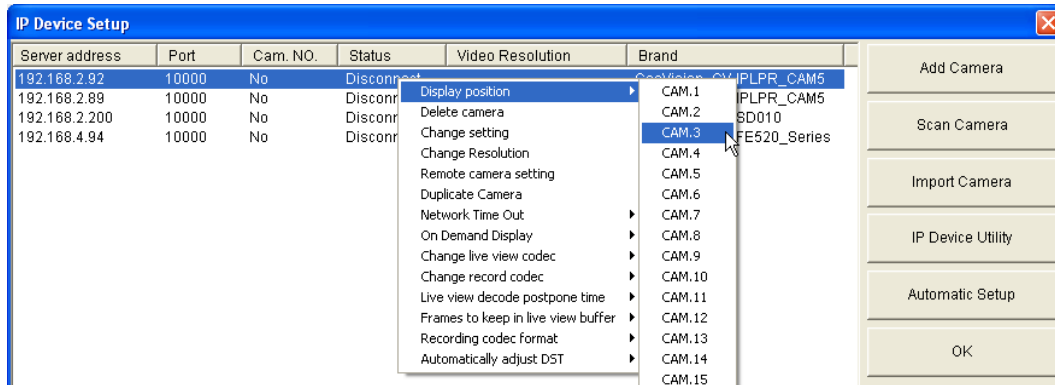
6. Click the listed camera, select **Display position** and select a channel number to map the camera to a channel on the GV-DVR / NVR.



7. The Status column now should display "Connected". Click **OK**. The dome view is displayed on the selected channel of GV-DVR / NVR.

## 5.1.1 Customizing Camera Settings

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






- **Change Setting:** Changes the IP address, port number, username and password of the camera. This function is only available when the camera is disconnected.
- **Change Resolution:** Changes the display ratio, live view resolution and record resolution.
- **Remote camera setting:** Accesses the configuration interface of the connected camera.
- **Network Time Out:** When network disconnection exceeds the specified time period, the camera status will be displayed as Connection Lost.
- **On Demand Display:** Enables automatic adjustment of live view resolution and produces good image quality without causing high CPU usage.
- **Change live view codec:** Changes the live view codec.
- **Change record codec:** Changes the recording codec.
- **Live view decode postpone time:** Specifies the number of milliseconds to postpone live view decoding. When network connection with the camera is unstable or when the time length between frames is not evenly distributed, postponing the live view decoding will make the video smoother.
- **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, H.264 codec.
- **Automatically Adjust DST:** If enabled, the time on the camera's Web interface will be synchronized with the time of the GV-DVR / NVR when DST period starts or ends on the GV-DVR / NVR.

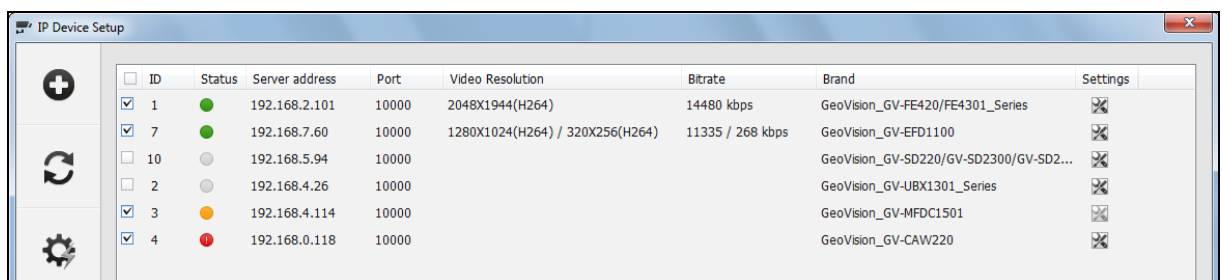
## 5.2 Setting up IP Cameras on GV-VMS

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

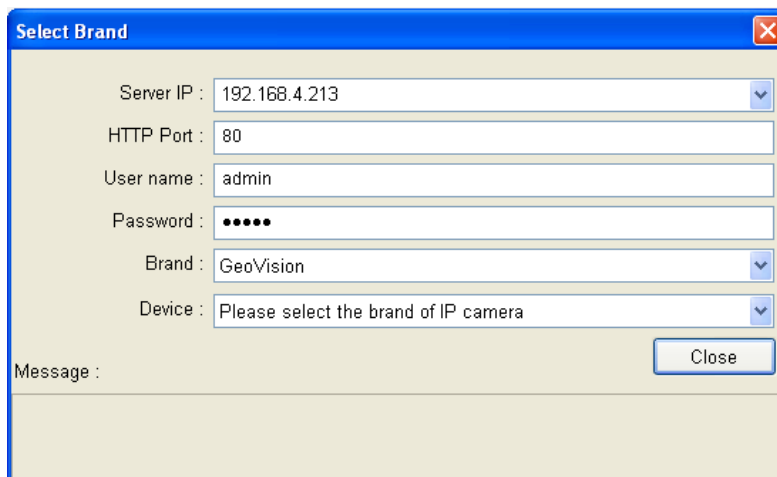
### Note:

1. The License Plate Recognition function is not supported on GV-VMS.
2. The following instructions are based on V14.10 software and user interfaces.

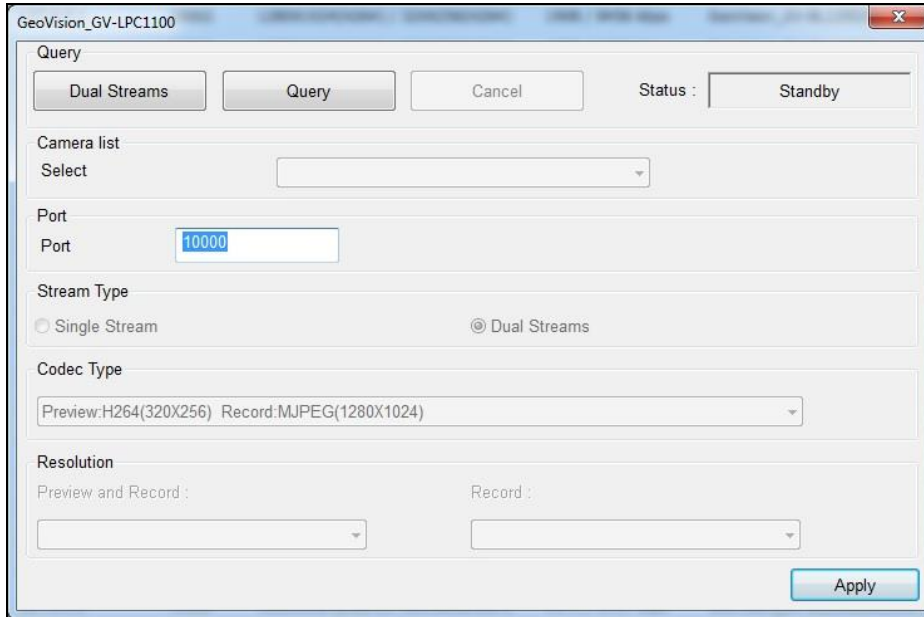
1. To access the IP Device Setup page, click **Home** , select **Toolbar** , click **Configure**  and select **Camera Install**. This dialog box appears.



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



3. Type the IP address, username and password of the IP camera. Modify the default HTTP port **80** if necessary.
4. Select a camera brand and model name from the **Brand** and **Device** dropdown lists respectively. This dialog box appears.









5. In the dialog box, configure the options which may vary depending on camera brands.

- **Dual Streams:** The camera 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.

5. Click **Apply** to add the IP camera to the IP Device List.

6. 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.

<input type="checkbox"/>	ID	Status	Server address	Port	Video Resolution	Bitrate	Brand	Setting
<input checked="" type="checkbox"/>	1		192.168.3.151	10000	1920X1080(H264) / 448X252(H264)	6902 / 51 kbps	GeoVision_GV-BX5200/BX5300_Series	
<input checked="" type="checkbox"/>	2		192.168.6.15	10000	1920X1080(H264) / 448X252(H264)	6854 / 137 kbps	GeoVision_GV-BX2200/BX2300_Series	
<input checked="" type="checkbox"/>	3		192.168.7.101	10000			GeoVision_GV-BL1500	

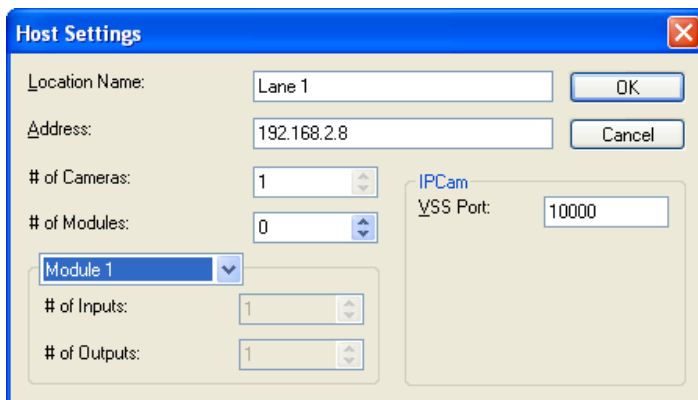
## 5.3 Remote Monitoring with E-Map

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

### Creating an E-Map for the 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 from 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 Video Server**.
5. Right-click the created New Host in the Host View, and select **Host Settings**. This dialog box appears.



6. Give the camera a location name, and type its IP address (or domain name). Keep the default VSS port **10000**, or modify it to match that of the camera.
7. Click **OK** to save the settings.
8. Expand the created host folder. Drag and drop the camera icon onto the imported E-Map.
9. Close the E-Map Editor. Click **Yes** when you are prompted to save the file.

For details on creating an E-Map file on the E-Map Server, see *E-Map Server*, Chapter 9, *DVR User's Manual*.

## Connecting to the Camera

Depending on where you save the created E-Map file (GV-DVR / NVR / VMS, 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 in the GV-DVR / NVR.

\*GV-DVR / NVR / VMS

1. To enable the remote access to the GV-DVR / NVR / VMS, 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 GV-DVR / NVR / VMS. The Single View page appears.
3. Select **Remote eMap**. The 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. The valid user name and password are required to log in the camera.

For details on the Remote E-Map functions, see *The Remote E-Map Window*, Chapter 9 or Chapter 8, respectively in *GV-DVR* or *GV-VMS User's Manual*.

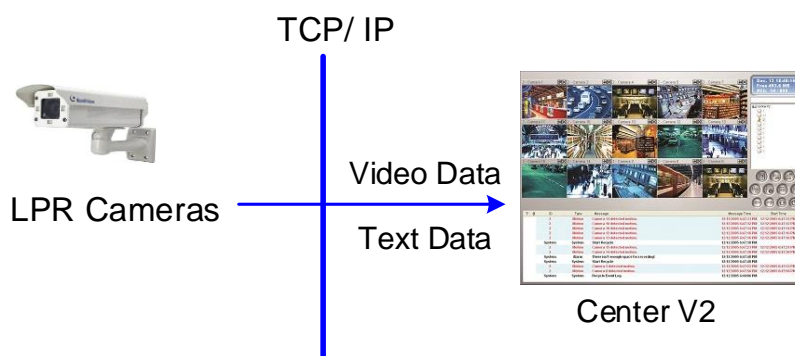


## Chapter 6 CMS Configurations

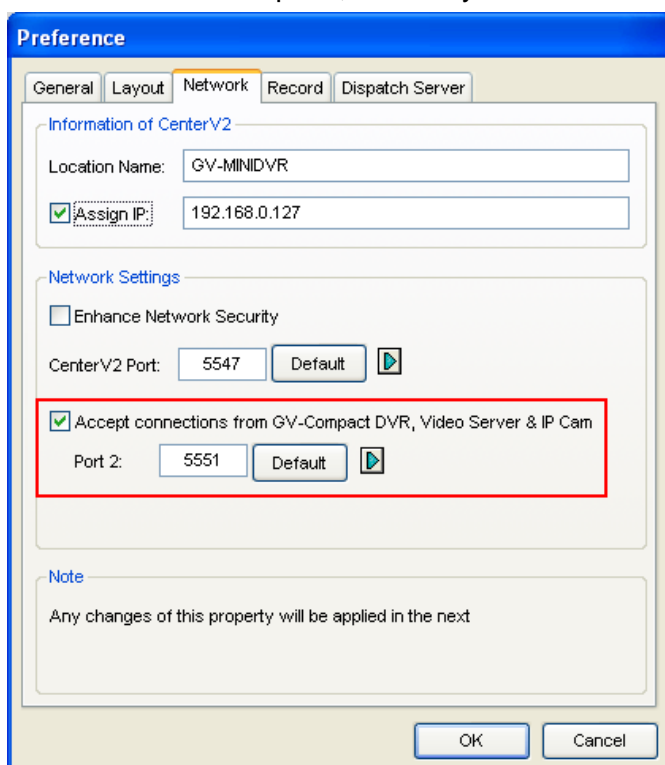
This section introduces the related settings to enable connecting to the camera in the central monitoring stations Center V2 and VSM (Vital Sign Monitor) and Dispatch Server.

### 6.1 Center V2

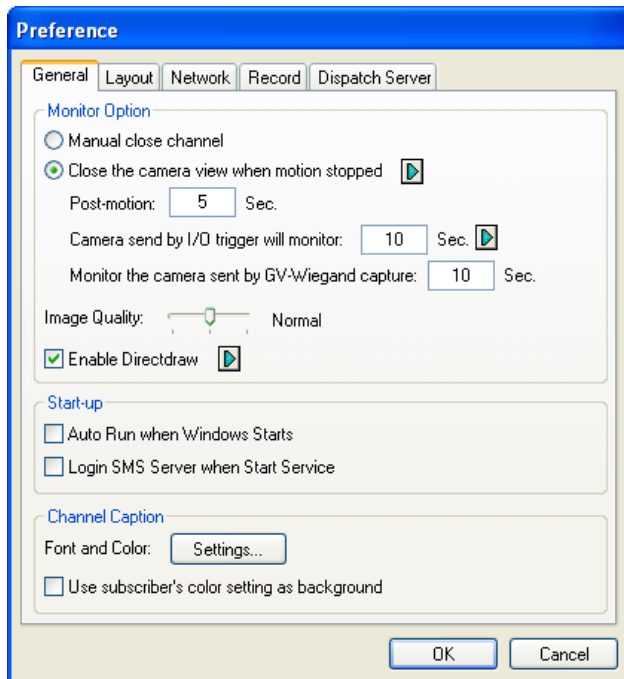
The Center V2 can monitor the camera.



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



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

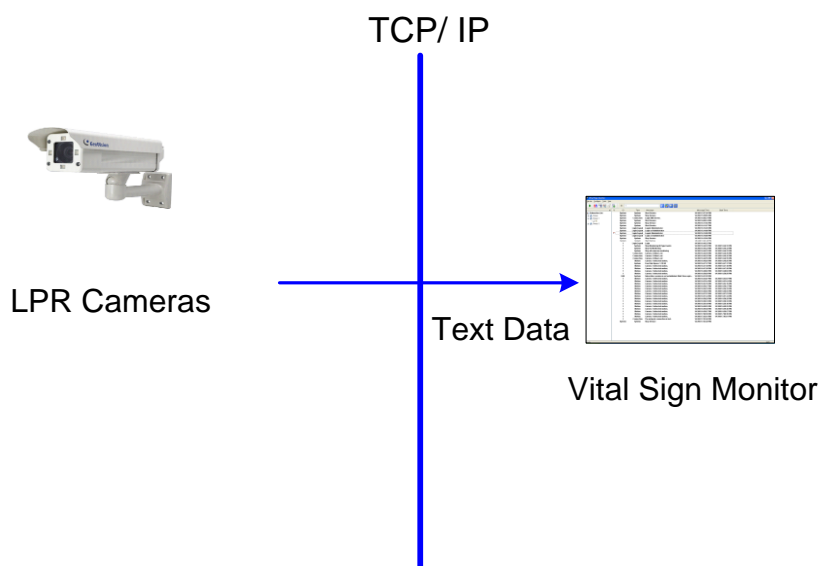


- **Manual close channel:** Closes the triggered camera view manually.
- **Close the camera view when motion stopped:** Closes the triggered camera view automatically when motion stops.
- **Post Motion:** Specify the duration of the camera view remaining on the monitoring window after motion stops.
- **Camera send by I/O trigger will monitor:** This feature is functional for cameras with I/O function only.

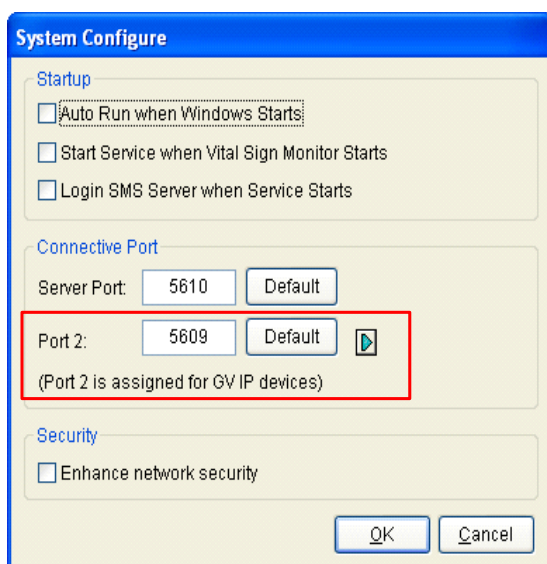
For further information on how to manage the received video from the camera, see *GV-CMS Series User's manual*.

## 6.2 Vital Sign Monitor

The Vital Sign Monitor can monitor the camera.



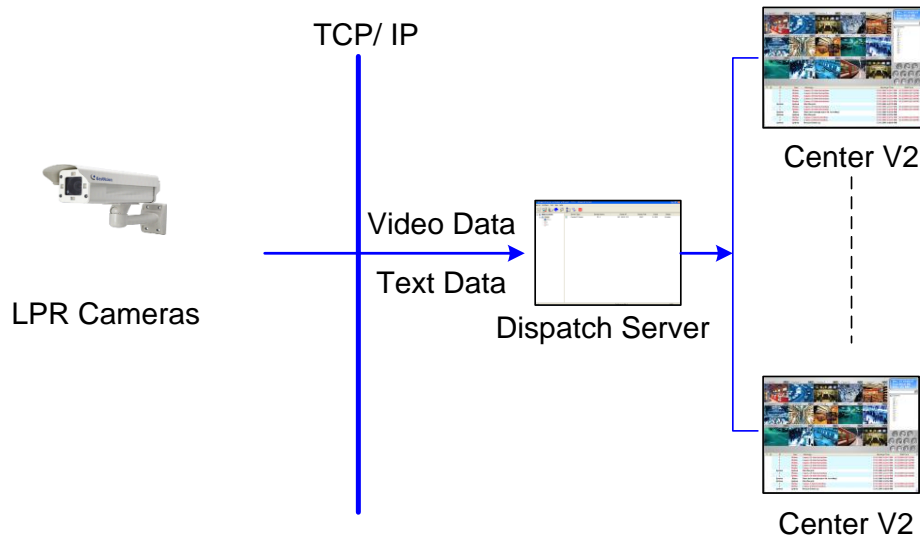
- To set the appropriate port connecting to the camera, click **Configure** on the window menu, and select **System Configure** to display this dialog box. In the Connective Port field, keep the default value **5609** for the Port 2 option, or modify it to match the VSM port on the camera.



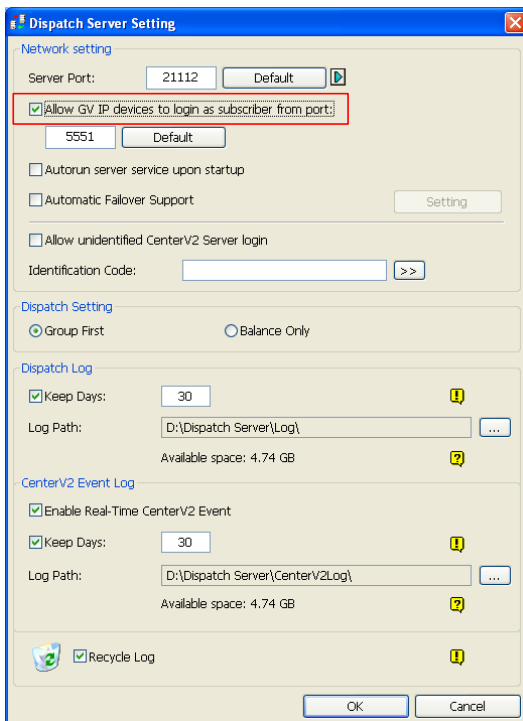
For further information on how to manage the received video from the camera, see *GV-CMS Series User's manual*.

## 6.3 Dispatch Server

The Dispatch Server can manage the camera and distribute them to the Center V2.



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



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

## Chapter 7 Smart Device Connection

You can access the live view 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 our [website](#):

## Chapter 8 GV-ASManager Connection

GV-IP LPR-DL camera can recognize license plates detected in the video source, and send the LPR results to GV-ASManager. Access can be granted when the detected license plate numbers match the vehicles registered in GV-ASManager's database. Before setting up GV-IP LPR-DL camera on GV-ASManager, see *4.3.10 Registry Database* to enable the Registry Database for data comparison.

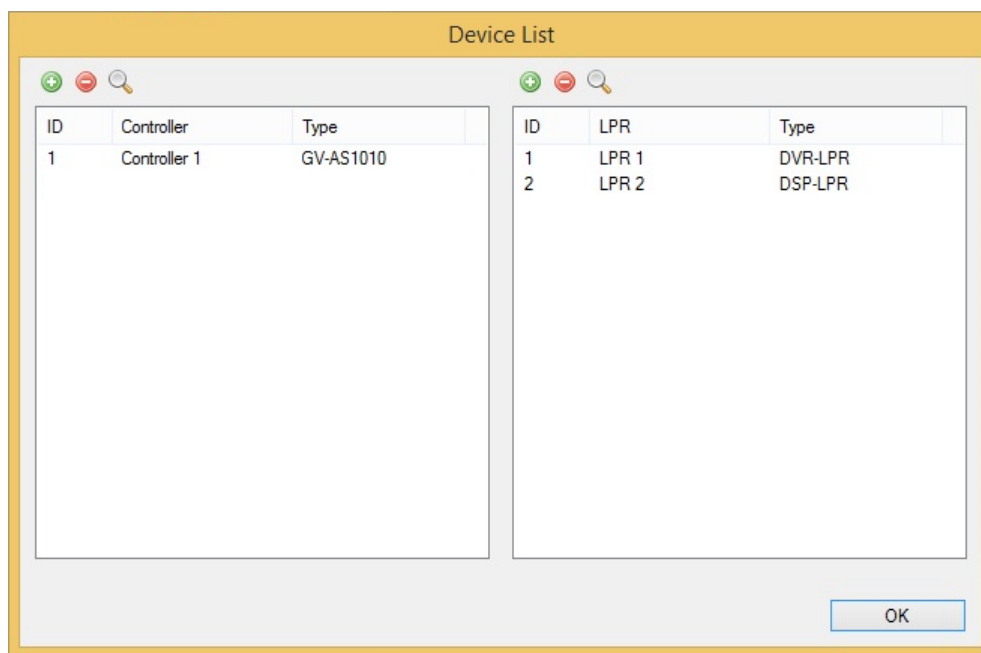
---

**Note:** GV-IP LPR-DL camera is only compatible with GV-ASManager V5.3.1 or later.


---

Follow the steps below to add the camera to GV-ASManager.

1. On the menu bar, click **Setup** and select **Devices**. This dialog box appears.

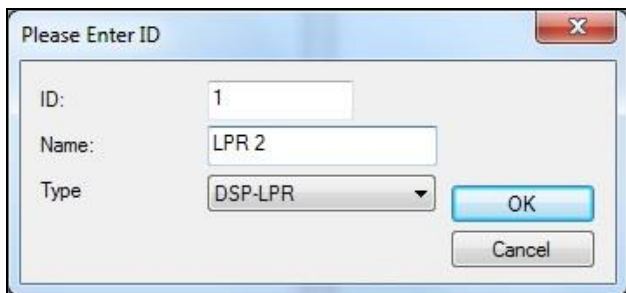


---

**Note:** You can also click the **Search** button  to search for the camera detected under the same LAN.

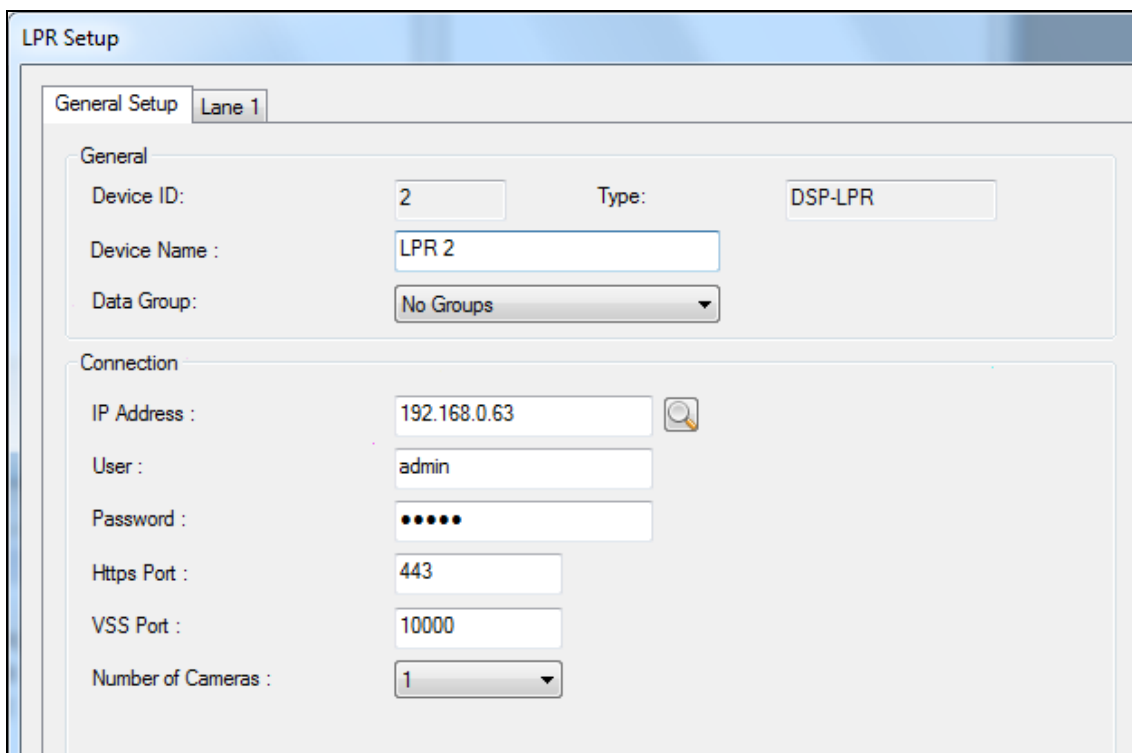
---

2. On the right pane for LPR, click the **Add** button . This dialog box appears.




A dialog box titled "Please Enter ID" with a close button (X) in the top right corner. It contains three input fields: "ID:" with the value "1", "Name:" with the value "LPR 2", and "Type:" with a dropdown menu showing "DSP-LPR". There are "OK" and "Cancel" buttons at the bottom right.

3. Type an **ID** number and **Name** for the LPR.
4. Use the drop-down list to select **DSP-LPR**.
5. Click **OK**. The LPR Setup page appears.



The "LPR Setup" dialog box is shown with the "General Setup" tab selected. It has a sub-tab "Lane 1". The "General" section contains: "Device ID:" (2), "Type:" (DSP-LPR), "Device Name:" (LPR 2), and "Data Group:" (No Groups). The "Connection" section contains: "IP Address:" (192.168.0.63), "User:" (admin), "Password:" (masked with dots), "Https Port:" (443), "VSS Port:" (10000), and "Number of Cameras:" (1).

6. Assign the camera to a **Data Group** if needed or select **No Groups** to disable the data group function. You can then allow or forbid a user to read / write / execute the functions assigned under the data group. Refer to *8.1 Setting Up System User*, Chapter 8 in *GV-ASManager User Manual* for more details.
7. Under Connection, type the **IP Address**, **User** name and **Password** of the camera. You can also click the **Search** button  to search for the camera detected in the same LAN.
8. You can modify the following settings if necessary.
  - **Https Port:** The default Https port is 443.
  - **VSS Port:** The default VSS port is 10000.

For the details on connecting the camera to GV-ASManager, see *13.3.2 Step 2: Adding Standalone LPR to GV-ASManager* and *13.3.3 Step 3: Configuring a Channel*, Chapter 13 in [GV-ASManager's User Manual](#).

For details on creating a vehicle database, see *13.4 Adding Vehicles*, Chapter 13 in [GV-ASManager's User Manual](#).



## Appendix

### A. The CGI Command

You can obtain a snapshot of the live view or access the User Account Web interface simply by executing CGI commands. Follow the details below:

IP address: 192.168.2.11

Username: admin

Password: admin

Desired Stream: 1

- To obtain a snapshot of 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 settings on the Web interface, type the following into your Web browser:

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

## B. Settings for Internet Explorer 8 or later

If you use Internet Explorer 8 or later, 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**.

