

GV-VMS

User's Manual V14.10





© 2014 GeoVision, Inc. All rights reserved.

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

Every effort has been made to ensure that the information in this manual is accurate.

GeoVision, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

GeoVision, Inc.

9F, No. 246, Sec. 1, Neihu Rd.,

Neihu District, Taipei, Taiwan

Tel: +886-2-8797-8377

Fax: +886-2-8797-8335

<http://www.geovision.com.tw>

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

December 2014

Important Notes

GPU Decoding Specifications

GPU (Graphics Processing Unit) decoding can lower the CPU loading and increase the total frame rate supported by a GV-VMS. GPU decoding only supports the following software and hardware specifications in GV-VMS:

Software Specifications

| | | Sandy Bridge | Ivy Bridge / Haswell |
|------------------|--------|---|----------------------------------|
| Operating System | 64-Bit | Windows 7 / 8 / 8.1 / Server 2008 R2 / Server 2012 R2 | |
| Resolution | | 1 MP / 2 MP | 1 MP / 2 MP / 3 MP / 4 MP / 5 MP |
| Codec | | H.264 | |

Hardware Specifications

| | |
|--|--|
| Motherboard | Intel chipset with onboard VGA Ex: Intel® Q87, Q85, B85, Z87, H87, H81, Q77, Q75, Z77, Z75, H77, B75, Q67, H67, H61, Q65, B65, Z68 Express Chipset. |
| Note: If you want to use an external VGA card, it is required to connect a monitor to the onboard VGA to activate GPU decoding. | |

Multi-Channel Playback Specifications

Multi-channel playback in ViewLog has been enhanced to improve the smoothness of the video by producing higher frame rate. However, playing back multiple channels at high resolution can increase the CPU loading especially if the GV-VMS is processing other tasks simultaneously. As a result of the high CPU loading, dropped frames may sometimes occur in recorded video when playing back multiple megapixel channels.

To avoid the problem, **it is recommended to play back megapixel video in single view.**

Contents

1

Configuring Main System 3

| | | |
|------------|---|-----------|
| 1.1 | Installing the GV-VMS..... | 3 |
| 1.1.1 | Dongle | 3 |
| 1.1.2 | Options | 4 |
| 1.1.3 | Minimum System Requirements | 5 |
| 1.1.4 | Minimum Network Requirements | 5 |
| 1.1.5 | Installing GV-VMS | 6 |
| 1.1.6 | Uninstalling and Upgrading GV-VMS..... | 8 |
| 1.2 | Getting Started | 9 |
| 1.2.1 | Main Screen | 10 |
| 1.2.2 | Adding Cameras..... | 12 |
| 1.2.3 | Accessing Live View..... | 14 |
| 1.2.4 | Enabling the Recording | 15 |
| 1.2.5 | Playing Back Video | 16 |
| 1.3 | Recording Settings..... | 17 |
| 1.3.1 | Setting Global Recording Settings for All Cameras | 18 |
| 1.3.2 | Setting Recording Settings for Individual Cameras | 20 |
| 1.3.3 | Setting Up the Video Storage Location | 21 |
| 1.3.4 | Setting Up Motion Detection | 23 |
| 1.4 | Live View and Layouts | 26 |
| 1.4.1 | Utilizing Live View Functions..... | 26 |
| 1.4.2 | Arranging Live View Layouts..... | 29 |
| 1.4.3 | Setting a Zoom Window | 31 |
| 1.4.4 | Setting a Scan Window | 33 |
| 1.4.6 | Setting Focus View..... | 35 |
| 1.5 | Start Monitoring | 36 |
| 1.6 | System Configuration | 38 |
| 1.6.1 | Configuring General Setting | 38 |
| 1.6.2 | Customizing Startup Settings | 40 |
| 1.6.3 | Customizing Display Position and Panel Resolution | 42 |
| 1.6.4 | Setting Up Email Notification..... | 43 |
| 1.6.5 | System Idle Protection | 46 |

| | | |
|-------------|--|-----------|
| 1.6.6 | Configuring Fast Key Lock | 48 |
| 1.7 | Account and Password | 49 |
| 1.7.1 | Creating a New Account..... | 50 |
| 1.7.2 | Configuring Account Settings | 51 |
| 1.7.3 | Changing or Retrieving Password at Login..... | 53 |
| 1.7.4 | Preventing Unauthorized System Termination..... | 54 |
| 1.7.5 | Setting a Startup Auto Login User..... | 55 |
| 1.8 | Schedule..... | 56 |
| 1.8.1 | Creating a Schedule with Setup Wizard..... | 57 |
| 1.8.2 | Creating a Schedule Manually | 60 |
| 1.8.3 | Exporting and Importing Schedule Settings | 61 |
| 1.9 | System Log | 62 |
| 1.9.1 | Setting System Log | 62 |
| 1.9.2 | Viewing System Log..... | 64 |
| 1.10 | Other Functions | 66 |
| 1.10.1 | Setting Live View Pop-Up Video | 66 |
| 1.10.2 | Adjusting to Daylight Saving Time | 67 |
| 1.10.3 | Setting Network Failure Detection..... | 69 |
| 1.11 | PTZ Camera | 70 |
| 1.11.1 | Accessing PTZ Control Panel and Auto Functions | 71 |
| 1.11.2 | Setting PTZ Idle Protection and Advanced Functions | 73 |

2

IP Camera Setup76

| | | |
|------------|--|-----------|
| 2.1 | Adding IP Cameras..... | 76 |
| 2.1.1 | Adding Cameras Manually | 78 |
| 2.1.2 | Scanning Camera..... | 81 |
| 2.1.3 | Mapping GV-IP Cameras Using GV-IP Device Utility | 82 |
| 2.2 | Configuring Individual IP Cameras..... | 84 |
| 2.2.1 | Configuring Video Setting..... | 84 |
| 2.2.2 | Configuring Audio Setting..... | 87 |
| 2.2.3 | Configuring General Setting | 88 |
| 2.3 | Connection through RTSP, ONVIF & PSIA | 90 |
| 2.4 | On Demand Display..... | 93 |

3

Video Analysis97

| | |
|---|------------|
| 3.1 Object Counting and Intrusion Alarm..... | 97 |
| 3.1.1 Object Counting..... | 97 |
| 3.1.2 Intrusion Alarm | 101 |
| 3.2 Object Index | 106 |
| 3.2.1 Setting Object Index | 106 |
| 3.2.2 Viewing Object Index..... | 109 |
| 3.2.3 Searching Object Index | 110 |
| 3.3 Automatic Video Snapshots | 112 |
| 3.3.1 Setting Video Snapshots | 112 |
| 3.3.2 Searching Video Snapshots | 115 |
| 3.4 Face Detection | 117 |
| 3.4.1 Setting Face Detection | 117 |
| 3.4.2 Searching Face Detection Snapshots..... | 119 |
| 3.5 Face Count | 120 |
| 3.5.1 Installing the Camera | 120 |
| 3.5.2 Setting Face Count..... | 121 |
| 3.6 Privacy Mask Protection | 125 |
| 3.6.1 Setting a Privacy Mask..... | 125 |
| 3.6.2 Granting Access Privileges to Recoverable Areas | 127 |
| 3.7 Panorama View | 128 |
| 3.7.1 The Main Window..... | 128 |
| 3.7.2 Stitching a Panorama View with Overlapping Areas..... | 130 |
| 3.7.3 Easy Mode with No Overlapping Area | 133 |
| 3.7.4 Accessing a Panorama View | 136 |
| 3.8 Video Defogging | 137 |
| 3.9 Video Stabilization | 139 |
| 3.10 Wide Angle Lens Dewarping | 141 |
| 3.11 Advanced Motion Detection | 143 |
| 3.12 Crowd Detection | 146 |
| 3.13 Advanced Scene Change Detection | 149 |
| 3.14 Advanced Unattended Object Detection | 152 |
| 3.15 Advanced Missing Object Detection | 155 |
| 3.16 Text Overlay | 158 |

| | | |
|-------------|---|------------|
| 3.17 | Fisheye View | 160 |
| 3.17.1 | Setting Up a GV-Fisheye Camera..... | 161 |
| 3.17.2 | Setting Up a Third-Party Fisheye Camera | 164 |
| 3.17.3 | Object Tracking | 166 |
| 3.18 | Specifications | 173 |

4

Video Playback 175

| | | |
|------------|---|------------|
| 4.1 | Playing Back on ViewLog | 176 |
| 4.1.1 | ViewLog Control Panel..... | 178 |
| 4.1.2 | Adjusting the Camera View | 181 |
| 4.1.3 | Searching a Video Event..... | 182 |
| 4.1.4 | Merging and Exporting Video | 183 |
| 4.1.5 | Saving Images..... | 186 |
| 4.1.6 | Printing Images | 187 |
| 4.1.7 | Adjusting Distorted Views..... | 188 |
| 4.2 | Object Search..... | 190 |
| 4.3 | Advanced Log Browser | 193 |
| 4.3.1 | Filter Settings | 195 |
| 4.4 | Remote ViewLog Service | 196 |
| 4.4.1 | Retrieving Recordings from GV-VMS | 196 |
| 4.4.2 | Retrieving Images of Object Index | 198 |
| 4.4.3 | Resuming Backup | 199 |
| 4.5 | Single Player | 200 |
| 4.5.1 | Single Player Window | 200 |
| 4.6 | Specifications | 202 |

5

Backup, Deletion and Repair 204

| | | |
|------------|--|------------|
| 5.1 | Backing Up Log Data..... | 204 |
| 5.2 | Backing Up Recorded Files | 206 |
| 5.3 | Deleting Recorded Files..... | 209 |

| | | |
|-----|-------------------------------------|-----|
| 5.4 | Repairing Damaged File Paths | 211 |
| 5.5 | Repairing Damaged Video Files | 213 |

6

I/O Applications 216

| | | |
|-------|---|-----|
| 6.1 | Setting I/O Devices | 217 |
| 6.1.1 | Adding I/O Devices..... | 218 |
| 6.1.2 | Setting the Input and Output Devices | 219 |
| 6.1.3 | Latch Trigger | 221 |
| 6.1.4 | Keeping Last Toggle Status | 223 |
| 6.2 | Advanced I/O Applications | 225 |
| 6.2.1 | Setting Up Actions Upon Input Trigger..... | 226 |
| 6.2.2 | Moving PTZ Camera to Preset Points upon Input Trigger | 227 |
| 6.2.3 | Setting Momentary and Maintained Modes..... | 228 |
| 6.2.4 | Deactivating Alarm and Alert upon Input Trigger | 229 |
| 6.2.5 | Other I/O Application Functions | 230 |
| 6.3 | I/O Devices in Content List | 231 |
| 6.4 | Visual Automation | 232 |

7

Remote Viewing 236

| | | |
|-------|--|-----|
| 7.1 | Remote Viewing Using a Web Browser | 237 |
| 7.2 | WebCam Server Settings | 240 |
| 7.2.1 | General Settings..... | 240 |
| 7.2.2 | Server Settings..... | 241 |
| 7.2.3 | Video Settings | 242 |
| 7.2.4 | Audio Settings | 243 |
| 7.2.5 | JPG Settings | 244 |
| 7.2.5 | JPG Settings | 244 |
| 7.2.6 | UPnP Settings | 245 |
| 7.2.7 | Network Port Information..... | 246 |
| 7.3 | Single View Viewer | 247 |
| 7.3.1 | Adjusting Video Quality and Recording Videos | 249 |

| | | |
|-------------|---|------------|
| 7.3.2 | Control Panel..... | 250 |
| 7.3.3 | Configuring Single View Viewer Options..... | 251 |
| 7.3.4 | PTZ Control Panel..... | 256 |
| 7.3.8 | Visual PTZ Control | 257 |
| 7.3.5 | I/O Control | 258 |
| 7.3.6 | Visual Automation | 259 |
| 7.3.7 | Picture-in-Picture View | 260 |
| 7.3.8 | Picture-and-Picture View..... | 261 |
| 7.4 | 2-Window Viewer | 262 |
| 7.5 | Multi-Window Viewer..... | 263 |
| 7.6 | JPEG Image Viewer | 264 |
| 7.7 | Playing Back Events..... | 265 |
| 7.7.1 | Event List Query..... | 265 |
| 7.7.2 | Remote Playback | 267 |
| 7.8 | Remote ViewLog..... | 268 |
| 7.9 | Download Center | 269 |
| 7.10 | Mobile Phone Applications..... | 270 |
| 7.10.1 | Activating Mobile Functions on GV-VMS | 270 |
| 7.10.2 | Installing GV-Eye..... | 271 |
| 7.10.3 | Connecting to GV-VMS..... | 272 |
| 7.11 | Web Browsers on Smartphones | 274 |

8

E-Map Application 277

| | | |
|------------|--|------------|
| 8.1 | The E-Map Editor | 277 |
| 8.1.1 | The E-Map Editor Window | 278 |
| 8.1.2 | Creating an E-Map | 279 |
| 8.1.3 | Creating an E-Map for a Remote Host..... | 284 |
| 8.2 | Starting E-Map..... | 285 |
| 8.2.1 | Setting Up the Pop-up Map | 287 |
| 8.3 | Remotely Accessing E-Map..... | 289 |
| 8.3.1 | The Remote E-Map Window | 290 |
| 8.3.2 | Accessing E-Maps of Multiple Hosts..... | 292 |
| 8.3.3 | Configuring the Remote E-Map..... | 293 |
| 8.3.4 | Viewing Event List and Playing Back Videos | 295 |
| 8.4 | E-Map Server..... | 296 |

| | | |
|-------|----------------------------------|-----|
| 8.4.1 | Installing E-Map Server | 296 |
| 8.4.2 | The E-Map Server Window | 297 |
| 8.4.3 | Setting up E-Map Server | 298 |
| 8.4.4 | Connecting to E-Map Server | 298 |

9

Useful Utilities 301

| | | |
|------------|--|------------|
| 9.1 | Dynamic DNS | 301 |
| 9.1.1 | Running Dynamic DNS | 302 |
| 9.1.2 | Registering Domain Name with DDNS | 303 |
| 9.1.3 | Starting Dynamic DNS | 305 |
| 9.2 | Watermark Viewer..... | 307 |
| 9.2.1 | Activating Watermark Protection..... | 307 |
| 9.2.2 | Running the Watermark Proof..... | 308 |
| 9.2.3 | The Main Window..... | 309 |
| 9.3 | Windows Lockup | 310 |
| 9.3.1 | The GV-Desktop Screen | 310 |
| 9.3.2 | GV-Desktop Features..... | 311 |
| 9.3.3 | Token File for Safe Mode..... | 314 |
| 9.4 | Authentication Server | 315 |
| 9.4.1 | Installing the Server..... | 315 |
| 9.4.2 | The Main Window..... | 316 |
| 9.4.3 | Creating Clients..... | 318 |
| 9.4.4 | Creating User Accounts | 319 |
| 9.4.5 | Importing Groups and Users from Active Directory | 323 |
| 9.4.6 | Starting the Server | 325 |
| 9.4.7 | Connecting GV-VMS to the Server | 327 |
| 9.4.8 | Remote Access from Control Center and Remote E-Map | 330 |
| 9.5 | Fast Backup and Restore | 333 |
| 9.5.1 | Running the FBR Program | 333 |
| 9.5.2 | Plugin Component..... | 334 |
| 9.5.3 | Customizing the Features | 335 |
| 9.5.4 | Backing up and Restoring Settings | 336 |
| 9.6 | Bandwidth Control Application | 338 |
| 9.6.1 | Installing the Bandwidth Control..... | 339 |

| | | |
|------------|--|------------|
| 9.6.2 | The Main Window..... | 340 |
| 9.6.3 | Allowing Remote Control..... | 341 |
| 9.6.4 | Connecting to a WebCam Server | 342 |
| 9.6.5 | Controlling Specific WebCam Server | 343 |
| 9.6.6 | Setting up the Bandwidth | 344 |
| 9.6.7 | Block List Setup..... | 345 |
| 9.6.8 | General Setup | 346 |
| 9.7 | Language Setting..... | 347 |
| 9.7.1 | Installing the MultiLang Tool | 347 |
| 9.7.2 | Revising the Translated Text | 348 |
| 9.7.3 | Setting Up the UI Language to English | 352 |
| 9.8 | Skype Video Utility | 354 |
| 9.8.1 | Installing GV-Skype Video Utility..... | 355 |
| 9.8.2 | Setting Up Notifications Upon Motion or I/O Trigger..... | 356 |
| 9.8.3 | Requesting Live View | 361 |
| 9.9 | GV-SDSyncCard Utility..... | 362 |
| 9.9.1 | Installing GV-SDCardSync Utility | 362 |
| 9.9.2 | Setting Up GV-SDCardSync Utility | 363 |
| 9.9.3 | The Main Window..... | 366 |

Chapter 1

Configuring Main System 3

| | | |
|------------|---|-----------|
| 1.1 | Installing the GV-VMS..... | 3 |
| 1.1.1 | Dongle..... | 3 |
| 1.1.2 | Options..... | 4 |
| 1.1.3 | Minimum System Requirements..... | 5 |
| 1.1.4 | Minimum Network Requirements..... | 5 |
| 1.1.5 | Installing GV-VMS..... | 6 |
| 1.1.6 | Uninstalling and Upgrading GV-VMS | 8 |
| 1.2 | Getting Started | 9 |
| 1.2.1 | Main Screen..... | 10 |
| 1.2.2 | Adding Cameras | 12 |
| 1.2.3 | Accessing Live View | 14 |
| 1.2.4 | Enabling the Recording | 15 |
| 1.2.5 | Playing Back Video | 16 |
| 1.3 | Recording Settings..... | 17 |
| 1.3.1 | Setting Global Recording Settings for All Cameras..... | 18 |
| 1.3.2 | Setting Recording Settings for Individual Cameras | 20 |
| 1.3.3 | Setting Up the Video Storage Location..... | 21 |
| 1.3.4 | Setting Up Motion Detection | 23 |
| 1.4 | Live View and Layouts | 26 |
| 1.4.1 | Utilizing Live View Functions | 26 |
| 1.4.2 | Arranging Live View Layouts | 29 |
| 1.4.3 | Setting a Zoom Window..... | 31 |
| 1.4.4 | Setting a Scan Window..... | 33 |
| 1.4.6 | Setting Focus View | 35 |
| 1.5 | Start Monitoring | 36 |
| 1.6 | System Configuration | 38 |
| 1.6.1 | Configuring General Setting | 38 |
| 1.6.2 | Customizing Startup Settings | 40 |
| 1.6.3 | Customizing Display Position and Panel Resolution | 42 |
| 1.6.4 | Setting Up Email Notification | 43 |
| 1.6.5 | System Idle Protection..... | 46 |
| 1.6.6 | Configuring Fast Key Lock..... | 48 |
| 1.7 | Account and Password | 49 |

| | | |
|-------------|---|-----------|
| 1.7.1 | Creating a New Account | 50 |
| 1.7.2 | Configuring Account Settings | 51 |
| 1.7.3 | Changing or Retrieving Password at Login | 53 |
| 1.7.4 | Preventing Unauthorized System Termination | 54 |
| 1.7.5 | Setting a Startup Auto Login User | 55 |
| 1.8 | Schedule | 56 |
| 1.8.1 | Creating a Schedule with Setup Wizard | 57 |
| 1.8.2 | Creating a Schedule Manually | 60 |
| 1.8.3 | Exporting and Importing Schedule Settings..... | 61 |
| 1.9 | System Log | 62 |
| 1.9.1 | Setting System Log..... | 62 |
| 1.9.2 | Viewing System Log | 64 |
| 1.10 | Other Functions | 66 |
| 1.10.1 | Setting Live View Pop-Up Video..... | 66 |
| 1.10.2 | Adjusting to Daylight Saving Time | 67 |
| 1.10.3 | Setting Network Failure Detection | 69 |
| 1.11 | PTZ Camera..... | 70 |
| 1.11.1 | Accessing PTZ Control Panel and Auto Functions..... | 71 |
| 1.11.2 | Setting PTZ Idle Protection and Advanced Functions..... | 73 |

Configuring Main System

1.1 Installing the GV-VMS

1.1.1 Dongle

GV-VMS supports connection with up to connection with up to 64 IP devices. You can connect up to 32 channels of GV-IP Devices for free. If you need to connect more than 32 channels of GV-IP Devices or connect with third-party IP devices, license is required.

| Supported Devices | Channels | License |
|---------------------------|----------|---|
| GV IP Devices Only | 32 ch | No license required. |
| | 64 ch | GV-VMS Pro license required, 32 ch per license. |
| GV + 3rd-Party IP Devices | 32 ch | 3rd-Party license required, in increments of 1 ch. |
| | 64 ch | 2 licenses required: <ul style="list-style-type: none"> • GV-VMS Pro license, 32 ch per license. • 3rd-Party license, in increments of 1 ch. |

Note: GV-USB Dongle comes in internal and external dongles. It is recommended to use the internal GV-USB Dongle to have the Hardware Watchdog function, which restarts the PC when Windows crashes or freezes.

For the list of supported third-party IP camera models, please visit GeoVision's website:

http://www.geovision.com.tw/english/4_21.asp

1.1.2 Options

The following optional devices are available to expand your GV-VMS's capabilities and versatility. Contact your dealer for more information.

| Optional Devices | Description |
|-----------------------------|---|
| Internal USB Dongle | The USB dongle can provide the Hardware Watchdog function to the GV-VMS by restarting the computer when Windows crashes. You need to connect the dongle internally on the motherboard. |
| GV-Hub V2 | An easy way for serial port extension, this hub can add 4 RS-232 / RS-485 serial ports through the GV-VMS's USB port. |
| GV-COM V2 | GV-COM V2 can add 1 RS-232 / RS-485 serial port through the GV-VMS's USB port. |
| GV-IO Box (4 Ports) | GV-IO Box 4 Ports provides 4 inputs and 4 relay outputs, and supports both DC and AC output voltages. A USB port is also provided for PC connection. |
| GV-IO Box (8 Ports) | GV-IO Box 8 Ports provides 8 inputs and 8 relay outputs, and supports both DC and AC output voltages. You can connect the unit to the PC either by using its USB port or through network by using its Ethernet module. |
| GV-IO Box (16 Ports) | GV-IO Box 16 Ports provides 16 inputs and 16 relay outputs, and supports both DC and AC output voltages. You can connect the unit to the PC either by using its USB port or through network by using its Ethernet module. |
| GV-Joystick V2 | GV-Joystick V2 allows you to easily control PTZ cameras. It can be either plugged into the GV-VMS for independent use or connected to GV-Keyboard. |
| GV-Keyboard V3 | GV-Keyboard V3 is used to program and operate GV-VMS and PTZ cameras. Through RS-485 configuration, it can control up to 36 GV-VMS. In addition, you can connect PTZ cameras directly to the keyboard for PTZ control. |

1.1.3 Minimum System Requirements

Below are the minimum PC requirements needed to connect GV-VMS with 32 and 64 channels of GV and 3rd party IP cameras (dual streams).

| | GV-VMS (Up to 32 Channels) | GV-VMS Pro (Up to 64 Channels) |
|---------------|--|---------------------------------|
| OS | 64-bit Windows 7 / 8 / 8.1 / Server 2008 R2 / Server 2012 R2 | |
| CPU | 4th Generation i3-4130, 3.4 GHz | 4th Generation i7-4770, 3.4 GHz |
| Memory | 4 GB RAM | 8 GB RAM |

1.1.4 Minimum Network Requirements

The data transmitting capacity of GV-VMS depends on the number of Gigabit connections available.

The numbers of Gigabit network cards required to connect 64 channels are listed below according to the resolution and codec of the source video.

| Codec | Resolution | Bitrate Used (Mbps) | Total FPS for 64 ch | Gigabit Network Cards Required | Max. Channels Supported per Network Card |
|--------------|---------------|---------------------|---------------------|--------------------------------|--|
| H.264 | 1.3 MP | 5.05 | 1920 | 1 | Max. 64 ch / card |
| | 2 MP | 7.01 | 1920 | 1 | Max. 64 ch / card |
| | 3 MP | 10.48 | 1280 | 1 | Max. 64 ch / card |
| | 4 MP | 11.65 | 960 | 2 | Max. 50 ch / card |
| | 5 MP | 16.48 | 640 | 2 | Max. 38 ch / card |
| MJPEG | 1.3 MP | 32.36 | 1920 | 3 | Max. 22 ch / card |
| | 2 MP | 44.96 | 1920 | 4 | Max. 16 ch / card |
| | 3 MP | 38.73 | 1280 | 4 | Max. 18 ch / card |
| | 4 MP | 40.35 | 960 | 4 | Max. 17 ch / card |
| | 5 MP | 30.48 | 640 | 3 | Max. 22 ch / card |

Note: The network requirements may vary depending on the bit rate of the streams.

1.1.5 Installing GV-VMS

Before You Start

For optimal performance of your system, it is important to follow these recommendations before installing the GV-VMS:



- It is strongly recommended to use separate hard disks. One is for installing Windows OS and GV-VMS software, and the other is for storing recorded files and system logs.
- When formatting the hard disks, select NTFS as the file system.
- GV-VMS is a multi-channel video recording system. With normal use of the system, the drive containing video files will become fragmented. This is because GV-VMS constantly stores video files of multi channels simultaneously, and video files will be scattered all over the drive. It is not necessary to regularly perform disk defragmentation. Since GV-VMS software and video files are stored on separated hard disks, the performance of GV-VMS will not be affected.
- Since the size of transmitted data from IP cameras may be quite large and reach beyond the transfer rate of a hard disk, you should note the total of recording frame rates that you can assign to a single hard disk, as listed below:

Frame rate limit in a single hard disk

| Video Resolution | H.264 | | MJPEG | |
|--|------------|--------------|------------|--------------|
| | Frame Rate | Bit Rate | Frame Rate | Bit Rate |
| 1.3 MP (1280 x 1024) | 660 fps | 5.05 Mbit/s | 300 fps | 32.26 Mbit/s |
| 2 MP (1920 x 1080) | 660 fps | 7.01 Mbit/s | 210 fps | 44.93 Mbit/s |
| 3 MP (2048 x 1536) | 440 fps | 10.48 Mbit/s | 140 fps | 38.67 Mbit/s |
| 4 MP (2048 x 1944) | 330 fps | 11.65 Mbit/s | 105 fps | 40.53 Mbit/s |
| 5 MP (2560 x 1920) | 220 fps | 16.48 Mbit/s | 80 fps | 30.4 Mbit/s |
| Note: The data above was determined using the bit rate listed above and hard disks with average R/W speed above 110 MB/s. | | | | |

The frame rate limit is based on the resolution of video sources. The higher video resolutions, the lower frame rates you can assign to a single hard disk. In other words, the higher frame rates you wish to record, the more hard disks you need to install. For the information of recording frame rates, you may consult the user's manual of the IP camera that you wish to connect to.

Installing GV-VMS

1. To download GV-VMS, go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. To install GV-VMS, find the **Primary Applications** section under the Video Management Software tab and click the **Download** icon  of **GV-VMS**.
3. Double-click **GVVMSInstaller.exe** and follow the instructions in the wizard to complete installation.
4. If you are using a USB dongle, insert the dongle to your computer. The GV-USB dongle is needed if you want to connect to more than 32 channels of IP devices or to third-party IP devices.
5. To install USB driver, find the **Driver** section under the Video Management Software tab, and click the **Download** icon  of **GV-USB Devices Driver**.

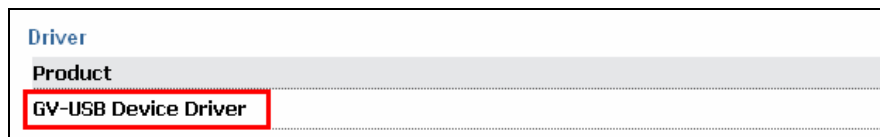


Figure 1-1

If you are using the GV-USB dongle, verify that the driver is installed correctly after the steps above. Go to Windows Device Manager and expand **DVR-Devices**. You should see the **GV-Series USB Protector**.



Figure 1-2

1.1.6 Uninstalling and Upgrading GV-VMS

GeoVision will periodically release software updates on our website. **Before installing software upgrade, be sure to uninstall GeoVision Software first.** By default, GeoVision software and log files are stored on one drive, while video files are stored on a different drive. Uninstalling GV-VMS will not remove the video, log, and setting files previously saved in the computer.

To uninstall the GV-VMS, follow these steps:

1. Close any open programs because your computer will restart during the uninstalling process.
2. Click the **Start** button, click **Control Panel**, and then click **Uninstall a Program** under Programs.
3. In the list of currently installed programs, select **GV-VMS**, and then click **Uninstall/Change**.

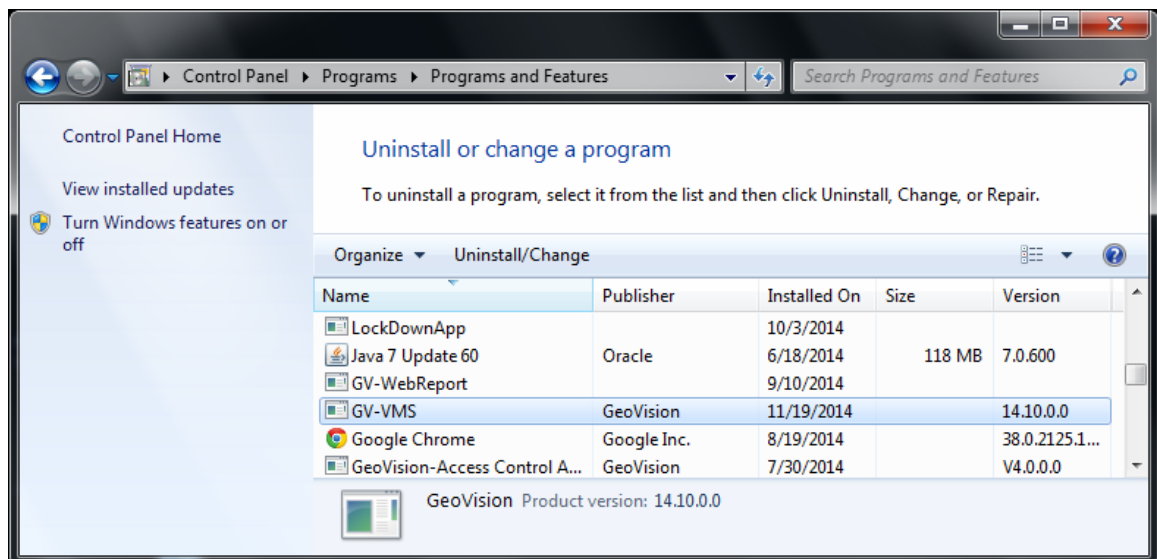


Figure 1-3


4. When you are prompted to confirm the program removal, click **Yes**.

To upgrade, download the newest GV-VMS from GeoVision's website and re-install on your computer: http://www.geovision.com.tw/english/5_8_VMS.asp. For details, see *[Installing GV-VMS]*, 1.4 Installing GV-VMS in this Quick Start Guide.

1.2 Getting Started

When you run GV-VMS for the first time, the system will prompt you for a Supervisor ID and Password.

Figure 1-4

1. Type an **ID** and a **password**. Type the password again for confirmation.
2. Type a hint that would remind you of the password.
3. It is recommended to click **E-Mail List** and enter e-mail addresses. When you forget the password, the password can be sent to your e-mail account.
4. Click **OK** to enter the main screen. You can also select the following options:
 - **Auto Login:** Allows auto login as the current user every time when the system is launched. For security purposes, this feature is only recommended for single-user systems.
 - **Allow removing password System:** It is recommended to select this option which allows removing the password database once you forget passwords. For details, see the same option in *Account and Password* later in this chapter.
 - : Click to open the onscreen keyboard and enter the login information.

1.2.1 Main Screen



Figure 1-5




| Name | Description |
|----------|--|
| Login ID | Click to manage accounts and passwords for accessing GV-VMS. |
| Home | Shows the live view of connected cameras. |
| ViewLog | Shows a timeline of recorded events for playback. |
| Toolbar | Brings up these options when Home is selected: |
| | <ul style="list-style-type: none"> • Monitor: Start / Stop monitoring, I/O monitoring and schedule monitoring |
| | <ul style="list-style-type: none"> • Network: Enable Webcam Server and connection to other GeoVision software. |
| | <ul style="list-style-type: none"> • Tools: Show / hide volume indicator and set up Object Index. |
| | <ul style="list-style-type: none"> • Configure: Set up camera, recording, system, schedule, video processing and I/O devices |
| | <ul style="list-style-type: none"> • Content List: Access live view layout, camera list, I/O device list and Panorama view. |

Brings up these options when **ViewLog** is selected:

- **Display Play Panel:** Display or hide the ViewLog timeline. This function is grayed out when the **Pinned** button is selected in the bottom-right corner.
- **Tools:** Manage event search, system log, event backup and event export.
- **Configure:** Apply video effects and text overlay during playback.
- **Content List:** Manage playback layout and access camera list.

| | |
|------|---|
| Exit | Brings up these options: Minimize and Exit. |
|------|---|

1.2.2 Adding Cameras

To add cameras to the GV-VMS, click **Home** , select **Toolbar** , click **Configure**  and then select **Camera Install**. When the camera list is empty, the Automatic Setup dialog box automatically pops up.

1. Click **Automatic Setup** to search for IP cameras on the LAN.

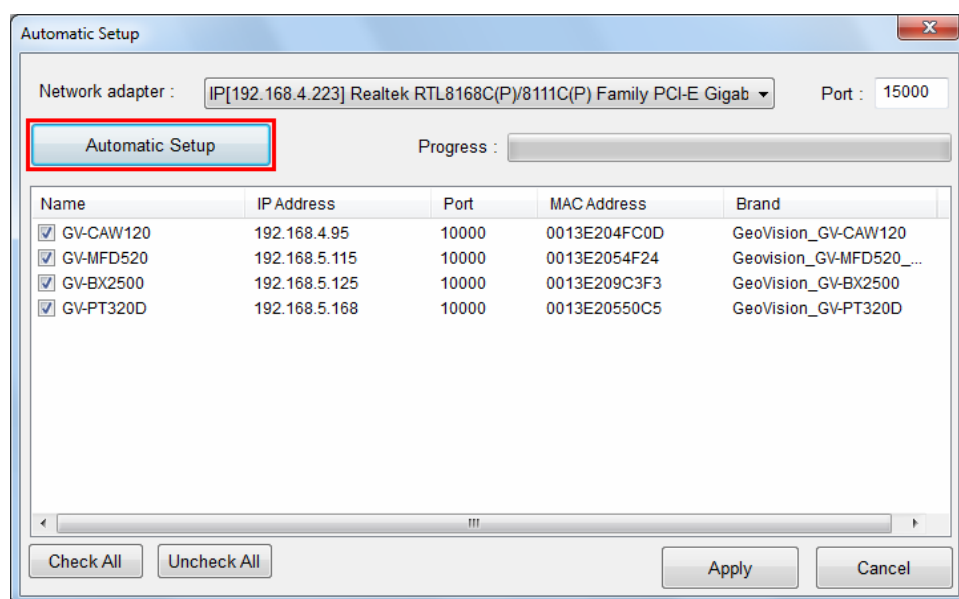


Figure 1-6

2. The default login information for cameras is **admin / admin**. If the camera uses different ID and password, double-click the camera to specify the login information and click **OK**. If you select **Apply All**, the login information will be applied to all selected cameras.

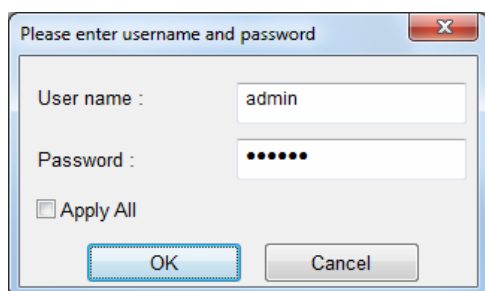


Figure 1-7

3. Make sure the cameras you want to add are selected and click **Apply**. The cameras added are now listed in the Camera List.
4. Close the dialog box by clicking X on top-left corner. When adding camera for the first time, the cameras will be automatically assigned to the live view grid.

Tip: You can change the camera ID by clicking the ID of an inactive camera. The ID number does not affect where the camera is positioned in the live view grid, but the cameras will be listed according to the camera ID in setup pages such as Video Processing dialog box.

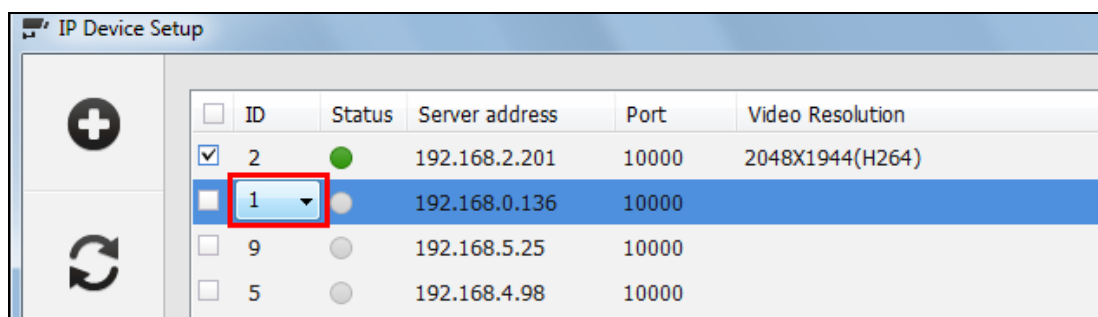





Figure 1-8

To add cameras using manual setup, camera scan or GV-IP Device Utility, refer to *Adding IP Cameras* in Chapter 2

1.2.3 Accessing Live View

After adding cameras, you can access camera live view by dragging the camera in the Content List to the live view grid.

1. Click **Home** , select **Toolbar** , and select **Content List** . The Content List appears.
2. Click **Camera** in the content list to see the list of cameras added.
3. Drag the cameras to the live view grid.

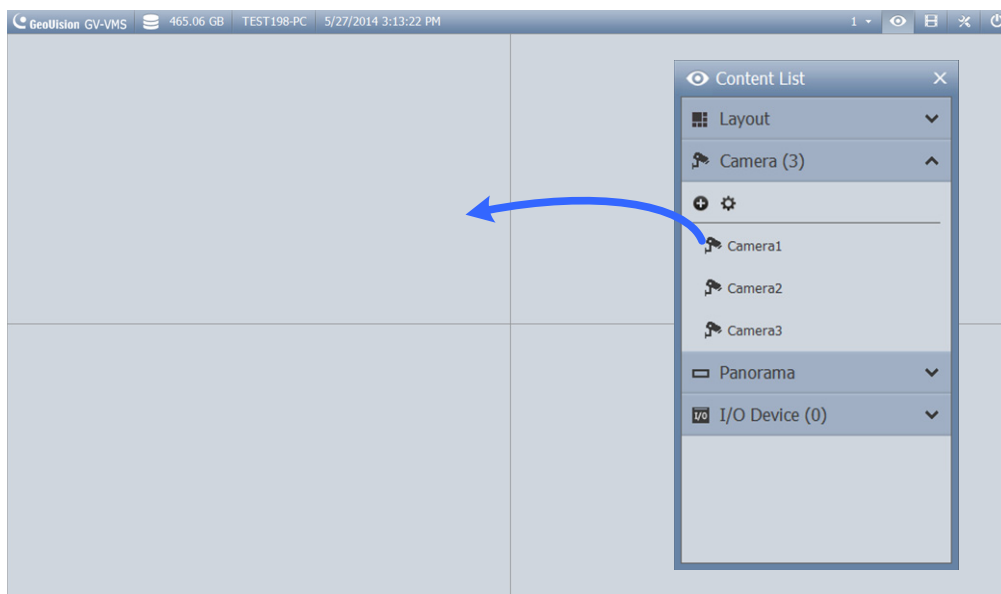





Figure 1-9

For details on the live view, see *Live View and Layout* in later in this chapter.

1.2.4 Enabling the Recording

To start recording, click **Home** , select **Toolbar** , click **Monitor**  and then select **Start All Monitoring**. You can also individually select the cameras you want to start monitoring. By default, every camera records with the following settings:

| Default Recording Settings | |
|----------------------------|---|
| Recording Mode | Motion Detection |
| Resolution / Codec | The camera's current resolution / codec will be used. |

When working with the system, you will undoubtedly want to change the settings as you go along.

- To change **recording mode**, see *Record Setting* later in this chapter.
- To change **resolution** and **codec**, see *Configuring Video Setting* in Chapter 2.

1.2.5 Playing Back Video

Instant Playback

You can instantly play back the recorded video of a single camera from the camera live view. Place the cursor on the live view, click the **Instant Playback** button, and select the time length: 10 seconds, 30 seconds, 1 minute or 5 minutes.

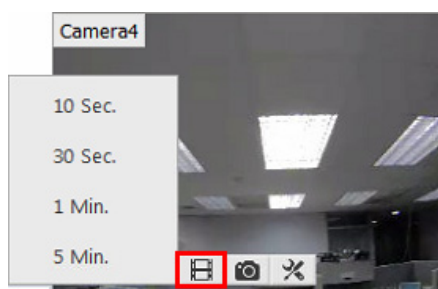





Figure 1-10

ViewLog

For more comprehensive playback functions, click **ViewLog**  in the top-right corner.

1. Open the Content List by clicking **Toolbar**  and selecting **Content List** .
2. Drag the camera you want to play back onto the playback screen from the Content List. The colored areas in the timeline indicate that videos have been recorded during that time period.

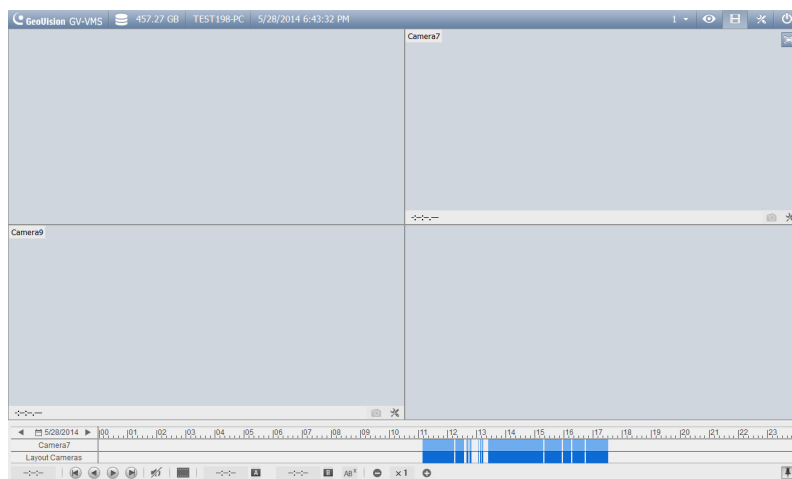






Figure 1-11

3. Select a camera in the grid, click on a colored area and click the **Play** button .

For details on the ViewLog player, see *Video Playback* in Chapter 4.

1.3 Recording Settings

This section introduces the recording settings of the GV-VMS. To configure the recording setting of the cameras, click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **Record Setting**. This dialog box appears.

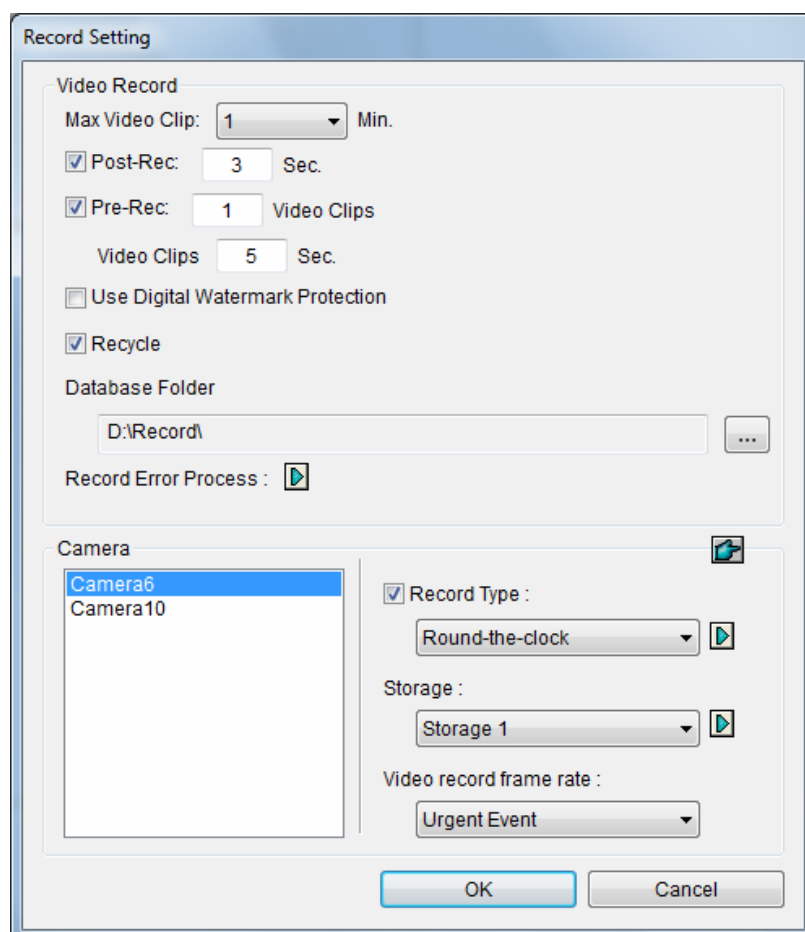


Figure 1-12

By default, the system has the following recording settings.

| Default Data Storage Settings | | |
|-------------------------------|----------------------|---|
| Storage Location | Recorded Files | D:\Record\ <camxx audxx="" folder>.<="" or="" td=""></camxx> |
| | Event Database Files | D:\CameraDBs\ |
| Recycle Function | | Enabled with recycling threshold set to 32 G. |
| Recording Mode | | Motion Detection |

1.3.1 Setting Global Recording Settings for All Cameras

In the top half of the Record Setting dialog box, you can configure global recording settings that will be applied to all cameras, such as maximum length of each video clip, recycling function and the actions to take upon recording errors.

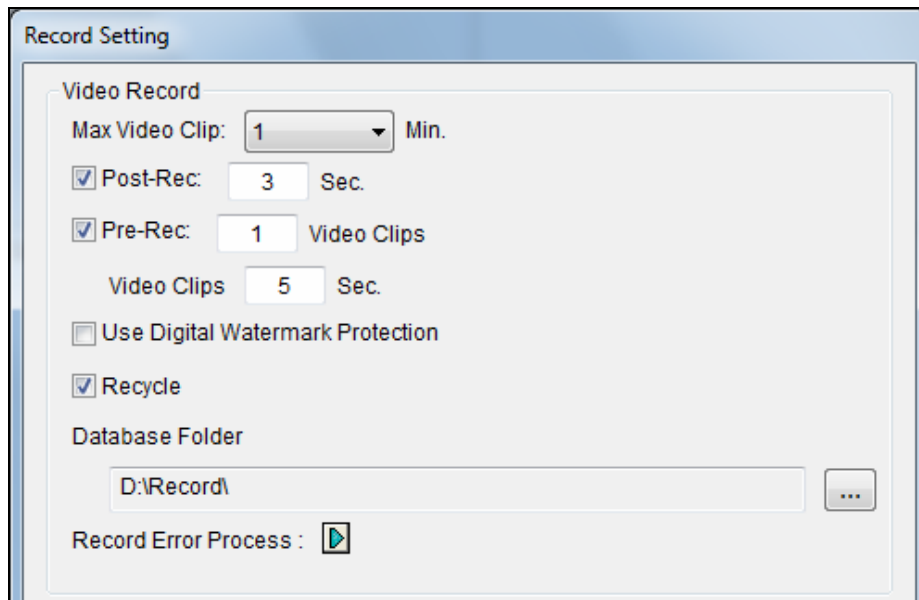




Figure 1-13

[Video Record]

- **Max Video Clip:** Specifies the maximum time length of each recorded file (from 1 to 5 minutes). If you select **5 Min**, a 30-minute event will be chopped into six 5-minute event files; if you select **1 Min**, a 30-minute event will be chopped into thirty 1-minute event files. To decide what to set up here, consider how often you back up your event files, and how frequent the activity is in your surveillance area. Smaller file size makes backup process faster.
- **Post-Rec:** Keeps on recording for a set period of time after motion stops.
- **Pre-Rec:** Records video for a set period of time before motion starts or an input device is triggered. Specify the number of video clips to pre-record and specify the number of seconds per video clip. For example, if you specify **3 video clips** and **5 seconds**, 15 seconds of video before each motion or input event will be recorded. There will be a total of 3 video clips and each clip is 5 seconds long.
- **Use Digital Watermark Protection:** Click to watermark all recorded videos. Watermark is a way to verify the authenticity of video streams, and to ensure that they have not been tampered with or modified in any way. For details, see *Watermark Viewer* in Chapter 9.

- **Recycle:** When selected, the oldest recordings will be deleted when the system requires storage space for new files. If it is not selected, the system will stop recording when disk space is full.
- **Database Folder:** The default storage path for Event Database (.db files) is at D:\CameraDBs\.
Click the ... button  to specify a new storage path. Note that the storage path for the actual recordings is specified in the Storage option under the Record Type option.
- **Record Error Process:** Click the Arrow button  to select what actions to take when there is a recording error.
 - ⊙ **Invoke Alarm:** Activates computer alarm by playing the selected sound file.
 - ⊙ **Invoke to Send Alerts:** Sends e-mail notification. To see how to set up the e-mail server, refer to *Setting Up Email Notification* later in this chapter.
 - ⊙ **Register Event:** Records the error to System Log.
 - ⊙ **Output Module:** Triggers the selected output device. To see how to set up I/O devices, refer to *Chapter 6 I/O Applications*.

1.3.2 Setting Recording Settings for Individual Cameras

In the lower half of the Record Setting dialog box, you can select a camera and configure the recording mode and video storage location for the selected camera(s) only.

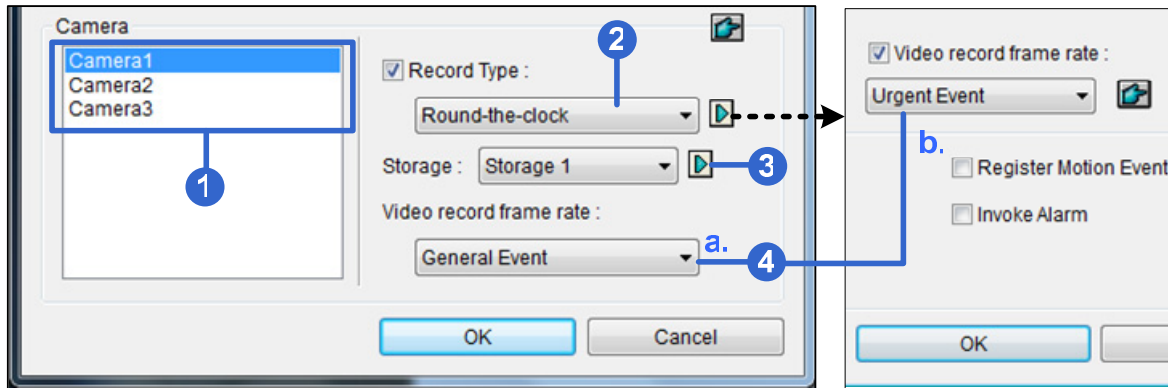




Figure 1-14

1. Select the camera you want to configure. Hold the Shift key to select multiple cameras if needed.
2. Under Record Type, select **Round-the-clock** or **Motion Detect**.
3. Click the Arrow button  next to **Storage** to specify where to store the recorded videos. For details, see *Setting Up the Video Storage Location* later in this section.
4. You can set different recording frame rates for motion and non-motion recordings. In Round-the-Clock mode, the camera will use the frame rate setting in 4a for non-motion events and 4b for motion events. For Motion Detection recording mode, the frame rate setting in 4b will be used.
 - a. Define **non-motion** events as General or Urgent Event under **Video Record Frame Rate**.
 - b. For **motion** events, click the arrow button  next to Record Type and define motion events as General or Urgent Event under **Video Record Frame Rate**.


The frame rate for General Event and Urgent Event can be defined in the camera's General Setting dialog box (Figure 2-11). Normally, you would set a higher frame rate for Urgent Events (Ex: full frame) and a lower frame rate for General Events (Ex: key frame only).

Note:

1. Refer to *Configuring General Settings* in Chapter 2 for setting the frame rate for General Event and Urgent Event.
 2. For details on other motion detection settings, refer to *Setting Up Motion Detection* later in this section.
-

1.3.3 Setting Up the Video Storage Location

You can create a maximum of 24 storage groups with different storage locations. The default storage location is D:\Record\.

1. In the Record Setting dialog box, click the Arrow button  next to **Storage**. This dialog box appears.

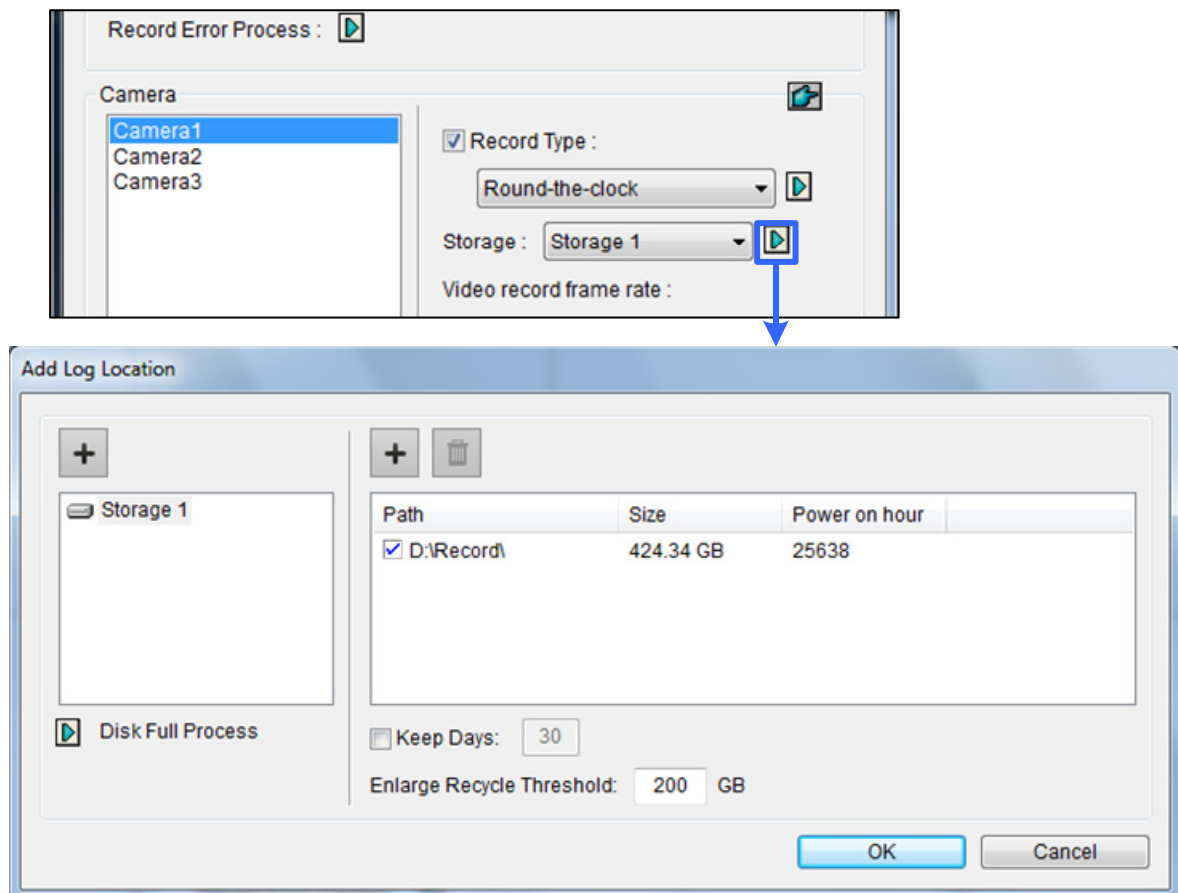





Figure 1-15

2. To add a new folder in the first storage group, click the **Add** button  above Path and select a folder. Only 1 folder can be assigned as storage folder per partition (e.g. only 1 folder in D drive).
3. To add a new storage group, click the **Add** button  in the top-left corner and repeat the step above to assign at least one folder to the storage group.
4. Select **Keep Days** and specify the number of days to keep the video files in storage.
5. In the **Enlarge Recycle Threshold** field, adjust the recycle threshold if needed. Recycle threshold is the file size at which the recycling begins. The minimum and default recycle threshold is 32 GB.

6. To specify the actions to take when hard disks become full, click the Arrow button  next to **Disk Full Process**.
 - **Invoke Alarm:** Activates computer alarm by playing the selected sound file.
 - **Invoke to Send Alerts:** Sends e-mail notification. To see how to set up the e-mail server, refer to *Setting Up Email Notification* later in this chapter.
 - **Register Event:** Records the error to System Log.
 - **Output Module:** Triggers the selected output device. To see how to set up I/O devices, refer to *Chapter 6 I/O Applications*.
7. Click **OK**.

Note: If the designated storage space is not big enough to keep all video files for the defined days, the **Recycle Threshold** setting will override the **Keep Days** setting.


1.3.4 Setting Up Motion Detection

The motion detection settings will be applied to motion events in both Round-the-Clock mode and Motion mode. The following features are available to prevent false motion detection:

- **Object Size:** Set a minimum and maximum object size to only detect objects within the size range
- **Sensitivity:** Designate up to 10 levels of motion detection sensitivity for each outlined area
- **Mask Region:** Mask off unwanted areas for monitoring, such as cloud and tree movement
- **Noise Tolerance:** Ignore video noise when the lighting condition is poor or changed
- **Ignore environmental changes:** Ignore changes such as rain, snow and tree movement

Note:

1. You can only enable motion detection either by sensitivity or by object size at a time.
 2. By default, the entire camera view is set to a motion sensitivity level of 9 with Noise Tolerance and Process Video in Lower Resolution function enabled.
-

1. In the Record Setting dialog box, click the Arrow button  next to **Record Type**. This dialog box appears.

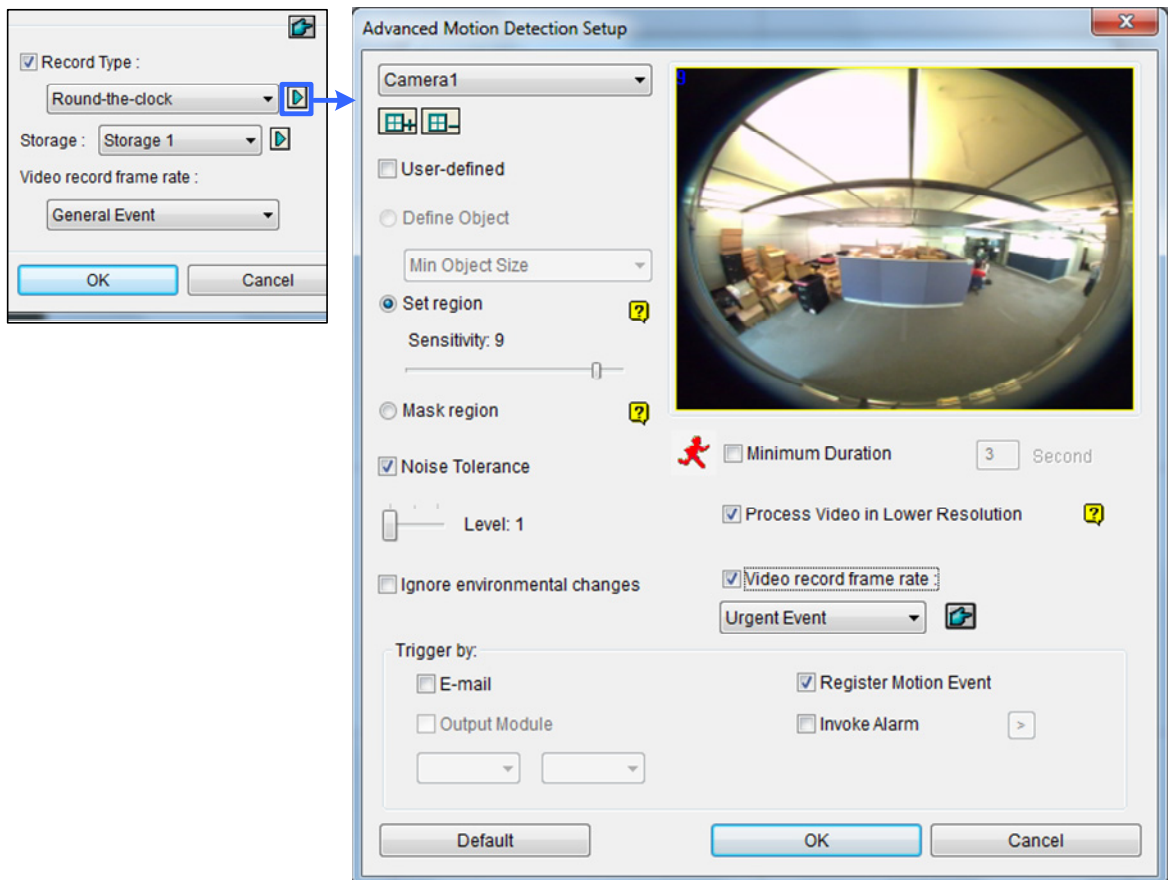






Figure 1-16

2. You can refine motion detection by setting Object Size or Region Sensitivity.
 - **Object Size:** Limits motion detection to objects within a size range. Select **User-defined**. Select **Min. Object Size** from the drop-down list and then drag an area on the image. Repeat the process and set a **Max. Object Size**.
 - **Set Region Sensitivity:** Sets different detection sensitivities for different parts of the camera image. Uncheck **User-defined**, adjust the sensitivity level by moving the slider, and then drag an area on the image. You can create several areas with different sensitivity levels. You can use the **Add Mask**  and **Cut Mask**  buttons to create irregular shapes. By default, the entire image is set to the sensitivity level 9.
3. To ignore motions in a certain area, click **Mask Region**, and then drag an area on the image. You can use the **Add Mask**  and **Cut Mask**  buttons to create irregular shapes.

4. The following options are available to further reduce false alarm:
 - **Noise Tolerance:** Enable to ignore video noise and move the slider to adjust the level. The higher the level, the more tolerant the system is to video noise. If the surveillance area is prone to produce high noise possibly due to weather or light changes, set the level to High.
 - **Ignore environmental changes:** Ignores environmental changes such as rain or snow. When selected, objects moving steadily and repeatedly in the same direction for over 1.5 seconds will be filtered out and ignored.
 - **Minimum Duration:** Sets the minimum duration for which motions must persist for the system to issue a motion alarm. Specify the minimum duration in seconds (Max. 60 seconds).
5. You can reduce CPU loading by selecting **Process Video in Lower Resolution**. When enabled, GV-VMS compresses live view into a lower resolution before GV-VMS detects if there is motion, which reduces CPU loading, but may affect the accuracy.
6. To set the frame rate setting for motion events, click **Video record frame rate** and select **Urgent Event** or **General Event**. Normally, you would set a higher frame rate for Urgent Events (Ex: full frame) and select Urgent Event here for motion events. The frame rate for General Event and Urgent Event can be defined in the camera's General Setting page. See *Configuring General Setting* in Chapter 2 for details.
7. Under Event Trigger, select the actions to take when motion is detected.
 - **E-mail:** Sends e-mail notification. To see how to set up the e-mail server, refer to *Setting Up Email Notification* later in this chapter.
 - **Output Module:** Triggers the selected output device. To see how to set up I/O devices, refer to *Chapter 6 I/O Applications*.
 - **Register Motion Event:** Registers motion events to System Log.
 - **Invoke Alarm:** Activates computer alarm by playing the selected sound file.
8. Click **OK** to save your settings.

1.4 Live View and Layouts

This section describes the functions on the camera live view and how to create new live view layouts using the Content List. After adding cameras, you can access camera live view by dragging the camera in the Content List to the live view grid. Refer to XXXX earlier in this chapter for details.

1.4.1 Utilizing Live View Functions

Live View Icons

Place the mouse cursor on the camera live view to see the icons below.

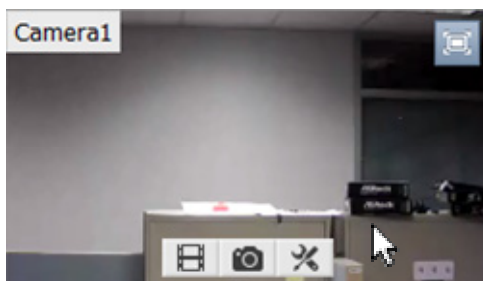







Figure 1-17




| Icons | Functions |
|--|--|
| Instant Play  | Plays back the video recorded in the last 10 seconds, 30 seconds, 1 minute, or 5 minutes. |
| Snapshot  | Captures a snapshot of the current live view. |
| Tools  | <p>Includes the following options:</p> <ul style="list-style-type: none"> ■ Monitor: Starts monitoring the camera. ■ Talk Back Toggle: Talks to the surveillance site from the PC. Only one camera can be enabled at a time. ■ Properties: <ul style="list-style-type: none"> ⊙ Show Caption: Shows camera name on live view. ⊙ Keep Image Ratio: Locks aspect ratio of the camera image. ■ Close: Removes the camera from the layout grid. |

| | |
|--|--|
| Tools  | <p>The following options are available when related function is enabled or supported:</p> <ul style="list-style-type: none"> ■ Set to Wave Out: Enables live view audio. (See <i>Configuring Audio Setting</i>, Chapter 2) ■ PTZ Control: Enables PTZ functions. (See <i>PTZ Camera</i> later in this chapter) |
| Zoom  | Switches the live view to full screen. If there is a designated Zoom window, clicking the Zoom button will replace the live view in the zoom window instead. |
| <p>Note: When PTZ Control is enabled on a PTZ camera, double-clicking the live view will make the camera zoom in instead of switching to full screen.</p> | |

Functions on Live View and Content List




The live view screen can be controlled using the actions below.

| Actions | Functions |
|--------------|--|
| Mouse scroll | Zooms in or out on the live view. |
| Double-click | Displays the live view in full screen. |

In the Content List (**Home**  > **Toolbar**  > **Content List** ) , right-click a camera to access the following options. Some options are only available when the related function is enabled or supported.

- **Monitor:** Starts monitoring the camera. (See *Start Monitoring* later in this section)
- **Video Process:** Opens the Video Processing dialog box. (See *Chapter 3 Video Analysis*)
- **Set to Wave Out:** Enables live view audio. (See *Configuring Audio Setting*, Chapter 2)
- **Talk Back Toggle:** Talks to the surveillance site from the PC. (See *Configuring Audio Setting*, Chapter 2)
- **Focus View Setup:** Creates up to 7 closed-up views in a camera. (See *Setting Focus View* later in this section)
- **PTZ Setup:** Enables PTZ functions. (See *PTZ Camera*, Chapter 1)
- **Fisheye Settings:** Opens the Fisheye Settings dialog box. (See *Fisheye View*, Chapter 3)

Volume Indicator

You can display an audio volume indicator on the top-left corner of the camera live view. Click the **Home** button , click the **Toolbar** button , click the **Tools** button , select **Audio** and select **Show Volume Indicator**.

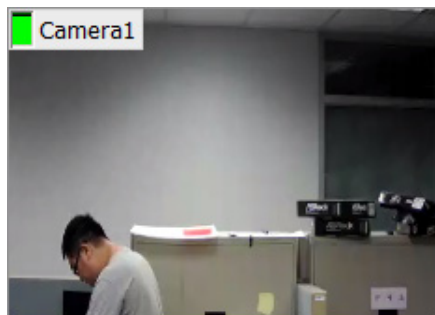


Figure 1-18

1.4.2 Arranging Live View Layouts

Follow the steps below to create new live view layouts.

1. In the Content List (Home  > Toolbar  > Content List ) , click **Layout**.



Figure 1-19

2. To add a layout, click the **Add** button  and click **Add Layout**. This dialog box appears.

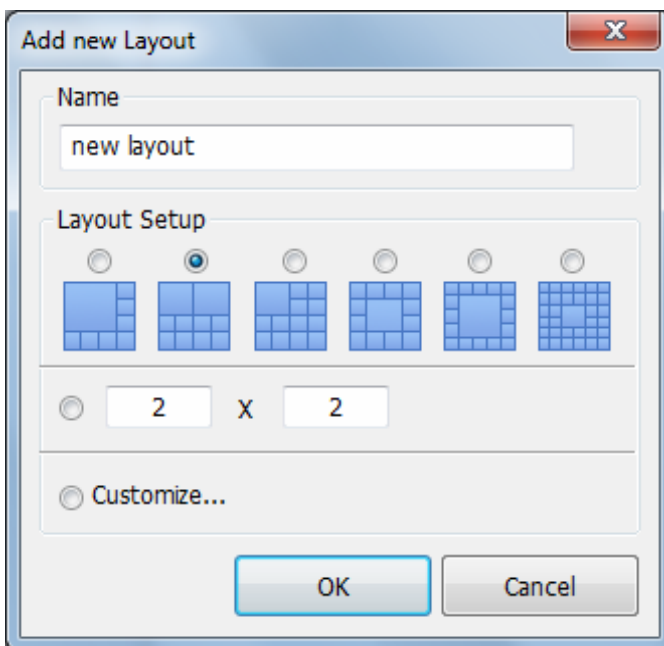


Figure 1-20

3. Name the new layout.
4. Select one of the three methods under Layout Setup and click **OK**.
 - Select an existing layout template.
 - Specify the number of live views in each row and column of the grid.
 - Customize your own layout.

5. If you select **Customize** in the step above, the Customize Layout dialog box will appear.
 - a. Click the **Reset** button to select a dimension for the grid if needed.

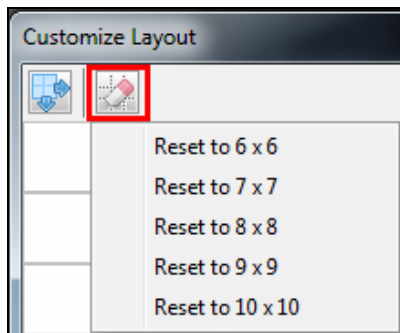


Figure 1-21

- b. Select multiple squares and click the **Merge** button to create a larger square.

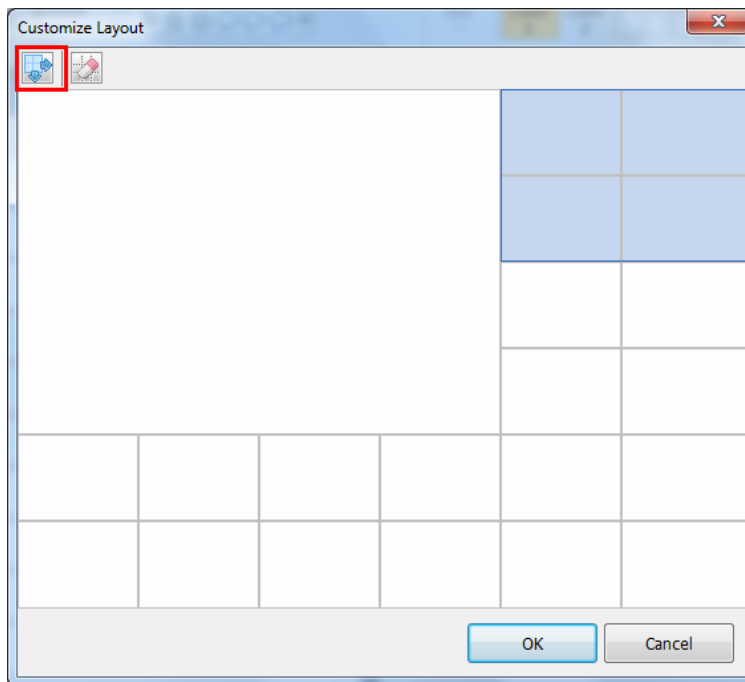





Figure 1-22

- c. Click **OK** when you are done.

A message appears. Click **Yes** if you want to automatically assign the cameras to the new layout. Alternatively, you can click **Camera** in the content list and manually drag the cameras to the live view.

1.4.3 Setting a Zoom Window

You can designate a Zoom Window to quickly see a close-up view of the camera image without changing the rest of the live view layout.

1. In the Content List (**Home**  > **Toolbar**  > **Content List** ) , select **Layout**, click **Windows** and drag **Zoom Window** to a live view grid.

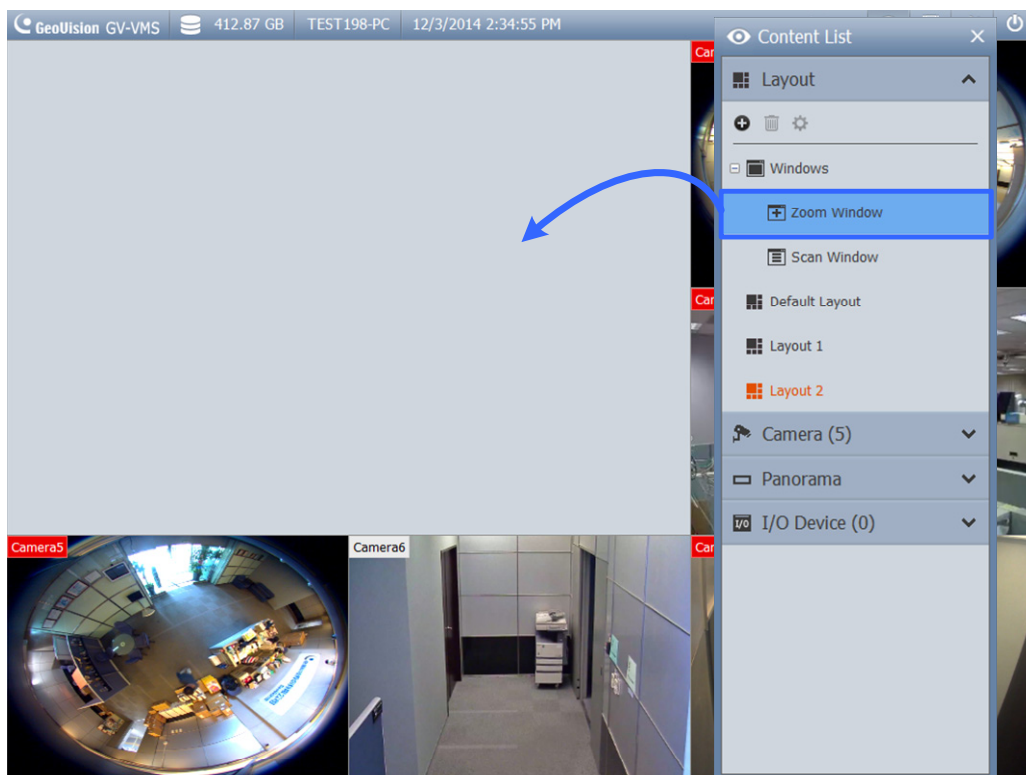



Figure 1-23

2. Move the mouse cursor to a camera live view and click the **Zoom** button  in the top-right corner. The camera live view is displayed in the Zoom Window.

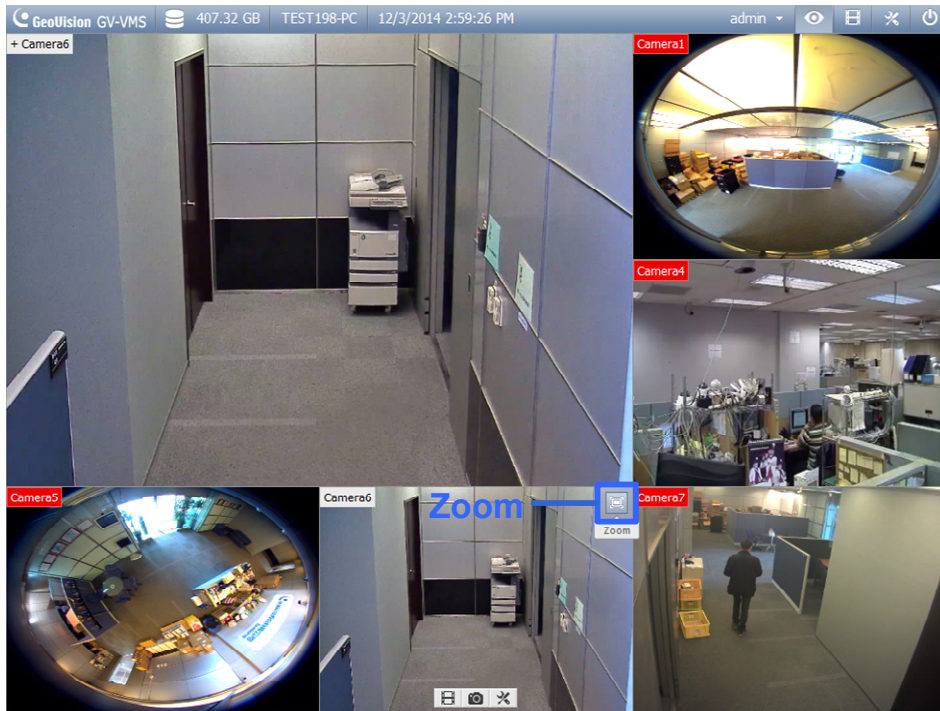






Figure 1-24

3. To remove the camera from the Zoom window, place the cursor on the live view, click the **Tools** icon  and select **Close**. To change the live view grid back to a normal window, repeat this step again to close the Zoom Window.

1.4.4 Setting a Scan Window

You can assign multiple cameras to a Scan Window, and each camera will be shown in sequence for the Scan Interval specified.

1. In the Content List (**Home**  > **Toolbar**  > **Content List** ) , select **Layout**, select **Windows**, and drag **Scan Window** to a live view grid.
2. Drag multiple cameras into the Scan Window.

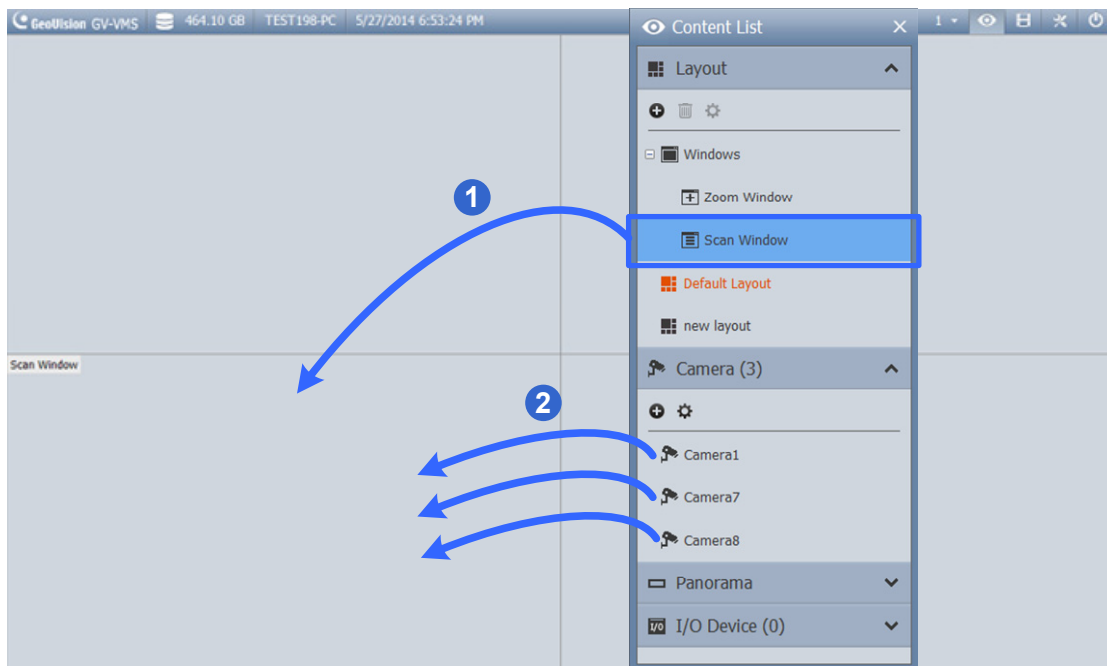



Figure 1-25

3. Move the cursor to the Scan Window, click the **Tools** icon , and select **Properties**. This dialog box appears.

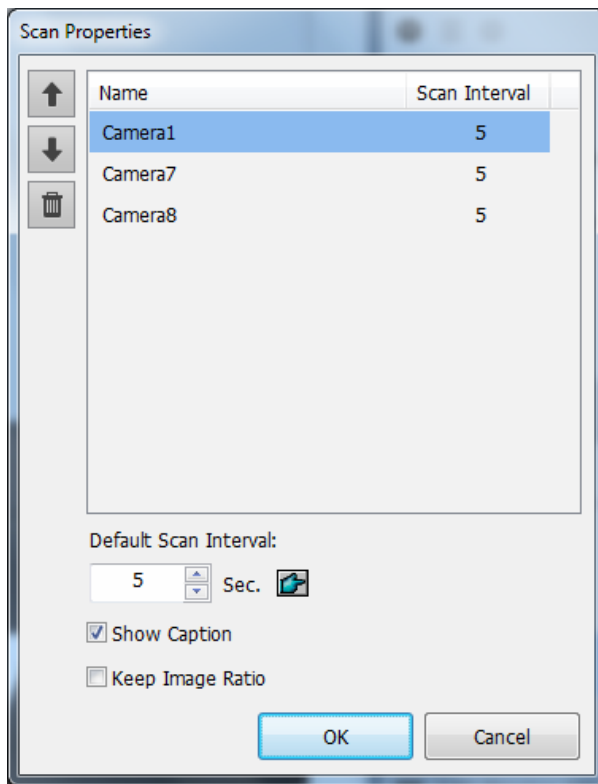








Figure 1-26

4. To adjust the order of a camera, select a camera and click the Up  and Down  arrows.
5. To specify how many seconds to show the live view of each camera, click and adjust the **Scan Interval** of each camera. In the figure above, each camera will be shown for 5 seconds. You can click the **Finger**  button to apply this Scan Interval to all cameras.
6. To show camera name on live view, select **Show Caption**.
7. To lock the original aspect ratio of the camera image, select **Keep Image Ratio**.
8. Click **OK**.

1.4.6 Setting Focus View

You can create up to 7 close-up views per camera and place these created close-up views inside live view grid. This function is not supported for Fisheye Cameras and PTZ Cameras.

1. In the Content List (Home  > Toolbar  > Content List ) , right-click a camera and select **Focus View Setup**. A dialog box appears.

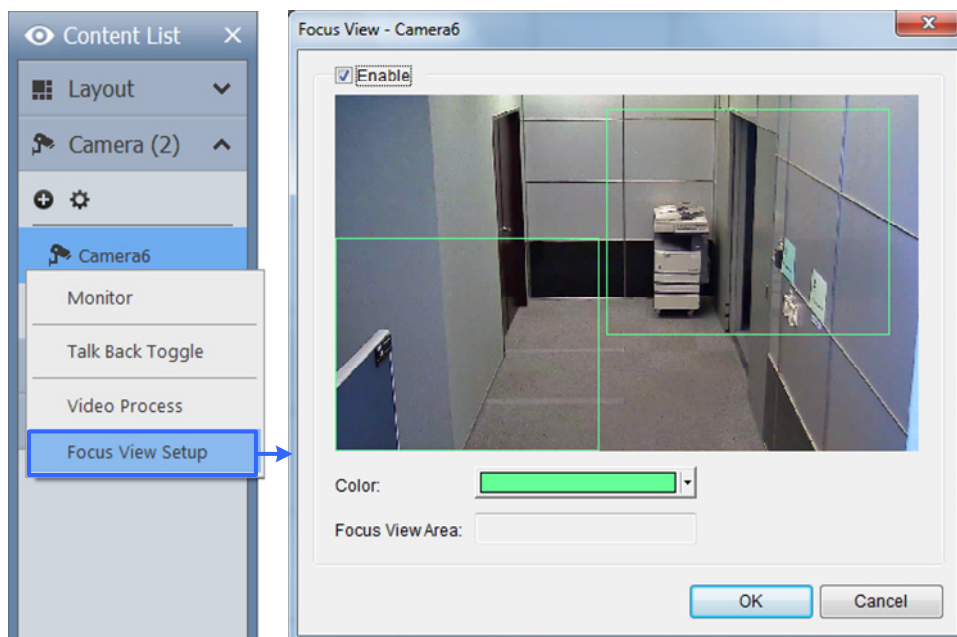


Figure 1-27

2. Click **Enable** and draw a box on the camera view to create a focus view. You can create multiple focus views if needed.
3. You can click the **Color** drop-down list to change the color of the box if needed.
4. Click **OK**. The created focus views are listed under the camera.
5. You can now drag the focus views to live view grids.

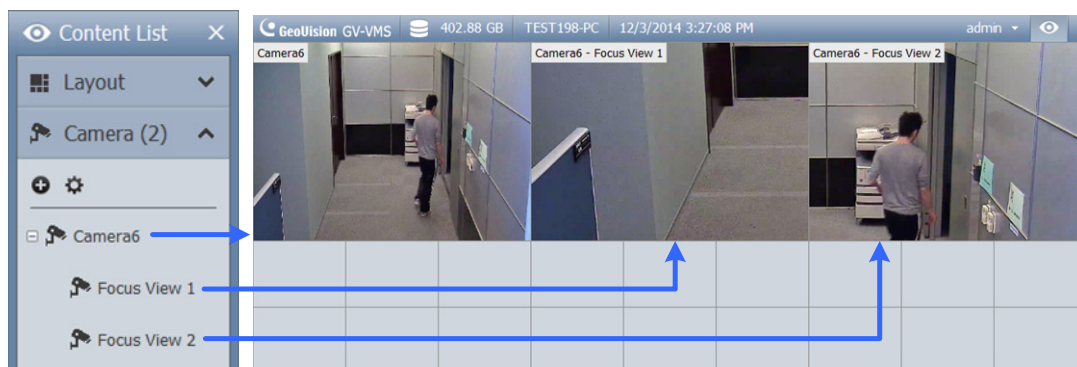


Figure 1-28

1.5 Start Monitoring

After setting up the following functions, it is important to start monitoring in order for the functions to start working: Recording, Video Analysis, I/O, Motion Event Trigger and Schedule.

To start monitoring, click **Home** , click **Toolbar** , select **Monitor** , and select one of the options:

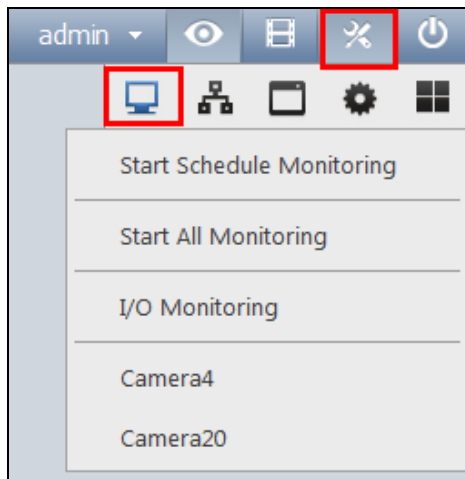





Figure 1-29

- **Start Schedule Monitoring:** If you want to start running a created schedule, select **Start Schedule Monitoring**. The schedule takes precedence over the current settings, and these functions will start and stop according to the schedule: Recording, Video Analysis, I/O, PTZ Auto Functions, Motion Event Trigger and Network Connections with Center V2 / Vital Sign Monitor.
- **Start All Monitoring:** Starts monitoring on all cameras to activate recording and video analysis functions.
- **I/O Monitoring:** Start I/O monitoring to activate I/O functions. I/O Monitoring is only available after at least one I/O device is set up. You can select I/O Monitoring to enable I/O functions independently without enabling recording and video analysis.

- **Camera#:** Start monitoring the selected cameras. You can also start monitoring individual cameras by right-clicking the camera in the Content List (**Home**  > **Toolbar**  > **Content List** ) and select **Monitor**.

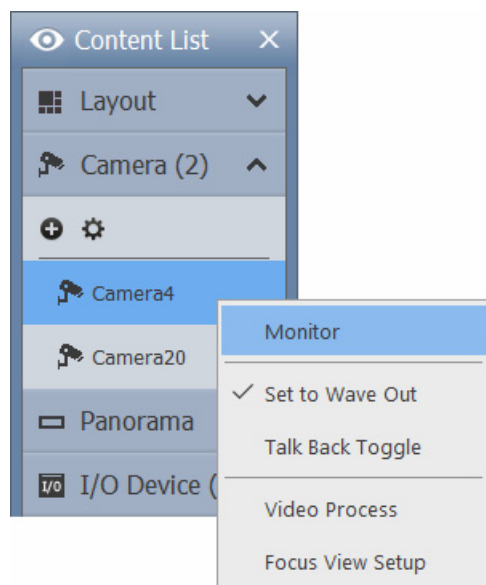





Figure 1-30

Note: Motion detection and I/O trigger will only be registered in System Log if monitoring is started. You will also need to enable Register Motion Event (Figure 1-16) and Register Input Event (Figure 6-7).

1.6 System Configuration

This section introduces system configurations of the GV-VMS.

1.6.1 Configuring General Setting

Let's start with the options on the General Setting dialog box. Changes made in the **General Setting** dialog box will be applied to the system. Click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **General Setting**. This dialog box appears.

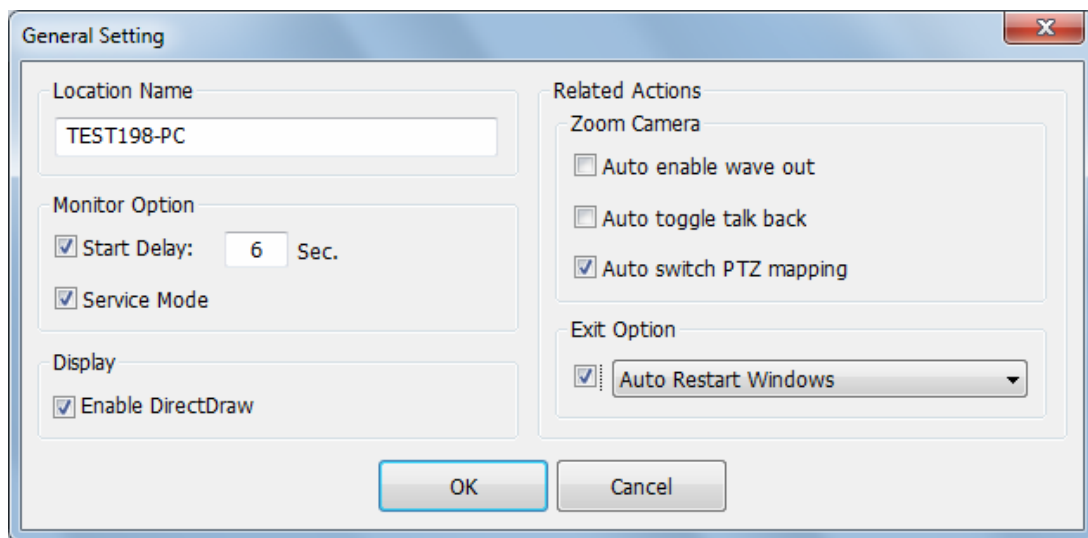


Figure 1-31

[Location Name] The given name (maximum 14 characters) is displayed in main screen as the name of the server.

[Monitor Option]

- **Start Delay:** Start recording x second(s) after **Start All Monitoring** or **Start I/O Monitoring** is selected.
- **Service Mode:** Under Service Mode, GV-VMS can start automatically after system startup and run in the background without logging into a Windows user account.

[Display]

- **Enable DirectDraw Scale:** Applies DirectDraw Scale to enhance image quality if your VGA card supports it. For certain VGA cards, DirectDraw Scale can result in blurred images. To avoid the image problem and maintain DirectDraw Scale, change the image quality from High to Standard [Video Setting] of the camera (Figure 2-4).

Note: The **Enable Directdraw Scale** function can greatly enhance image quality. Enable if your VGA card supports DirectX9. To check the version of your DirectX, click Start and run **dxdiag**. Open the file and find the related information.




[Zoom Camera]

- **Auto enable wave out:** Automatically enables Wave Out function of the camera in Zoom Window or in full screen. Note that the Wave Out function needs to be enabled in the Audio Setting page of the camera first.
- **Auto toggle talk back:** Automatically enables Toggle Talk Back function of the camera in Zoom Window or in full screen. Note that the Toggle Talk Back function needs to be enabled in the Audio Setting page of the camera first.
- **Auto switch PTZ mapping:** This function only applies to GV-Keyboards that are connected to GV-VMS. When selected, PTZ control from the GV-Keyboard will be applied to the selected PTZ camera. When not selected, the PTZ control buttons on GV-Keyboard will only be applied to the first available PTZ camera.

[Exit Option]

- **Auto Restart Windows:** Restarts Windows OS after exiting GV-VMS.
- **Auto Shut down Windows:** Shuts down Windows OS after exiting GV-VMS.

1.6.2 Customizing Startup Settings

The Startup dialog box allows you to set the system to enable selected features at system startup. To access the Startup settings, click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **Startup**. This dialog box appears.

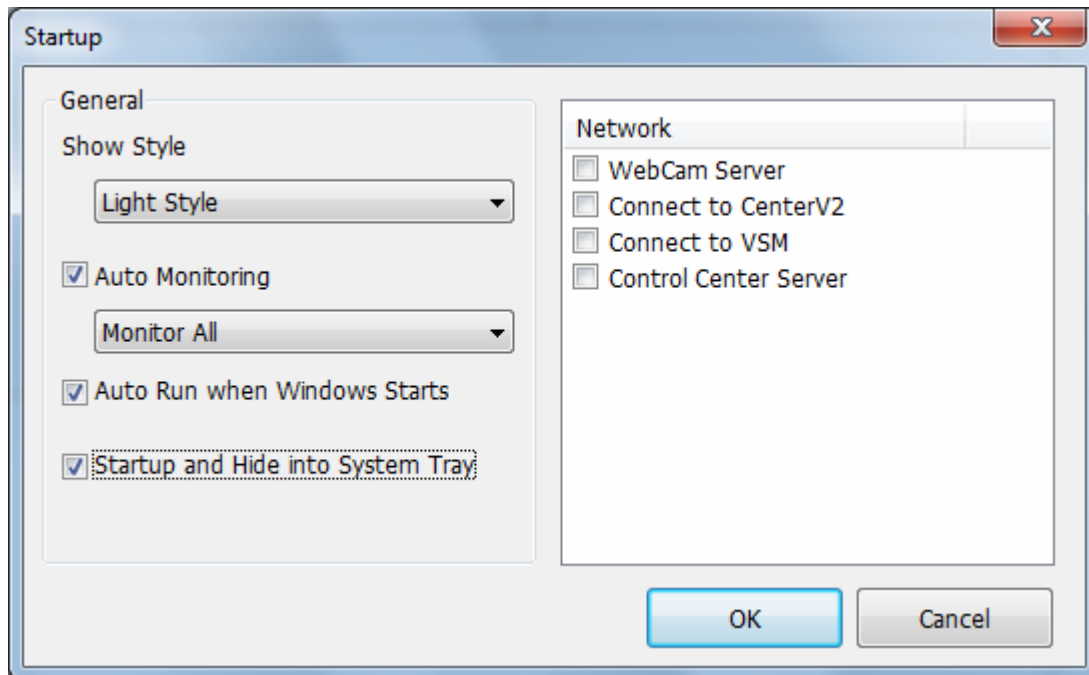


Figure 1-32

[General]

- **Show Style:** Change the color scheme of GV-VMS.
- **Auto Monitoring:** Select one of the following monitor control modes at system startup:
 - ⊙ **Monitor All:** Allows you to monitor all cameras and I/O (if available) at system startup.
 - ⊙ **Schedule Monitor:** Allows you to start monitoring cameras by schedule. Refer to *Schedule* later in this chapter.
 - ⊙ **I/O Monitor:** Allows you to monitor all I/O devices.
 - ⊙ **Camera Monitor:** Enables all cameras for monitoring.

Note: To manually start monitoring, click **Home** , click **Toolbar** , click **Monitor**  and select one of the functions.




- **Auto Run when Windows Starts:** Automatically runs GV-VMS after Windows starts. If you did not set an Auto Login account or an Auto Startup Login account, the Login dialog box will appear at startup asking for an account ID and password.
- **Startup and Hide into System Tray:** GV-VMS appears in the system tray when you launch Windows instead of displaying the system login window.






Note: **Startup and Hide into System Tray** and **Auto Startup Login** cannot function at the same time. When both are enabled, Auto Startup Login will not be applied. For details on Auto Startup Login, see *Setting a Startup Auto Login User* later in this chapter.

[Network]

- **WebCam Server:** Automatically enables connection to WebCam Server at system startup.
- **Connect to Center V2:** Automatically enables connection to Center V2 at system startup.
- **Connect to VSM:** Automatically enables connection to Vital Sign Monitor Server at system startup.
- **Control Center Server:** Automatically enables connection to Control Center Server at system startup.

Note: To manually enable the network connections listed above, click **Home** , click **Toolbar**  and click **Network** .

1.6.3 Customizing Display Position and Panel Resolution

You can customize the display settings of GV-VMS. Click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **Set Position**. This dialog box appears. The right side of the dialog box is only available when multiple monitors are installed.

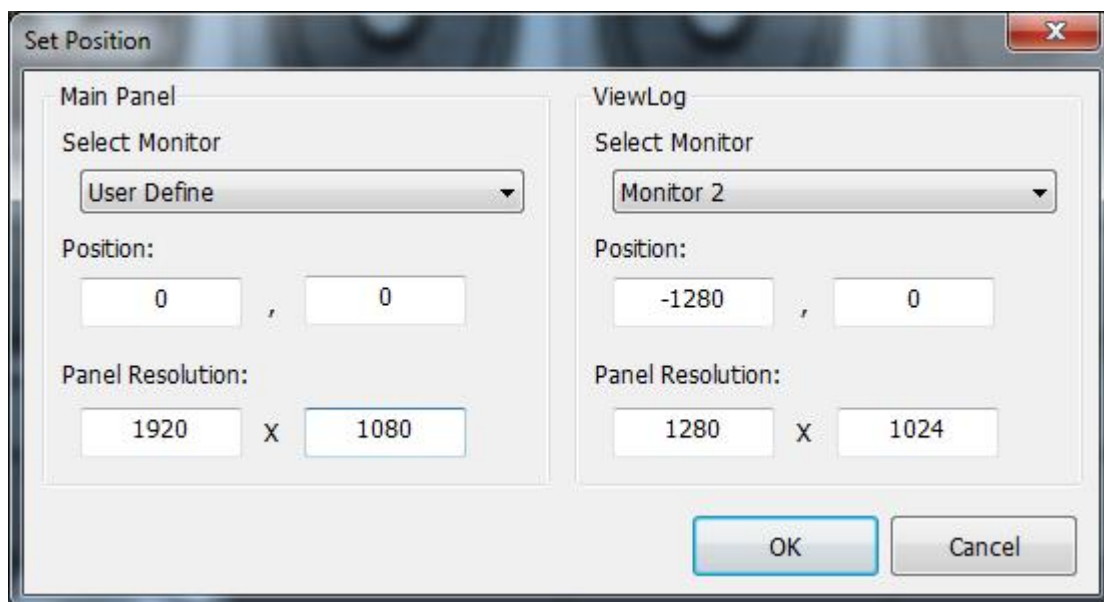


Figure 1-33

- **Select Monitor:** If you have multiple monitors connected, select the monitor you want to configure from the drop-down list.
- **Position:** Offsets the position of the GV-VMS window relative to the upper-left corner of the screen. The default position is 0, 0. A position of 100, 60 will place the GV-VMS window 100 pixels to the right and 60 pixels below the upper-left corner. This function is only supported when the GV-VMS window does not take up the entire screen.

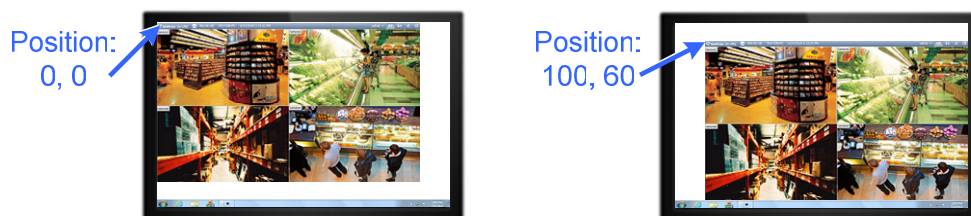





Figure 1-34

- **Panel Resolution:** Sets the Panel Resolution of the GV-VMS.

1.6.4 Setting Up Email Notification

When events occur, you can receive alert notification through e-mails. Follow the steps below to enable alert notification and set up the e-mail server.

The events that can trigger alert notification include: Video Lost, Recording Error, Disk Full, Motion Detection, I/O Trigger, Scene Change, Intruder Event, Missing Object, Unattended Object, Scene Change, Crowd Detection, Advanced Unattended Object, Advanced Scene Change Detection, Advanced Missing Object and Face Detection.

1. Click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **Send Alerts Approach Setup**. This dialog box appears.

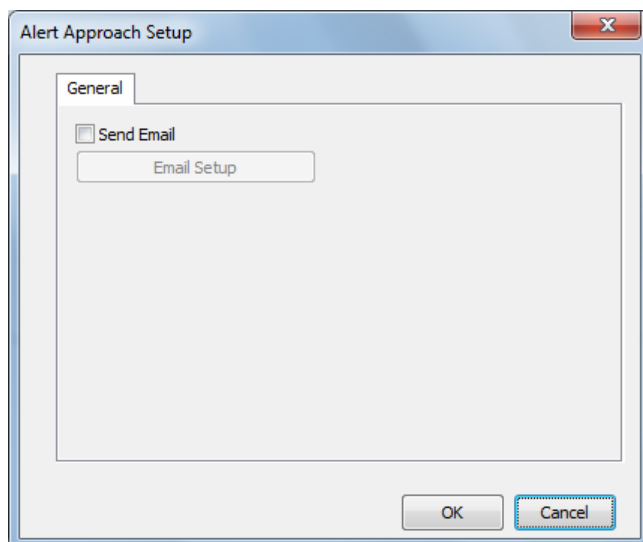
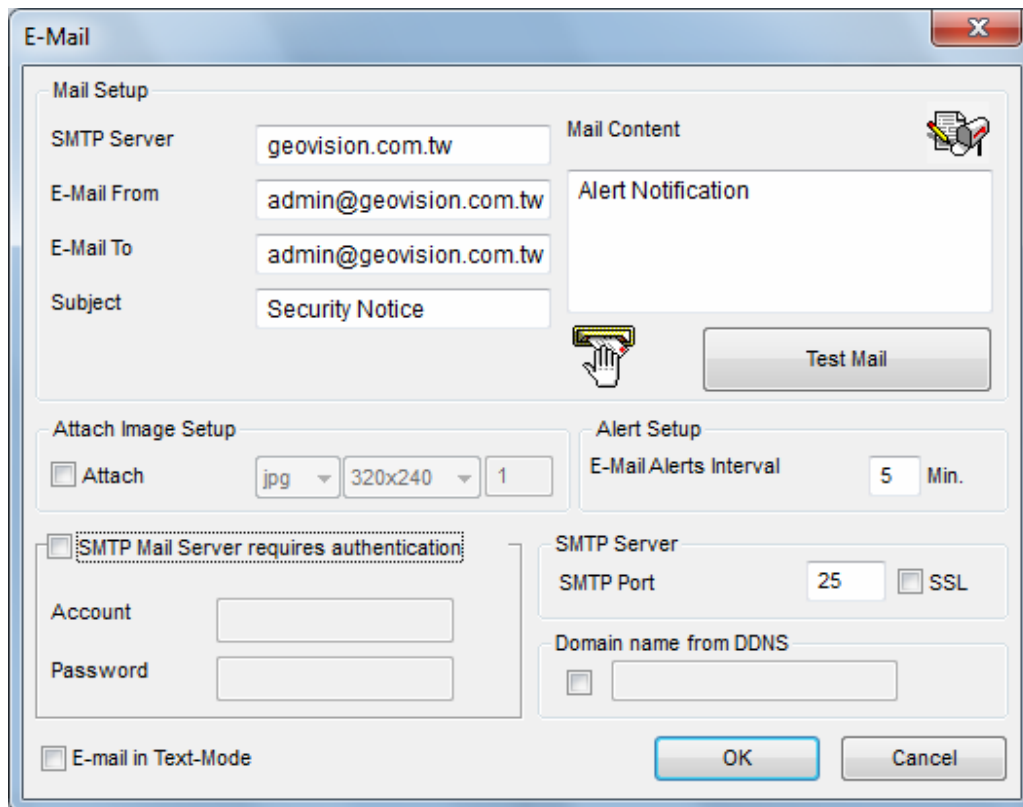


Figure 1-35

2. To enable e-mail notification, select **Send Email** and click **Email Setup**. This dialog box appears.



The image shows the 'E-Mail' dialog box with the following fields and options:

- Mail Setup:**
 - SMTP Server: geovision.com.tw
 - E-Mail From: admin@geovision.com.tw
 - E-Mail To: admin@geovision.com.tw
 - Subject: Security Notice
- Mail Content:** Alert Notification
- Attach Image Setup:**
 - ☐ Attach
 - Format: jpg
 - Size: 320x240
 - Count: 1
- Alert Setup:**
 - E-Mail Alerts Interval: 5 Min.
- SMTP Mail Server requires authentication:**
 - ☐ SMTP Mail Server requires authentication
 - Account: [Empty field]
 - Password: [Empty field]
- SMTP Server:**
 - SMTP Port: 25
 - ☐ SSL
- Domain name from DDNS:**
 - ☐ [Empty field]
- E-mail in Text-Mode:** ☐
- Buttons:** Test Mail, OK, Cancel

Figure 1-36

3. Set up the following fields (required):
 - **SMTP Server:** Type your mail server's URL address or IP address.
 - **E-Mail From:** Type the sender's e-mail address.
 - **E-Mail To:** Type recipients' e-mail addresses. For multiple recipients, add a semicolon between each e-mail address.
 - **Subject:** Type a subject for the e-mail alert.
4. Click the **Test Mail** button to send a test e-mail and see whether the setup is correct. If the e-mail fails to send, you may need to check the following settings:
 - **SMTP Mail Server requires authentication:** If the SMTP mail server needs authentication for login, select this option and type your account name and password.
 - **SMTP Server:** Keep the default port 25 which is common for most SMTP servers. However webmail providers such as Gmail, Yahoo, and Hotmail generally use different SMTP port. In this case, check your e-mail provider for the SMTP port number. Select **SSL** if your e-mail server requires the SSL authentication for connection.




5. Complete other optional settings as needed:

- **Mail Content:** Type the e-mail content that will be included in all e-mail notifications.
- **Attach Image Setup:** Select **Attach** to include up to 6 snapshots in the e-mail. The image format and size are selectable from drop-down lists.
- **Email-Alerts Interval:** Specify the time interval (0-60 seconds) between e-mail alerts to prevent e-mails from being sent too frequently. The default interval is 5 minutes, which means that if motion lasts for more than 15 minutes, you will receive 3 e-mails at most. If motion lasts for less than 5 minutes, you will receive one e-mail only.
- **Domain Name from DDNS:** This option generates URL links for remote video playback in the sent e-mails. For this function to work, enter the fixed IP address or domain name of the GV-VMS, and enable **WebCam Server**.
- **E-mail in Text Mode:** When **WebCam Server** is enabled, your e-mail alert will be sent in HTML format. If you want to send the e-mail alert in pure text format, select this option.

Note: To enable WebCam Server, click **Home** , click **Toolbar** , click **Network**  and click **WebCam Server**.

1.6.5 System Idle Protection

When the computer is idle over a set period of time, the System Idle Protection can automatically log out the administrator, and/or start monitoring.

1. Click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and select **System Idle Protection Setting**. This dialog box appears.

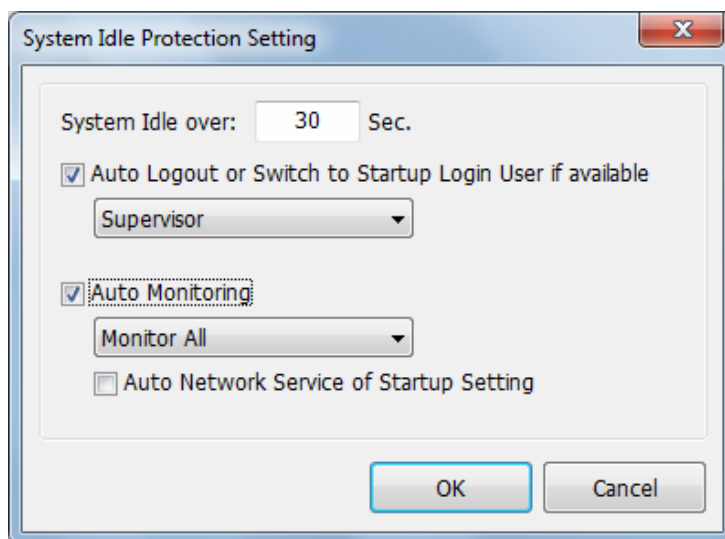


Figure 1-37

2. To automatically log out or switch to Startup Auto Login User, select **Auto Logout or Switch to Startup Login User if available**, and then select the type of account to log out from the drop-down list.

If you have set up a Startup Auto Login User, GV-VMS will switch to the Startup Login User instead of logging out. The Startup Auto Login User is typically a user account with limited access rights. For details, see *Setting a Startup Auto Login User* later in this chapter.




3. To automatically start monitoring, select **Auto Monitoring**, and use the drop-down list to select **Monitoring All**, **Schedule Monitoring**, **I/O Monitoring** or **Camera Monitoring**. When Monitoring All is selected, both I/O Monitoring and Camera Monitoring will be enabled.
 - Select **Auto Network Service of Startup Setting** to enable network connections selected in Startup Setting (WebCam Server, CenterV2, Vital Sign Monitor, Control Center Server, Backup Server (GV-Failover Server and GV-Redundant Server) and/or Backup Center). To specify which network connections to enable at startup, see *Customizing Startup Settings* earlier in this chapter.

4. In the **System Idle Over** field, type an idle time between 10 and 14400 seconds, after which the settings configured in Step 2 or 3 will be applied.
5. Click **OK**.

Note: The feature can monitor keystrokes or mouse clicks, even from IR Remote Control and GV-Keyboard.

1.6.6 Configuring Fast Key Lock

If you do not want to use certain fast keys to avoid interfering with keyboard use, you can disable the fast key functions.

1. Click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and select **Fast Key Lock Setup**. This dialog box appears.

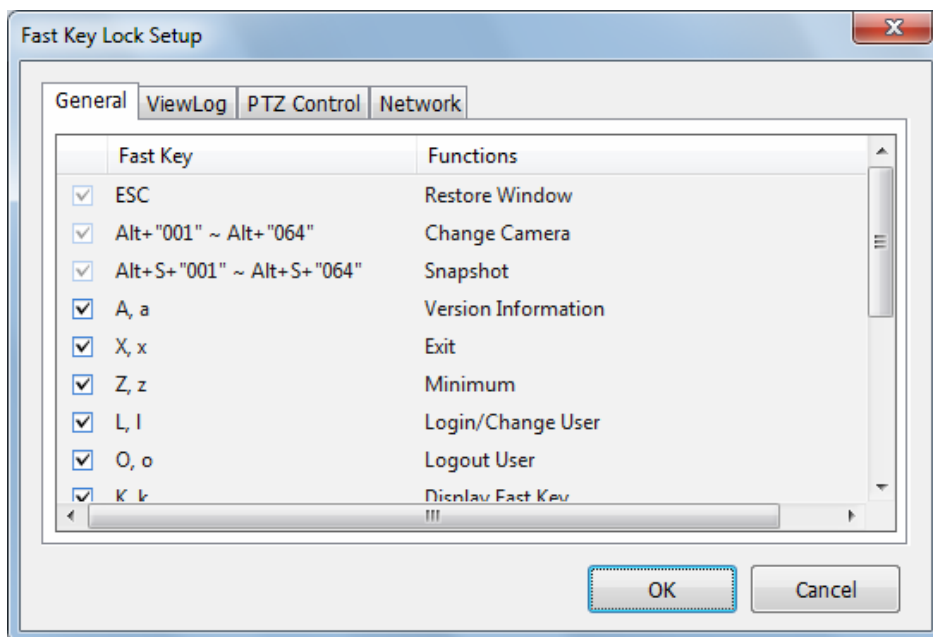


Figure 1-38

2. Select one of the four tabs: General, ViewLog, PTZ Control and Network.
3. Clear the checkmark for the fast keys you want to disable. To restore the fast keys, select the checkbox again.
4. Click **OK** to apply your settings.

1.7 Account and Password

The password setup allows you to assign permission and rights to accounts. You can create up to **1,000** passwords. The system will control access to functions based on the permission and rights configured for each account. Only Supervisor-level accounts are pre-set with access to the Password Setup function. Click the account ID, click **Password Setup**, and select **Local Account Edit**. This dialog box appears.

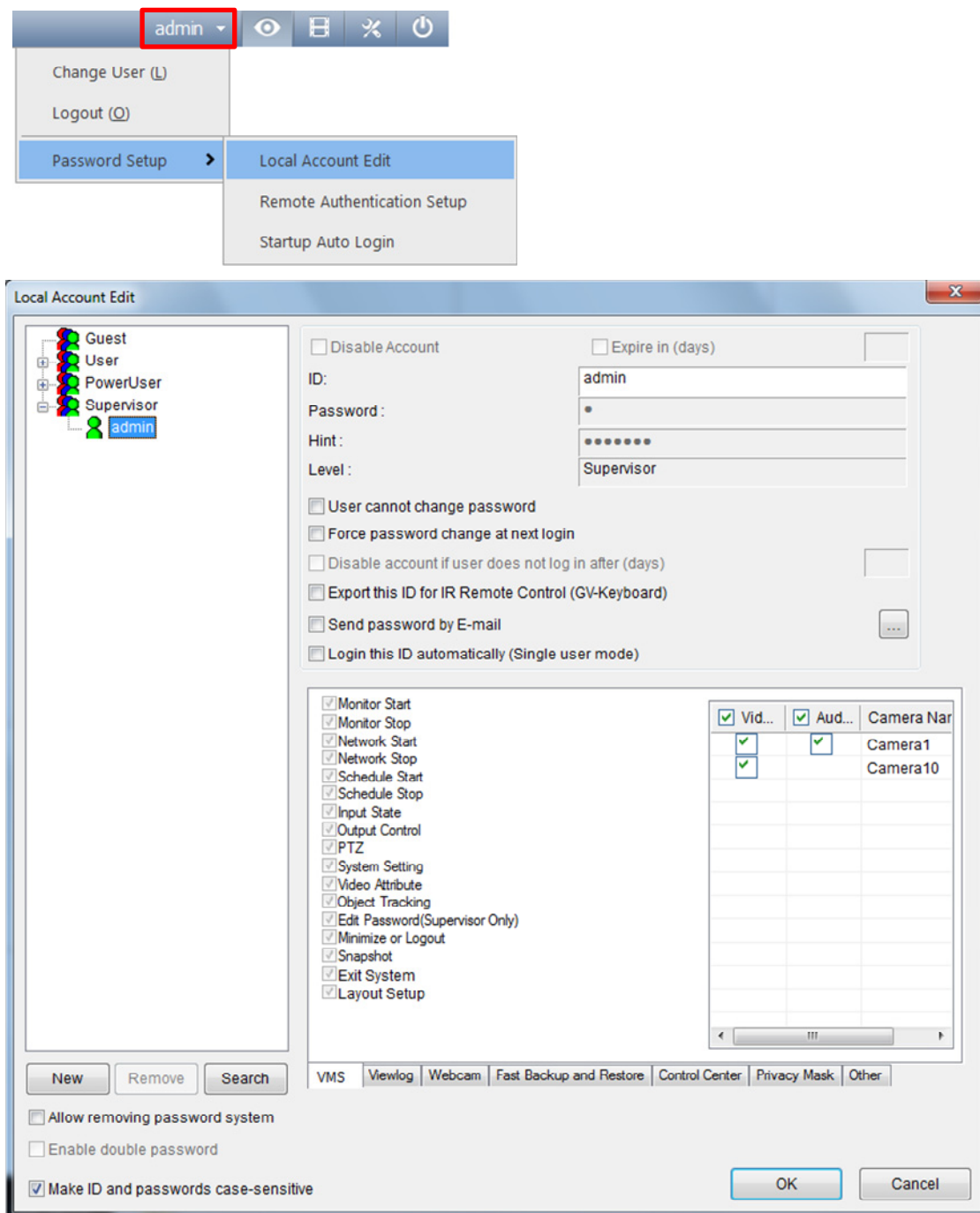
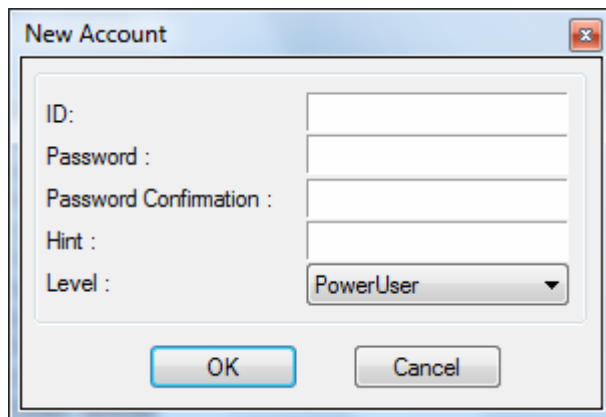


Figure 1-39

1.7.1 Creating a New Account

To create a new account:

1. Click the **New** button at the lower-left hand corner. This dialog box appears.



The 'New Account' dialog box is a standard Windows-style window with a title bar containing the text 'New Account' and a close button (X). The main area contains five labeled text input fields: 'ID:', 'Password:', 'Password Confirmation:', 'Hint:', and 'Level:'. The 'Level:' field is a dropdown menu currently showing 'PowerUser'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

Figure 1-40

2. Type the user's **ID** name and **password**. Re-enter the same password in the Password Confirmation field.
3. Give a **Hint** (optional) that would remind you of the password.
4. Select the account's authorization level: **Supervisor**, **PowerUser** or **User**.
 - Accounts belonging to the Supervisor level have permissions over all GV-Vital Sign Monitor settings.
 - By default, PowerUsers have the same permission and rights as Supervisors, except that they cannot edit user information and delete the password system (described later).
 - Accounts belonging to the User level are restricted from all system settings, and have only limited access to certain functions.
5. Click **OK** to add the user.
6. If you want to enable the guest account, click **Guest** and clear the selection for **Disable Account**. Guests are only allowed to watch live view.

After an account is created, only supervisors are allowed to edit the account in the future. To edit, select an account from the account list. Or, right-click an account level (User, PowerUser, Supervisor), and click **Find Specific Account** for a quick search. A valid password is required to edit a supervisor.

1.7.2 Configuring Account Settings

You may find these options to the right of the account list depending on the authorization level.

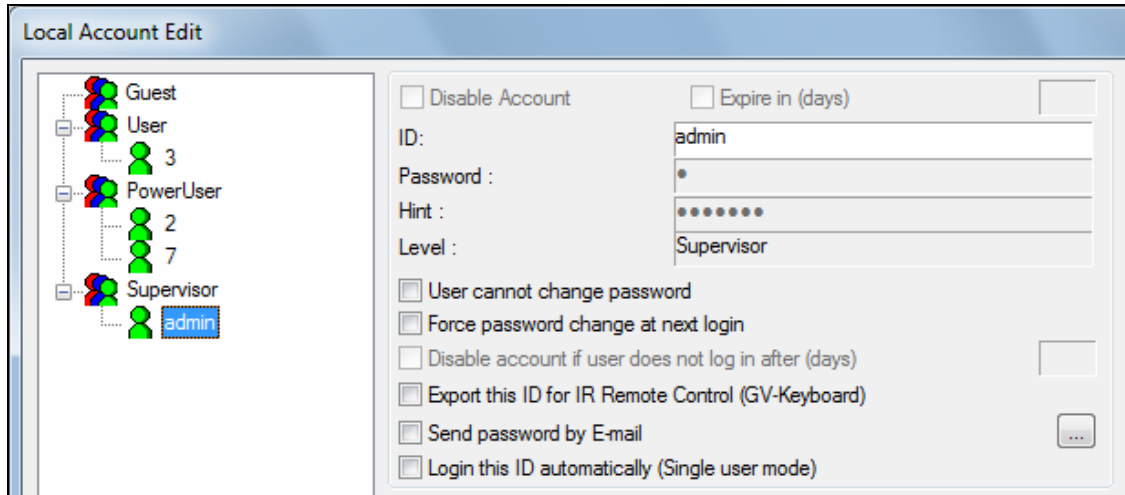


Figure 1-41

- **Disable Account:** Select if you want to disable this account.
- **Expire in xx day(s):** The account will expire and be disabled automatically after a set number of days. The number you set will count down automatically. Specify the number between 1 and 9999.
- **User cannot change password:** The user is not allowed to change the set password.
- **Force password change at next login:** The user must change the password at next login.
- **Disable account if user does not login after xx day (s):** When the user does not log in the system after a set number of days, its account will be disabled automatically.
- **Export this ID for IR Remote Control:** Allows you to log into the system by using the GV-Keyboard instead of using the general keyboard and mouse. For details see *GV-Keyboard User's Manual*.
- **Send password by Email:** Allows you to retrieve passwords through e-mails. To specify e-mails, click the [...] button. For details on this feature, see *Changing or Retrieving Password at Login* later in this chapter.
- **Login this ID automatically (Single User Mode):** GV-VMS will automatically log into this account after you click **Login** at startup.

At the bottom of the page are global settings, which are applied to all accounts.

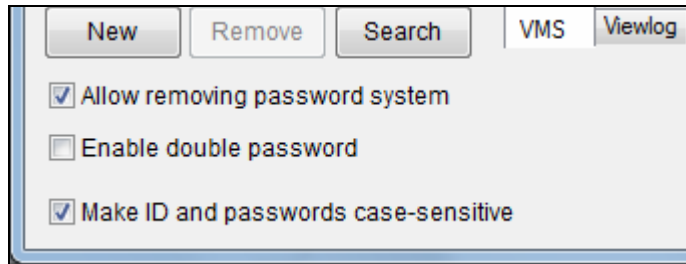


Figure 1-42

- **Allow removing password System:** Enables the password removal utility. The option is critical if you forget or is unable to retrieve any Supervisor password. With this option selected, you can run the password removal utility **PassUNINStall.exe** from the GV folder and remove the password database. Otherwise, you can only remove the password database by reinstalling Windows operating system.
- **Enable double password:** When selected, after clicking ViewLog, you will need to type the passwords of any two supervisors to be able to continue. This option is only available when at least two supervisor accounts have been created.
- **Make ID and passwords case-sensitive:** Select to make account ID and passwords case-sensitive.

Note: The loss of passwords can be solved in the following two ways:

1. Retrieving password through e-mails.
2. Removing password database by using the *PassUNINStall.exe* utility and rebuilding all accounts.

However, if both **Send Password by Email** and **Allow Removing Password System** options are not selected in advance, it is required to reinstall Windows operating system once you loss the passwords.

1.7.3 Changing or Retrieving Password at Login

When logging in GV-VMS, the Login dialog box allows you to change password or retrieve password through e-mail.

Changing Password

1. In the Login dialog box, click the **Change Password** button. The Change Password dialog box appears.

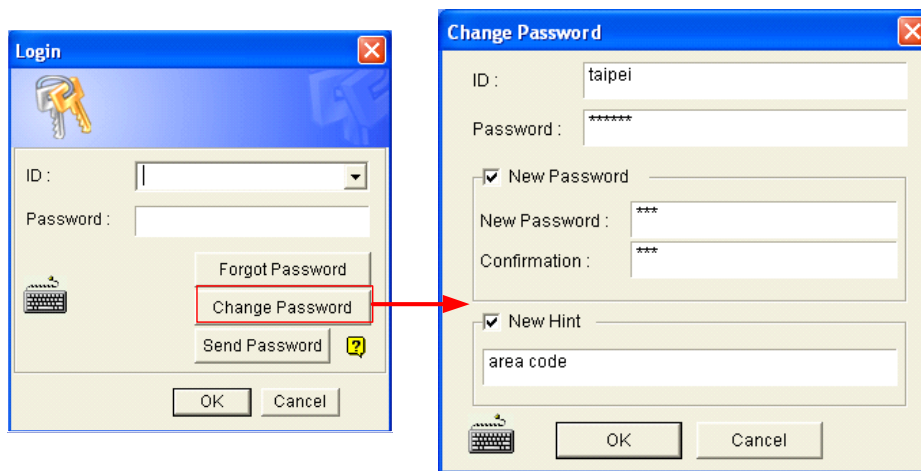


Figure 1-43

2. Type the new password information, and click **OK** to save the changes.

Note: Only Supervisors can change the password.

Retrieving Password through E-mail

The password retrieval function works in the following ways after you click the **Send Password** button in the Login dialog box.

- If you are one of supervisors but do not remember your ID, separate passwords will be sent to all supervisor e-mail accounts after you click the **Send Password** button.
- If you are one of the supervisors and remember your ID but forgot your password, enter your ID and then click the **Send Password** button. The password will be sent to your e-mail account.
- If you are not a supervisor, enter your ID and then click the **Send Password** button. The e-mail with your password will be sent to you.

1.7.4 Preventing Unauthorized System Termination

The GV-VMS can be protected from stopping or restarting by an unauthorized account. To restrict an account that does not belong to the **Supervisor** level from exiting or restarting the system, follow the steps below:

1. Click the account ID, click **Password Setup**, and select **Local Account Edit**. The Password Setup dialog box appears.
2. Select a user from the user list to display its properties.
3. Select the **VMS** tab at the bottom, and clear the **Exit System** option to restrict the user from quitting or restarting the system.

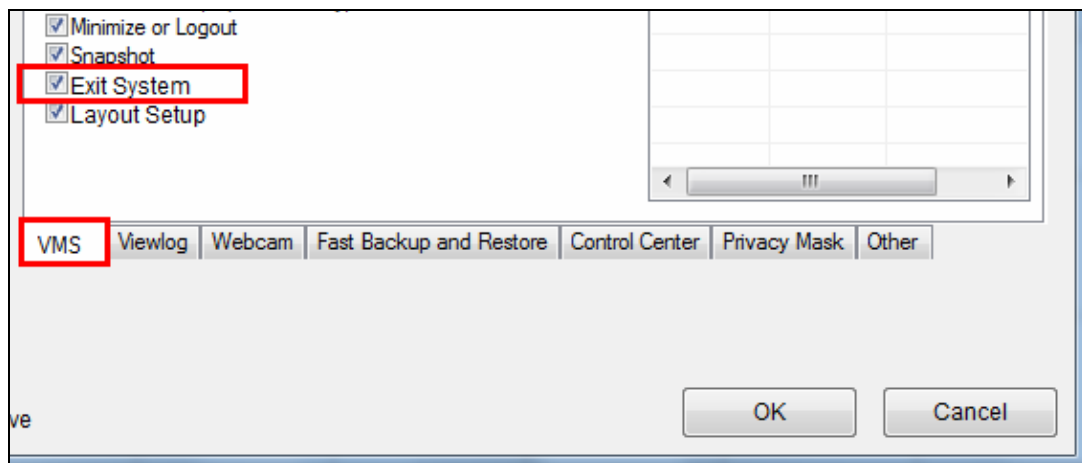


Figure 1-44

1.7.5 Setting a Startup Auto Login User

The Startup Auto Login User is typically a user account with limited access rights. After system is started, the GV-VMS will automatically log in with the Startup Auto Login User instead of showing the Login dialog box. The user can see that the system is on and working, but cannot tamper with the system settings.

1. Create an account you want to use for Startup Auto Login. Refer to *Creating an Account* earlier in this section for instructions.
2. Click the account ID, click **Password Setup**, and select **Startup Auto Login**. This dialog box appears.

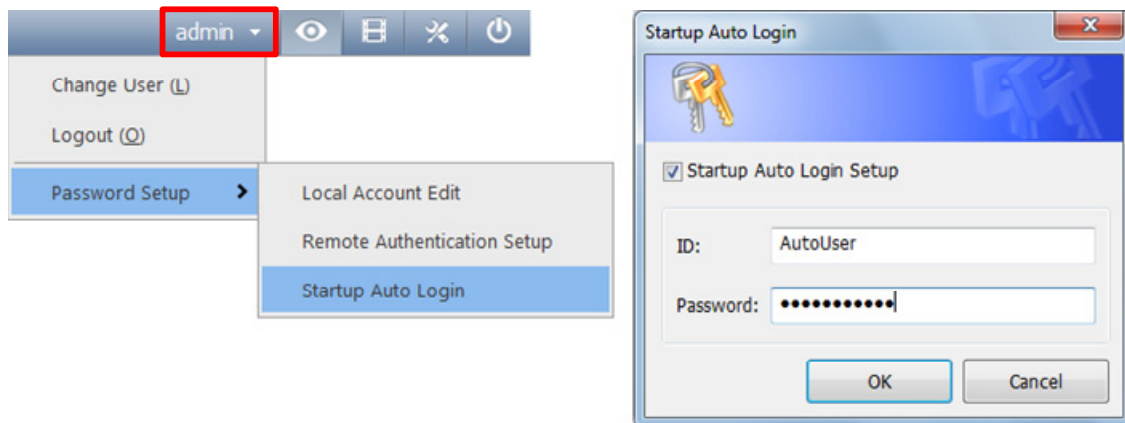


Figure 1-45


3. Select **Startup Auto Login Setup**.
4. Type the ID and Password of the existing account you want to use.
5. Click **OK**.

If you have selected **Auto Logout or Switch to Startup Login User if available** in System Idle Protection Setting dialog box (Figure 1-37), GV-VMS will switch to the Auto Startup Login account after a period of system idle.

1.8 Schedule

You can create schedules to enable and disable the following functions at specific times of a day and apply the schedule to a weekly plan, monthly plan or a specific date.

- Recording
- Alert upon motion detection
- PTZ object tracking
- PTZ Auto functions
- Video Processing
- I/O monitoring
- Network connections to Center V2 and/or Vital Sign Monitor

Click **Home** , select **Toolbar** , select **Configure** , and then select **Schedule Edit**. This dialog box appears.

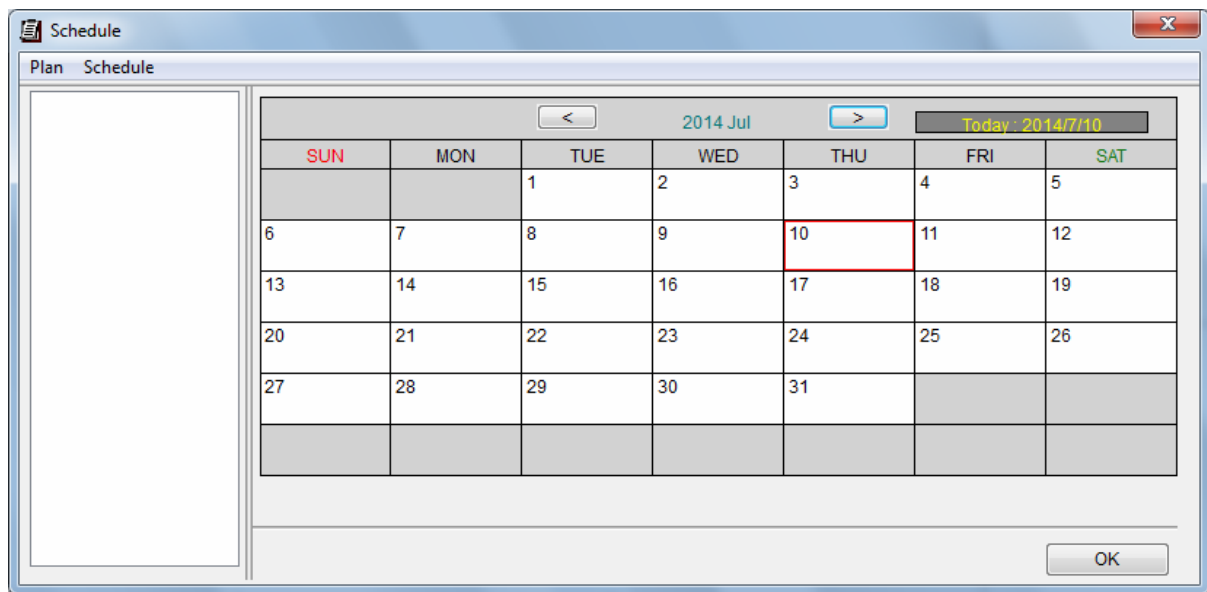


Figure 1-46

1.8.1 Creating a Schedule with Setup Wizard

The Setup Wizard is an easy way to create new schedule.

1. In the Schedule dialog box, click **Schedule** and select **Setup Wizard**. A dialog box appears.
2. Specify when to apply the schedule plan and click **Next**.

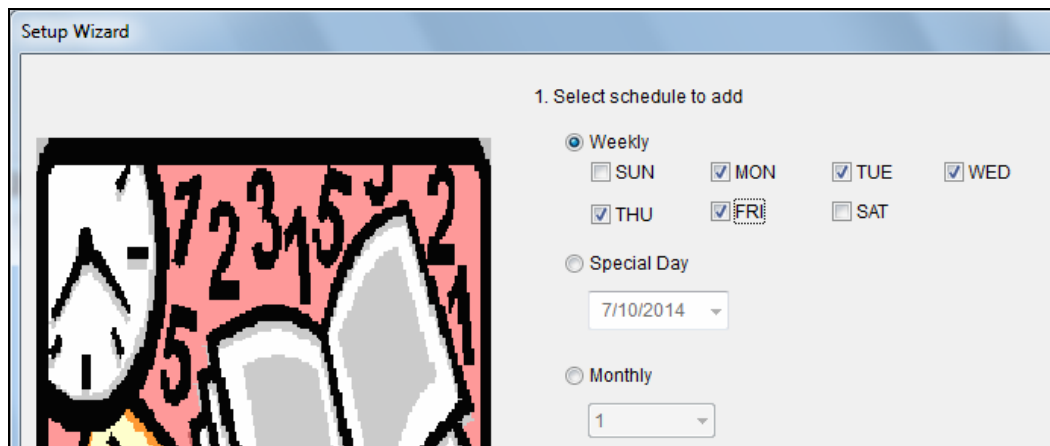


Figure 1-47

- **Weekly:** Applies the schedule plan to the selected days each week.
- **Special Day:** Applies the schedule plan to a specific date each year.
- **Monthly:** Applies the schedule plan to a specific day each month.

Note: You can apply the schedule plan to additional days or modify the time settings later. After the schedule plan is created, refer to Step 3 in *Creating a Schedule Manually* later in this section.

3. Type a name for the schedule plan. If you have existing schedule plans, you can select **Use current plan** and apply the selected plan to different days.

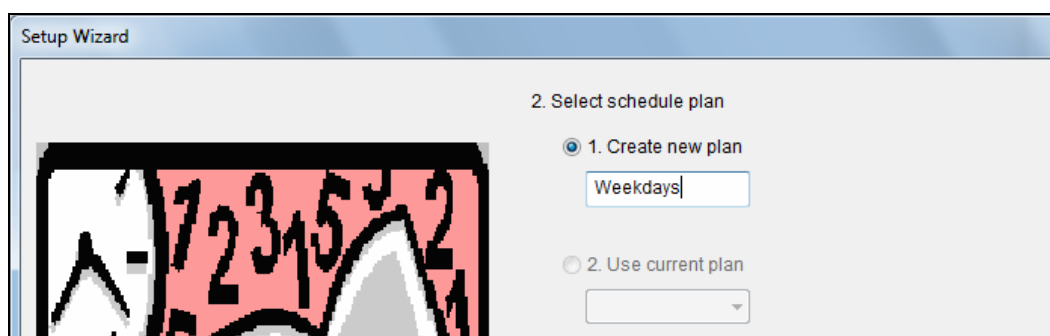


Figure 1-48

- Click **Next**. This dialog box appears.

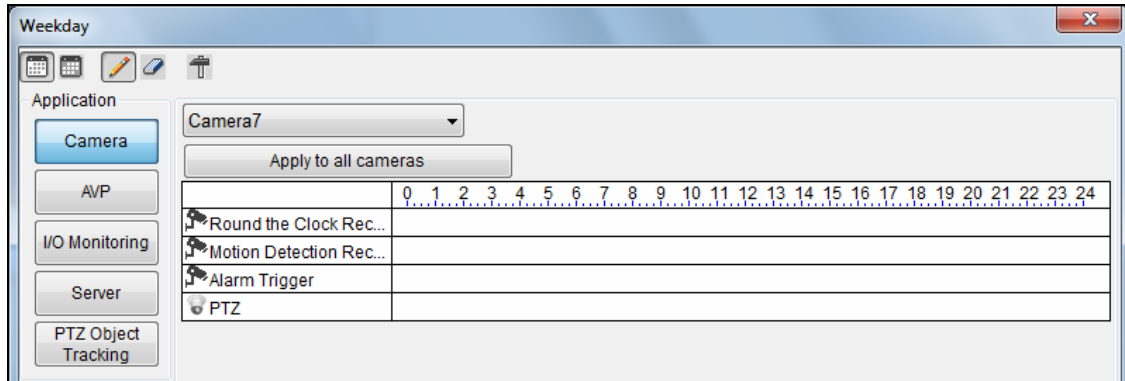





Figure 1-49

- When the **Include** button  is selected, you will start with an empty timeline. Click the **Add** button  and drag across the timeline when you want the function to be enabled. Use the **Erase** button  when you want disable the function.

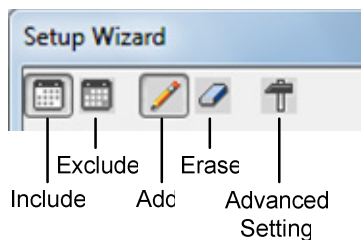






Figure 1-50

- You can also click the **Exclude** button  and start with everything disabled. The **Add** button  is now used for disabling the function instead and the **Erase** button  is now used for enabling the function.
- Four categories are available on the left.

■ **Camera:**

- ⊙ **Round-the-Clock Recording:** When highlighting the timeline, you can choose to apply the frame rate settings for **General Event** or **Urgent Event**. The settings here will override the settings in Record Setting once schedule monitoring is started. For information on General Event and Urgent Event, refer to *Configuring General Setting*, Chapter 2.
- ⊙ **Motion Detection Recording:** When highlighting the timeline, you can apply different motion sensitivity levels. If you select **User Define**, the sensitivity level selected in Advanced Motion Detection Setup (Fig 1-16) will be used.
- ⊙ **Alarm Trigger** The Event Trigger methods selected in Advanced Motion Detection Setup (Fig 1-16) will be triggered upon motion during the highlighted times.

- **PTZ:** When highlighting the timeline, you can select a PTZ Auto function to enable during that time. This option only appears when at least one PTZ camera is connected.
 - **AVP:** During the enabled times, the selected video processing functions will be enabled even if the cameras are not recording.
 - **I/O Monitoring:** Enables I/O Monitoring.
 - **Server:** Enables network connections to Center V2 and/or Vital Sign Monitor.
8. To apply the Camera and AVP schedules to selected cameras, use the camera drop-down list above the timeline or click the **Advanced Setting** button .
 9. Click **OK**. The schedule plan created appears on the days you specified.

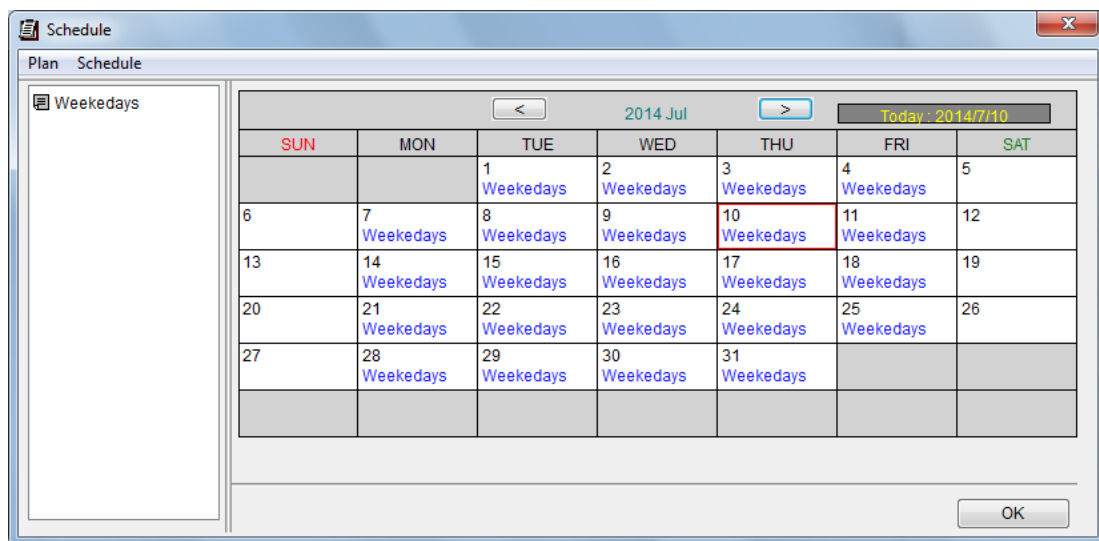


Figure 1-51

Tip:

1. You can drag the created plan on the left of the Schedule dialog box to the calendar on the right and the plan will be apply to the date.
2. To edit the schedule timeline, simply double-click the plan in the calendar.

1.8.2 Creating a Schedule Manually

To manually create a schedule:

1. In the Schedule dialog box, click **Plan** and click **Add**. A dialog box appears.

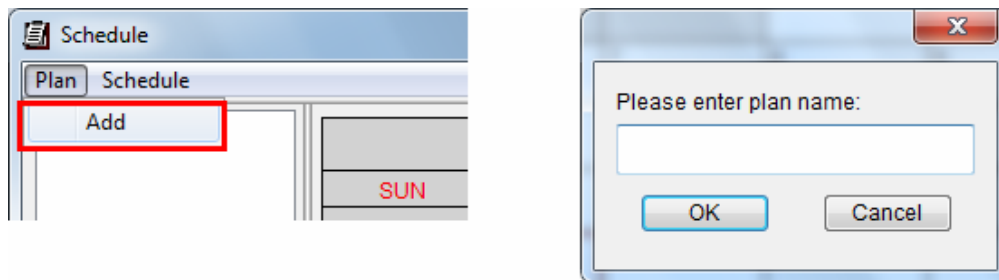


Figure 1-52

2. Type a name for the plan and click **OK**.
3. Click **Schedule** and select an option below:
 - **Edit Special Day:** Applies the schedule plan to a specific date each year. Select a **Date** and a **Plan**, and then click the **Add** button.
 - **Edit Weekly:** Applies the schedule plan to the selected days each week.
 - **Edit Monthly:** Applies the schedule plan to a specific date each month. Select a **Day** of the month and a **Plan**, and then click the **Add** button.
4. Double-click the Plan to edit the schedule timeline. Refer to *Creating a Schedule with Setup Wizard* earlier in this section for details.

1.8.3 Exporting and Importing Schedule Settings

You can export your current schedule settings into an .xml file, and import it back later or to GV-VMS on another computer.

To Export:

1. In the Schedule dialog box, click **Schedule** and click **Export**. A dialog box appears.
2. Specify the path to save the .xml file.
3. Click **OK**.




To Import:

1. In the Schedule dialog box, click **Schedule** and click **Import**. A dialog box appears.
2. Specify where the exported .xml file is stored.
3. Click **OK**.

1.9 System Log

System Log provides historical information that can help you track down events, system problems and object counting data.

1.9.1 Setting System Log

In System Log Setting, you can specify which events to record, the interval time to write the event into the system, and the number of days to keep the logs. To access System Log Setting, click **ViewLog** button , select **Toolbar** , select **Configure** , and then select **System Log Setting**. This dialog box appears.

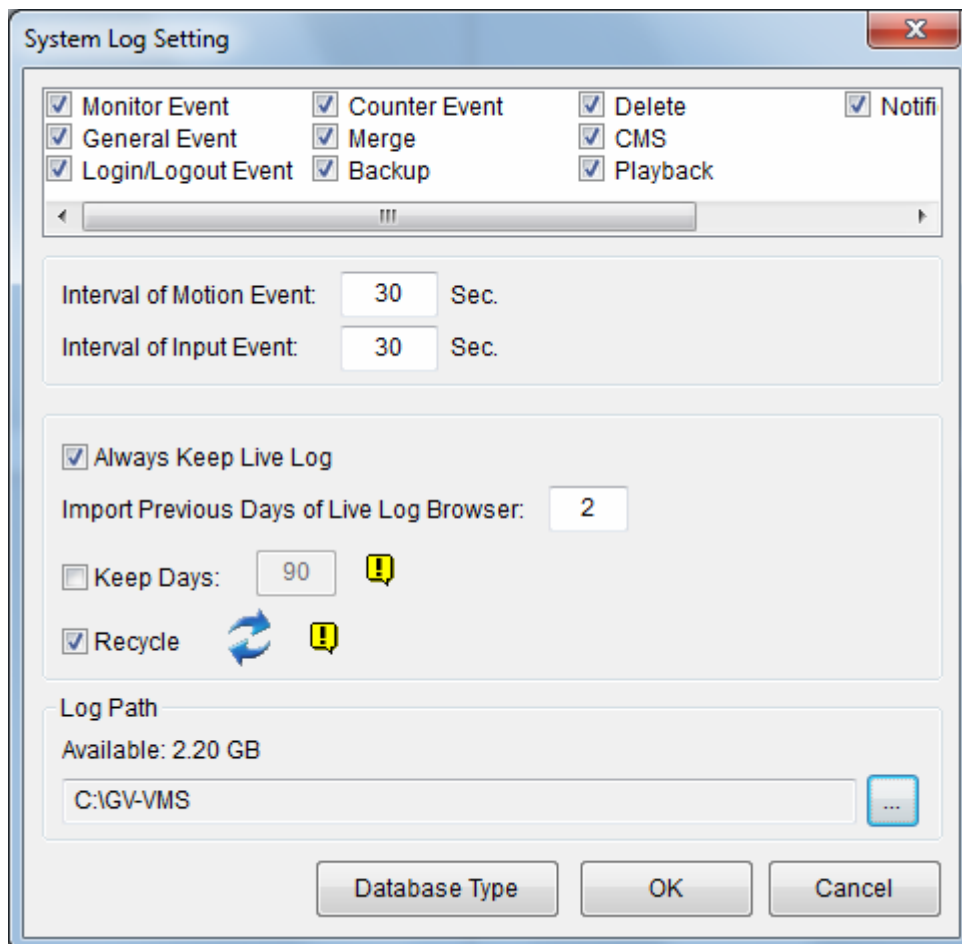


Figure 1-53

Select the types of event to register in System Log:

- **Monitor Event:** Registers motion-triggered and I/O-triggered events. For this feature to work, you must enable the **Register Motion Event** option in Figure 1-11 or the **Register Input Event** option in Figure 6-7 in Chapter 6.




- **General Event:** Registers system startup/exit, network server start/stop, and monitoring start/stop.
- **Login/Logout Event:** Registers the login/logout activities of local users to GV-VMS and WebCam Server.
- **Counter Event:** Registers counting results.
- **Merge:** Registers merging of recorded videos.
- **Backup:** Registers backing up of recorded videos.
- **Delete:** Registers deletion of recorded videos through remote connection.
- **CMS:** Registers CMS related events.
- **Playback:** Registers playback of recorded videos.
- **Notification:** Registers email notifications.

The following settings are available:

- **Interval of Motion Event:** Specifies the log interval between motion-triggered events. This setting could prevent the System Log from becoming too large in a motion-intensive surveillance area.
- **Interval of Input Event:** Specifies the log interval between I/O-triggered events.

- **Always Keep Live Log:** When selected, the current log will be displayed in system log. When not selected, system log of the time selected in ViewLog timeline will be displayed if available.
- **Import Previous Days of Live Log Browser:** Specifies how many days of data to be loaded into the System Log.
- **Keep Days:** Set the number of days to keep logs.
- **Recycle:** Enable the system to delete old log files to make space for new files when the space of assigned Log Path is below 500 MB.
- **Log Path:** Click the ... button to specify a storage path. The default log path is :\\GV folder\\. The available free space of the storage path will be displayed above.
- **Database Type:** To choose how to save your system database, select **Microsoft Office Access Database** or select **Microsoft SQL Server** and fill out the required fields

1.9.2 Viewing System Log

To view the System Log, click **ViewLog** , select **Toolbar** , select **Tools** , and then select **System Log**. Three options are available: Monitor Table, CMS Table, and Advanced.

Monitor Table

Local events on GV-VMS are displayed.

Monitor Table

Monitor

System

Login

Counter

Merge

Backup

Delete

Notification

I/O

Playback

| Time | Device | Information | Event | Note |
|--------------------|---------|-------------|--------------------|------|
| 12/3/2014 11:58:41 | Camera1 | | Motion | |
| 12/3/2014 11:59:26 | Camera1 | | Motion | |
| 12/3/2014 11:59:45 | Camera4 | | Camera Connecti... | |
| 12/3/2014 11:59:46 | Camera4 | | Camera Connecti... | |
| 12/3/2014 12:00:05 | Camera1 | | Motion | |
| 12/3/2014 12:00:49 | Camera1 | | Motion | |
| 12/3/2014 12:01:21 | Camera1 | | Motion | |

Figure 1-54

[Monitor] Shows events related to camera connection and motion. Double-clicking an event will allow you to view the related video (if available) in ViewLog.

[System] Shows system startup/exit, network server start/stop, and monitoring start/stop.

[Login] Shows whom and when has logged in and out of GV-VMS and WebCam server.

[Counter] Shows information and results of GV-VMS's counter functions.

[Merge] Shows merging event of recorded videos.

[Backup] Shows backup event of recorded videos.

[Delete] Shows deletion of recorded videos through remote connection.

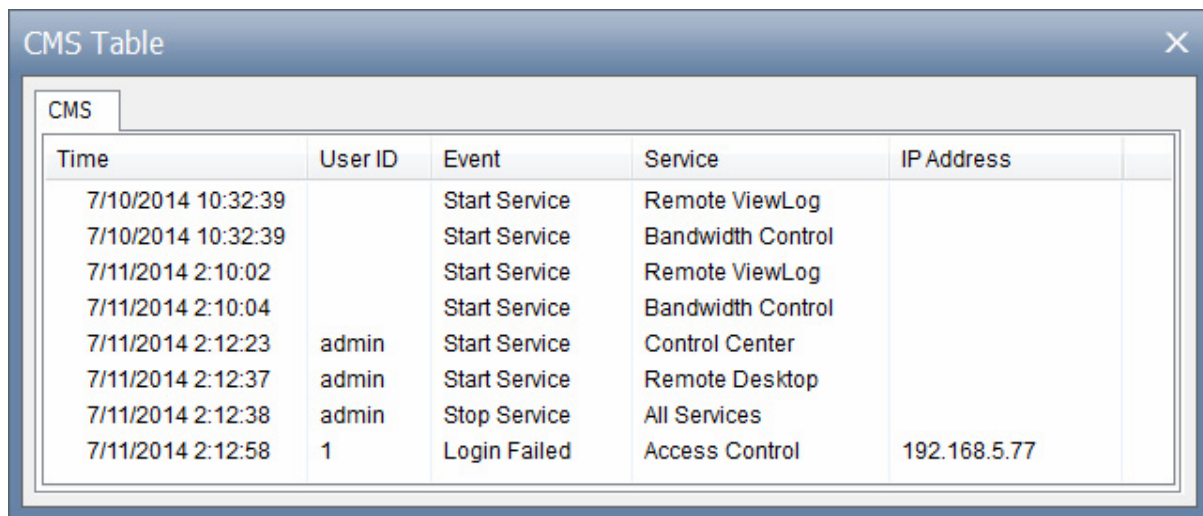
[Notification] Shows email notifications.

[I/O] Shows events related to I/O trigger.

[Playback] Shows playback of recorded videos.

CMS Table

CMS Table shows the connection status, login activities and service start related to CMS.



The screenshot shows a window titled "CMS Table" with a close button (X) in the top right corner. Inside the window, there is a tab labeled "CMS" and a table with the following data:

| Time | User ID | Event | Service | IP Address |
|--------------------|---------|---------------|-------------------|--------------|
| 7/10/2014 10:32:39 | | Start Service | Remote ViewLog | |
| 7/10/2014 10:32:39 | | Start Service | Bandwidth Control | |
| 7/11/2014 2:10:02 | | Start Service | Remote ViewLog | |
| 7/11/2014 2:10:04 | | Start Service | Bandwidth Control | |
| 7/11/2014 2:12:23 | admin | Start Service | Control Center | |
| 7/11/2014 2:12:37 | admin | Start Service | Remote Desktop | |
| 7/11/2014 2:12:38 | admin | Stop Service | All Services | |
| 7/11/2014 2:12:58 | 1 | Login Failed | Access Control | 192.168.5.77 |




Figure 1-55

Advanced Log Browser

To search for log data, click **ViewLog** , select **Toolbar** , select **Tools** , select **System Log** and click **Advanced** to bring up the Advanced Log Browser. See *Advanced Log Browser* in Chapter 4.

1.10 Other Functions

1.10.1 Setting Live View Pop-Up Video

The live view can pop up immediately whenever motion detection or input trigger occurs. To set up, click **Home** , select **Toolbar** , select **Configure** , select **System Configure**, and click **Camera Popup Setting**. This dialog box appears.

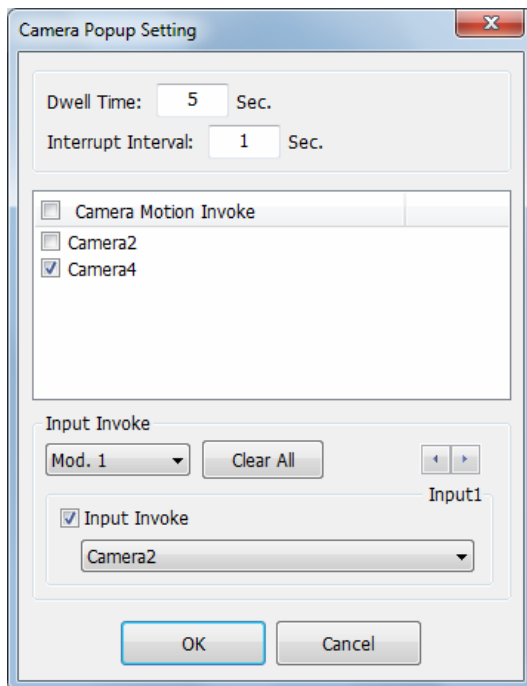


Figure 1-56

- **Dwell Time:** Specify the amount of time a pop-up live video to remain in the foreground.
- **Interrupt Interval:** Specify the interval between live video pop-ups. This feature is useful when several cameras are activated for a pop-up alert at the same time.
- **Camera Motion Invoke:** Select the camera to enable auto pop-up upon motion detection. Note that you need to start monitoring on the camera for this function to work.
- **Input Invoke:** Select an input module using the drop-down list and select the input number using the arrow buttons. Select **Input Invoke** and assign a camera to the input device. Whenever the input is triggered, the live video of the assigned camera will pop up. Note that you need to start I/O monitoring for this function to work.

Note: You can use the **Mask Region** function in the Advanced Motion Detection Setup dialog box (Figure 1-16) to mask off certain areas of the camera image that you don't want to detect motion.

1.10.2 Adjusting to Daylight Saving Time

GV-VMS can automatically adjust to Daylight Saving Time (DST). If you are in a time zone that uses DST, make sure DST is enabled. In Windows' Control Panel, go to **Date and Time**, click **Change Time Zone**, and make sure **Automatically adjust clock for Daylight Saving Time** is selected.

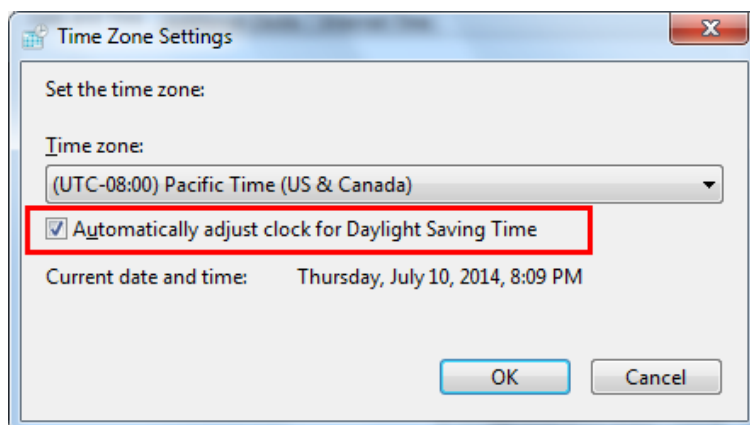


Figure 1-57

In System Log, the DST events will be labeled in the **DST Rollback** column.

| Monitor Table | | | | | | |
|-------------------|---------|-------------|---------|-------|--------------|--------|
| Monitor | System | Login | Counter | Merge | Backup | Delete |
| Time | Device | Information | Event | Note | DST Rollback | |
| 7/11/2014 1:21:28 | Camera1 | | Motion | | Yes | |
| 7/11/2014 1:22:28 | Camera4 | | Motion | | Yes | |
| 7/11/2014 1:22:29 | Camera1 | | Motion | | Yes | |
| 7/11/2014 1:22:36 | Camera4 | | Motion | | | |

Figure 1-58

In ViewLog, click the **Camera Date Viewer** and click the **Search Event in DST** button.

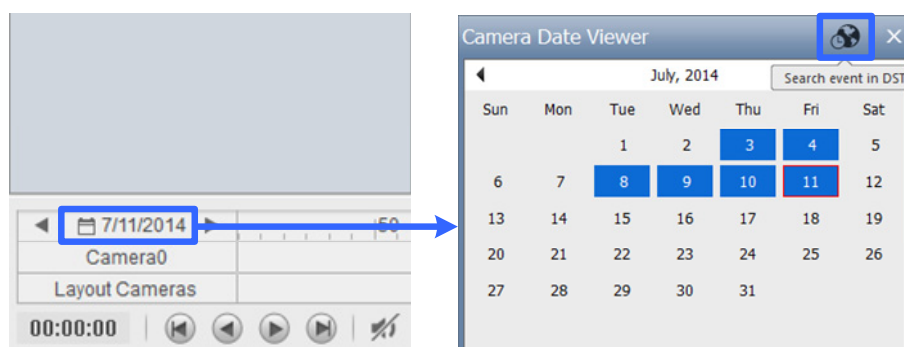


Figure 1-59

Note: Videos recorded during DST periods start with “GvDST”, e.g. GvDST20140722.avi, to differentiate from regular video files that start with “Event”, e.g. Event20081022.avi.

1.10.3 Setting Network Failure Detection

The Network Failure Detection function triggers an output device when the network connection between GV-VMS and the specified network host has failed.

1. Click **Home** , select **Toolbar** , select **Network** , and click **Network Failure Detection**.

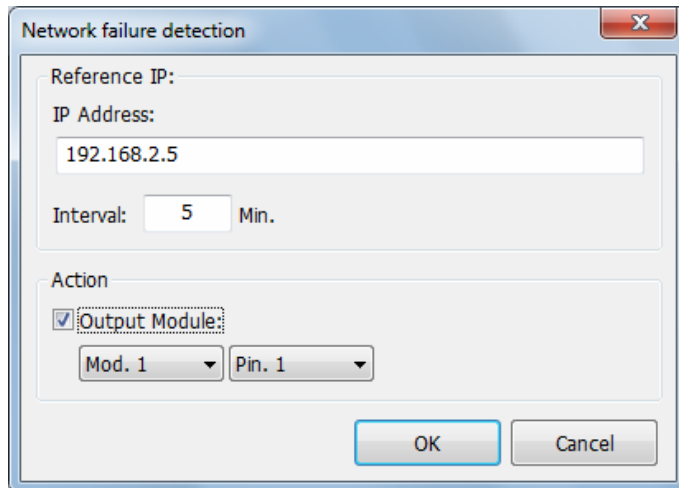


Figure 1-60

2. Under **IP Address**, type the IP address or domain name of the remote host.
3. Next to **Interval**, type the time interval between each ping in minutes ranging from 1 to 999. If the interval is 5 minutes, GV-VMS will ping the network host every 5 minutes to check if the connection is still active.
4. Under Action, enable **Output Module** and select the output module and pin number.
5. Click **OK**.

The selected output device will be triggered when the network host does not respond to GV-VMS's ping message.

1.11 PTZ Camera

With the PTZ control panel, you can control PTZ functions, e.g. pan, tilt, zoom, focus and preset points. After you have added a PTZ camera, follow the steps below to enable PTZ functions.

1. Move the cursor to the camera live view and click the **Tools** button .

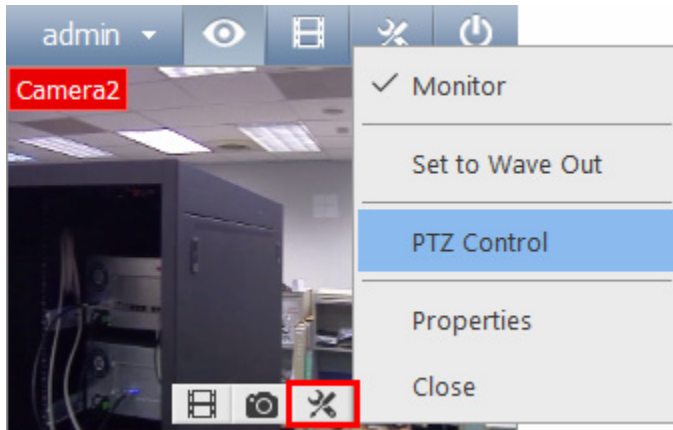


Figure 1-61


2. Click **PTZ Control** to enable PTZ function.
3. You can control the GV-SD220 and GV-SD200 using the following actions:
 - **Double-Click:** The camera will center on the spot you clicked.
 - **Drag:** You can select Random Move or Center Move after right-clicking the live view.
 - ⦿ **Random Move:** Drag a line on the live view and the camera will move toward the direction you dragged.
 - ⦿ **Center Move:** Drag a box on the live view and the camera will zoom in on the area you dragged. Center Move is only supported by GV-SD200.

1.11.1 Accessing PTZ Control Panel and Auto Functions

After PTZ Control is enabled, move the cursor to the live view to see the PTZ control panel. Note that the PTZ control panel is hidden when live view resolution is less than 240 x 180.



Figure 1-62



In the PTZ control panel, click the **Home** button  to access the advanced PTZ functions below. The options available may differ depending on the model of your PTZ camera.

- **Home:** Returns the camera to Home position.
- **Iris Open / Close:** Adjusts the camera iris. The iris Control buttons are only available for GV-IP Speed Dome.
- **Auto Focus:** Adjusts the camera focus according to the subject.
- **Auto Iris:** Adjusts the iris opening according to amount of light in the environment.
- **Auto Go:** Allows you to enable Cruise, AutoPan, Sequence and Tour functions. You can click **Stop Auto Go** to stop the Auto function you have enabled.
- **Auto Set:** Allows you to set up AutoPan and Cruise functions. See the section below for details.
- **Preset Go:** Moves the PTZ to a preset point by clicking the preset number.
- **Preset Set:** Allows you to configure up to 256 PTZ preset points. Move the camera to the position where you want set a preset point and then select a preset point number here.

To see how to set up the Sequence and Tour function, consult the manual of the connected PTZ model.

Auto Pan



The PTZ camera will continuously move between two horizontal positions. You can configure up to 8 sets of Auto Pan mode.


1. Move the camera to the start position of the AutoPan.
2. To mark the start position, click the **Home** button  in the PTZ Control Panel, select **Auto Set**, and select **Start AutoPan1**.
3. Move the camera to the end position of the AutoPan. Any movement in the vertical direction will not be included in the AutoPan.
4. To mark the end position, click the **Home** button , select **Auto Set**, and select **End AutoPan1**.
5. To create another Auto Pan mode, repeat the steps above using a different Auto Pan number.

To enable the AutoPan, click the **Home** button , select **Auto Go**, and select the AutoPan number created. To stop the AutoPan, simply click a Pan/Tilt button in the PTZ Control Panel to interrupt the AutoPan, or you can click the **Home** button , select **Auto Go**, and select **Stop Auto Go Function**.

Cruise

You can set up a route consisting of different directions, angles, and zooms for the PTZ camera to follow. Up to 4 Cruises can be created.

1. Move the camera to the start position of the Cruise.
2. To mark the start position, click the **Home** button  in the PTZ Control Panel, select **Auto Set**, and select **Set Cruise 1**.
3. Move the camera according to how you want the camera to move during the Cruise. The camera positions, zooms, and speed of the movement will all be recorded for the Cruise. .
4. When you are finished with setting up the Cruise, click the **Home** button , select **Auto Set**, and select **Set Cruise Stop**.
5. To set up another Cruise route, repeat the steps above and select a different Cruise number.

To enable the Cruise route, click the **Home** button , select **Auto Go**, and select the Cruise number created. To stop the Cruise route, simply click a Pan/Tilt button in the PTZ Control Panel to interrupt the Cruise function, or you can click the **Home** button , select **Auto Go**, and select **Stop Auto Go Function**.

1.11.2 Setting PTZ Idle Protection and Advanced Functions

In the Content List (Home  > Toolbar  > Content List ) , right-click the PTZ camera and select **PTZ Setup**. This dialog box appears.

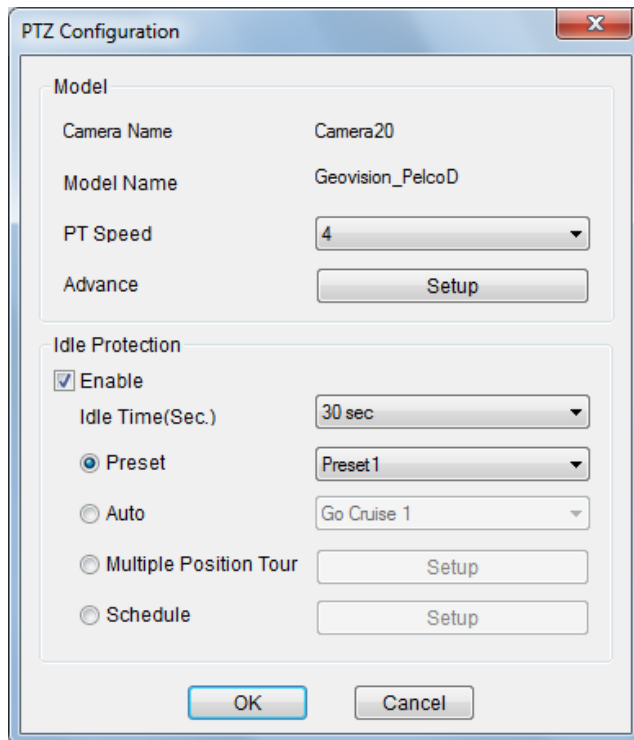


Figure 1-63

- **PT Speed:** Adjusts the speed of pan and tilt movement.
- **Advanced:** Click **Setup** to access advanced functions such as image attributes, sequence, tour and Home position. Consult the manual of the connected PTZ model for details.

[Idle Protection]

When the PTZ camera remains stationary for a certain time, the PTZ can automatically move to a Preset Point, enable an Auto function, begin a Multi Position Tour or start the PTZ schedule.

1. Click **Enable**.
2. Set the **Idle Time**. The PTZ camera will follow the action selected in the next step after the idle time exceeds the specified Idle Time.
3. Select **Preset**, **Auto**, **Multi Position Tour** or **Schedule** as protection mode. See *Setting Multi Position Tour* below.
4. Click **OK**.

Setting Multi Position Tour

You can create a PTZ tour with up to 64 preset points. Note the number of preset points depends on your PTZ capacity.

1. Select **Multi Position Tour** in the PTZ Configuration dialog box, and click the **Setup** button. This dialog box appears.

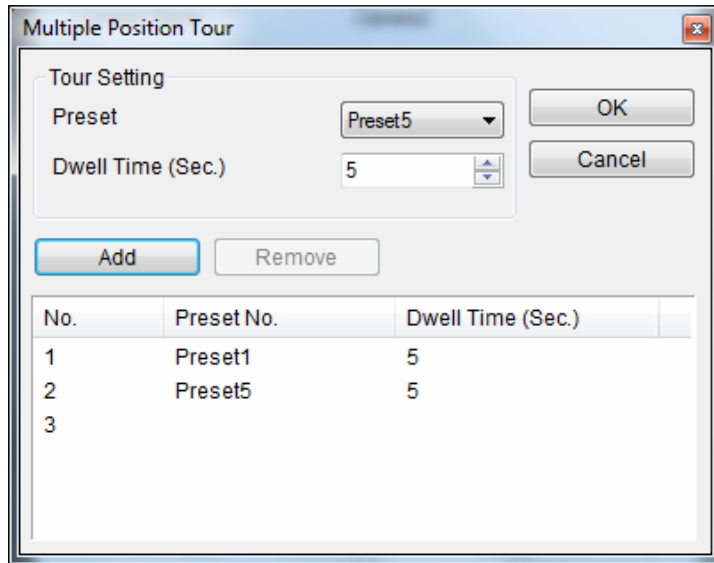


Figure 1-64

2. Select a **Preset** as a start point.
3. Set the **Dwell Time** that the PTZ will remain in a preset point.
4. Click **Add** and repeat Steps 2-3 to build more points in the tour.

Chapter 2

IP Camera Setup 76

| | | |
|------------|--|-----------|
| 2.1 | Adding IP Cameras | 76 |
| 2.1.1 | Adding Cameras Manually..... | 78 |
| 2.1.2 | Scanning Camera | 81 |
| 2.1.3 | Mapping GV-IP Cameras Using GV-IP Device Utility | 82 |
| 2.2 | Configuring Individual IP Cameras | 84 |
| 2.2.1 | Configuring Video Setting | 84 |
| 2.2.2 | Configuring Audio Setting | 87 |
| 2.2.3 | Configuring General Setting | 88 |
| 2.3 | Connection through RTSP, ONVIF & PSIA | 90 |
| 2.4 | On Demand Display | 93 |

IP Camera Setup

2.1 Adding IP Cameras

There are several ways to set up IP cameras in GV-VMS, and the setup procedures may vary depending on the device.

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

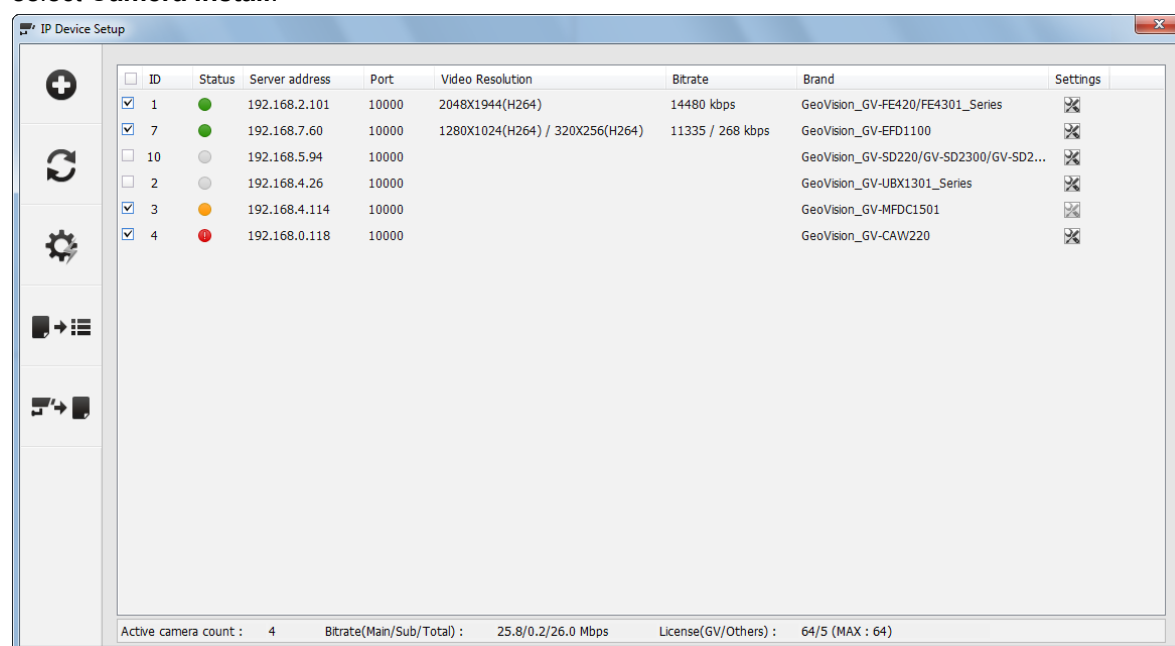


Figure 2-1

- To manually set up an IP camera, click **Add Camera**.
- To add an IP camera detected on the LAN, click **Scan Camera**.
- To add multiple IP cameras detected on the LAN, click **Automatic Setup**.
- To import IP cameras from the GV-IP Device Utility, click **Import Camera**.
- To map IP devices through the GV-IP Device Utility, click **IP Device Utility**.

For details on Automatic Setup, refer to *Adding Cameras* in Chapter 1. For other methods, refer to the sections below.

Third-Party IP Devices

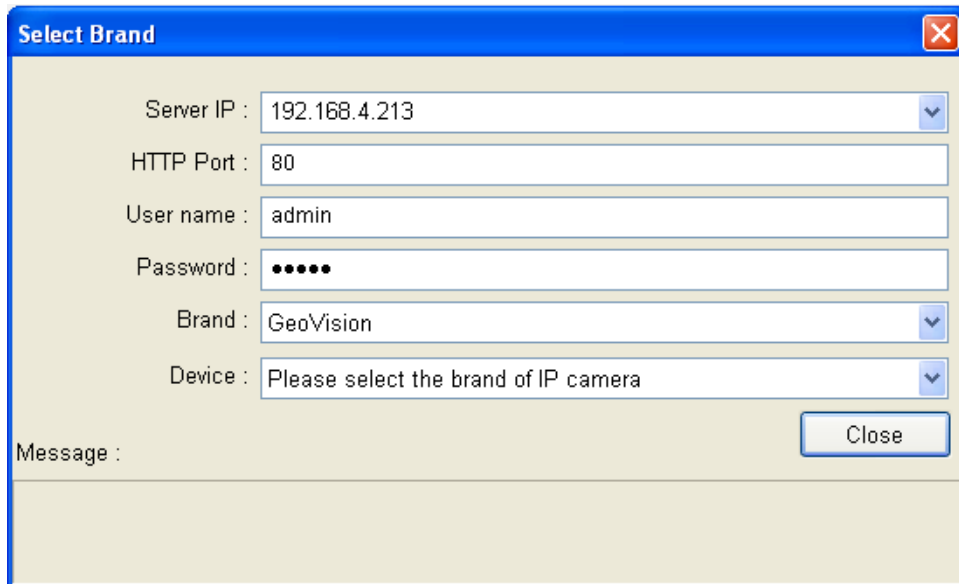
GV-VMS supports not only GeoVision's own IP devices but also products from other leading manufacturers. For the supported IP devices, refer to the *Supported IP Camera List* at http://www.geovision.com.tw/english/4_21.asp.

If the third-party camera is not detected using the scan in Scan Camera or Automatic Setup, you will need to add the camera using **Manual Setup**. You may need to add the camera using RTSP, ONVIF or PSIA protocols. Refer to *Connection through RTSP, ONVIF & PSIA* later in this chapter for details.

2.1.1 Adding Cameras Manually

To manually add IP cameras, follow the steps below.

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

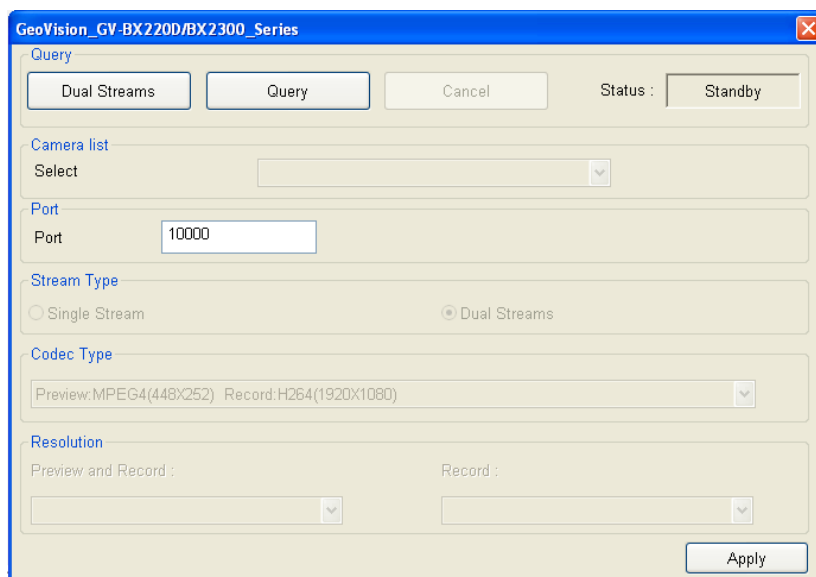


The 'Select Brand' dialog box contains the following fields:

- Server IP : 192.168.4.213
- HTTP Port : 80
- User name : admin
- Password : •••••
- Brand : GeoVision
- Device : Please select the brand of IP camera
- Message :
- Close button

Figure 2-2

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



The 'GeoVision_GV-BX220D/BX2300_Series' dialog box contains the following sections:

- Query**
 - Dual Streams
 - Query
 - Cancel
 - Status : Standby
- Camera list**
 - Select
- Port**
 - Port : 10000
- Stream Type**
 - Single Stream
 - Dual Streams (selected)
- Codec Type**
 - Preview: MPEG4(448X252) Record: H264(1920X1080)
- Resolution**
 - Preview and Record :
 - Record :
- Apply button

Figure 2-3

4. In the dialog box, configure the options which may vary depending on camera brands.
 - **Dual Streams:** GV-IP Cameras are 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-BX520D/BX5300_Series |  |
| <input checked="" type="checkbox"/> | 2 |  | 192.168.6.15 | 10000 | 1920X1080(H264) / 448x252(H264) | 6854 / 137 kbps | GeoVision_GV-BX220D/BX2300_Series |  |
| <input checked="" type="checkbox"/> | 3 |  | 192.168.7.101 | 10000 | | | GeoVision_GV-BL1500 |  |

Figure 2-4

7. To change the number of the camera, click the camera's ID and select a desired number. Note this function is only available for the disconnected cameras.

Note: The indication of status icons is as below.

| | | |
|---|---------------------------|---|
|  | Connected | The camera is connected. |
|  | Connecting | GV-VMS is trying to connect to the camera. |
|  | Connection Failed | Unable to connect to the camera. Place the cursor on the red icon to see the error message. |
|  | Inactive Camera | The camera is inactive. Select the checkbox to connect to the camera. |
|  | Started Monitoring | The camera is under monitoring. |
|  | Pre-Rec Enabled | Pre-recording is enabled. |

Tips: You can access the configuration interface of the connected IP camera by right-clicking the IP camera and selecting **Remote Camera Setting**.

2.1.2 Scanning Camera

You can add camera by scanning the cameras in the LAN.

1. Click **Scan Camera** .
2. In the Scan Camera dialog box, click **Start Scan**. The IP devices detected are displayed.

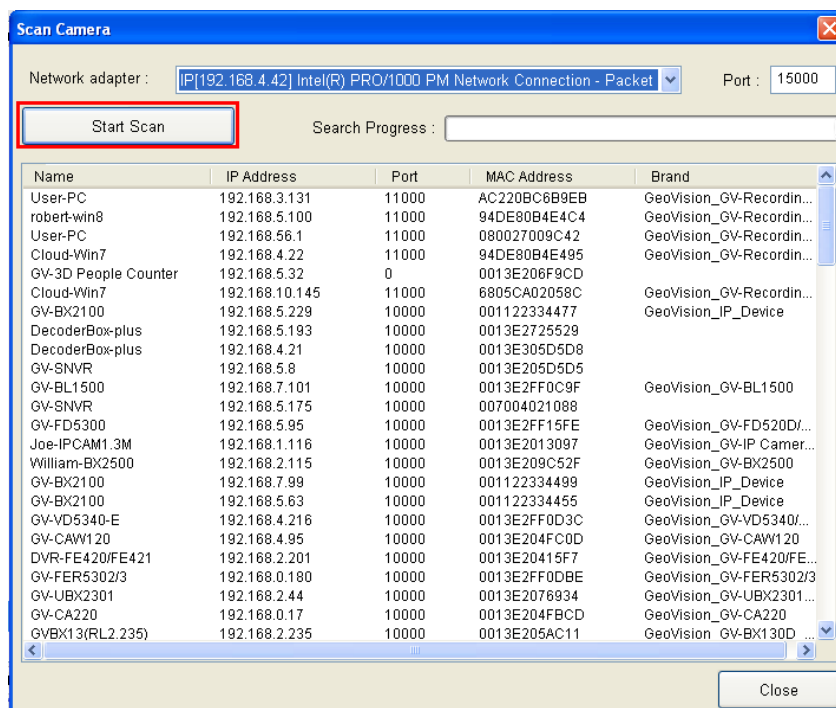


Figure 2-5

3. Double-click the IP device you wish to connect. This dialog box appears.

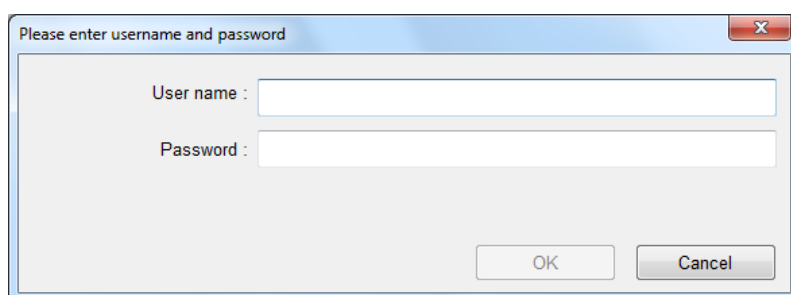



Figure 2-6

4. Type the username and password of the IP device and click **OK**. Figure 2-3 appears.
5. Click **Apply**. The IP camera is added to the IP Device List and automatically enabled for connection (Figure 2-1).

2.1.3 Mapping GV-IP Cameras Using GV-IP Device Utility

The GV-IP Device Utility detects all available GV-IP Devices on the same LAN and allows you to map detected cameras to channels. You can then export the device list and import it to another GV-VMS. This method is useful when you want to connect to the same cameras from multiple GV-VMS. The GV-IP Device Utility also allows you to quickly set the IP address, upgrade firmware, export/import device settings and reboot the device.

To set up multiple GV-IP Cameras using GV-IP Device Utility:

1. Click **IP Device Utility** . All the available IP cameras on the LAN are detected and listed in the window.

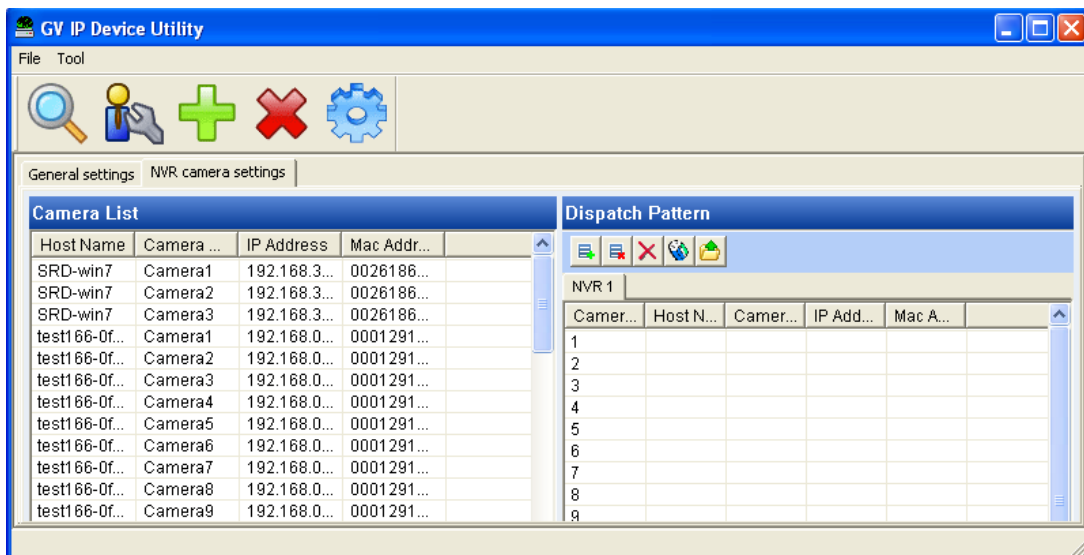



Figure 2-7

2. To map the desired IP camera to a channel, drag the IP camera from the **Camera List** to the desired channel number in the **Dispatch Pattern** section.
3. By default, the login username and password for the IP camera both are set as **admin**. If the added IP camera does not use the default settings, you need to right-click the IP camera in the **Dispatch Pattern** section and select **Login User Information** to modify its login information.
4. To map more IP cameras, repeat steps 2 and 3.

5. To create another set of the IP camera mapping settings, click the **Add** button  on the **Dispatch Pattern** toolbar. A new tab (NVR2) is created.

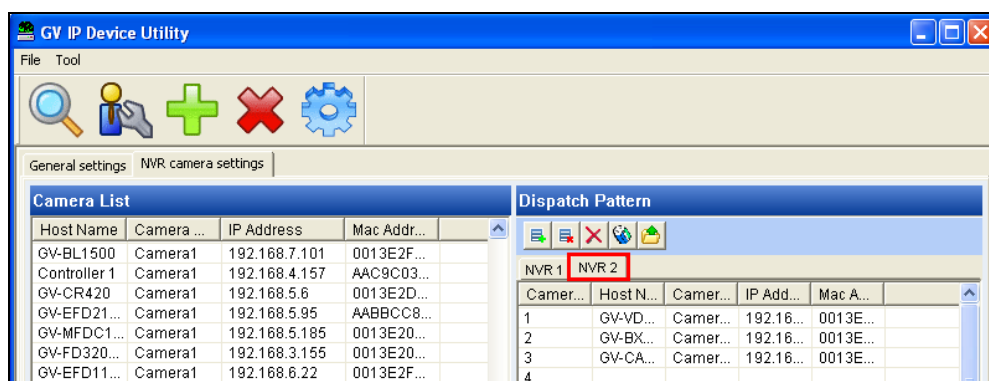




Figure 2-8

6. When you finish selecting the IP cameras, export the IP camera mapping settings.
- Select the tab of the IP camera mapping settings (NVR1, 2, 3,...) you want to apply and click the **Export** button  on the **Dispatch Pattern** toolbar. The Save As dialog box appears.
 - Specify the file name (.ipcd) and the storage path of the IP camera mapping settings.
 - To export more sets of IP camera mapping settings, repeat the steps above.
7. To import the IP camera mapping settings into the GV-VMS:
- Close the GV-IP Device Utility window, return to the IP Device Setup dialog box and select **Import Camera** . This dialog box appears.

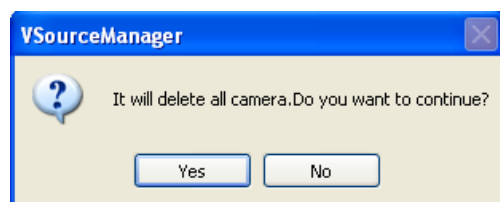



Figure 2-9

- Click **Yes**, locate the storage path of the IP camera mapping settings you want to import and click **OK**. The settings are imported to the GV-VMS.

2.2 Configuring Individual IP Cameras

To configure the IP camera settings such as video, audio and other general settings, click the **Setup** button  of the connected camera on the IP Device List.

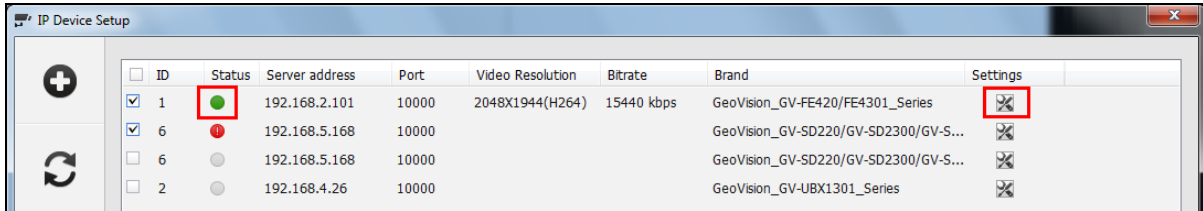


Figure 2-10

2.2.1 Configuring Video Setting

You can configure video settings such as frame rate, codec type and resolution of the camera.

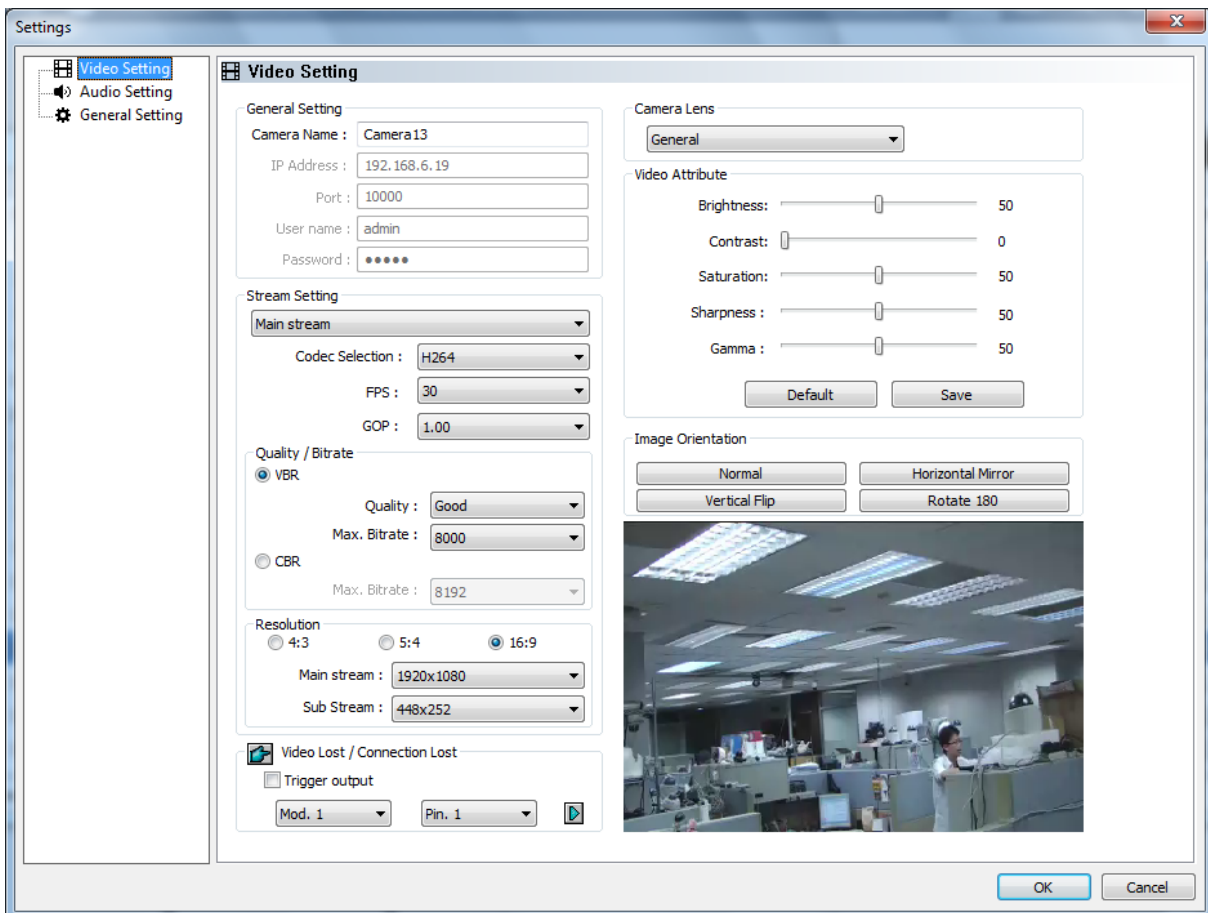


Figure 2-11

[General Setting]

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

[Stream Setting] Select a stream from the drop-down list. Settings for Main Stream will be used for recording. Live view can use either Main Stream or Sub Stream depending on the On Demand settings. For details, see the *On Demand Display* section later in this chapter.

- **Codec Selection:** Set the codec to **MJPEG** or **H.264**.
- **FPS:** Set the number of frame per second.
- **GOP:** Set the number of seconds between each key frame. For example, when the FPS is set to 30, a GOP of 0.5 means there will be 1 key frame among every 15 frames.
- **Quality and Bitrate:** When using the H.264 codec, you can select between **VBR** and **CBR**.
 - ⊙ **VBR (Variable Bitrate):** The quality of the video stream is kept as constant as possible at the cost of a varying bitrate. Set the image quality to one of the 5 standards: **Standard**, **Fair**, **Good**, **Great** and **Excellent**. Set a **Max. Bitrate** if needed, or select **Auto** if you do not want to enable this function.
 - ⊙ **CBR (Constant Bitrate):** CBR is used to achieve a set bitrate by varying the quality of the H.264 stream. Select one of the bitrates from the drop-down list.
- **Resolution** Change the display ratio and resolution.

[Video Lost / Connection Lost]

- **Trigger Output:** Trigger the specified output module upon video lost or connection lost until the output device is manually turned off. Use the drop-down lists to select the output module and pin number to perform this function. To configure the output device, see *I/O Device Setup* in Chapter 6.
 - ⊙ **Right-Arrow button:** Set the counting time between 0 and 1000 seconds to delay the activation of the specified output module.

[Camera Lens] Select **Wide Angle** if you want to correct warping toward the edge of the camera image. See *Wide Angle Lens Dewarping* in Chapter 3 for details.

If you are using third-party fisheye cameras, select **IMV1 Panorama** for cameras installed with an ImmerVision IMV1 Panorama Lens, and select **Fisheye** for other third-party fisheye cameras. Refer to *Setting Up a Third-Party Fisheye Camera* in Chapter 3 for details.

[Video Attribute] Adjust video characteristics such as brightness, contrast, saturation, sharpness and gamma. To restore the default settings, click **Default**.

[Image Orientation] Adjust the image orientation by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip** or **Rotate 180**. A preview image is available.

Note: Changes made to the Video Setting page will change the settings on the IP camera.

2.2.2 Configuring Audio Setting

On the Audio Setting page, you can adjust audio devices and listens to live sound.

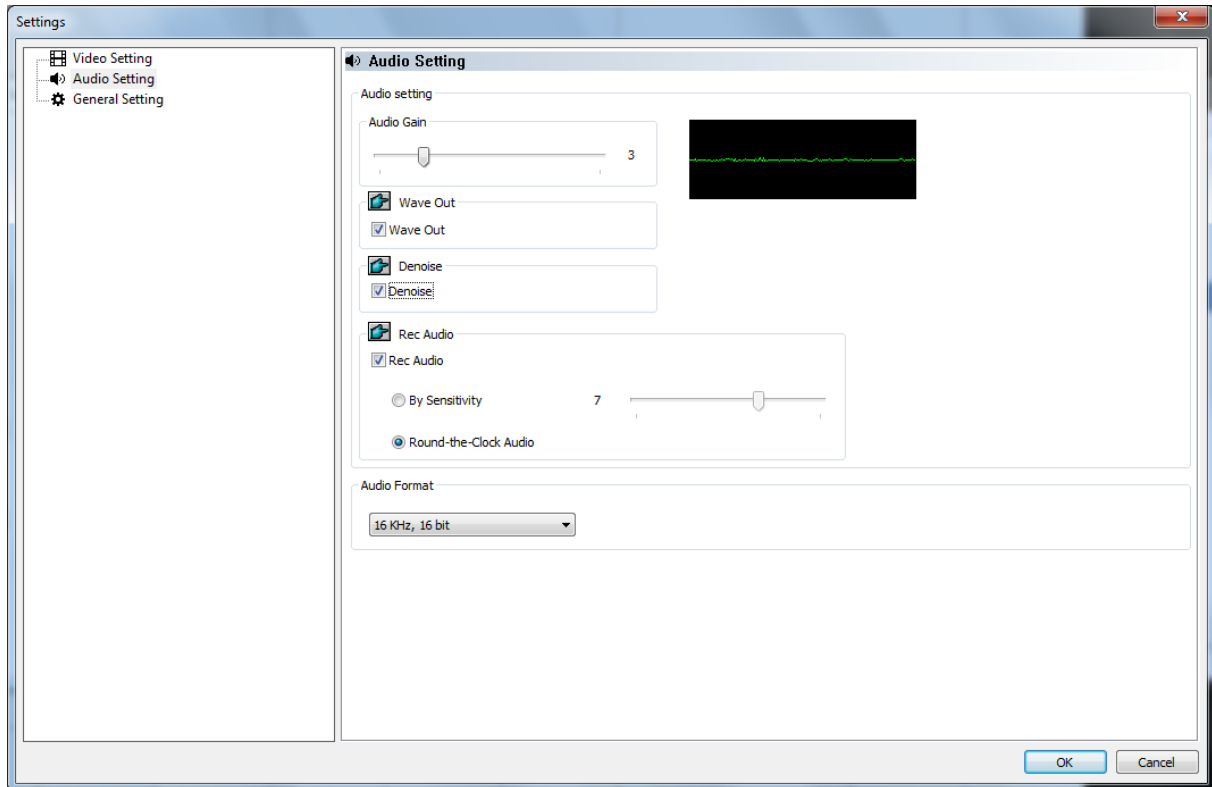


Figure 2-12

- **Audio Gain:** Increase or decrease the gain of the microphone.
- **Wave Out:** Click to listen to the audio around the camera.
- **Denoise:** Click to reduce audio noise.
- **Rec Audio:** Click **Rec Audio** to record the audio around the camera.
 - ⊙ **By sensitivity:** Audio recording is activated when the volume reaches the sensitivity level indicated.
 - ⊙ **Round-the-Clock Audio:** Audio recording is continuously enabled.
- **Audio Format:** Select an audio format from the drop-down list. The default is **16 KHz, 16 bit**.

2.2.3 Configuring General Setting

You can configure the general settings such as for video recording.

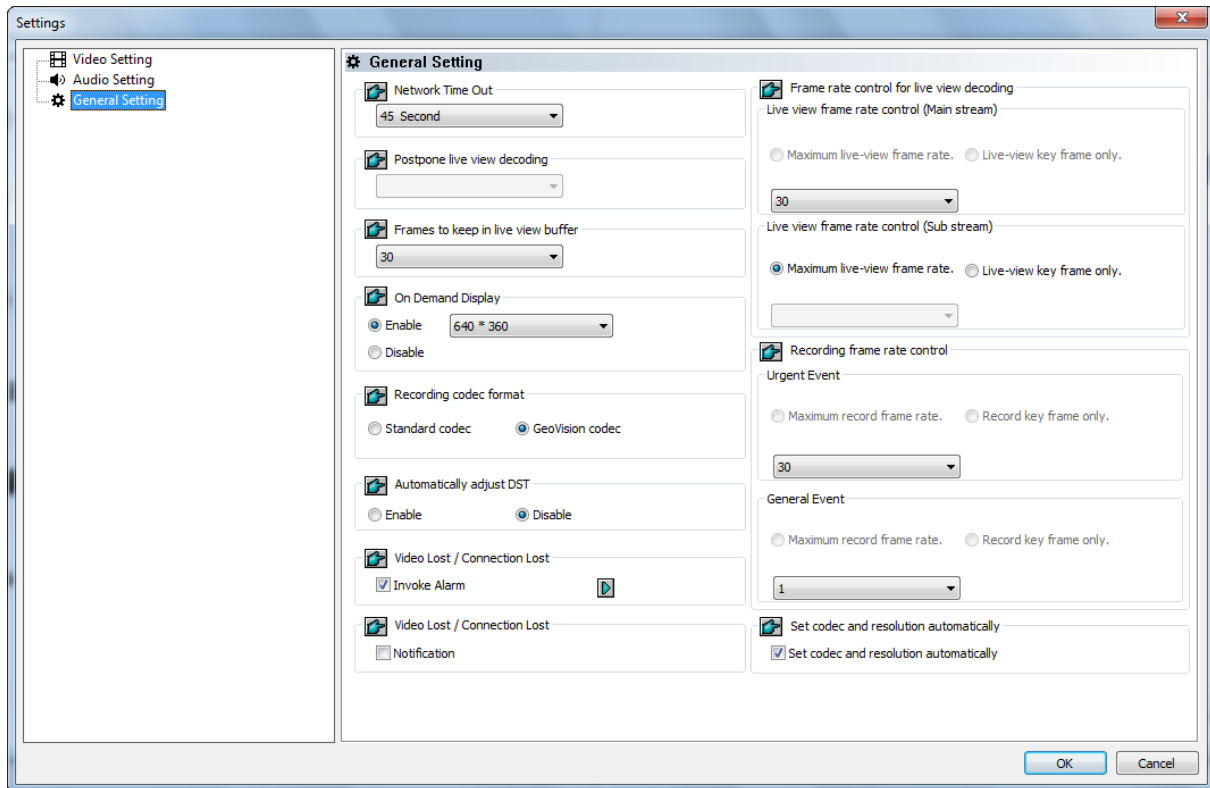






Figure 2-13

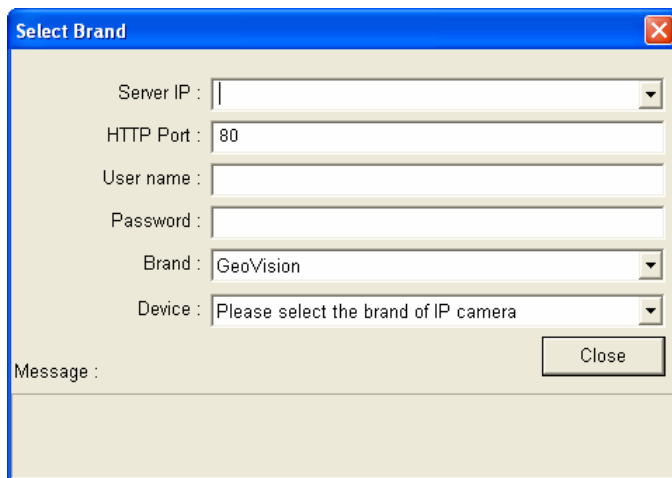
- **Network Time Out:** Specify the number of seconds for network timeout. When network disconnection exceeds the specified time period, the status icon on the IP Device List (Figure 2-1) will be yellow.
- **Live View Decode Postpone Time:** Specify the number of milliseconds to postpone live view decoding. When the network connection with IP devices is unstable or when the time length between frames is not evenly distributed, postponing the live view decoding will make the video smoother. Note this function is only available for configuration when the camera is disconnected.
- **Frames to Keep in Live View Buffer:** Specify the number of frames to keep in the live view buffer. When CPU performance is insufficient, you can reduce the number of frames kept in buffer to achieve a real-time appearance by dropping frames. This setting does not affect the frame rate of the recorded videos.
- **On Demand Display:** Enable automatic adjustment of live view resolution. For details, see the *On Demand Display* section later in this chapter.
- **Recording Codec Format:** Specify whether to record in standard or GeoVision codec.
- **Automatically Adjust DST:** If enabled, the time on the GV-IP Device Web interface will be synchronized with the time of the GV-VMS when DST period starts or ends on the GV-VMS.

- **Video Lost / Connection Lost (Invoke Alarm):** Enable if you want to trigger an alarm sound upon connection lost. Click the Arrow button to select a sound.
- **Video Lost / Connection Lost (Notification):** Enable if you want to send an e-mail notification upon connection lost. See *Setting Up Email Notification* in Chapter 1 to see how to set up the e-mail server.
- **Live View Decode Frame Control (Main / Sub Stream):** Set the live view frame rate for main stream and sub stream.
 - ⊙ When using **MJPEG**, every frame is a key frame, so the options of **Max. frame** and **Key only** will be grayed out. In the drop-down list, you can specify the number of key frames to decode for live view.
 - ⊙ When using **H.264**, only one key frame is transmitted per the specified number of frames, so you can select **Key only** to decode key frames only and omit all intermediate frames or **Max. frame** to include key frames and all intermediate frames.
- **Recording Frame Rate Control:** Set the recording frame rate for **Urgent Event** and **General Event**. This function allows you to set different recording frame rates for motion, non-motion and other alarm events. For details, see *Setting Recording Settings for Individual Cameras* in Chapter 1
 - ⊙ When using **MJPEG**, every frame is a key frame, so the options of **Max. frame** and **Key only** will be grayed out. You can specify the recording frame rate for **Urgent Event** and **General Event** respectively.
 - ⊙ When using **H.264**, only one key frame is transmitted per the specified number of frames. You can select **Max. frame** for **Urgent event** and select **Key only** for **General event**.
- **Set Codec and Resolution Automatically:** If enabled, the GV-VMS will resume the configured codec and resolution when it detects the changes made by the camera. For example, if you have configured the resolution of Stream 1 as 1920 x 1080 after connecting the camera, when the resolution is changed to 640 x 480 on the camera end, the system will resume the resolution as 1920 x 1080.

2.3 Connection through RTSP, ONVIF & PSIA

You can add an IP camera to the GV-VMS by using the RTSP (Real Time Streaming Protocol), ONVIF (Open Network Video Interface Forum) and PSIA (Physical Security Interoperability Alliance) if the protocol is supported by your IP camera. This is useful to set up an IP camera which is not on the list of Supported IP Devices (see http://www.geovision.com.tw/english/4_21.asp).

1. Click **Home** , select **Toolbar** , click **Configure**  and select **Camera Install**.
2. Click **Add Camera**  to manually add an IP camera. This dialog box appears.

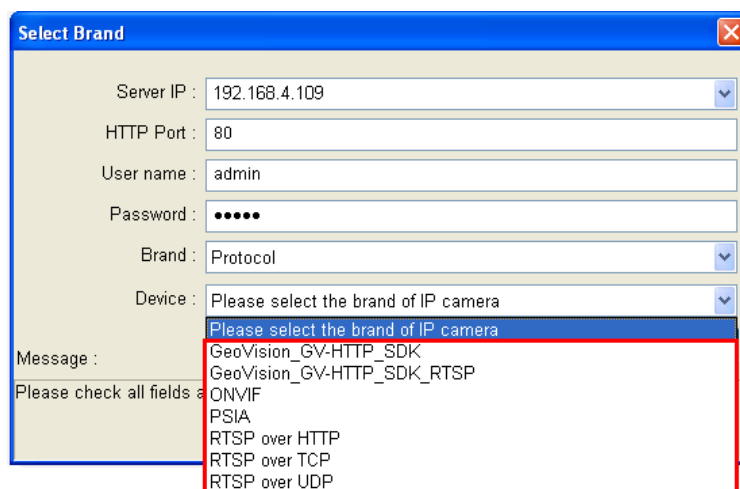


The 'Select Brand' dialog box is shown. It contains the following fields:

- Server IP :
- HTTP Port :
- User name :
- Password :
- Brand :
- Device :
- Message :
- Close button

Figure 2-14

3. Type the IP address, username and password of the IP camera. Modify the default HTTP port if necessary.
4. Select **Protocol** from the **Brand** drop-down list.
5. Select the protocol that is supported by your IP camera from the **Device** drop-down list.



The 'Select Brand' dialog box is shown with the following values entered:

- Server IP : 192.168.4.109
- HTTP Port : 80
- User name : admin
- Password :
- Brand : Protocol
- Device : Please select the brand of IP camera
- Message : Please check all fields

The 'Device' drop-down list is open, showing the following options:

- Please select the brand of IP camera
- GeoVision_GV-HTTP_SDK
- GeoVision_GV-HTTP_SDK_RTSP
- ONVIF
- PSIA
- RTSP over HTTP
- RTSP over TCP
- RTSP over UDP

Figure 2-15

- **GV_HTTP_SDK:** This option is for SDK users. The RTSP protocol uses a HTTP port for data streaming from the IP camera.
 - **GV_HTTP_SDK_RTSP:** This option is for GeoVision SDK users. The RTSP protocol uses a HTTP port for data streaming from the IP camera.
 - **ONVIF:** This option is for connecting the camera using ONVIF standards.
 - **PSIA:** This option is for connecting the camera using PSIA standards.
 - **RTSP over HTTP:** The RTSP protocol uses a HTTP port for data streaming from the IP camera.
 - **RTSP over TCP:** The RTSP protocol uses a TCP port for data streaming from the IP camera.
 - **RTSP over UDP:** The RTSP protocol uses an UDP port for data streaming from the IP camera.
6. If you select **ONVIF**, this dialog box appears after the system confirms that the camera is ONVIF compatible. Click **Dual Stream** to enable the second stream if needed, and click the **Setting** button [...] next to Stream1 and Stream 2 to adjust the following information.

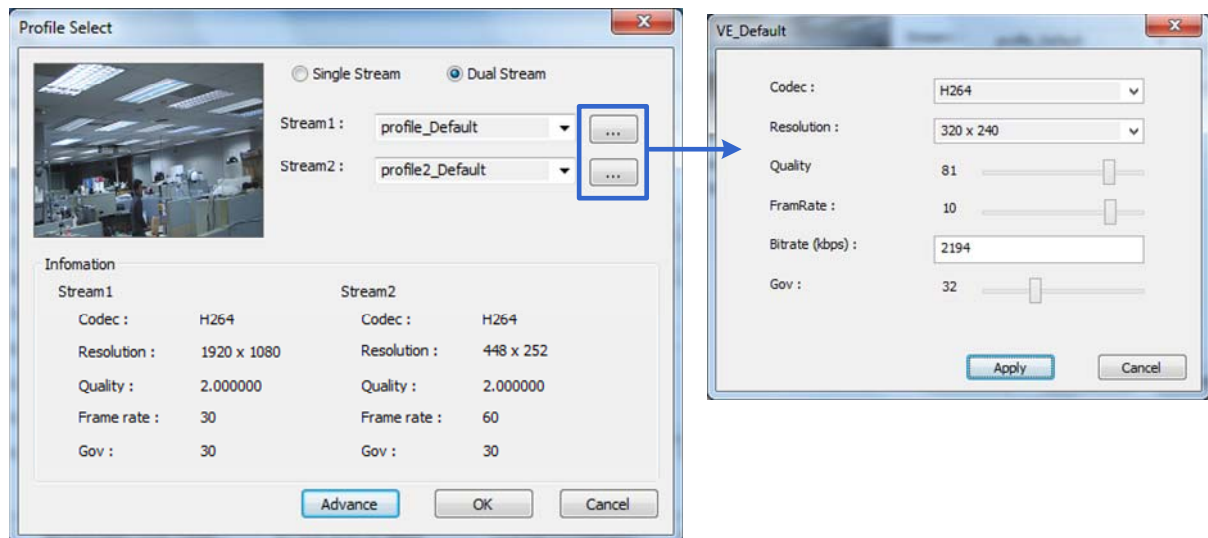
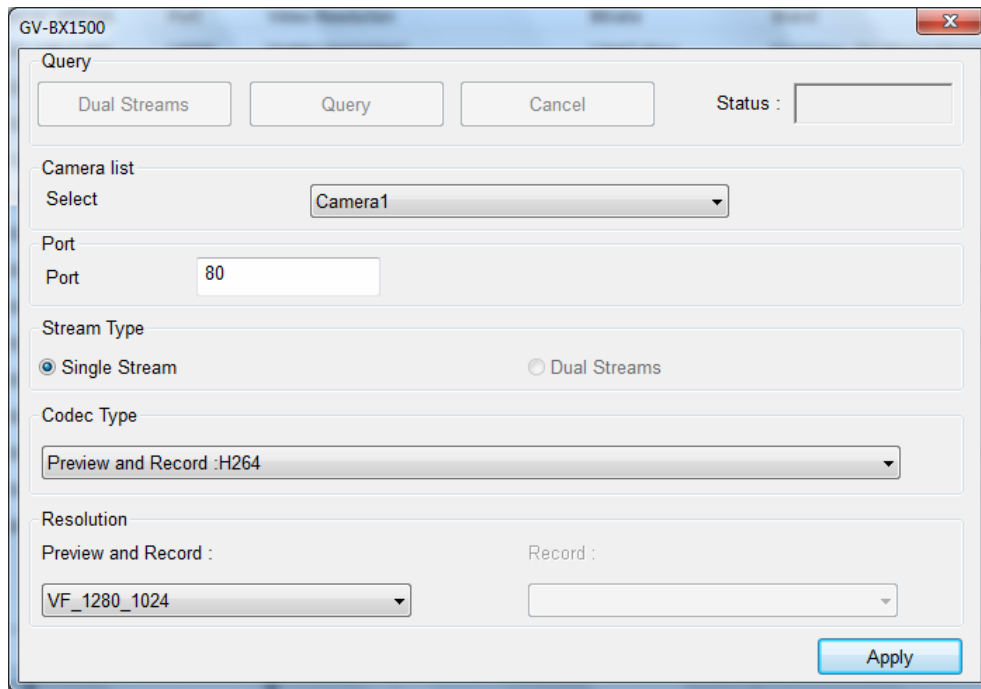


Figure 2-16

- **Codec:** Select H.264 or JPEG.
- **Resolution:** Set a resolution.
- **Quality:** Adjust the image quality. The range of image quality varies for different brands.
- **Frame Rate:** Set a maximum frame rate. The range of frame rate varies for different brands.
- **Bitrate:** The current bit rate setting of the IP device will be displayed. You can adjust the bit rate limit within the device's supported bit rate range if needed.
- **GOV:** Set the number of frames between each key frame. For example, a GOV of 10 means there will be 1 key frame every 10 frames.

7. If you select **PSIA**, this dialog box appears after the system confirms that the camera is PSIA compatible. Click **Apply**.

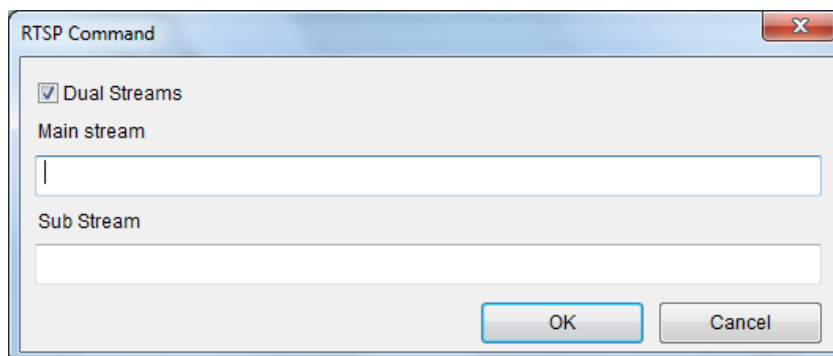


The dialog box titled "GV-BX1500" contains the following fields and controls:

- Query** section: Includes buttons for "Dual Streams", "Query", and "Cancel", along with a "Status :" label and an empty text field.
- Camera list** section: A "Select" dropdown menu currently showing "Camera1".
- Port** section: A "Port" label and a text field containing the value "80".
- Stream Type** section: Two radio buttons, "Single Stream" (which is selected) and "Dual Streams".
- Codec Type** section: A dropdown menu showing "Preview and Record :H264".
- Resolution** section: Two dropdown menus. The first is labeled "Preview and Record :" and shows "VF_1280_1024". The second is labeled "Record :" and is currently empty.
- An **Apply** button is located at the bottom right.

Figure 2-17

8. If you select **RTSP**, select **Dual Streams** to enable the Sub Stream if needed and type the RTSP link address.



The dialog box titled "RTSP Command" contains the following fields and controls:

- A checked checkbox for **Dual Streams**.
- Main stream** section: A text input field.
- Sub Stream** section: A text input field.
- OK** and **Cancel** buttons at the bottom.

Figure 2-18

For the RTSP command, consult the documentation of your IP camera. For instance:





- For an AXIS IP camera, enter RTSP://<IP of the IP camera>/<codec>/media.amp
 - For a HIKVISION IP camera, enter RTSP://username:password@<IP of the IP Camera>
9. Click **OK** to add the IP camera to the IP Device List.

2.4 On Demand Display

For cameras that support dual streaming with different resolutions, you can select the **On Demand Display** option to enable automatic adjustment of live view resolution. This option produces good image quality without causing high CPU usage.

You will need to set one video streaming of the camera to be higher than the other streaming. The system will switch to the higher resolution streaming when using the view modes that require higher quality images, such as single view or PIP / PAP mode. When watching live view in the view modes where higher resolution does not make a difference, such as the maximum screen division of 100 channels, the system will switch to the lower resolution streaming to reduce CPU usage.

To enable the function:

1. Make sure the IP camera has been added to the GV-VMS and you have selected **Dual Stream** during setup. For details on adding IP camera, see *Adding IP Cameras* earlier in this chapter.
2. Click **Home** , select **Toolbar** , click **Configure**  and select **Camera Install**.
3. In the IP Device Setup dialog box, click the **Setup** button  of the desired connected camera on the IP Device List.
4. In the Setting dialog box, select **General Setting**.

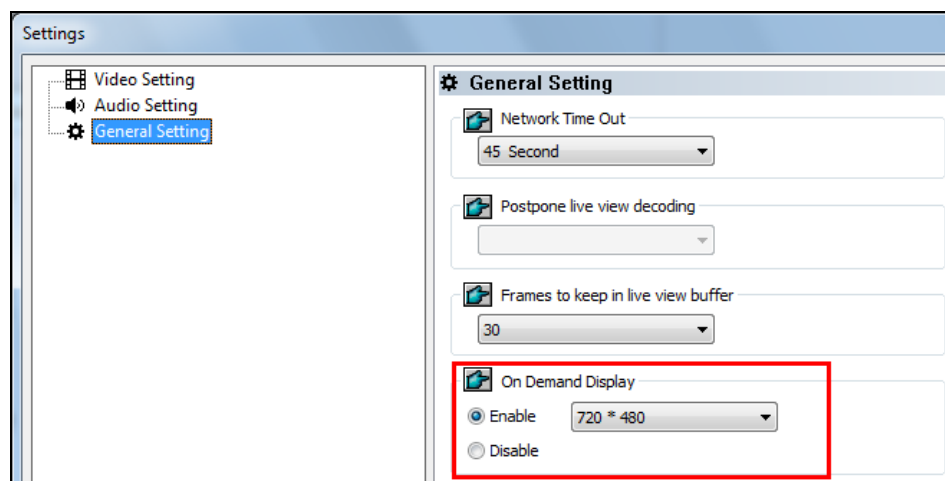


Figure 2-19

5. In the On Demand Display field, click **Enable** and select a resolution. When the resolution of the camera image on the screen is bigger than or equal to the selected resolution, the system will switch to the higher resolution streaming.

Note:

1. The **On Demand Display** function is not supported for **Privacy Mask**.
2. The **On Demand Display** function is not supported for GV-Fisheye Camera.
3. If the same resolution has been set for both video streams, the On Demand Display option will still be visible, but automatic resolution adjustment will not occur.

Application Example

A resolution of 720 x 480 has been selected for the On Demand Display function.

- **Higher Resolution Streaming**

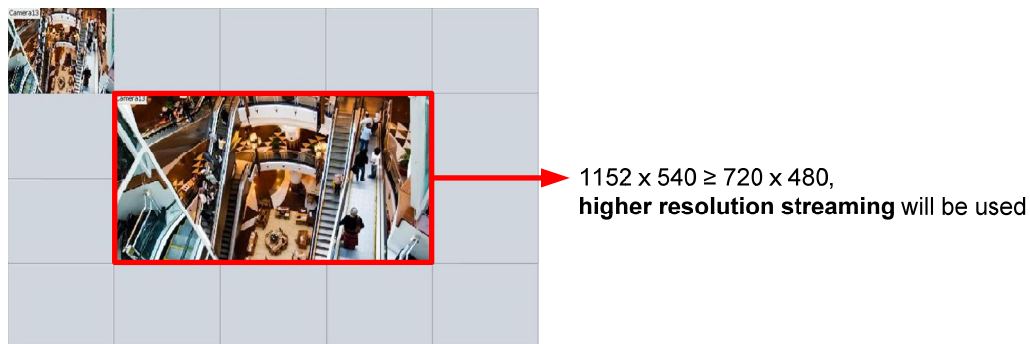


Figure 2-20

The camera image in the middle has a resolution of 1152 x 540, so the higher resolution streaming will be used, because 1152 x 540 is bigger than the selected 720 x 480.

- **Lower Resolution Streaming**



Figure 2-21

After switching to 9-channel screen division, the resolution for each channel is 640 x 360, which is smaller than the selected 720 x 480, so the lower resolution streaming will be used.

Chapter 3

| | |
|--|------------|
| Video Analysis | 97 |
| 3.1 Object Counting and Intrusion Alarm | 97 |
| 3.1.1 Object Counting..... | 97 |
| 3.1.2 Intrusion Alarm..... | 101 |
| 3.2 Object Index..... | 106 |
| 3.2.1 Setting Object Index..... | 106 |
| 3.2.2 Viewing Object Index | 109 |
| 3.2.3 Searching Object Index | 110 |
| 3.3 Automatic Video Snapshots | 112 |
| 3.3.1 Setting Video Snapshots..... | 112 |
| 3.3.2 Searching Video Snapshots | 115 |
| 3.4 Face Detection | 117 |
| 3.4.1 Setting Face Detection | 117 |
| 3.4.2 Searching Face Detection Snapshots | 119 |
| 3.5 Face Count | 120 |
| 3.5.1 Installing the Camera..... | 120 |
| 3.5.2 Setting Face Count..... | 121 |
| 3.6 Privacy Mask Protection | 125 |
| 3.6.1 Setting a Privacy Mask | 125 |
| 3.6.2 Granting Access Privileges to Recoverable Areas | 127 |
| 3.7 Panorama View | 128 |
| 3.7.1 The Main Window..... | 128 |
| 3.7.2 Stitching a Panorama View with Overlapping Areas | 130 |
| 3.7.3 Easy Mode with No Overlapping Area | 133 |
| 3.7.4 Accessing a Panorama View | 136 |
| 3.8 Video Defogging..... | 137 |
| 3.9 Video Stabilization..... | 139 |
| 3.10 Wide Angle Lens Dewarping..... | 141 |
| 3.11 Advanced Motion Detection | 143 |
| 3.12 Crowd Detection | 146 |
| 3.13 Advanced Scene Change Detection | 149 |

3.14 Advanced Unattended Object Detection..... 152

3.15 Advanced Missing Object Detection 155

3.16 Text Overlay 158

3.17 Fisheye View 160

3.17.1 Setting Up a GV-Fisheye Camera..... 161

3.17.2 Setting Up a Third-Party Fisheye Camera 164

3.17.3 Object Tracking..... 166

3.18 Specifications 173

Video Analysis

3.1 Object Counting and Intrusion Alarm

Object Counting provides bi-directional counting of objects under the surveillance area. It is able to count any moving objects (such as vehicles), people or animals. Intrusion Alarm can be set up to notify the administrator when an object crosses or moves into the defined region.

Note: It is not suggested to apply the counter function to Fisheye cameras.

3.1.1 Object Counting

You can select up to 16 cameras to set up Object Counting.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

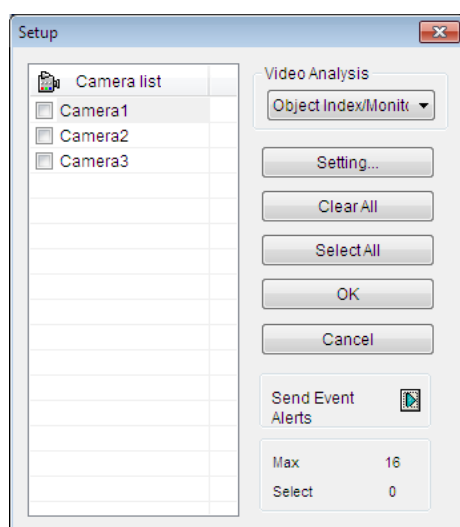


Figure 3-1

2. From the Video Analysis drop-down list, select **Counter/Intrusion Alarm Setting**, select the desired cameras, and click **Setting**. This page appears.

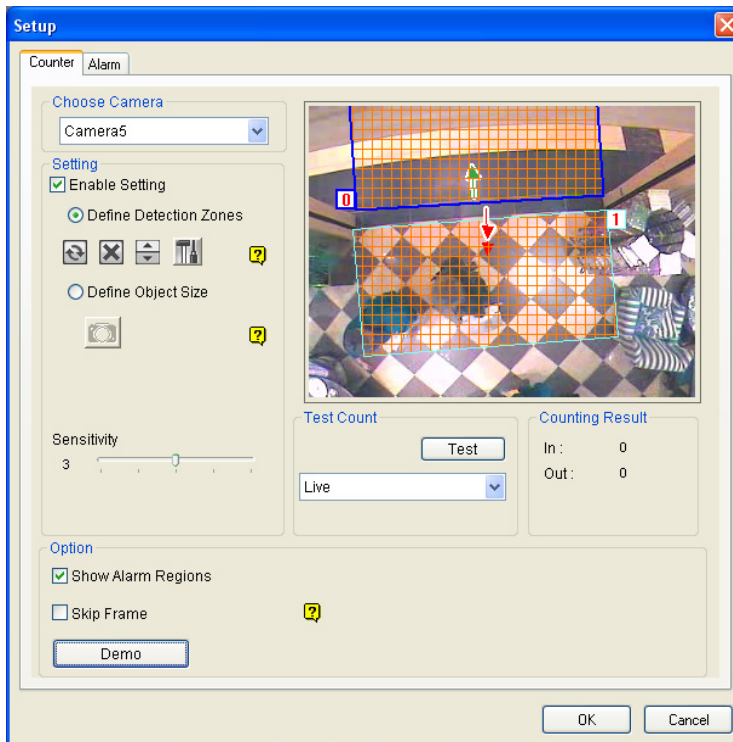









Figure 3-2

3. In the Choose Camera section, select a camera from the drop-down list for setup.
4. Select **Enable Setting** to define the criteria for the counter.
 - **Define Detection Zones:** Select this option to define the detection zones.
 - a. On the live view, draw at least two boxes to mark the in and out detection zones. Each detection zone is numbered. Use these buttons to edit the detection zones:

| Name | Button | Function |
|-----------|---|--|
| Reverse |  | Click this button to flip-flop the detection zone. |
| Switch |  | Click this button to switch to another detection zone and then use the  button to delete or the  button to edit. |
| Delete |  | Click this button to delete the detection zone. |
| Direction |  | Click this button to configure the in and out directions. See step 2b for details. |

- b. Click the  button to define the in and out criteria. This dialog box appears.

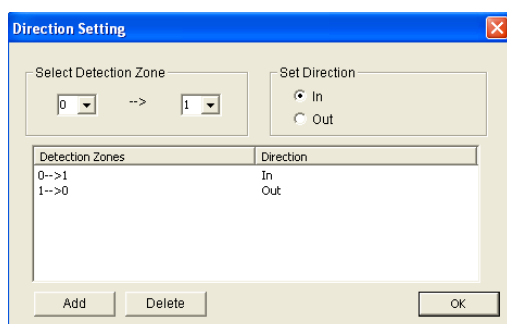




Figure 3-3

- c. In the Set Direction section, select **In** and define the direction using the drop-down lists in the Select Detection Zone section.
- d. Click the **Add** button. This setting appears under Detection Zones and Direction table.
- e. Select **Out** in the Set Direction section, define the direction using the drop-down lists in the Select Detection Zone section, and click the **Add** button.
- f. Click **OK**. The directions are indicated by arrows on the live view.

You have now set up the object counter with the in and out criteria defined. In the illustrated example (*Figure 3-3*), a target object is counted as in when it moves along the direction of the **red arrow** through detection zone 0 and 1, and the object is counted as out when it moves along the direction of the **green arrow** through detection zone 1 and 0.

- **Define Object Size:** Select this option and click the  button to pause the live view.

Use the mouse to outline a region matching the normal size of the targeted object. Click the  button to resume.

5. To test your counting settings, select **Live** from the Test Count drop-down list and click the **Test** button to start testing. Notice how the number changes in the Counting Result section when objects move through the detection zone. Use the **Sensitivity** slider to increase or decrease detection sensitivity if the passing objects are not counted correctly.
6. Click **OK** to apply the settings.
7. Start monitoring to begin counting.

More options in the Counter dialog box:

- **Show Alarm Regions:** Displays the detection zones on the preview image.
- **Skip Frame:** Skips frames when counting objects to lower the CPU loading. The system will count objects in every other three frames approximately. Note this option may reduce the accuracy of counting result.

Note:

1. Draw the detection zones as closely as possible to avoid omission of counting when target objects show up from the unmarked area and move only through one of the two boundaries.

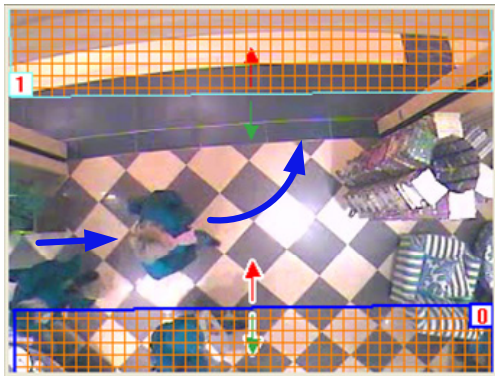


Figure 3-4

2. To include counting results in the recorded files, see *Setting Text Overlay* later in this chapter.
 3. To view the logs for counter events, click **View Log, Toolbar, Tools, System Log, Monitor Table** and then click the **Counter** tab.
 4. Optionally create a schedule for counter to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.1.2 Intrusion Alarm

When any object crosses or is inside the defined region, the alarm will be activated for warning. You can select up to 16 cameras to set up Intrusion Alarm.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

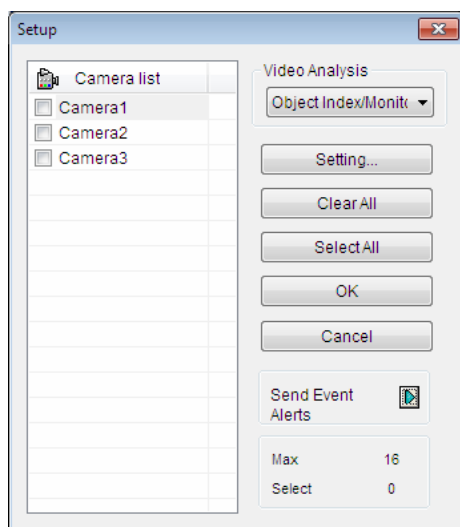


Figure 3-5

2. From the Video Analysis drop-down list, select **Counter/Intrusion Alarm Setting**, select the desired cameras, and then click **Setting**.

3. Click the **Alarm** tab. This dialog box appears.

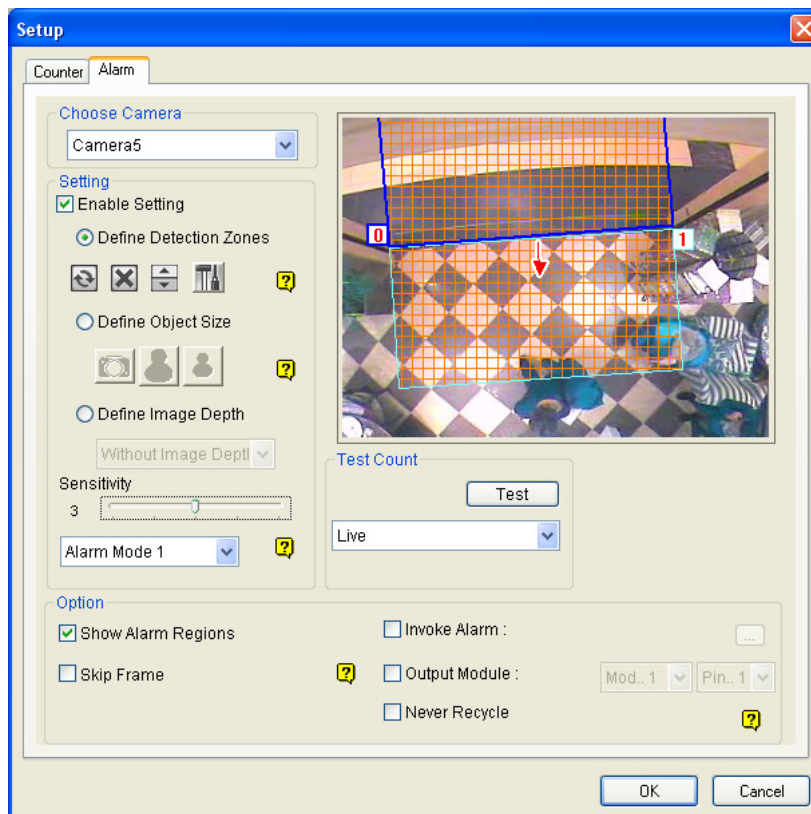









Figure 3-6

4. In the Choose Camera section, select a camera from the drop-down list for setup.
5. Select **Enable Setting** to define the criteria for intrusion alarm.
 - **Define Detection Zones:** Select this option to define the detection zones.
 - a. On the live view, draw at least two boxes to mark the in and out detection zones. Each detection zone is numbered. Use these buttons to edit the detection zones:

| Name | Button | Function |
|-----------|---|--|
| Reverse |  | Click this button to flip-flop the detection zone. |
| Switch |  | Click this button to switch to another detection zone and then use the  button to delete or the  button to edit. |
| Delete |  | Click this button to delete the detection zone. |
| Direction |  | Click this button to configure the intrusion directions. See step 2b for details. |

- b. Click the  button to define the alarm criteria. This dialog box appears.

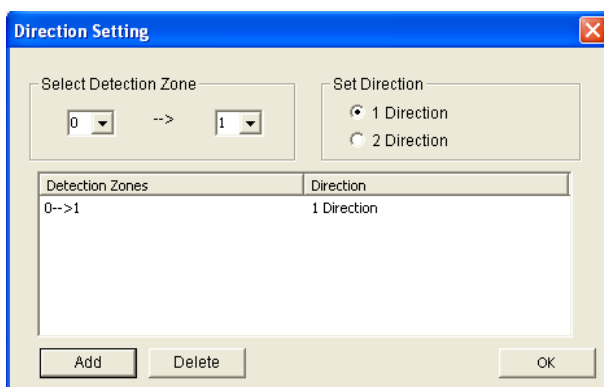




Figure 3-7

- In the Set Direction section, select **1 Direction** for uni-direction or **2 Direction** for dual-direction criteria, and use the drop-down lists in Select Detection Zone section to define the direction.
- Click the **Add** button. This setting appears in the Detection Zones and Direction table.
- Click **OK**. The directions are indicated by arrows on the live view.

You have now defined the criteria for intrusion alarm. In the illustrated example (*Figure 3-7*), when a target moves along the direction of the **red arrow** through detection zone 0 and 1, the alarm will be activated.

- **Define Object Size:** Select this option and click the  button to pause the live view. Use the mouse to outline a region matching the normal size of the targeted object. Click the  button to resume.
- **Define Image Depth:** When the object moves toward or away from the camera along a path, for example, a hallway, it appears larger when it is closer to the camera and vice versa. Rather than using a fixed object size, you can define a maximum and minimum object size according to the object's proximity to the camera.

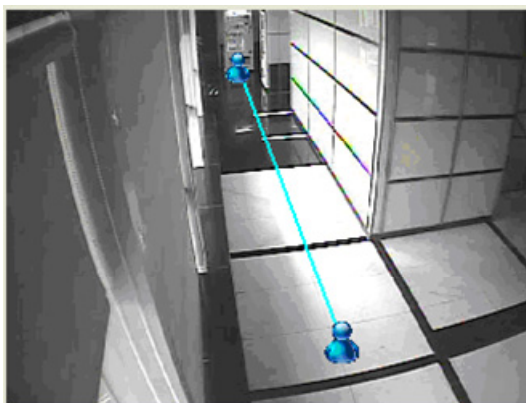







Figure 3-8

- a. Select **Define Image Depth** and then select **With Image Depth** using the drop-down list.
A line  appears.
- b. Drag and place the line along the path where the objects will be moving. The larger icon indicates the point closer to the camera and the smaller icon indicates the point farther away from the camera.
- c. Select **Define Object Size**. Click the larger icon  and click the  button to pause the live view. Use the mouse to outline the maximum size of objects when they are close to the camera.
- d. Click the smaller icon  and repeat the step above to define the minimum size of objects when they are far from the camera.

You have now defined two sets of object sizes at the two ends of the  line.

6. In the Setting section, there are two kinds of alarm modes:
 - **Alarm Mode 1:** The alarm sets off when the target object moves through the first detection zone and touches the second detection zone in the defined direction.
 - **Alarm Mode 2:** The alarm sets off when the target object moves through the first detection zone and its center moves through the second detection zone in the defined direction.
7. To set up alarm devices, configure any or both of the following options.
 - **Invoke Alarm:** Enable the computer alarm when an object enters the defined region. Click the button next to the option to assign a .wav sound file.
 - **Output Module:** Enable an installed output device when an object enters the defined region. Assign the output module and pin number.
8. To test your alarm settings, select **Live** from the Test Count drop-down list and click the **Test** button to start testing. When the intrusion object is detected, the configured computer alarm or output device will be activated. Adjust the **Sensitivity** slider if the intrusion is not detected accurately.
9. Click **OK** to apply the setting.
10. Enable monitoring to start intrusion detection.

When an intrusion event occurs, the configured computer alarm or output device will be activated, and the event will be recorded as **Intruder** in System Log for later retrieval.

More options in the Alarm dialog box:

- **Show Alarm Regions:** Displays the detection zones on the preview image.

- **Skip Frame:** Skips frames when detecting intrusion events to lower the CPU loading. The system will detect intrusion events in every other three frames approximately. Note this option may reduce the accuracy of detection.
- **Never Recycle:** When the option is selected, the alarm-triggered events will not be recycled when recycle threshold is reached.

Note:

1. Draw the detection zones as closely as possible to avoid omission of intrusion events when target objects show up from the unmarked area and only move through one of the two boundaries. In this case, the alarm will not set off.

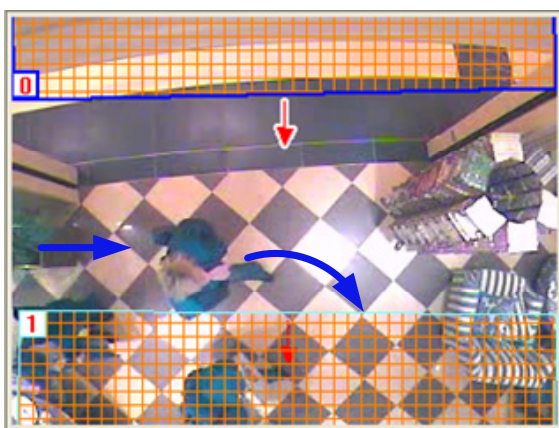


Figure 3-9

2. To view the logs for intrusion events, click **View Log, Toolbar, Tools, System Log, Monitor Table** and then click the **Monitor** tab.
 3. Optionally create a schedule for intrusion alarm to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.2 Object Index

The Object Index feature allows you to view the very first frame of a *continuous* movement in a video stream. With Live Object Index, you may view the most recent 50 frames captured. With Object Index Search, you may easily locate a desired event and instantly play it back by double-clicking on the image frame.

3.2.1 Setting Object Index

You can select up to 16 cameras to view live video frames.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

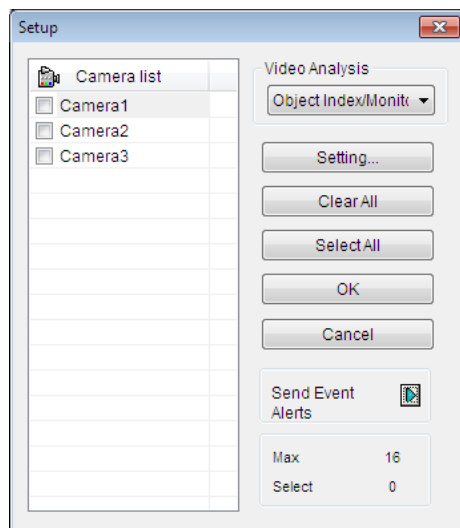


Figure 3-10

2. From the Video Analysis drop-down list, select **Object Index/Monitor Setup**, select the desired cameras, and then click **Setting**. This dialog box appears.

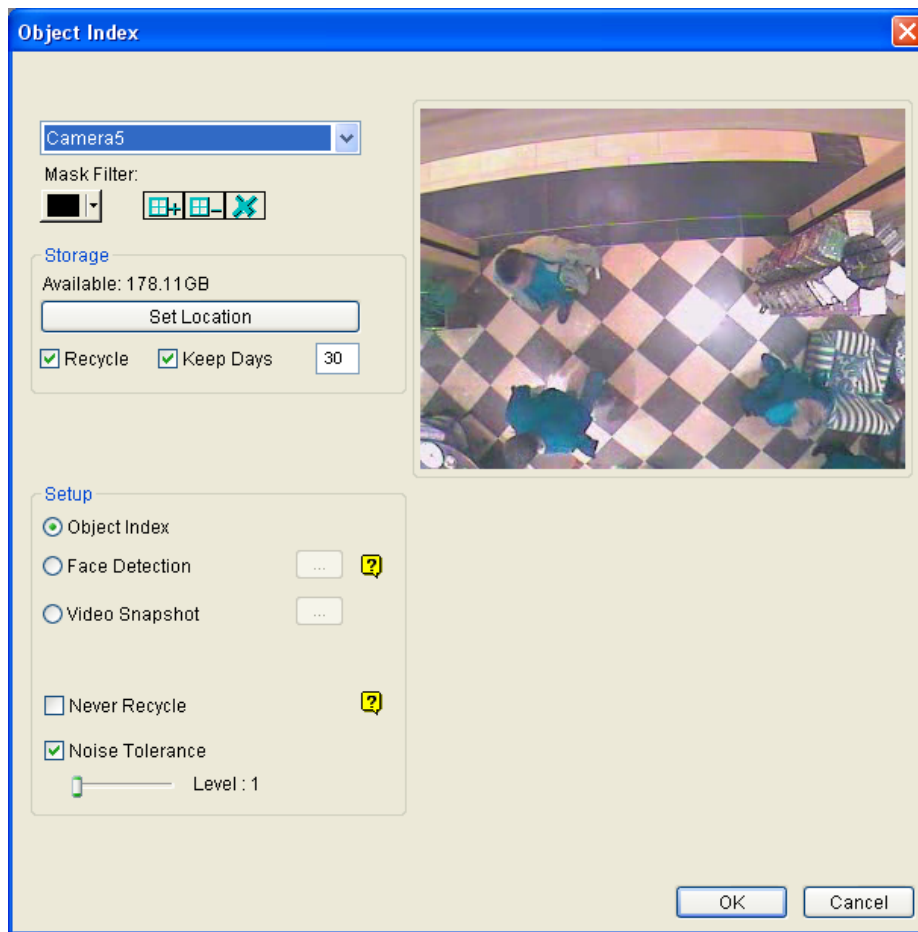





Figure 3-11

4. Select one camera from the drop-down list and configure the following.
 - **Mask Filter:** Use the mouse to outline a mask area where motions will be ignored.
 - **Set Location:** Click the button to assign a path to save the file.
 - **Keep Days:** Select the option and specify the days to store the files, from 1 day to 999 days.
 - **Recycle:** Select this option for GV-VMS to recycle the camera's storage when the free space is less than 500 MB. When both Keep Days and Recycle are selected, the system applies whichever condition that comes first. For example, if storage space is lower than what is required to hold the days of data specified in Keep Days, recycle comes first.
 - **Never Recycle:** With the option selected, the event files of object index, face detection and snapshot will not be recycled when the recycle threshold is reached.
 - **Noise Tolerance:** Use the slider to adjust the level. The higher the level, the more tolerant the system is to video noise.
5. Click **OK** to apply the settings.

Note: Optionally create a schedule for object index to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.

3.2.2 Viewing Object Index

After configuring Object Index, you can start to view the most recent frames captured, with 50 frames at most.

1. Start camera monitoring.
2. Click **Home** , select **Toolbar** , click **Tools** , and select **Live Object Index**. The Live Viewer window appears.

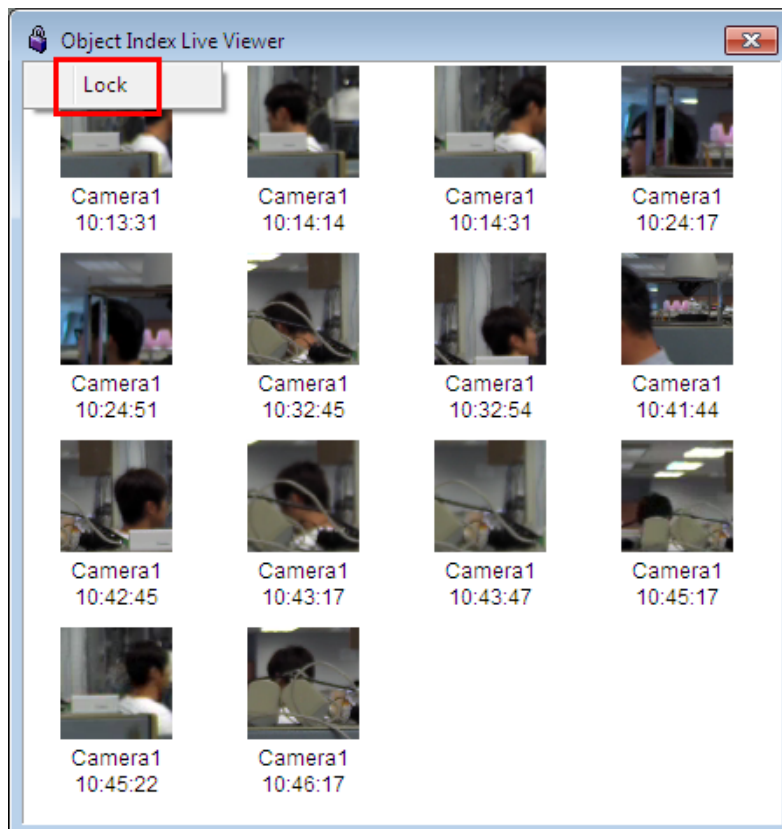




Figure 3-12

3. Click the lock icon on the Object Index Live Viewer and select **Lock** to pause the updating process.
4. Double-click a frame to play back its recorded file.

3.2.3 Searching Object Index

You can locate frames for the selected cameras and within a specific time frame.

1. Click **Home** , select **Toolbar** , click **Tools** , and select **Search Object Index**. The search window appears.

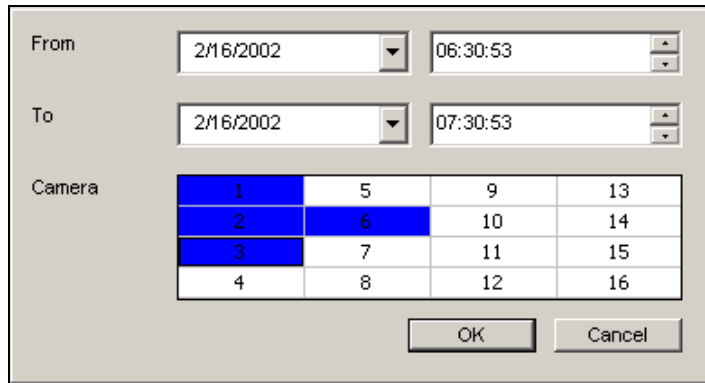


Figure 3-13 The Search Window

2. Specify a time frame and cameras, and click **OK** to start searching. The Record List dialog box appears.

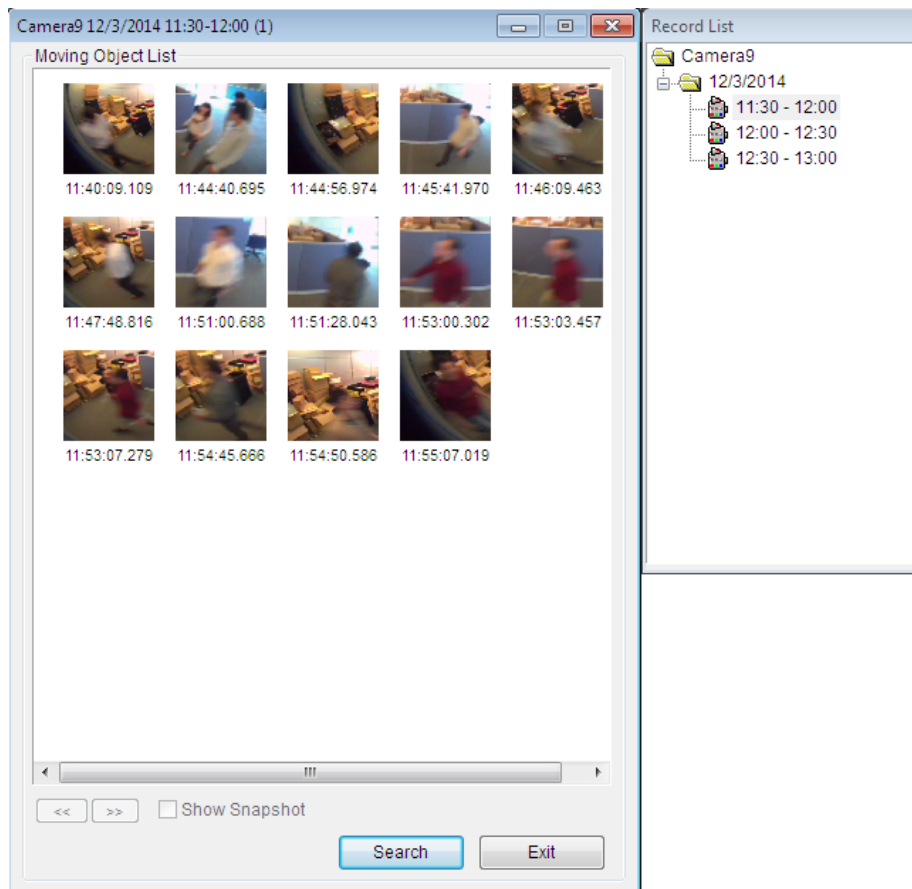



Figure 3-14 The Moving Object List Window (left) and the Record List (right)

[Record List] The list contains the search results. Double-click a camera folder to display all files found. Click one time-segment file (e.g. 10:00) to open its included frames in the Moving Object List window.

[The Moving Object List window]

- **Frames:** Double-click any frame in the window to play back its video file using the ViewLog player.
- : Click the **Next Page** button for the next page.
- **Search:** Click the button to launch the search window.
- **Exit:** Click the button to close the window.

Note: The time segments are 30-minute apart from each other, as shown in Record list in Figure 3-14.

3.3 Automatic Video Snapshots

The Video Snapshot allows the system to take up to 30 snapshots per second as monitoring starts. This function gives you a choice to keep the surveillance records in still images of JPEG format when you do not have enough disk space to store AVI-format videos.

Note: After you start monitoring, the system will start taking video snapshots whether there is motion or not.

3.3.1 Setting Video Snapshots

You can select up to 16 cameras to take video snapshots.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

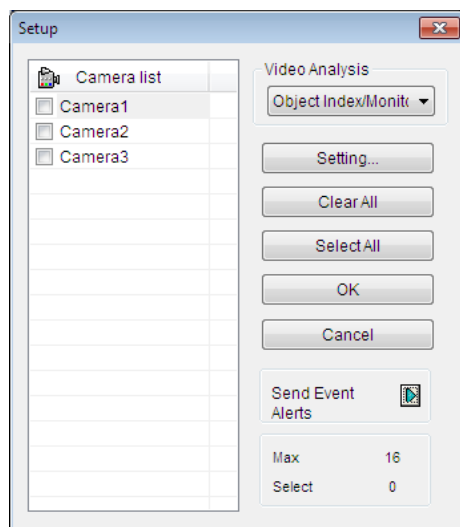


Figure 3-15

2. From the Video Analysis drop-down list, select **Object Index/Monitor Setup**, select the desired cameras, and then click **Setting**. The Object Index dialog box appears.

3. Configure the Video Snapshot settings.

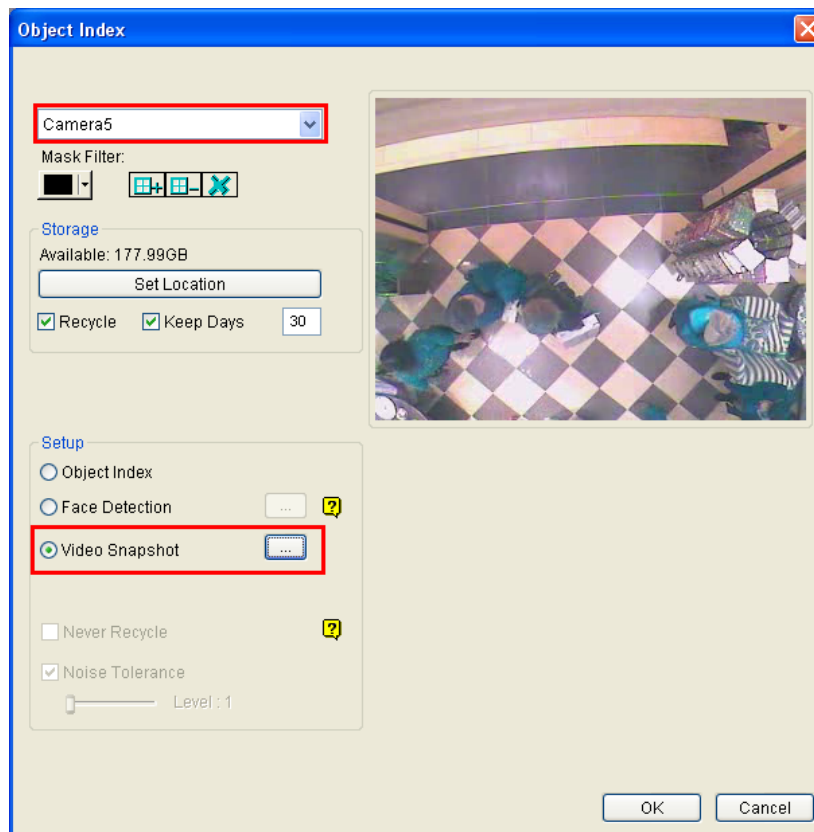


Figure 3-16

- A. Select one camera from the drop-down list.
- B. Optionally configure the Storage settings. For details, see step 4, *Setting Object Index* in Chapter 3.
- C. From the Setup section, select **Video Snapshot**.
- D. Click [...] after Video Snapshot for further setup.

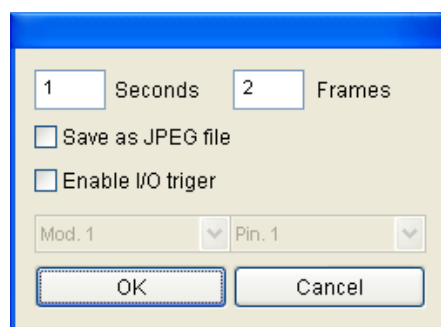


Figure 3-17

- **Frames:** Specifies the frequency of automatic video snapshot. By default, the system will take 2 frames every second when the monitoring starts.
- **Save as JPEG file:** Saves the images in JPEG format. Otherwise, you can only access the snapshots using the ViewLog player.




- **Enable I/O Trigger:** Takes snapshots only when the assigned input device is triggered.
4. To configure another camera, repeat step 2 and select a different camera.
 5. Click **OK** to apply the settings.
 6. Start monitoring to take snapshots.

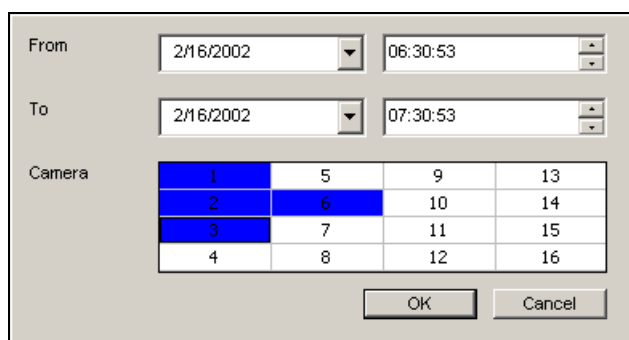
Note:

1. For details on other settings of the Video Object dialog box, see step 4, *Setting Object Index* earlier in this chapter.
 2. Optionally create a schedule for video snapshot function to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.3.2 Searching Video Snapshots

You can locate snapshots within the specified cameras and period of time with **Object Index Search**.

1. Click **Home** , select **Toolbar** , click **Tools** , and select **Search Object Index**. The search window appears.



From: 2/16/2002 06:30:53

To: 2/16/2002 07:30:53

Camera

| | | | |
|---|---|----|----|
| 1 | 5 | 9 | 13 |
| 2 | 6 | 10 | 14 |
| 3 | 7 | 11 | 15 |
| 4 | 8 | 12 | 16 |

OK Cancel

Figure 3-18

2. Specify a time period, select cameras, and click **OK** to start searching. The Record List appears.

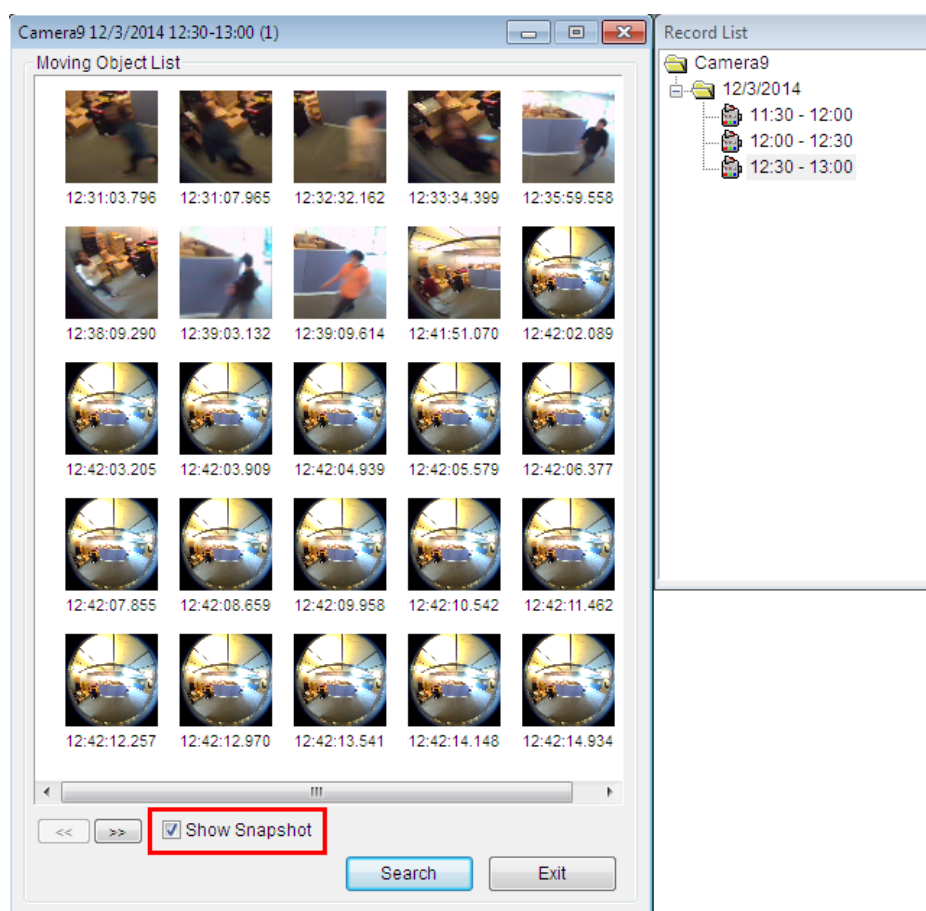


Figure 3-19

3. In the **Record List** window, expand a Camera folder to display all the date folders found and time-segment files.
4. Click one time-segment file to open its included frames in the **Moving Object List** window.
5. To display the image with your default image viewer of Windows, e.g. Paint, select **Show snapshot** at the bottom of the Moving Object List window and double-click the desired frame.



Note: The **Show snapshot** function is only supported for video snapshots, with **Save as JPEG file** disabled (Figure 3-17).

3.4 Face Detection

The Face Detection enables the system to detect and record human faces. This feature captures human faces only, ignoring other body parts, objects or background views. Moreover, it can capture each face separately when a group of people comes in the view together.

3.4.1 Setting Face Detection

Up to 16 cameras can be configured for this application.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

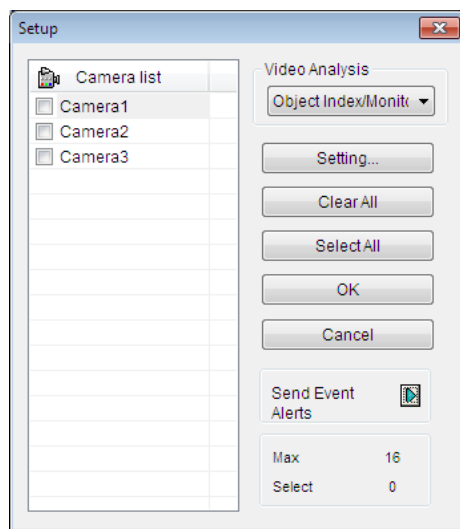


Figure 3-20

2. From the Video Analysis drop-down list, select **Object Index/Monitor Setup**, select the desired cameras, and then click **Setting**. The Object Index dialog box appears.

3. Configure the Face Detection settings.

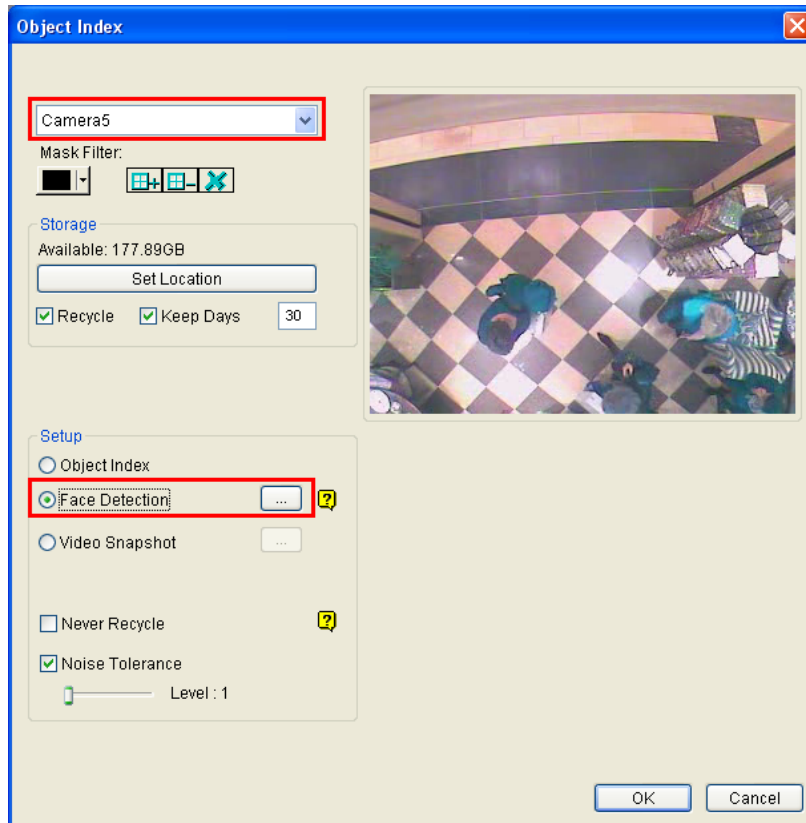


Figure 3-21

- A. Select one camera from the drop-down list.
 - B. Optionally configure the Mask Filter, Storage and Noise Tolerance settings. For details, see step 4, *Setting Object Index* earlier in this chapter.
 - C. From the Setup section, select **Face Detection**.
 - D. Click [...] after Face Detection to adjust the sensitivity. The higher the value, the more sensitive face detection is.
4. To configure another camera, repeat step 2 and select a different camera.
 5. Click **OK**.
 6. Start the monitoring.

Note:

1. For details on other settings of the Video Object Setup dialog box, see step 4, *Setting Object Index* earlier in this chapter.
 2. Optionally create a schedule for face detection to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.4.2 Searching Face Detection Snapshots

1. Click **Home** , select **Toolbar** , click **Tools** , and select **Live Object Index** to display the Live Viewer window.

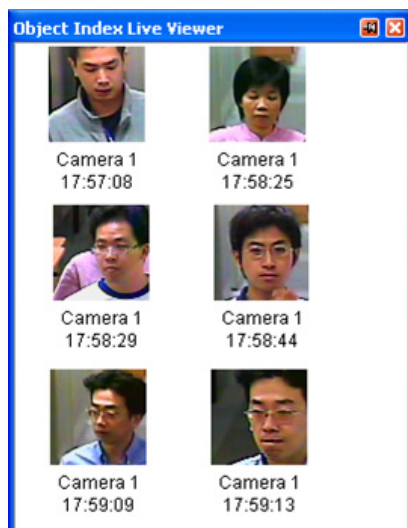


Figure 3-22

2. Double-click a desired frame to instantly play back its recorded file.

Note: Consider the following when installing the camera for face detection:

- Face contour must be clearly seen
 - Only faces tilting within the range of 15° vertically and 30° ~ 45° horizontally can be detected.
 - The face to be detected must cover least 1/10 of the screen.
-

3.5 Face Count

Note: This function will be supported in the near future.

The Face Count function allows you to count the number of faces that appear in the image. You can also select to invoke a computer alarm or trigger an output device when a face is detected or when the system is unable to detect a face.

The number of faces counted is saved to the GV-Web Report which can analyze counting data from multiple GV-VMS. For details, see *GV-Web Report User's Manual*.

Note:

1. Up to 16 cameras can be configured for this function.
2. The Face Count results are only available on GV-Web Report.

3.5.1 Installing the Camera

1. Install the camera inside an entrance pointing horizontally outward. The Face Count function is designed to detect front-view faces only, and the area of the detected face must take up 10% to 50% of the live image.

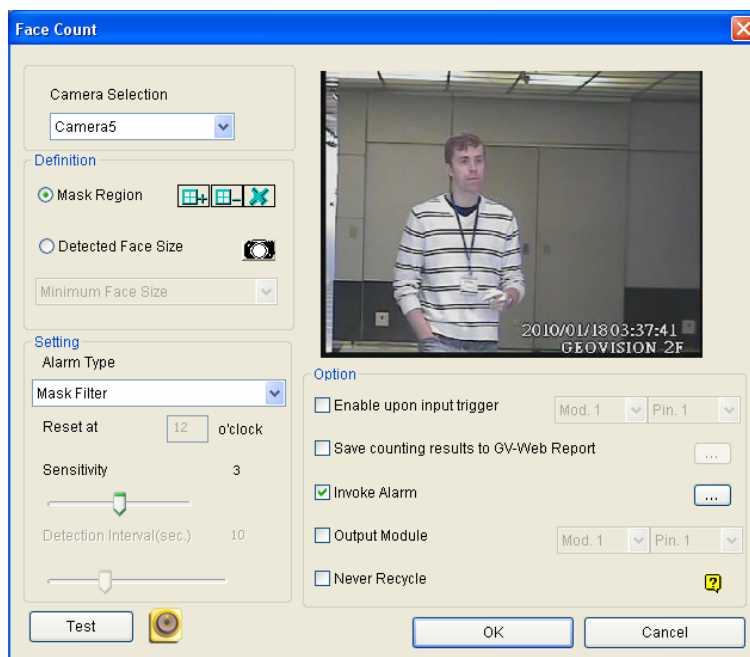


Figure 3-23

2. Avoid installing the camera where it is subjected to direct sunlight or reflections. The lighting of the entrance where you set the camera should be sufficient but not be too bright or dark. Light should be distributed evenly across faces without too much light coming from one side. If sharp shadow edges are visible in the camera view, the count accuracy might be less than what it normally is.

3.5.2 Setting Face Count

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

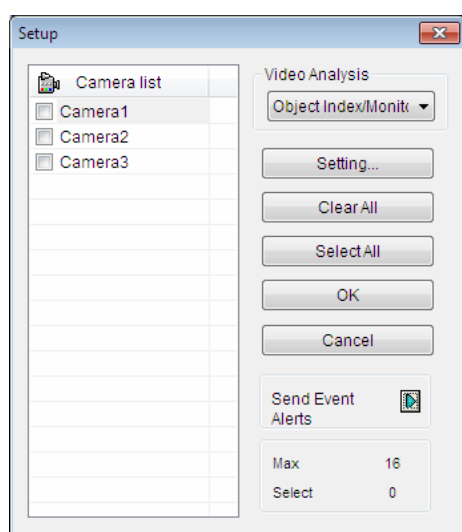


Figure 3-24

- From the Video Analysis drop-down list, select **Face Count**, select the desired cameras, and then click **Setting**. This dialog box appears.

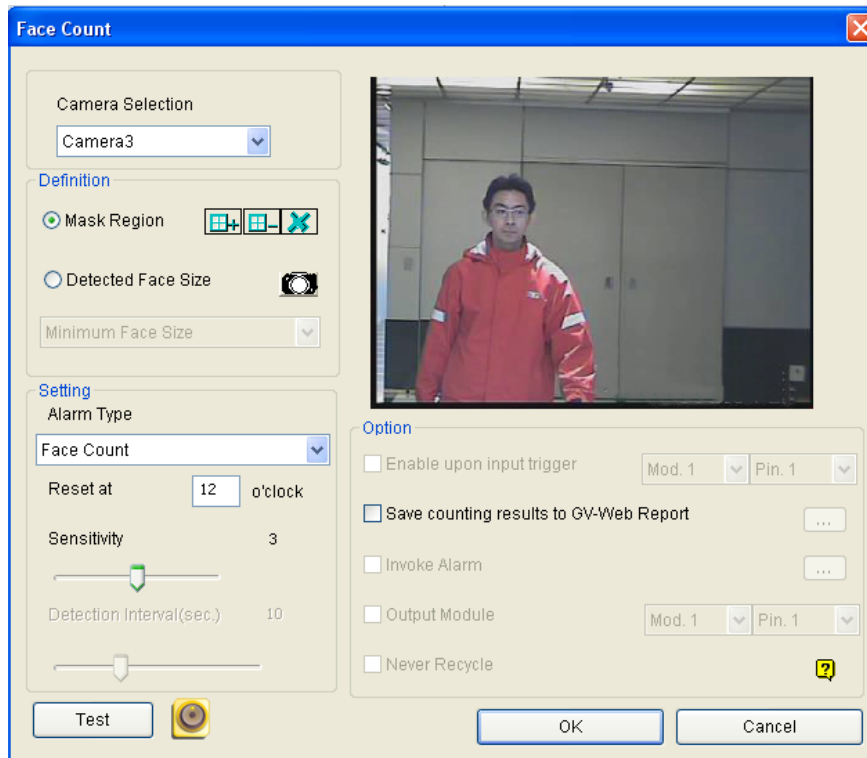



Figure 3-25

- Under **Camera Selection**, select a camera from the drop-down list to be configured.
- The following configurations are available:

[Definition]

- **Mask Region:** Use the mouse to outline a mask area where motion will be ignored.
- **Detected Face Size:** You can adjust the **Minimum Face Size** and the **Maximum Face Size** to instruct the system to only detect faces within that size range. Pause the live image by clicking the  button before you can adjust the size.

[Setting]

- **Alarm Type**
 - ⊙ **Face Count:** Counts the number of faces. The counting results are only available on the GV-Web Report. To connect to the GV-Web Report, see the **Saves counting results to GV-Web Report** option below.
 - ⊙ **Mask Filter:** Detects faces and invokes a computer alarm or triggers an output device.
 - ⊙ **Mask Filter (Inverse Alarm):** Invokes a computer alarm or triggers an output device when the system is unable to detect a face after the number of seconds specified in the **Detection Interval**.

- **Reset at:** Type a counting reset time between 0 and 23. For example, if you type 23, the number of faces counted will become zero at 23 o'clock daily.
- **Sensitivity:** Adjust the detection sensitivity by moving the slider. The higher the value the more sensitive the system is to motion. The default value is 3.
- **Detection Interval:**
 - When **Mask Filter** and **Enable Upon Input Trigger** are both selected, the **Detection Interval** slider specifies the number of seconds you want the system to detect faces when the input device is triggered. For example, the input device is a card reader and a door lock has been set up as the output device. After you swipe the card triggering the reader, the system starts to detect the face for the duration specified. If the face is detected within the duration, the door will be open; otherwise the door will remain locked.
 - When **Mask Filter (Inverse Alarm)** is selected, the system will attempt to detect the faces for the duration specified for **Detection Interval**. For example, if you set the interval to 15 seconds, the alarm will be triggered if the system cannot detect any faces within 15 seconds after motion is detected.

[Option]

- **Enable upon input trigger:** The system will begin detecting only when the input device is triggered. Assign an input module and pin number for the device.
- **Saves counting results to GV-Web Report:** Saves the face counting results to the GV-Web Report. When the option is selected, the dialog box below appears. Type the **Domain Name or IP Address**, **Port**, **User Name**, and **Password** of the GV-Web Report. After settings, click the **Test** button to see if the connection succeeds.

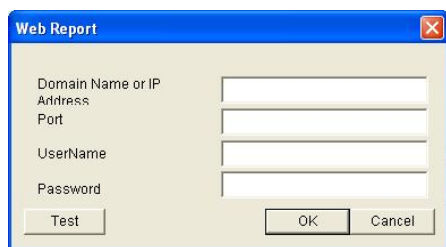


Figure 3-26

- **Invoke Alarm:** Activates the computer sound alarm when faces are detected under **Mask Filter** or when the system is unable to detect faces under **Mask Filter (Inverse Alarm)**. Click the [...] button to designate a sound file to be the alarm sound.
- **Output Module:** Activates the output device when faces are detected under **Mask Filter** or when the system is unable to detect faces under **Mask Filter (Inverse Alarm)**. Assign an output module and pin number for the device.

- **Never Recycle:** Prevents recorded events from being recycled when the recycle threshold is reached.
5. Click the **Test** button to see if the settings have been configured according to your preference. If you have set a detection interval, the test will only run for the number of seconds you specified.
 6. Click **OK** to apply the settings.
 7. Start monitoring to run the application.

Note:


1. Events triggered under **Mask Filter** or **Mask Filter (Inverse alarm)** will be recorded to the System Log for later retrieval. In the System Log, the events are recorded as **Face Count** under the **Monitor** tab (ViewLog < Toolbar < Tools < System Log).
 2. The **Face Count** results will only be saved when **Saves counting results to GV-Web Report** is selected and the GV-Web Report is connected.
 3. The counter function is not suggested to be applied in fisheye cameras.
 4. Optionally create a schedule for face count to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.6 Privacy Mask Protection

The Privacy Mask can block out sensitive areas from view, covering the areas with black boxes in both live view and recorded clips. This feature is ideal for locations with displays, keyboard sequences (e.g. passwords), and for anywhere else you don't want sensitive information visible.

You can also choose to retrieve the block-out areas during playback. The retrievable areas will be protected by password.

3.6.1 Setting a Privacy Mask

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

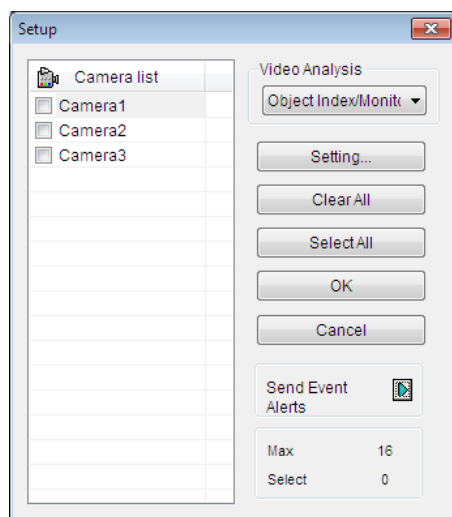


Figure 3-27

2. From the Video Analysis drop-down list, select **Privacy Mask Setup**, select the desired cameras, and then click **Setting**. This dialog box appears.

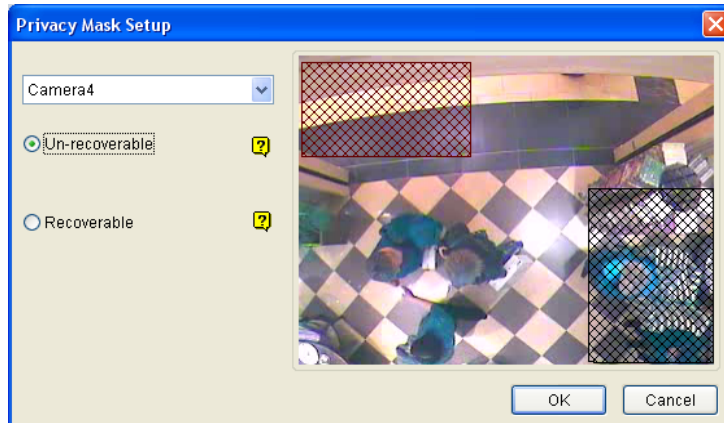


Figure 3-28


3. Select a camera from the drop-down list.
4. Select Un-recoverable and/or Recoverable.
 - **Un-recoverable:** The block-out area(s) will not be retrievable in the recorded clips.
 - **Recoverable:** The block-out area(s) will be retrievable with password protection.
5. Drag on the area(s) where you want to block out on the image. You will be prompted to click **Add** to save the setting. The Un-recoverable region is marked in black, while the recoverable region is shown in red.
6. Click **OK** to apply the settings.

Note: Optionally create a schedule for Privacy Mask to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.

3.6.2 Granting Access Privileges to Recoverable Areas

By default, only a Supervisor account is granted access to see the block-out areas on recorded videos.

To grant access rights to Power Users and Users, follow the steps below.

1. Click the login user button  on the main screen, select **Password Setup**, and select **Local Account Edit**. The Local Account Edit dialog box appears.
2. Select one account, click the **Privacy Mask** tab, select **Restore Recoverable Video** and select the camera to grant the privilege.

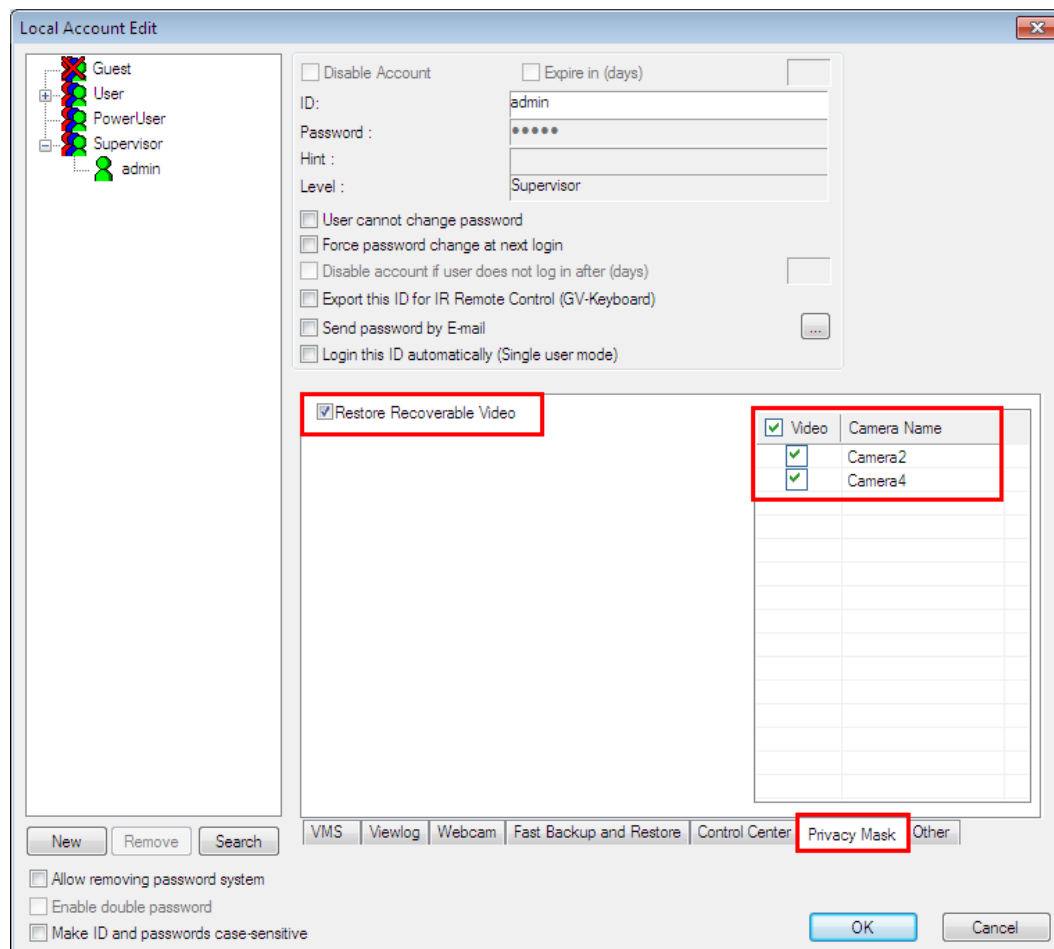


Figure 3-29





Note: If you open the event files (*.avi) directly from local disks, the valid ID and password are also required to access the block-out areas. For details on retrieving the block-out areas in the exported files, see *Merging and Exporting Video* in Chapter 4.

3.7 Panorama View

A panorama view joins multiple camera images together and allows you to monitor a large area in one view. The cameras selected for the panorama view will keep the recording in original format. Up to 4 sets of panorama views can be created. There are two ways to create a panorama view:

- Stitch camera images together by overlapping and matching reference points
- Use the Easy Mode to place camera images next to each other with no overlapping

Follow the steps below to access this feature.

1. Click **Home** , select **Toolbar** , and select **Content List** . The Content List appears.
2. Select **Panorama** and click **Configure** . The Panorama View Setup dialog box appears.

3.7.1 The Main Window

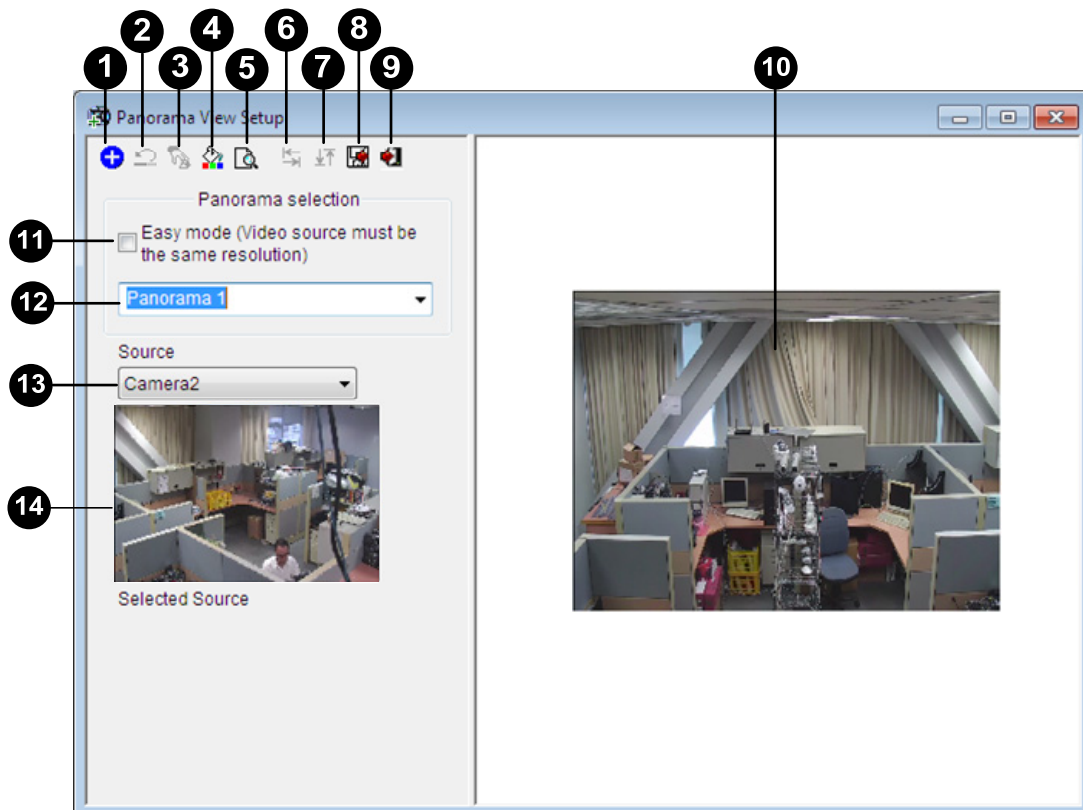


Figure 3-30

The controls on the Panorama View Setup dialog box:

| No. | Name | Description |
|-----|--------------------|---|
| 1 | Add | Adds an image for automatic splicing. |
| 2 | Undo | Cancels the settings. |
| 3 | Manual Setting | Manually splices the images together. |
| 4 | Blending | Makes the spliced images seamless. |
| 5 | Demo | Displays the setup procedure. |
| 6 | Left / Right | Place the selected image to the left or right of the previous image. |
| 7 | Top / Bottom | Place the selected image on the top or bottom of the previous image. |
| 8 | Save Before Exit | Saves the created panorama view and closes the dialog box. |
| 9 | Exit | Closes the dialog box. |
| 10 | Preview Window | Displays the selected source image or the spliced images. |
| 11 | Easy Mode | Places camera views next to each other with no overlaps. |
| 12 | Panorama Selection | Selects the panorama set for the images to be spliced together. Clicks again to rename the panorama set. |
| 13 | Source | Selects the source image to be spliced. |
| 14 | Selected Source | Displays the selected image. |

3.7.2 Stitching a Panorama View with Overlapping Areas

To stitch images from different cameras together, follow these steps:

1. Select one panorama set (No. 12, Figure 3-30) from the drop-down list. If you want to rename the selected panorama set, type the name in the field.
2. Select one camera from the Source drop-down list and click **Add**. The image will be the reference image on which other images will be sliced.
3. Select another camera from the Source drop-down list (No. 13, Figure 3-30) and click **Manual Setting** (No.3, Figure 3-30). This dialog box appears.

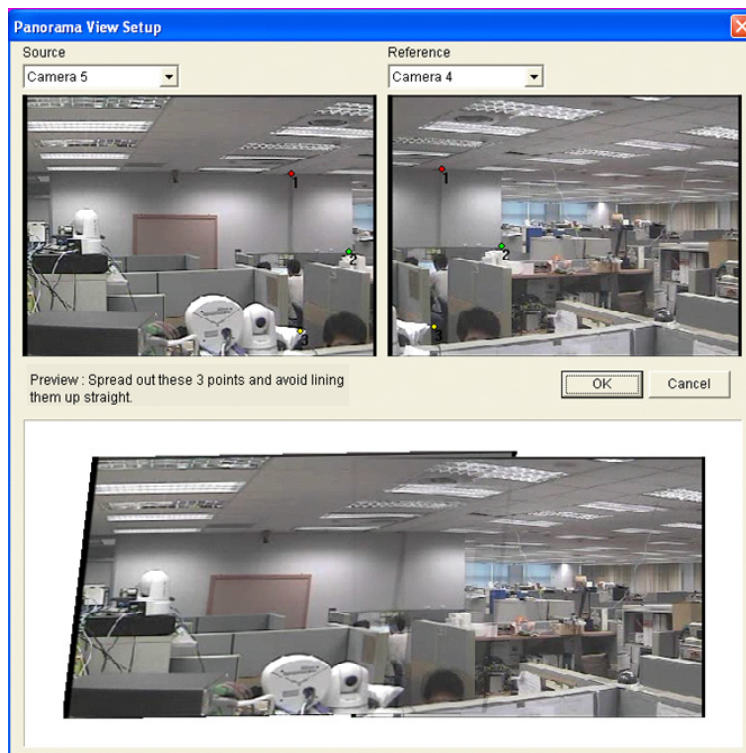


Figure 3-31

4. From the Source drop-down list, select one camera as the Source image to be stitched with the Reference image.

5. To stitch the two images together, click on a significant point in the Reference image and then look for the same point in the Source image. A dialog box of point selection will prompt you to confirm. You need to set up 3 points for stitching.

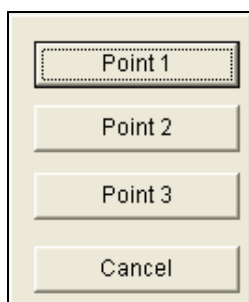


Figure 3-32

Note: For the best result, position the points in the overlapping areas on both images. Avoid placing the points in a cluster or lining them up straight.

6. The resulting image is displayed in the Preview window. If satisfied with the result, click **OK** to exit the setup dialog box. If not, re-enter the 3 points for stitching.
7. If you want to stitch a third image or more, click **Manual Setting** and repeat Steps 3 to 5 multiple times.
8. When you finish stitching images, click the **Save Before Exit** button (No.6, Figure 3-30) to save the created panorama view before exiting the Panorama View Setup dialog box.

Note: The resolution of the images to be stitched will be reduced to 320 x 240. A panorama view has a resolution limit of 1920 x 1080. Once the limit is reached, you cannot stitch more images to the created panorama view.

9. This panorama view is saved to the Panorama category in the Content List.

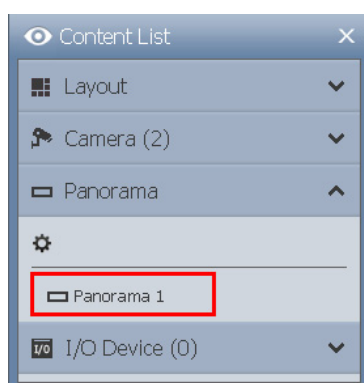


Figure 3-33

10. Drag the created panorama view to the live view grid for display.

3.7.3 Easy Mode with No Overlapping Area

When you have multiple camera views covering areas right next to each other with no overlaps, the Easy Mode allows you to simply place camera views together.

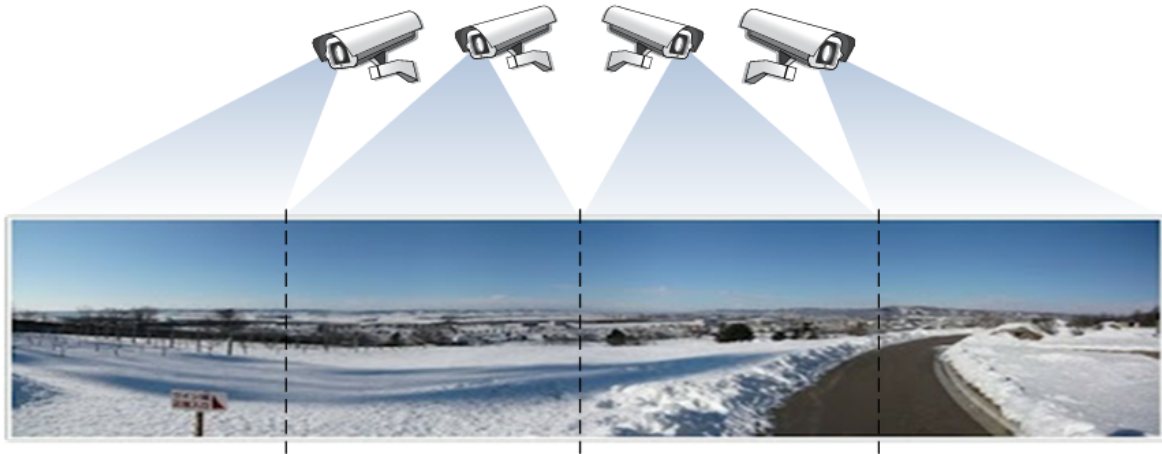



Figure 3-34

1. Select **Easy Mode (Video source must be of the same resolution)** (No. 11, Figure 3-30).
2. Use the **Source** drop-down list (No. 13, Figure 3-30) to select the first camera view to be placed in the panorama and click the **Add**  button. The first camera view is added to the Preview Window.

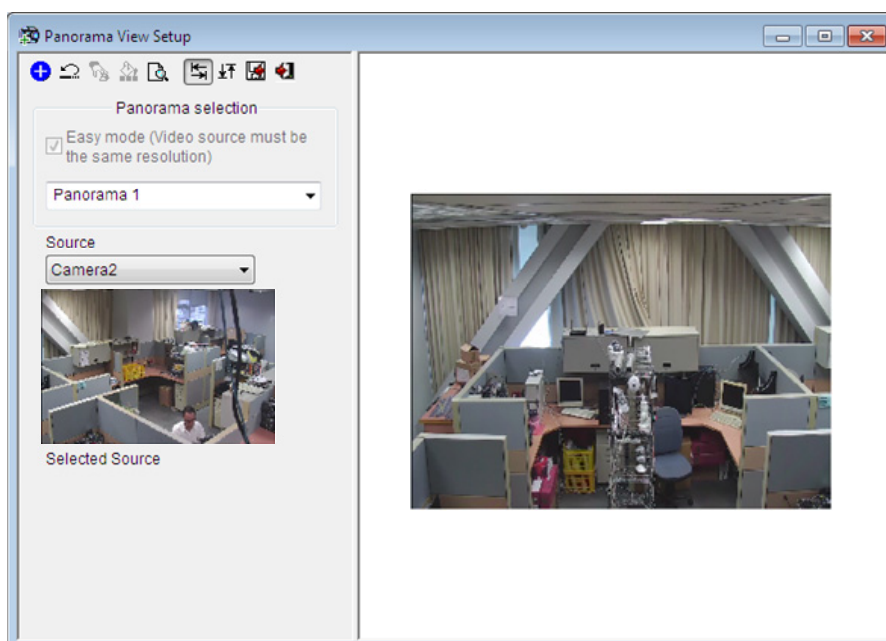



Figure 3-35

3. To add a second camera view, select the camera from the **Source** drop-down list.

4. To place the camera view on the left or right of the first camera view, click the  icon and select to place the second view on the **Left** or **Right** of the first view.

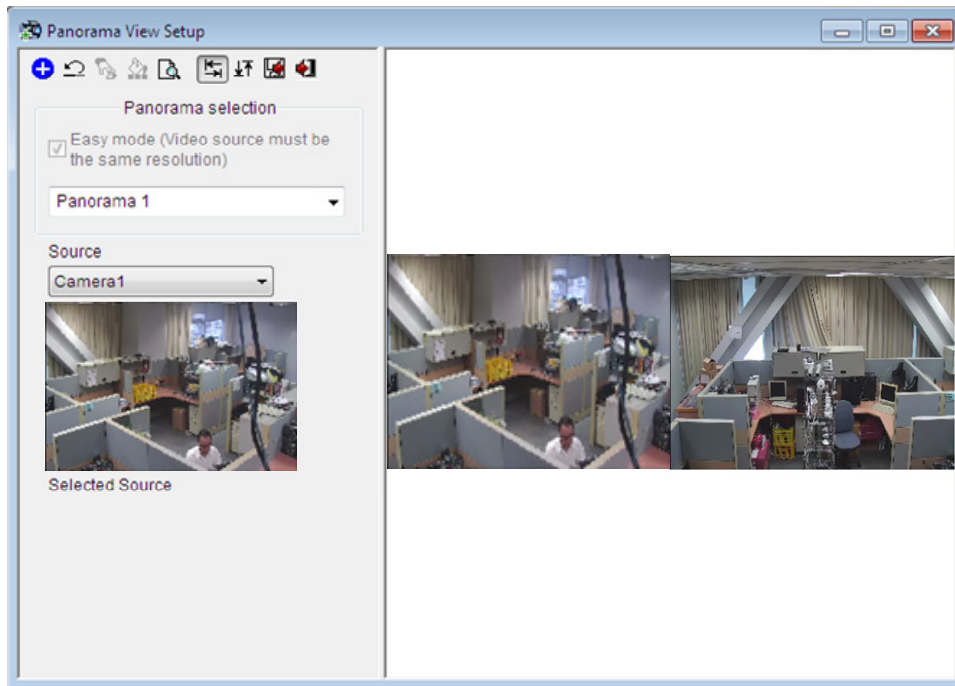






Figure 3-36

5. To place the camera view above or below the first camera view, click the  icon and select to place the second view on the **Top** or **Bottom** of the first view.
6. Repeat the steps for any additional cameras.

Note: You will only be able to add additional cameras next to the last camera view added. For example, when adding a third camera, you can only use the direction buttons   in relation to the second camera. You will not be able to go back and select the first camera.

7. When you finish stitching images, click the **Save Before Exit** button  before exiting.

8. This panorama view is saved to the Panorama category in the Content List.

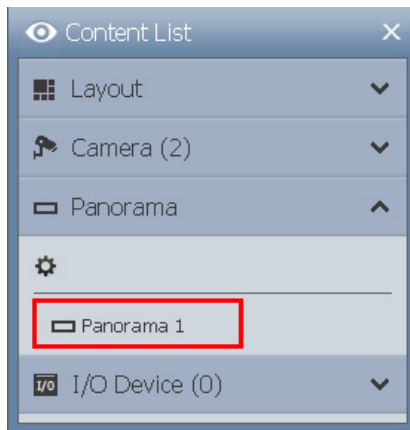


Figure 3-37

9. Drag the created panorama view to the live view grid for display.

3.7.4 Accessing a Panorama View

Drag the configured panorama from the Content List (Figure 3-38) to the live view. The panorama view is displayed on the main screen.

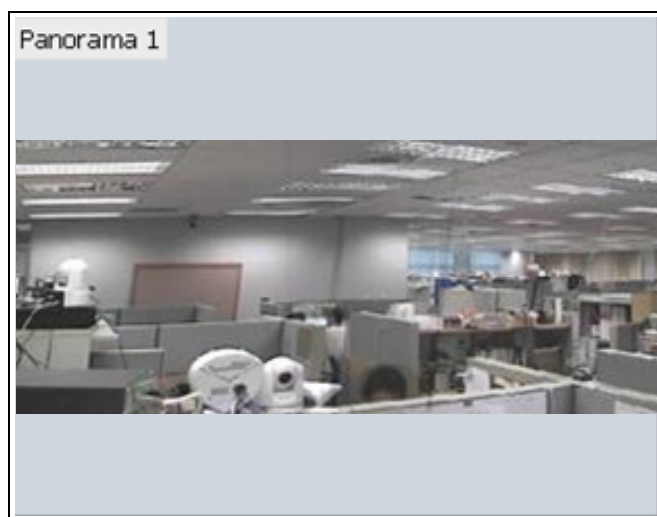


Figure 3-39

Right-click the panorama view to have these options:

- **Snapshot:** Save the current panorama view as an image file.
- **Zoom:** Put the cursor on the live view and scroll your mouse to zoom the live view.

3.8 Video Defogging

Smoky environments and bad weather, such as rain, snow or fog, all affect image quality and reduce scene visibility. This feature helps to enhance image quality for live viewing.

Note: This function takes high CPU and memory usage. Make sure at least 1 GB of RAM is installed on your system.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

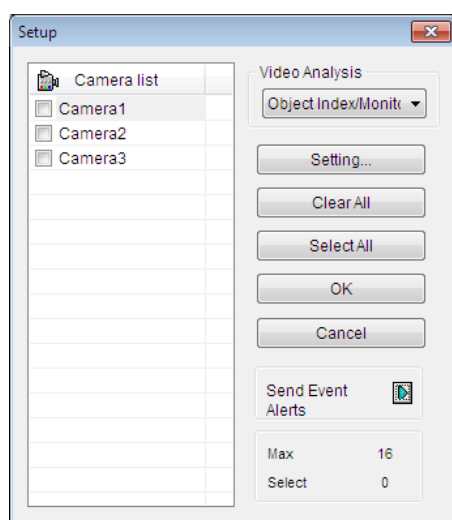


Figure 3-40

2. From the Video Analysis drop-down list, select **Defog**, select the desired cameras, and then click **Setting**. This dialog box appears.

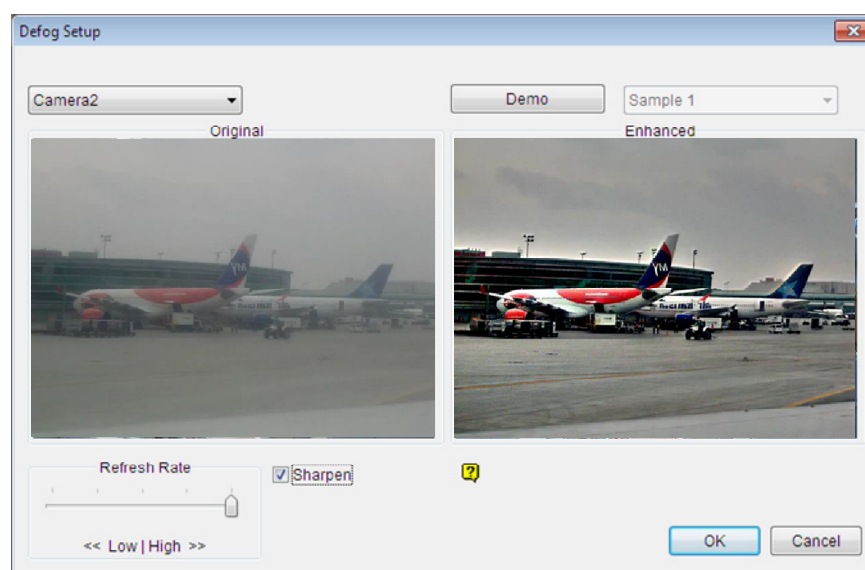





Figure 3-41

3. Use the drop-down list to select a camera.
4. When the image enhancement is enabled, the system load will increase. Adjust the **Refresh rate** by moving the slider bar to optimize system performance.
5. If you want to view the demonstration of this function, click the **Demo** button.

Note:

1. This function only applies to live view and does not affect the recorded video. To apply defogging to recorded videos during playback, select **ViewLog** , select **Toolbar** , select **Configure** , select **Effects** and then select **Defog**.
 2. If dual-stream IP channels are applied, for better image quality, it is recommended to change the streaming to single stream before you enable these video analysis effects. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.
 3. Optionally create a schedule for video defogging to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.9 Video Stabilization

Images from a shaky camera are jittery or blurry. This feature helps to reduce camera shake, leaving you with clear and steady images.

Note: This function takes high CPU and memory usage. Make sure at least 1 GB of RAM is installed on your system.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

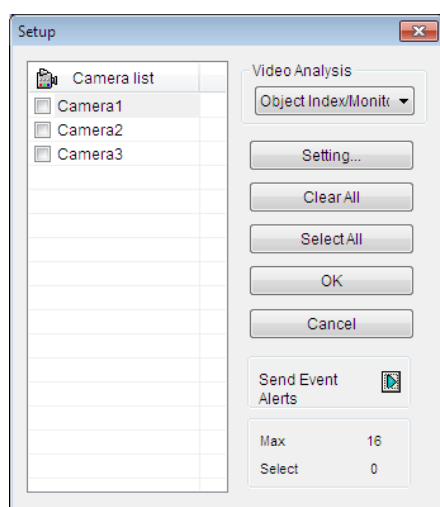


Figure 3-42

2. From the Video Analysis drop-down list, select **Stabilizer**, select the desired cameras, and then click **Setting**. This dialog box appears.

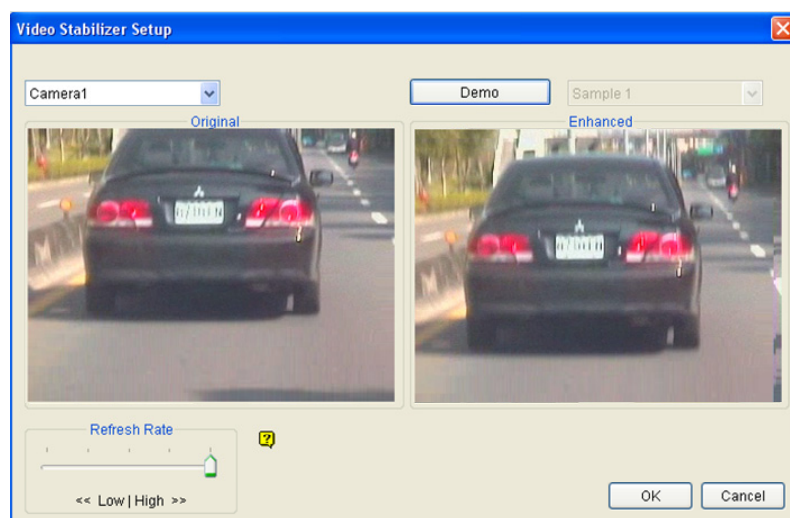





Figure 3-43

3. Use the drop-down list to select one camera. The enhanced view is shown on the right.




4. When the image enhancement is enabled, the system load will increase. Adjust the **Refresh rate** by moving the slider to optimize system performance.
5. If you want to view the demonstration of this function, click the **Demo** button.

Note:

1. This function only applies to live view and does not affect the recorded video. To apply stabilization to recorded videos during playback, select **ViewLog** , select **Toolbar** , select **Configure** , select **Effects** and then select **Stabilizer**.
 2. For better image quality, it is recommended to change the streaming to single stream before you enable video stabilization. However, system loading will increase. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.
 3. Optionally create a schedule for stabilization to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-

3.10 Wide Angle Lens Dewarping

Camera images can sometimes appear curved toward the edges of the view. This feature helps correct distortion towards the edge of the camera view.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Camera Install**. The IP Device Setup dialog box appears.

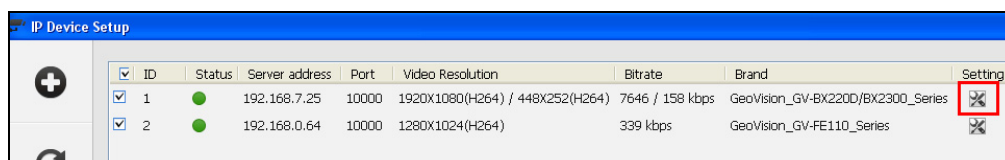


Figure 3-44

2. Click **Settings** . This dialog box appears.

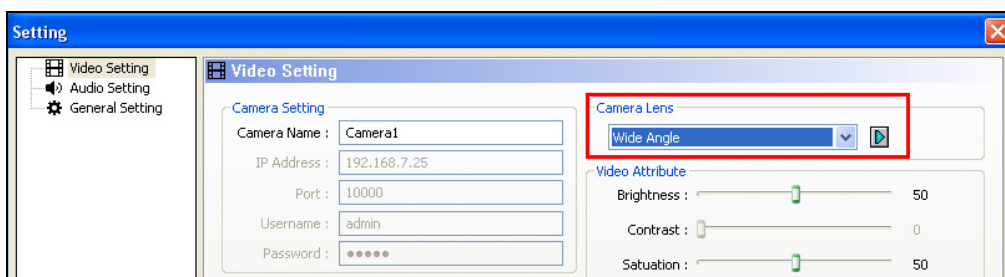



Figure 3-45

3. Use the **Camera Lens** drop-down list to select **Wide Angle**.
4. Click the  button. This dialog box appears.

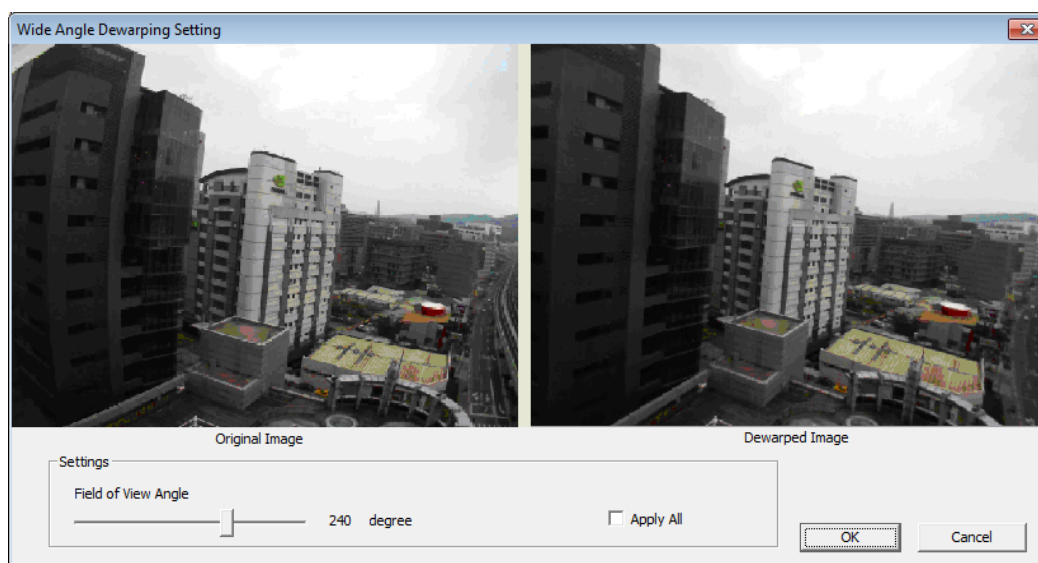





Figure 3-46

5. Move the slider to adjust the degree of warping. The adjusted view is shown on the right.

6. Click **OK**. The dewarping is immediately applied on the live view.

Note:

1. This function only applies to live view and does not affect the recorded video. To apply stabilization to recorded videos during playback, select **ViewLog** , select **Toolbar** , select **Configure** , select **Effects** and then select **Wide angle lens dewarping**.
 2. If dual-stream IP channels are applied, for better image quality, it is recommended to change the streaming to single stream before you enable wide angle lens dewarping. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.
-

3.11 Advanced Motion Detection

To avoid false motion detection, the Advanced Motion Detection feature provides five solutions:

- Designate up to 5 levels of motion detection sensitivity for each outlined area
- Mask off unwanted areas for monitoring, such as cloud and tree movement
- Ignore video noise when the lighting condition is poor or changed
- Set a minimum and maximum object size to only detect objects within the size range
- Ignore environmental changes such as rain, snow and tree movement

Note: You can only enable either motion detection by sensitivity or by object size at a time.

1. Click **Home** , select **Toolbar** , click **Configure** , select **System Configure** and click **Record Setting**. This dialog box appears.

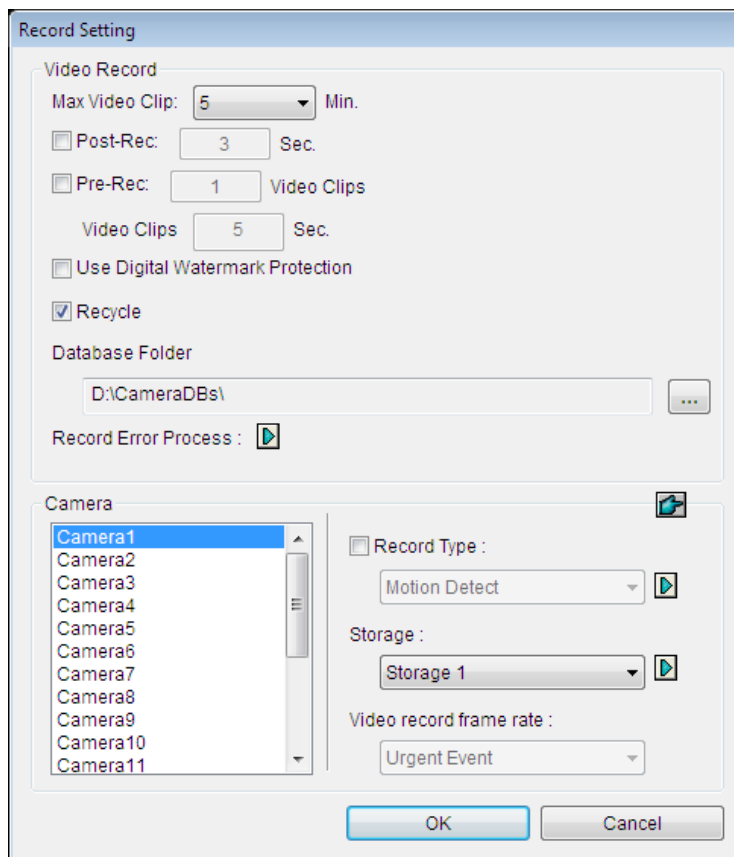



Figure 3-47

2. From the Camera section, select one camera, select **Motion Detect** from the Record Type drop-down list, and click the  button. This dialog box appears.

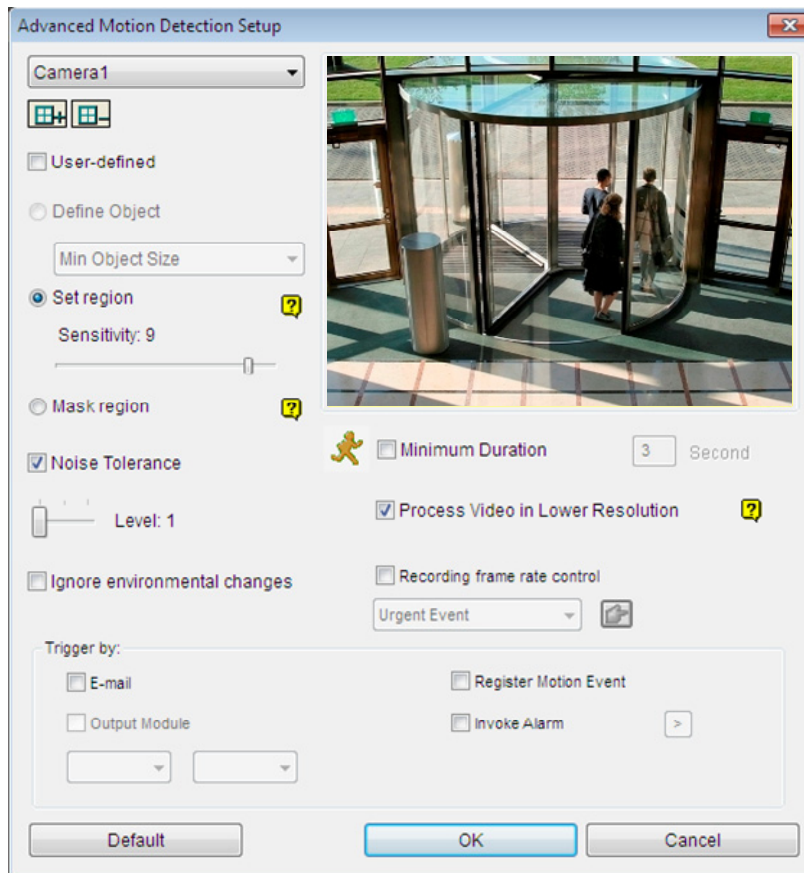


Figure 3-48 Advanced Motion Detection Setup

3. Optionally configure the following.
 - **User-defined:** Limits motion detection to objects within a size range. Select **User-defined** and select **Define Object**. Select **Min. Object Size** or **Max. Object Size** from the drop-down list and then drag an area on the image.
 - **Set Region Sensitivity:** Sets different detection sensitivities to the specified areas. Uncheck **User-defined**, adjust the sensitivity level by moving the slider, and then drag an area on the image. By default, the whole camera view is set to level 9. You can create several areas with different sensitivity levels.
 - **Mask Region:** Ignores motions in a certain area. Click **Mask Region** and then drag an area on the image.
 - **Noise Tolerance:** Ignores video noise when light changes. Move the slider to adjust the level. The higher the level, the more tolerant the system is to video noise.
 - **Ignore environmental changes:** Ignores environmental changes such as rain or snow.

- **Minimum Duration:** Sets the minimum duration for which motions must persist for the system to issue a motion alarm. Specify the minimum duration in seconds (Max. 60 seconds).
 - **Process Video in Lower Resolution:** Reduces CPU loading by compromising detection accuracy.
 - **Recording Frame Rate Control:** Select **Urgent Event** to record detected motion in full frame rate. Select **General Event** to record only the key frames of the detected motion. To configure settings for Urgent and General Event, see *General Setting* in Chapter 2.
 - **Trigger By:** Sets the alarm type when a motion is detected. You can select to send an email notification (**E-mail**), activate an output device (**Output Module**), trigger a computer alarm (**Invoke Alarm**) and/or register the event to the system log for later retrieval (**Register Motion Event**).
4. Click **OK** to save your settings.

Note: When **Ignore environmental changes** is selected, objects moving steadily and repeatedly in the same direction for over 1.5 seconds will be filtered out and ignored.

3.12 Crowd Detection

Crowd detection is used to generate an alert when a crowd of people gathers in a specified area and exceeds the defined time threshold.

Note: Up to 16 cameras can be configured for this application.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

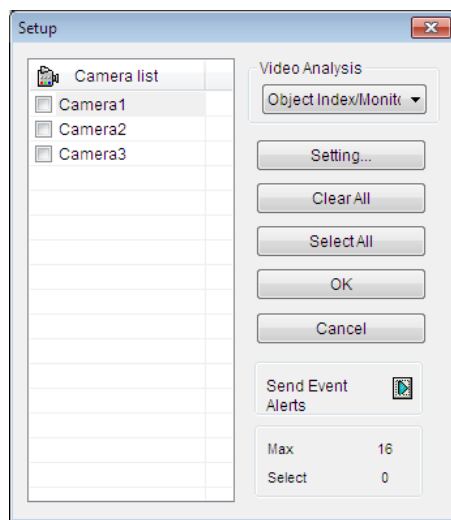


Figure 3-49

- From the Video Analysis drop-down list, select **Crowd Detection**, select the desired cameras, and then click **Setting**. This dialog box appears.

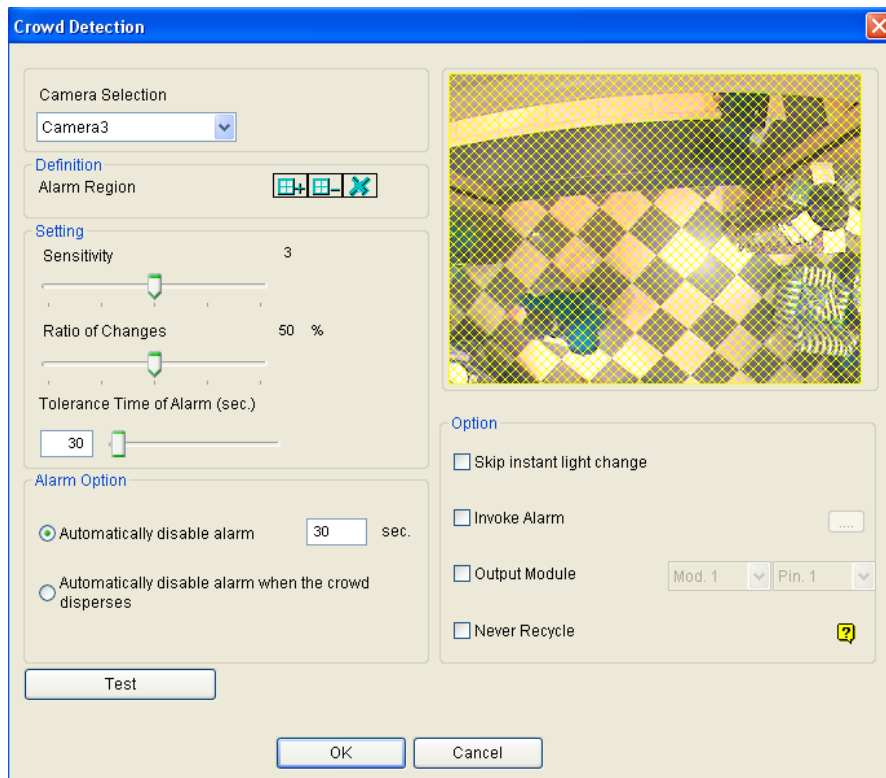





Figure 3-50


- Select a camera from the Camera Selection drop-down list.
- By default the whole camera view is set to be the alarm region. Click the  button to clear the default setting. Click the  button to freely draw the alarm region. To cancel the previously drawn area, click the  button.
- To adjust the Crowd Detection sensitivity, move the **Sensitivity** slider. The higher the sensitivity value, the more sensitive the system is to detecting crowds.
- To define the minimum ratio of change (in the alarm region) for the alarm to be activated, move the **Ratio of Changes** slider to set a value. The smaller the ratio of changes, the more sensitive the system is to the changes in the camera view.
- To define the minimum time that a crowd needs to stay for the alarm to be activated. Use the **Tolerance Time of Alarm** slider to specify a value or type a number in the blank.
- Optionally configure the following settings:
 - **Automatically disable alarm:** Triggered alarms are automatically disabled after the specified time (seconds). The default setting is **30** seconds.
 - **Automatically disable alarm when the crowd disperses:** Triggered alarms are immediately disabled when no crowds are detected.

- **Skip Instant Light Change:** Ignores sudden illumination changes to minimize false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** below for possible risk.
 - **Invoke Alarm:** Enables the computer alarm when an assemblage is detected. Click the [...] button next to the option to assign a .wav sound file.
 - **Output Module:** Activates the output device when a crowd is detected. Select this option and use the drop-down list to assign an installed output module and a pin number.
 - **Never Recycle:** Prevents the system from recycling the event files of crowd detection when the recycle threshold is reached.
9. You can click **Test** to test your settings. When an assemblage is detected in the camera view, a flashing box will appear on its location for warning. If an assemblage cannot be detected, decrease **Ratio of Changes** to increase the system sensitivity for detection.
 10. Click **OK** to apply the settings.
 11. Start monitoring to run the application.

When a crowd of people gathers in the alarm region for the specified time, its location will be highlighted on live view, the selected alarm or output will be activated, and the event will be recorded as **Crowd Detection** in System Log for later retrieval.

Note:

1. For the **Skip Instant Light Change** option:
 - When the option is selected, you may be subject to the risk that the system will not generate an alert whenever the lens of the camera is covered by malice.
 - This option is not recommended for infrared cameras.
 2. Optionally create a schedule for crowd detection to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-


To manually stop all triggered alerts, click the **Tools** button  on the triggered channel, select **Reset Alert** and select **Crowd Detection**.

- **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the crowd remains gathering over the specified tolerance time, the system will still detect it as a crowd gathering and keep generating alert.

3.13 Advanced Scene Change Detection

The Advanced Scene Change Detection detects any changes of scene, viewing angle or focus clearness made by malice in both indoor and outdoor environments.

Note: Up to 16 cameras can be configured for this application.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

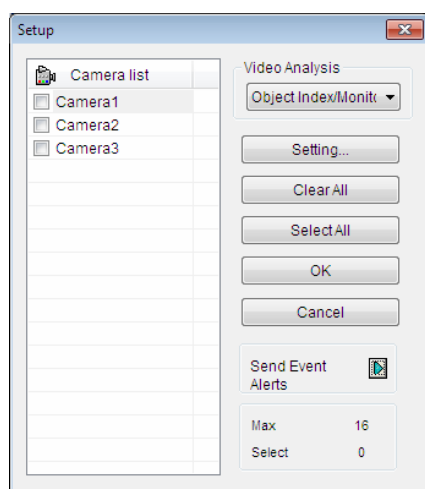


Figure 3-51

2. From the Video Analysis drop-down list, select **Advanced Scene Change Detection**, select the desired cameras, and then click **Setting**. This dialog box appears.

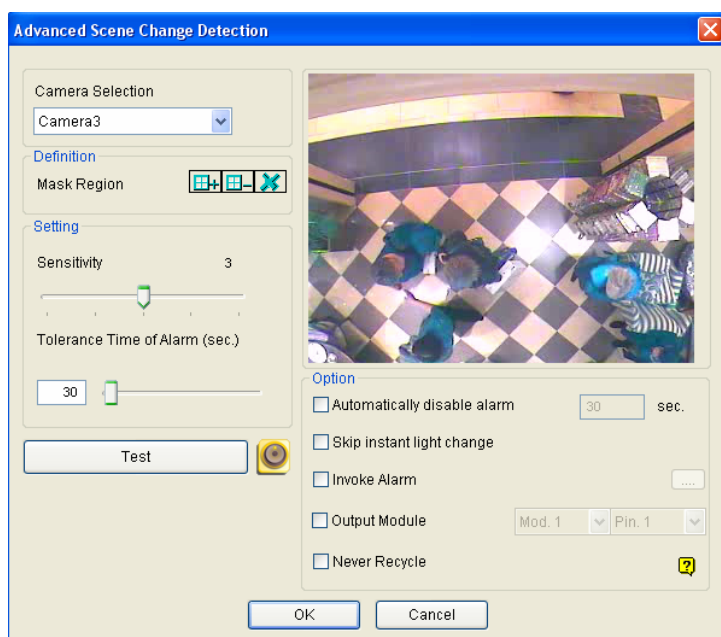



Figure 3-52

3. Select a camera from the Camera Selection drop-down list, and configure these settings:
 - **Mask Region:** If necessary, mask off the area on the camera view where any scene change will be ignored.
 - **Sensitivity:** Adjusts detection sensitivity. The higher the value, the more sensitive the system is for changes in the camera view.
 - **Tolerance Time of Alarm:** Sets the duration of scene change before an alarm condition is activated. Move the slider or type a value (in second) in the blank.
 - **Automatically Disable Alarm:** Stops all types of triggered alerts, including sound alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
 - **Skip Instant Light Change:** Ignores sudden illumination changes to minimize false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** below for possible risk.
 - **Invoke Alarm:** Enables the computer alarm when the scene change is detected. Click the [...] button next to the option to assign a .wav sound file.
 - **Output Module:** Activates the output device when the scene change is detected. Select this option and use the drop-down list to assign an installed output module and a pin number.
 - **Never Recycle:** Prevents the system from recycling the event files of scene change when the recycle threshold is reached.
4. You can click **Test** to test your settings. If the scene change cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.
5. Click **OK** to apply the settings.
6. Start monitoring to run the application.

When a scene change is detected in the camera view for the specified time, its location will be highlighted in live video, the selected alarm or output will be activated, and the event will be recorded as **Advanced Scene Change** in System Log for later retrieval.

Note:

1. For the **Skip Instant Light Change** option:
 - When the option is selected, you may be subject to the risk that the system will not generate an alert whenever the lens of the camera is covered by malice.
 - This option is not recommended for infrared cameras.
 2. Optionally create a schedule for Advanced Scene Change Detection to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.
-


To manually stop all triggered alerts, click the **Tools** button  on the triggered channel, select **Reset Alert** and select **Advanced Scene Change Detection**.

- **Reset Alert:** Disables and resets the triggered alert. After the alert is reset, if the scene change remains over the specified tolerance time, the system will still detect it as a scene change and keep generating alert.

3.14 Advanced Unattended Object Detection

The Advanced Unattended Object Detection can generate an alert when any unattended object stays within the camera view. This function can be applied to both the indoor and outdoor environments.

Note: Up to 16 cameras can be configured for this application.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

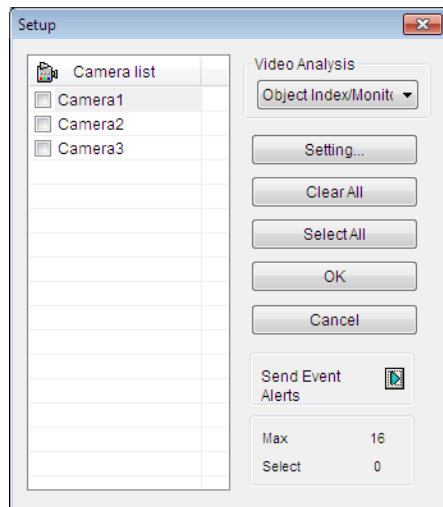


Figure 3-53

- From the Video Analysis drop-down list, select **Advanced Unattended Object Detection**, select the desired cameras, and then click **Setting**. This dialog box appears.

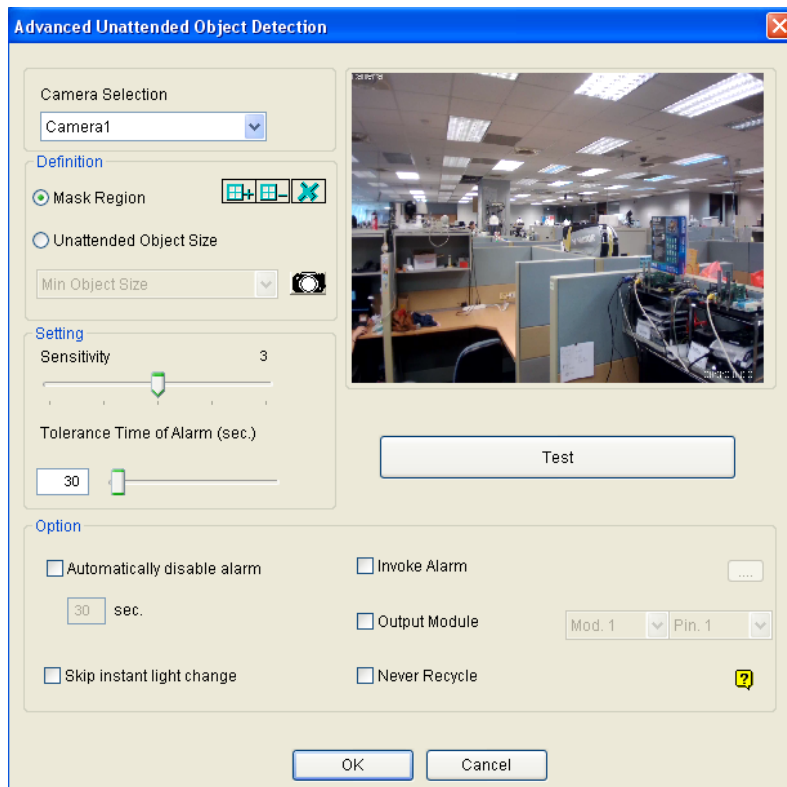


Figure 3-54

- Select a camera from the Camera Selection drop-down list.
- If necessary, use the **Mask Region** function to mask off the area on the camera view where motion will be ignored.
- Select **Unattended Object Size**, and click the Camera icon to pause live images.
- Outline **Min Object Size** on the camera view, and select **Max Object Size** from the drop-down list and outline the maximum object size on the camera view.
- To adjust the detection sensitivity, move the **Sensitivity** slider. The higher the value, the more sensitive the system is for changes in the camera view.
- To adjust the minimum time required for the alarm to be activated, adjust the **Tolerance Time of Alarm** slider or specify a value in the blank.
- Optionally configure these settings:
 - **Automatically Disable Alarm:** Stops all types of triggered alerts, including computer alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
 - **Skip Instant Light Change:** Ignores sudden illumination changes and avoids false alarms. For example, light switches can cause illumination changes suddenly. With the option

selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** in *Crowd Detection* earlier in this chapter for possible risk.

- **Invoke Alarm:** Enables the computer alarm when an unattended object is detected. Click the [...] button next to the option to assign a .wav sound file.
- **Output Module:** Enables the output device when an unattended object is detected. Select this option and use the drop-down list to assign an installed output module and a pin number.
- **Never Recycle:** With the option selected, the event files of unattended object detection will not be recycled when the recycle threshold is reached.

10. You can click **Test** to test your settings. When an object is left unattended in the camera view, a flashing box will appear on its location for warning. If the unattended object cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.

11. Click **OK** to apply the settings

12. Start monitoring to run the application.

When any unattended object is detected in the camera view for the specified time, its location will be highlighted on live view, the selected alarm or output will be activated, and the event will be recorded as **Advanced Unattended Object Detection** in System Log for later retrieval.

To manually stop all triggered alerts, click the **Tools** button  on the triggered channel, select **Reset Alert** and select **Advanced Unattended Object Detection**.




- **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the object remains unattended over the specified tolerance time, the system will still detect it as an unattended object and keep generating alert.

Note: Optionally create a schedule for Advanced Unattended Object Detection to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.

3.15 Advanced Missing Object Detection

The Advanced Missing Object Detection can generate an alert when any object disappears from the camera view. This function can be applied to both indoor and outdoor environments.

Note: Up to 16 cameras can be configured for this application.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

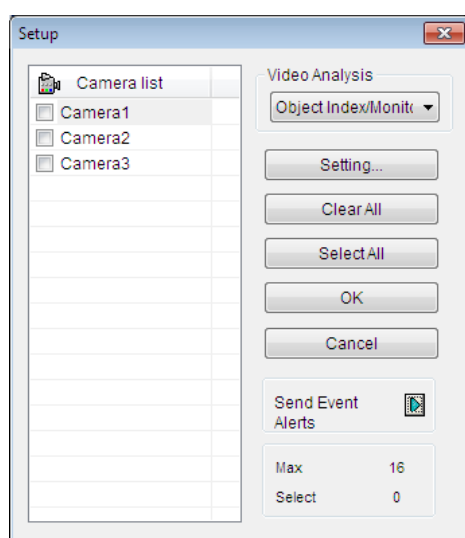


Figure 3-55

2. From the Video Analysis drop-down list, select **Advanced Missing Object Detection**, select the desired cameras, and then click **Setting**. This dialog box appears.

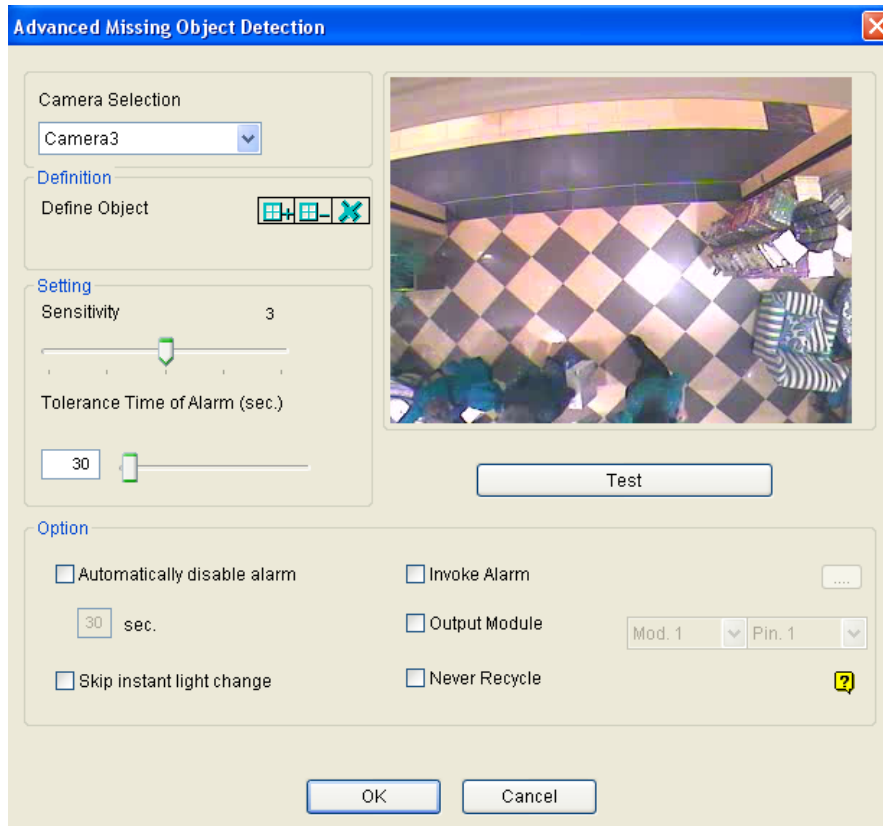





Figure 3-56

3. Select a camera from the Camera Selection drop-down list.
4. Click the  button to outline the regions on the objects you want to detect. To cancel a previously drawn area, click the  button and outline the area. To remove all previously drawn areas, click the  button.
5. To adjust detection sensitivity, move the **Sensitivity** slider. The higher the value, the more sensitive the system is for changes in the camera view.
6. To change the minimum duration required for the alarm to be activated, move the **Tolerance Time of Alarm** slider or specify a value (in seconds) in the blank.
7. In the Options section, configure these settings:
 - **Automatically Disable Alarm:** Stops all types of triggered alerts, including sound alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
 - **Skip Instant Light Change:** Ignores sudden illumination changes to avoid false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes and continue monitoring. See the **Note** in *Crowd Detection* earlier in this chapter.

- **Invoke Alarm:** Enables the computer alarm when an object is detected to be missing. Click the [...] button next to the option to assign a .wav sound file.
 - **Output Module:** Enables the output device when an object is detected to be missing. Select this option and use the drop-down list to assign an installed output module and a pin number.
 - **Never Recycle:** With the option selected, the event files of missing object detection will not be recycled when the recycle threshold is reached.
8. You can click **Test** to test your settings. When the defined object is missing, a flashing box will appear on its location for warning. If the missing object cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.
 9. Click **OK** to apply the settings.
 10. Start monitoring to run the application.

When any object, which you have outlined the regions for, disappears from the camera view for the specified time, its location will be highlighted in live view, the selected alarm or output will be activated, and the event will be recorded as **Advanced Missing Object Detection** in System Log for later retrieval.

To manually stop all triggered alerts, click the **Tools** button  on the triggered channel, select **Reset Alert** and select **Advanced Missing Object Detection**.

- **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the object remains missing over the specified tolerance time, the system will still detect it as a missing object and keep generating alert.

Note: Optionally create a schedule for Advanced Missing Object Detection to be enabled at certain times only. For details, see *Creating Schedules* in Chapter 1.

3.16 Text Overlay

You can align camera name, time stamp and triggered input name to different positions for each channel.

1. Click **Home** , select **Toolbar** , click **Configure** , and select **Video process**. This dialog box appears.

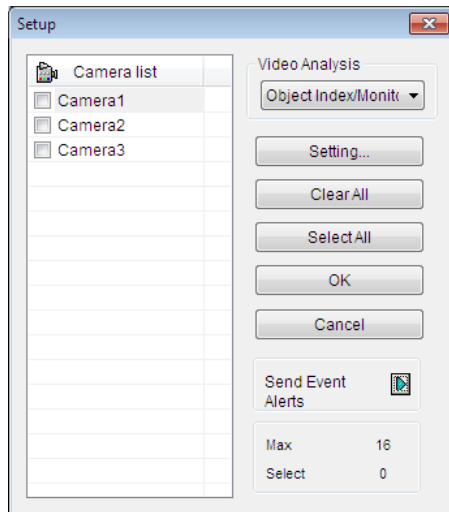


Figure 3-57

2. From the Video Analysis drop-down list, select **Text Overlay Setting**, select the desired cameras, and then click **Setting**. This dialog box appears.

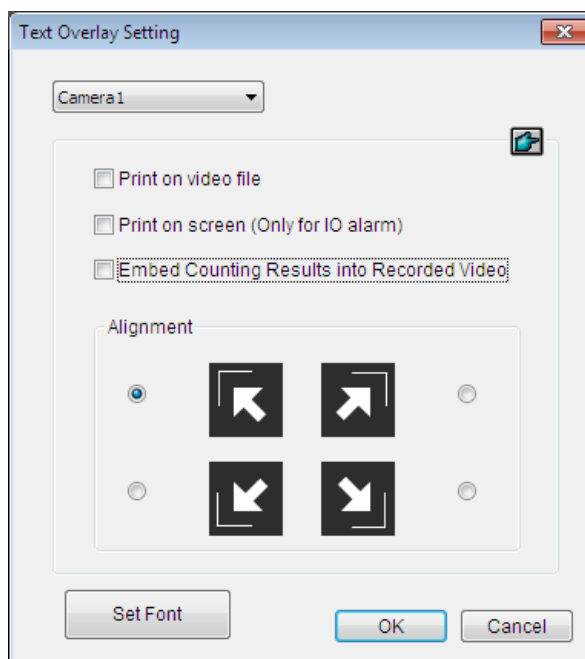






Figure 3-58

3. Select a camera from the drop-down list.
4. In the Options section, configure these settings:
 - **Print on video file:** Displays camera ID, location name, date and time on recorded videos.
 - **Print on screen (Only for IO alarm):** Displays the name of triggered input device on the camera screen. For this function to work, it is required to map a camera to an input device, see *Other I/O Application Functions* in Chapter 6.
 - **Embed Counting Results into Recorded Video:** Displays counter results to recorded videos. For details on establishing a counter alarm, see *Object Counting* later in this chapter.

Note: Text overlay is not supported when standard format codec is enabled. To change this setting, select **Home** , select **Toolbar** , select **Configure** , select **Camera Install**, click the **Settings**  button for the camera, click the **General Setting** tab and then locate the Recording codec format field.

- **Alignment:** Select how you want the camera information to be aligned on a camera screen.
- **Set Font:** Click to configure the font, font size, font style and related settings.

3.17 Fisheye View

A fisheye camera allows you to cover all angles of a location with just one fisheye camera. Using different fisheye view modes, the distorted hemispherical image produced by the fisheye camera can be converted to a conventional rectilinear projection.

Note: To use the fisheye dewarping function, the graphic card supporting DirectX 10.1 or above is required.

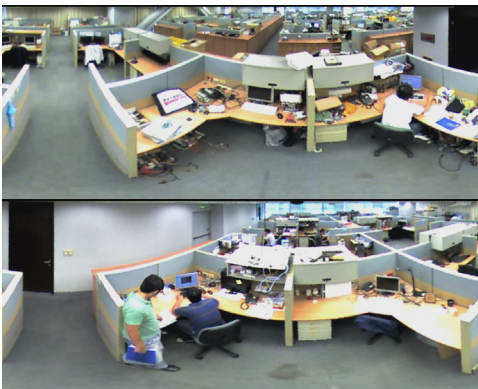
You can choose among four view modes and adjust the PTZ views to different angles.



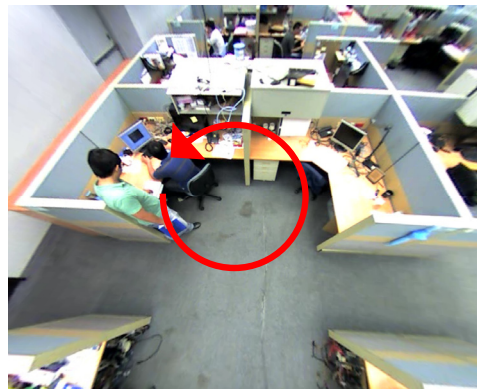
Quad view: 4 PTZ views



360 degree: 2 PTZ view & 1 360° view



Dual 180 degree: 2 180° views



Single view: 1 PTZ view

Figure 3-59

3.17.1 Setting Up a GV-Fisheye Camera

1. Make sure you have connected the fisheye camera to the GV-VMS. The camera should appear in the Content List.
2. From the Content List, drag the fisheye camera (circular source image) or one of the dewarpped fisheye images (e.g. Quad View) to the live view grid.
3. To change the fisheye settings, right-click the fisheye camera from the Content List and select **Fisheye Settings**. The Fisheye Setting dialog box appears.

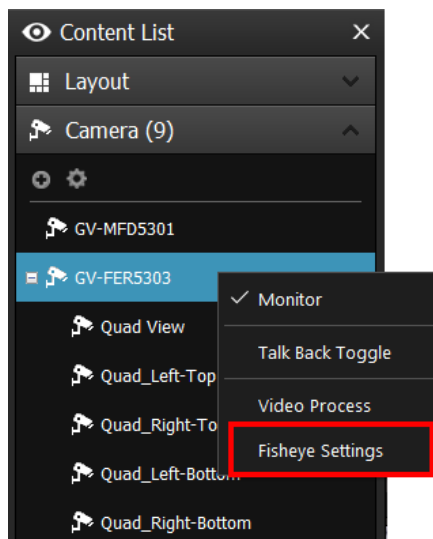


Figure 3-60

4. Right-click on the Fisheye Setting dialog box, point to **Fisheye Option** to access the following settings:
 - **Camera Modes:** You can choose among four view modes.
 - ⊙ **Geo Fisheye: Quad view:** Composed of four PTZ views.
 - ⊙ **Geo Fisheye: 360 degree:** Composed of two PTZ views and one 360° panoramic view.
 - ⊙ **Geo Fisheye: Dual 180 degree:** Composed of two 180° views.
 - ⊙ **Geo Fisheye: Single view:** Composed of one PTZ view. This view mode supports the advanced Picture-in-Picture (PIP) function, which allows you to have a close-up dewarpped image within the surveillance area without missing the entire view.
 - **Camera Position:** Select **Ceiling**, **Wall** or **Ground** according to where the camera is mounted.

- **Adjust Auto Pan Speed At Top-Left Channel:** Select low, medium, or high speed to enable Auto Pan for one PTZ view at the rotation speed of your choice. This option applies to **Quad view**, **360 degree** and **Single view**.
- **Zoom:** Select **Zoom In** or **Zoom Out** and then click on the image.
- **Show Source Video At Top-Right Channel:** You can display the circular source image in the top-right quadrant when **Quad view** is selected.
- **360 Object Tracking:** This option is only available for **360 degree** view. Select **Tracking** for moving object to be tracked in the top-right PTZ view and highlighted in the 360 degree view at the bottom. For details, see *Object Tracking* later in this chapter.
- **Disable PIP:** Disables the PIP function for the Single View mode.
- **Guard Tour Setting:** Guard tour is a PTZ tour for monitoring important spots on the live view. This option is only available under the **Single View** mode. For details, see *Virtual PTZ Tour* later in this chapter.
- **Settings:**

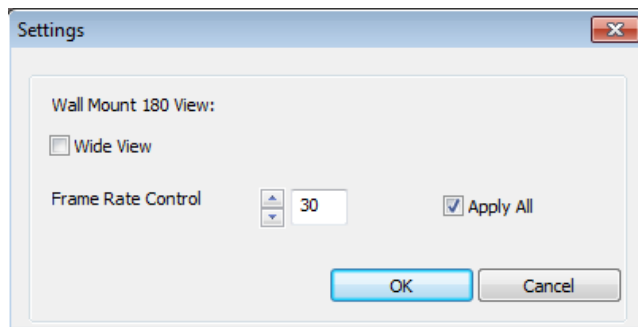


Figure 3-61

- **Wide View:** Increases the height of the 180 degree view when camera position is set to wall mount.

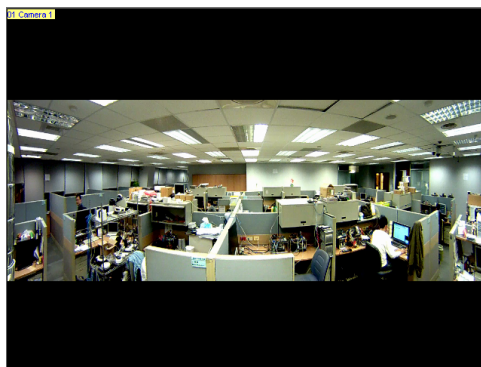


Figure 3-62: Wide View Disabled

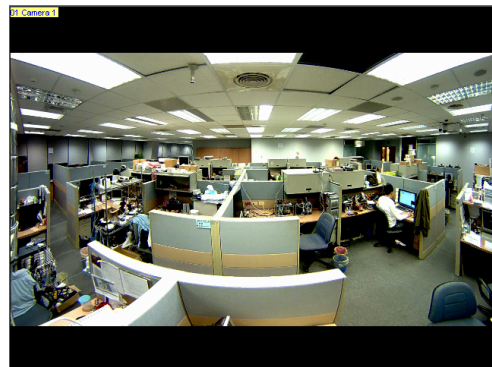






Figure 3-62: Wide View Enabled

- ⦿ **Frame Rate Control:** Limits the frame rate of the fisheye live view to the number specified here. Select **Apply All** to apply the frame rate control to other fisheye views.

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

3.17.2 Setting Up a Third-Party Fisheye Camera

You can also enable dewarping for 3rd party fisheye cameras and access fisheye related functions.

1. Make sure you have connected the fisheye camera to the GV-VMS. The camera should appear in the Content List.
2. Select the camera lens type to dewarp the image.
 - A. Click **Home** , click **Toolbar** , click **Configure** , and select **Camera Install**. The IP Device Setup dialog box appears.
 - B. Click the Settings button .
 - C. For the camera installed with an ImmerVision IMV1 Panorama Lens, select **IMV1 Panomorph** using the Camera Lens drop-down list.
 - D. For other third-party fisheye cameras, select **Fisheye** using the Camera Lens drop-down list.

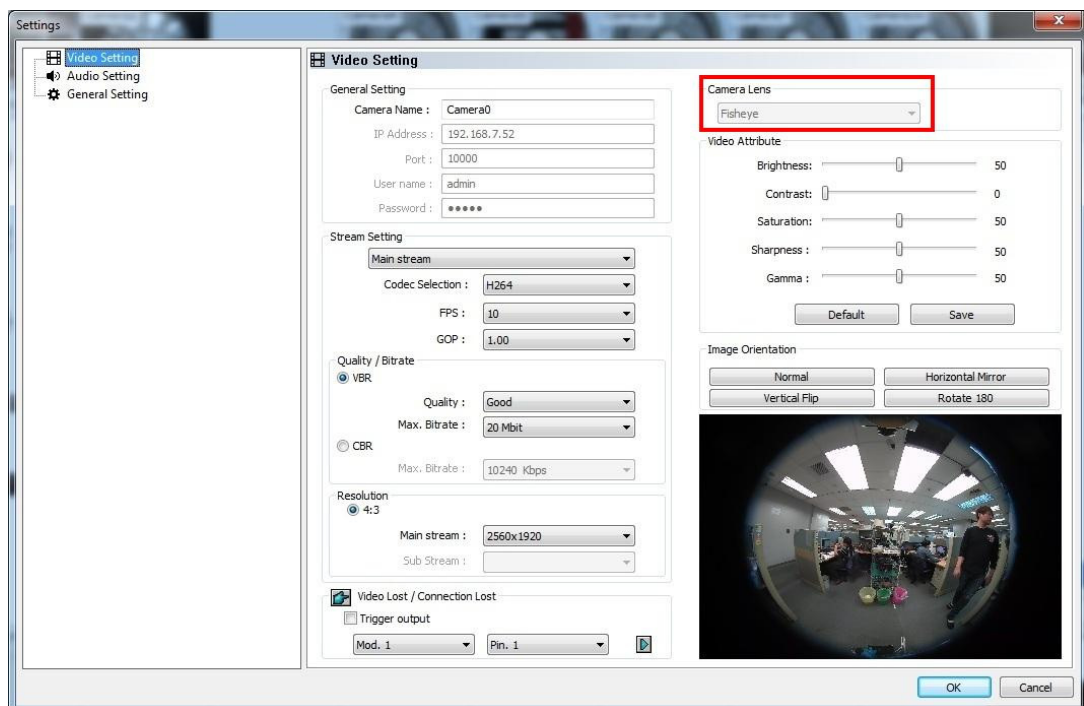


Figure 3-63

3. From the Content List, drag the fisheye camera (circular source image) or one of the dewarped fisheye images (e.g. Quad View) to the live view grid.

4. To access fisheye related functions, follow steps 2 to 4, *Setting Up a GV-Fisheye Camera* later in this chapter.
5. To adjust the image alignment for optimal results, follow steps 2 and 3, *Setting Up a GV-Fisheye Camera* later in this chapter and select **Image Alignment**. In the dialog box, align the dotted circle with the outer edge of the camera image, and then align it with the inner edge of the image frame.

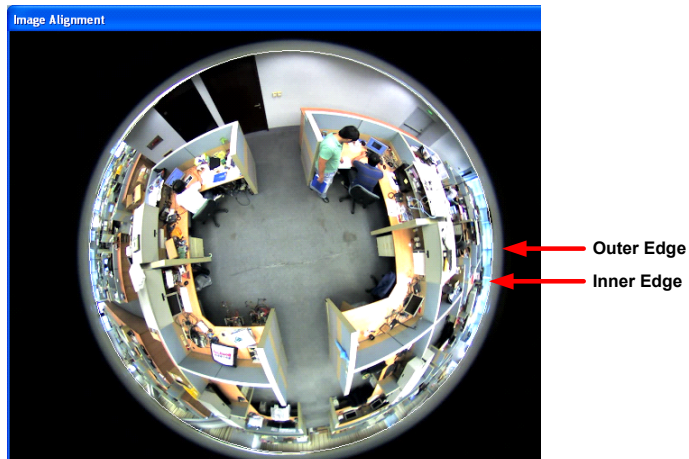





Figure 3-64

Note:

1. For GV-Fisheye Cameras, the image alignment function is only available on its Web interface.
 2. Regardless of the view mode selected here, the hemispherical fisheye source image will be recorded. When playing back fisheye events in ViewLog, GV-VMS can convert the source image to different view modes according to your preference. To play back the events in fisheye view mode, select **ViewLog** , select **Toolbar** , select **Content List**  and then select a dewarped view of the camera.
-

3.17.3 Object Tracking

You can now set up object tracking in fisheye live view to track moving object. The function is only available when the fisheye camera mode is set to be **Geo Fisheye: 360 degree**. When motion is detected in the fisheye, the top-right channel will start tracking the moving object and in the 360 degree view at the bottom, the moving object will be highlighted.

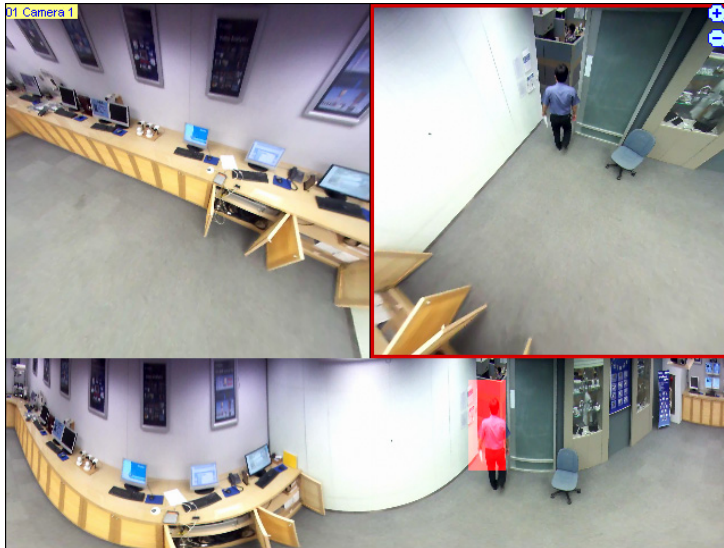


Figure 3-65

1. Make sure the fisheye view mode is set to the 360 degree mode. For details, see step 4 in *Setting Up a GV-Fisheye Camera*, earlier in this chapter.
2. Right-click the fisheye camera from the Content List and select **Fisheye Settings**. The FE Setting dialog box appears.

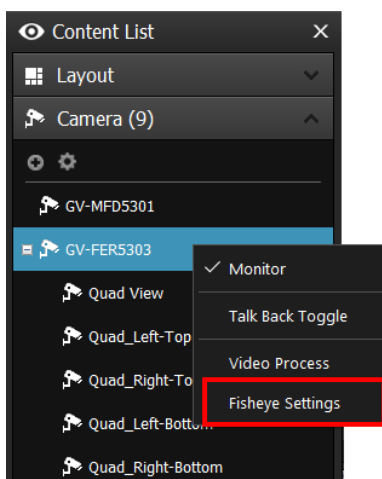


Figure 3-66

3. Right-click on the FE Setting dialog box, point to **Fisheye Option**, select **360 Object Tracking** and then select **Advanced Settings**. This dialog box appears.

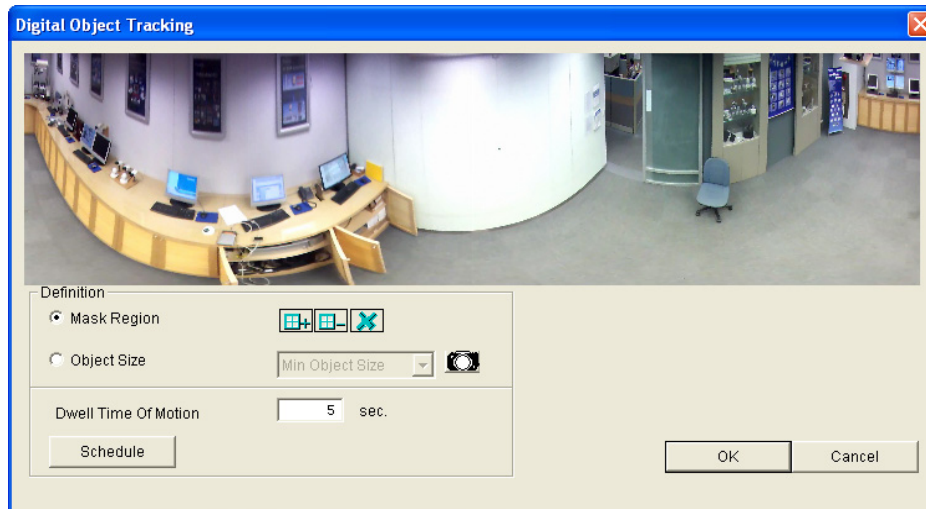



Figure 3-67

4. Use the options below to customize object tracking.
 - **Mask Region:** Use the mouse to outline a mask region where motion will be ignored.
 - **Object Size:** Click the  button to pause the live view and then use the mouse to outline the maximum and minimum size of the targeted object.
 - **Dwell Time of Motion:** After a targeted object stops moving, the highlighted region and the top-right channel will remain fixed on the area for the number of seconds specified. Any new motion detected during the dwell time will be ignored to prevent the camera view from frequently jumping from one area to another.
 - **Schedule:** Click **Schedule** to set up the times for object tracking. See the next step for details.

5. Set up a schedule.

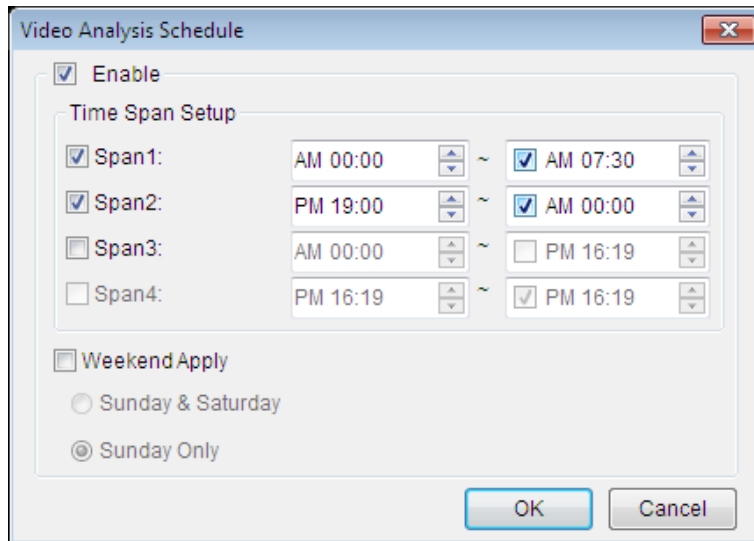


Figure 3-68

- A. Select **Enable**.
 - B. Select **Span 1** and specify a time period. The period that you specify is effective from Mondays to Fridays.
 - C. Optionally select more span and specify the time period.
 - D. To apply the week day time periods to weekends, select **Weekend Apply** and select **Sunday & Saturday** or **Sunday Only** according to your needs.
 - E. Click **OK** to save the settings.
6. To start object tracking, right-click the fisheye view, select **Fisheye Option**, select **360 Object Tracking** and select **Tracking**.

3.17.4 Virtual PTZ Tour

Set up a virtual PTZ tour to monitor important spots of your surveillance site. Before you start, make sure your GV-Fisheye Camera is set to the **Single View** mode. For details on the view mode, see *Cameras Modes*, in *Setting Up a GV-Fisheye Camera* section, earlier in this chapter.

1. Make sure your live view is set to the Single View mode. For details, see step 4, *Setting Up a GV-Fisheye Camera* earlier in this chapter.
2. Move your live view to a desired starting place for the PTZ tour by clicking on the inserted window on the bottom right of the live view.
3. Right-click the camera live view, select **Fisheye Option** and then select **Guard Tour Setting**. This dialog box appears.

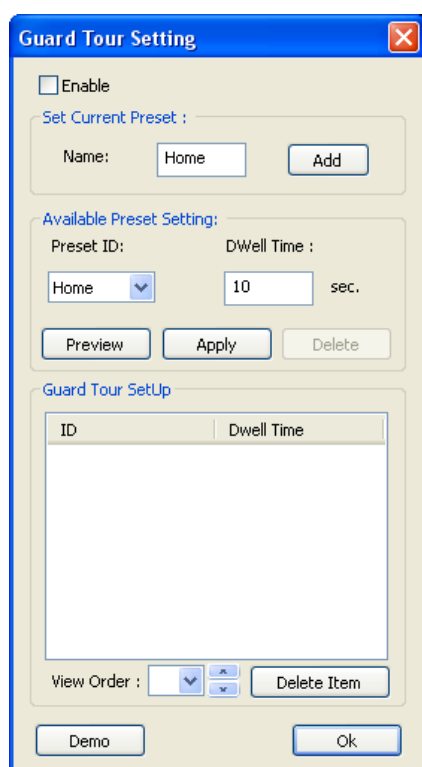


Figure 3-69

4. Type a name for the current live view and click **Add**. This live view point (preset point) automatically appears under Preset ID.

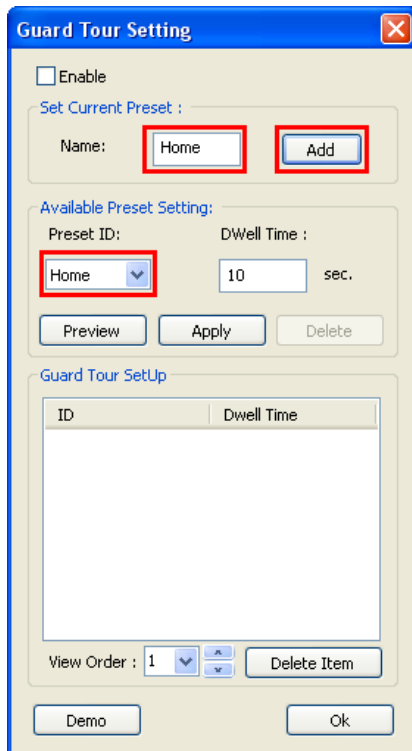
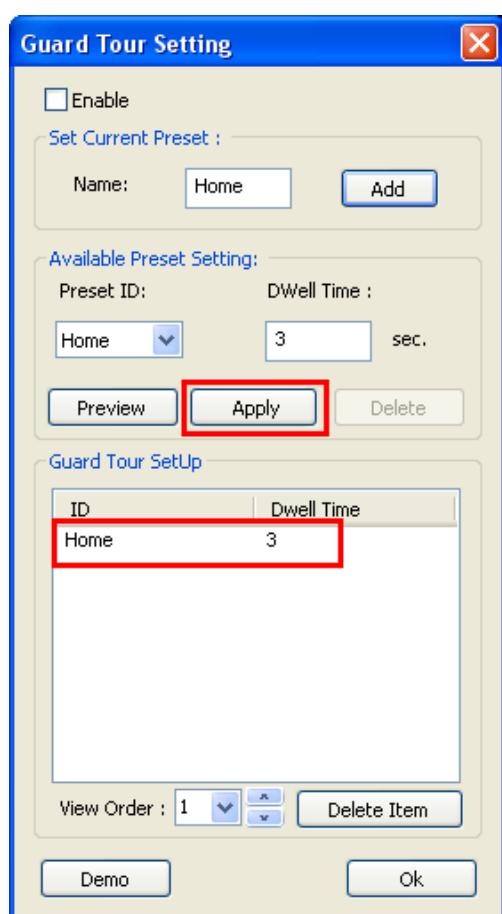


Figure 3-70

5. Specify the duration for the live view to stay on this preset point (dwell time). The default setting is **10** seconds.
6. Optionally click **Preview** to see a preview of the preset point.

7. Click **Apply**. This point is added to Guard Tour Setup.



The image shows a 'Guard Tour Setting' dialog box with a blue title bar and a close button. It contains several sections: 'Set Current Preset' with a text field 'Name:' containing 'Home' and an 'Add' button; 'Available Preset Setting' with 'Preset ID:' dropdown set to 'Home' and 'DWell Time:' text field set to '3' with 'sec.' label, and buttons 'Preview', 'Apply' (highlighted with a red rectangle), and 'Delete'; 'Guard Tour SetUp' with a table containing one row 'Home' with '3' in the 'Dwell Time' column (this row is highlighted with a red rectangle), and buttons 'View Order' (set to 1), 'Delete Item', 'Demo', and 'Ok'.

Guard Tour Setting

☐ Enable

Set Current Preset :

Name: Home Add

Available Preset Setting:

Preset ID: Home DWell Time : 3 sec.

Preview Apply Delete

Guard Tour SetUp

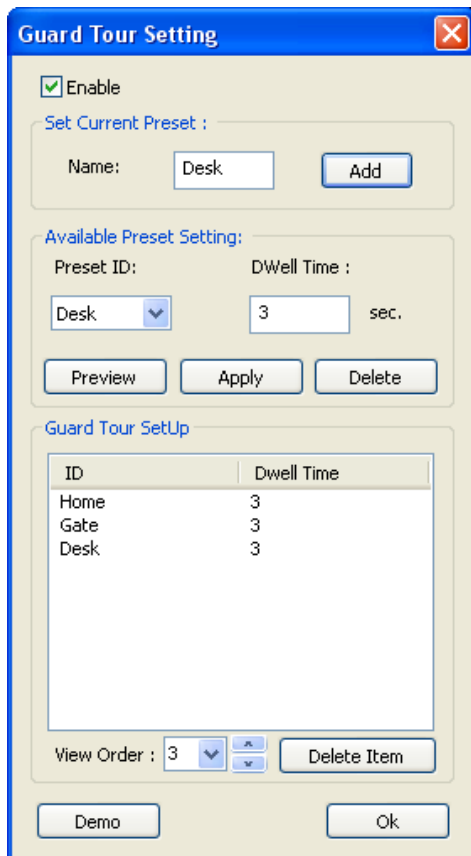
| ID | Dwell Time |
|------|------------|
| Home | 3 |

View Order : 1 Delete Item

Demo Ok

Figure 3-71

8. To add more preset points, follow steps 1 to 6. For example, three preset points Home, Gate and Desk are established in this setup.



The dialog box is titled "Guard Tour Setting" and contains the following sections:

- Enable:** A checked checkbox labeled "Enable".
- Set Current Preset:** A section with a "Name:" label, a text box containing "Desk", and an "Add" button.
- Available Preset Setting:** A section with "Preset ID:" and "DWell Time:" labels. The "Preset ID:" dropdown is set to "Desk", and the "DWell Time:" text box contains "3" with "sec." next to it. Below these are "Preview", "Apply", and "Delete" buttons.
- Guard Tour SetUp:** A section containing a table with two columns: "ID" and "Dwell Time".

| ID | Dwell Time |
|------|------------|
| Home | 3 |
| Gate | 3 |
| Desk | 3 |
- View Order:** A section with a "View Order:" label, a dropdown menu set to "3", and "Delete Item" and "Demo" buttons.
- Buttons:** "Ok" and "Cancel" buttons at the bottom right.

Figure 3-72

9. To change the order of the preset points, select a preset point from the ID column and select a number from the drop-down list to move this preset point up or down the list.
10. Optionally click **Demo** to watch a preview of the PTZ tour.
11. Select **Enable** to start the PTZ tour. To stop the PTZ tour, disable this function on the Guard Tour Setting.

3.18 Specifications

| Feature | Notes |
|---|--|
| Panorama View | <ul style="list-style-type: none"> 1 GB of RAM required at minimum 4 sets of panorama view for live view monitoring |
| Defogging | <ul style="list-style-type: none"> 35 MB of RAM required per channel at minimum Maximum of 64 channels |
| Stabilizer | <ul style="list-style-type: none"> 34 MB of RAM required per channel at minimum Maximum of 4 channels |
| Crowd Detection | <ul style="list-style-type: none"> Maximum of 16 channels |
| Advanced Scene Change Detection / Advanced Unattended Object Detection / Advanced Missing Object Detection | <ul style="list-style-type: none"> Maximum of 16 channels |
| Object Counting | <ul style="list-style-type: none"> 7 fps and 6 MB of RAM required per channel at minimum Maximum of 32 channels |
| Privacy Mask | <ul style="list-style-type: none"> 31 MB of RAM required per channel at minimum Maximum of 250 detection boxes can be set The overall size of detection boxes cannot exceed 102400 bytes. |
| Face Count | <ul style="list-style-type: none"> Maximum of 16 channels |
| Object Index / Object Monitor / Face Detection / | <ul style="list-style-type: none"> 7 fps and 16 MB of RAM required per channel at minimum Maximum of 16 channels |

Specifications are subject to change without notice.

Note:

- To use two or more of the following functions simultaneously, at least 2 GB of RAM is required: Advanced Video Analysis, Video Analysis, IP Camera and Pre-Record by Memory.
 - The Face Count function will be supported in the near future.
-

Chapter 4

Video Playback 175

| | | |
|------------|---|------------|
| 4.1 | Playing Back on ViewLog | 176 |
| 4.1.1 | ViewLog Control Panel | 178 |
| 4.1.2 | Adjusting the Camera View..... | 181 |
| 4.1.3 | Searching a Video Event | 182 |
| 4.1.4 | Merging and Exporting Video..... | 183 |
| 4.1.5 | Saving Images | 186 |
| 4.1.6 | Printing Images | 187 |
| 4.1.7 | Adjusting Distorted Views | 188 |
| 4.2 | Object Search..... | 190 |
| 4.3 | Advanced Log Browser..... | 193 |
| 4.3.1 | Filter Settings | 195 |
| 4.4 | Remote ViewLog Service | 196 |
| 4.4.1 | Retrieving Recordings from GV-VMS | 196 |
| 4.4.2 | Retrieving Images of Object Index..... | 198 |
| 4.4.3 | Resuming Backup..... | 199 |
| 4.5 | Single Player | 200 |
| 4.5.1 | Single Player Window | 200 |
| 4.6 | Specifications..... | 202 |





Video Playback

Recorded files can be played back using different software applications offered by the system – ViewLog, Object Search, WebCam Server, Single Player and Remote ViewLog Service. The following is a comparison table for these applications. This table is not meant to be exhaustive because many of these features are discussed in details throughout the manual. However, this table may help you to decide which application to use under a given situation.

| Application | Description |
|------------------------|--|
| ViewLog | A full-function player, allowing you to play back video, search a video event, merge and export video and etc. See <i>Playing Back on ViewLog</i> in this chapter. |
| Object Search | A more convenient tool that allows you to search video files recorded on motion or alarm. See <i>Object Search</i> in this chapter. |
| Remote ViewLog Service | Remote ViewLog Service allows you to retrieve files from a remote GV-VMS and it supports most functions provided by the ViewLog player. See <i>Remote ViewLog Service</i> in this chapter. |
| WebCam Server | WebCam Server allows you to remotely access live view and play back recordings on your Web browser without installing additional software. See <i>Remote Viewing</i> in Chapter 7. |
| Single Player | Plays back the backup recorded files. Provides simple and easy playback functions. See <i>Single Player</i> in this chapter. |

4.1 Playing Back on ViewLog

ViewLog is a video player that plays back recorded videos without affecting the recording in process. Follow the steps below to launch ViewLog and play back recordings.

1. Select **ViewLog**  Select **Toolbar**  and then select **Content List** . The Content List appears.
2. Select **Add**  and select **Import from Live** to import current live views to the playback screen. For details on configuring the ViewLog layout, follow steps 2 to 5 in *1.4.2 Arranging Live View Layouts*.

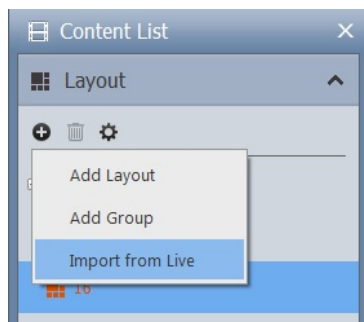


Figure 4-1

3. Optionally drag and drop more cameras from the Content List to the playback screen.
4. On the timeline, click the arrows to select a date or click on the date to select from a pop-up calendar.

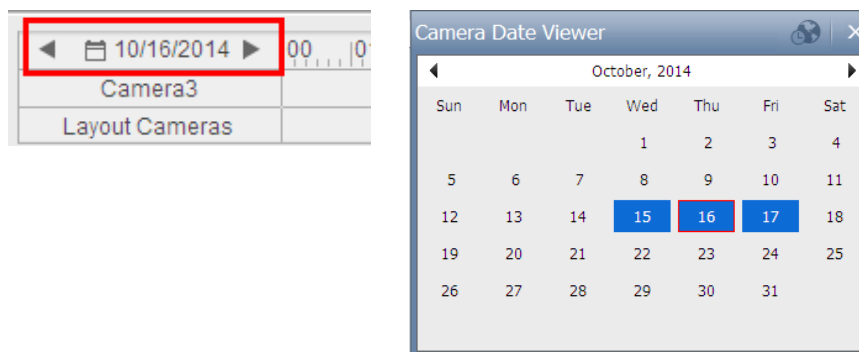



Figure 4-2

5. Click **Play**  to start playing back. For details on ViewLog control panel, see *ViewLog Control Panel* later in this chapter.

The Controls on ViewLog Player

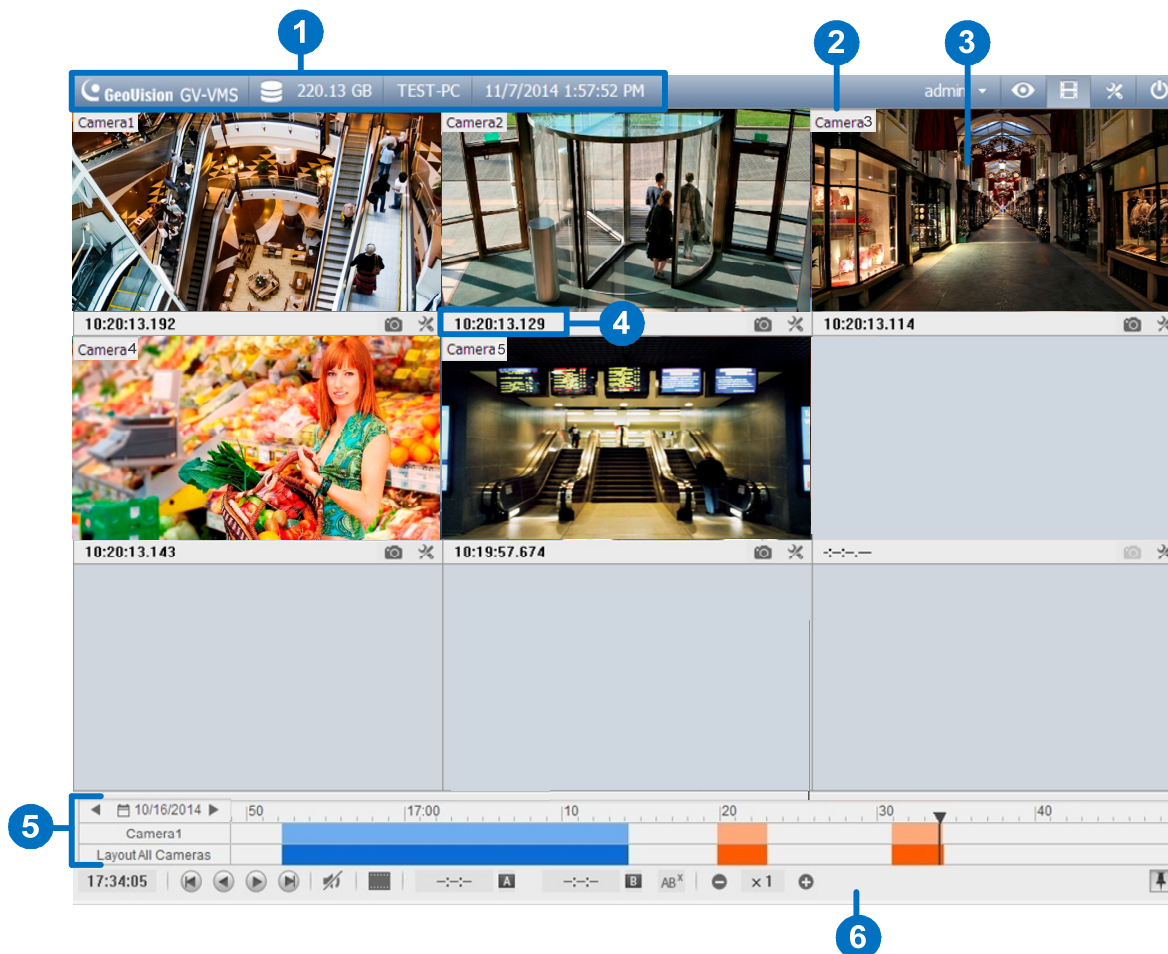


Figure 4-3 The ViewLog Player

| No. | Name | Description |
|-----|--------------------|---|
| 1 | VMS Information | Indicates the system version, available storage space, system name, date and time. |
| 2 | Camera Name | Indicates the camera name. |
| 3 | Camera View | Displays the playback video. |
| 4 | Recorded Time | Indicates the time of recording. |
| 5 | Recording Timeline | Indicates the recording date and reflects video recordings. Round-the-clock events are shown as blue, and alarm events are shown as orange. |
| 6 | Playback Panel | Contains typical playback control buttons. For details, see <i>ViewLog Control Panel</i> later in this chapter. |

4.1.1 ViewLog Control Panel

Preview Window

Move the cursor on the timeline to see a preview of recording. Click on the timeline to pause all channels at the selected time.

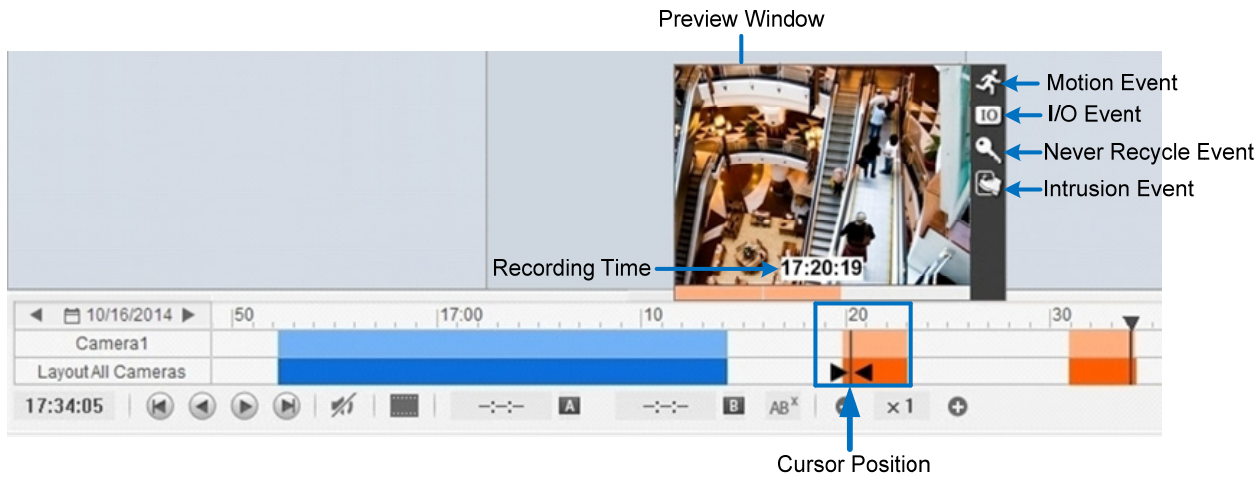


Figure 4-4

Timeline

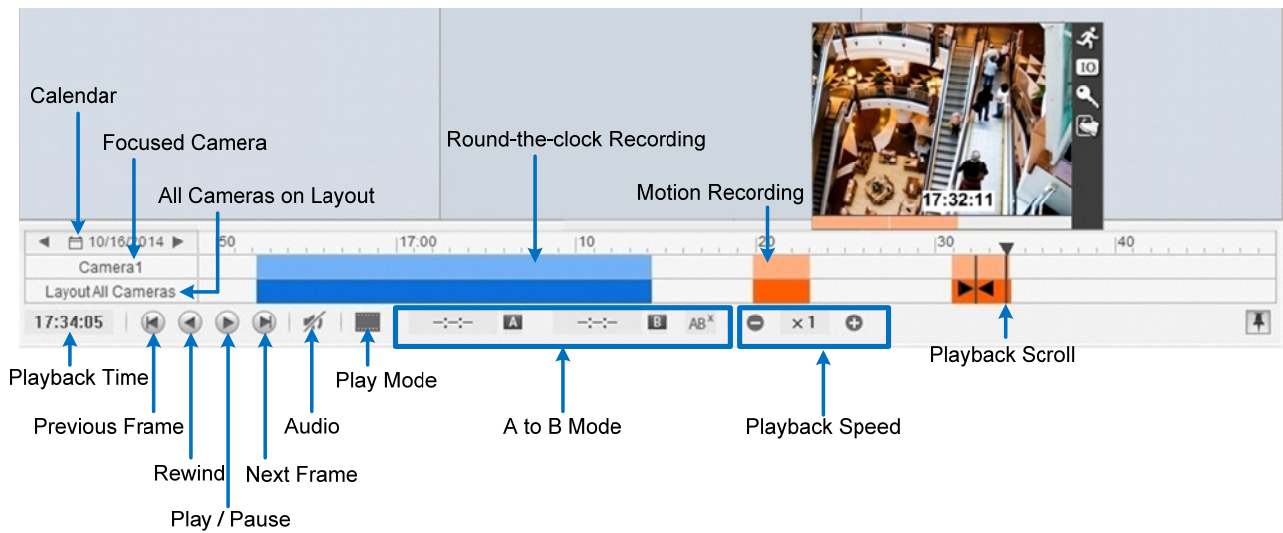


Figure 4-5

Tip: Right-click and drag on the timeline to back up, delete recorded files or apply event detection and counting functions to the selected time period. For details, see *Backing Up Recorded Files* in Chapter 5, *Deleting Recorded Files* in Chapter 5 and *Object Search* later in this chapter.

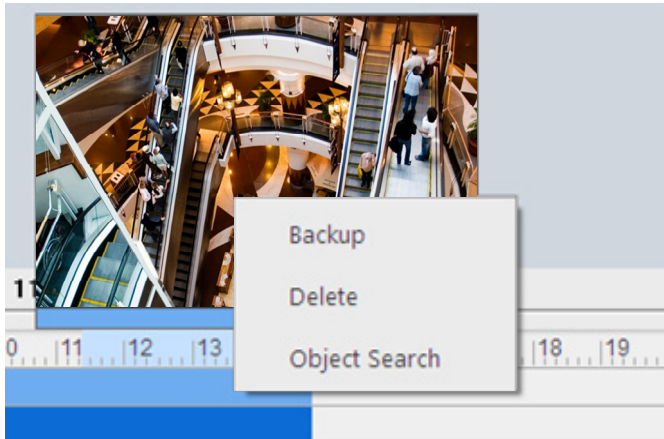



Figure 4-6

Playback Mode Option

By default, the ViewLog is set to play back video in the Frame by Frame mode. To change playback modes, click the  button on the ViewLog Control Panel.

- **Frame by Frame (without audio):** Plays back video frame by frame without audio. Playback can be delayed depending on the bandwidth and computer performance, but all video frames are fully played.
- **Real Time:** Plays back video on real time. This method saves waiting time for rendering, but drop frames to give the appearance of real-time playback.
- **Just Key Frame:** Plays back the most representative frames of video. When your network bandwidth is limited, select this option to enhance the playback smoothness.
- **Smooth Playback:** When the playback appears choppy, select this option to enhance the smoothness.

Note: For the MJPEG codec, every frame is key frame.

A to B Playback Mode

When playing video events, you can set a starting and an ending frame for auto-playing:







1. To set the starting frame A, click  and select a time by clicking the timeline. This icon changes to blue and the selected time appears on the ViewLog panel.



Figure 4-7

2. Click  and follow step 1 to set the ending point (frame B).
3. Click . ViewLog will start playing from frame A to B repeatedly.
4. To pause the playback, click . To cancel this playback mode, click .

4.1.2 Adjusting the Camera View

You can adjust the image quality for the recording videos. Right-click on the camera view (No. 3, Figure 4-3) or click the **Tools**  button on the camera view to access these settings:

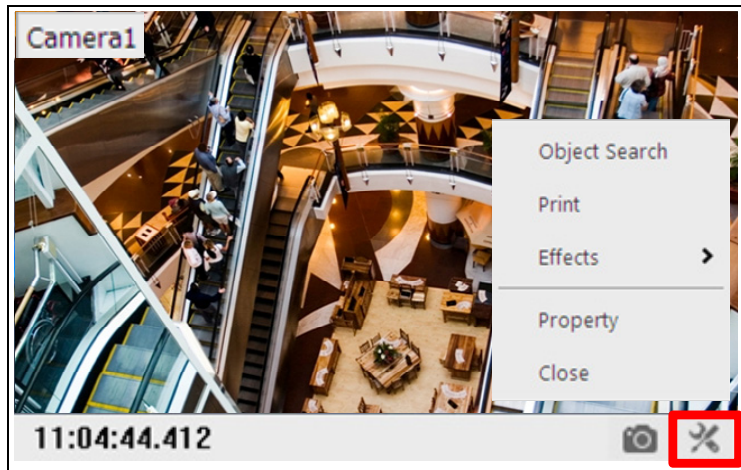





Figure 4-8

- **Keep Image Ratio:** Select to change the camera view to its original ratio.
- **Show Caption:** Shows the camera name. This function is enabled by default.
- **Print:** Prints the current image from the camera view. For details, see *Printing Images* later in this chapter.
- **Effects:**
 - ⊙ Click to apply effects including brightness, contrast, equalization, light enhancement, grayscale, sharpness, smoothness.
 - ⊙ To snapshot the current playback image, select **Copy** and then open a WORD or Paint file to paste and save the image.
 - ⊙ To undo the last enabled effect, click **Undo To Prev Action**. To restore to its original video settings, click **Undo All Effects**.

4.1.3 Searching a Video Event

You can browse for recordings by specifying a specific point in time.

1. Click **ViewLog** , click **Toolbar** , select **Tools**  and select **Basic Search**. This dialog box appears.

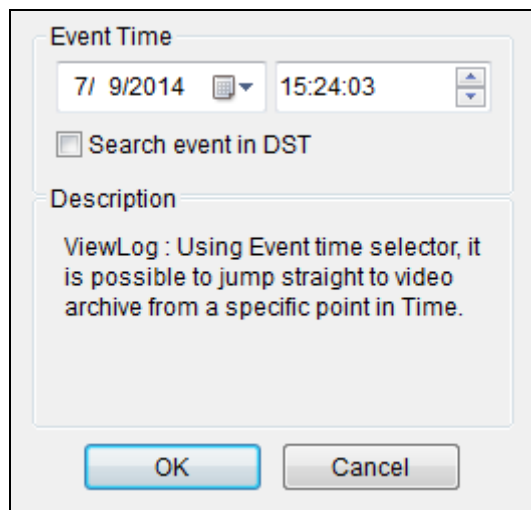





Figure 4-9

2. If you want to search the video events recorded during the Daylight Saving Time period, select **Search event in DST**.
3. Specify a desired date and time.
4. Click **OK** to start searching. The playback scroll appears at the selected time point on the timeline.

4.1.4 Merging and Exporting Video

You can merge several video files into a single one and export it in AVI format or EXE format. The latter allows you to play video with any multimedia player.

Note: The maximum size of the merged file is 2 GB. Any file exceeding 2 GB will be split into another file.

1. Make sure you have displayed the cameras you wish to merge/export. For details on configuring the ViewLog layout, follow steps 2 to 5 in *1.4.2 Arranging Live View Layouts*.
2. Click **ViewLog** , click **Toolbar** , select **Tools**  and select **Save as Avi**. This dialog box appears.

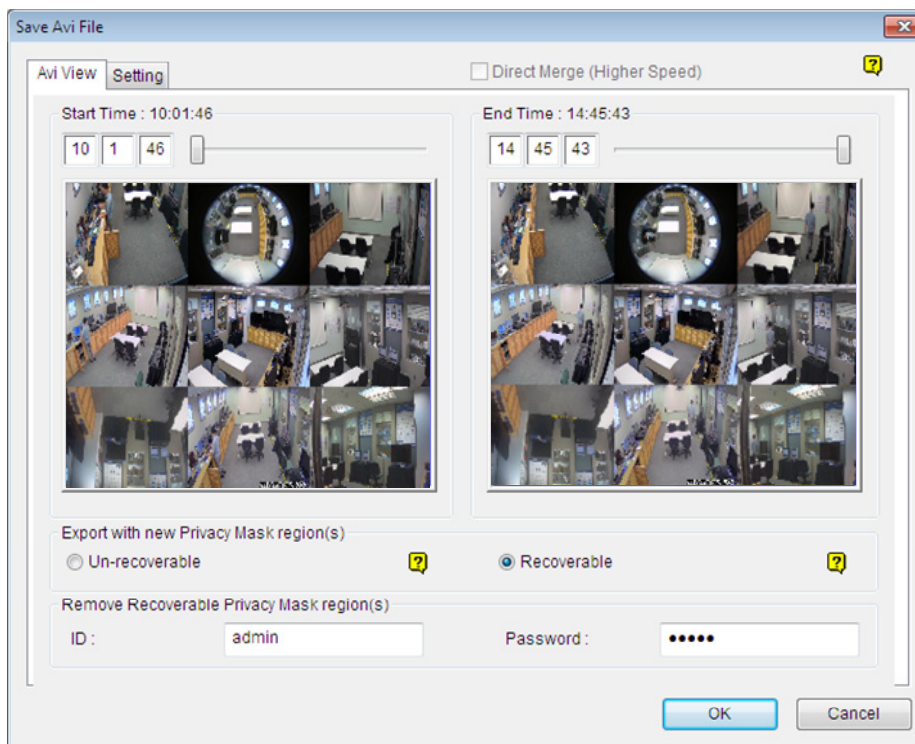


Figure 4-10 Save AVI File

3. Drag the timelines to define a starting and ending time of the file.
4. If the video event has the Privacy Mask settings, and you want to retrieve the recoverable block-out area(s) in the exported file, type a valid ID and password in the Remove Recoverable Privacy Mask region(s) field. If you want to retain the recoverable block-out area(s) in the exported file, leave the field blank. For details on the Privacy Mask, see *Privacy Mask Protection* in Chapter 3.

5. To speed up the video merging process, select **Direct Merge (Higher Speed)**.

This function saves the video file in the codec type that it was originally recorded.

Note: Once the **Direct Merge (Higher Speed)** is enabled, you will not be able to customize settings such as codec selection, privacy mask recoverability and digital watermark, but the time required for conversion is significantly reduced.

6. To optionally configure the saving path and format of the exported video, click the **Setting** tab.

This dialog box appears.

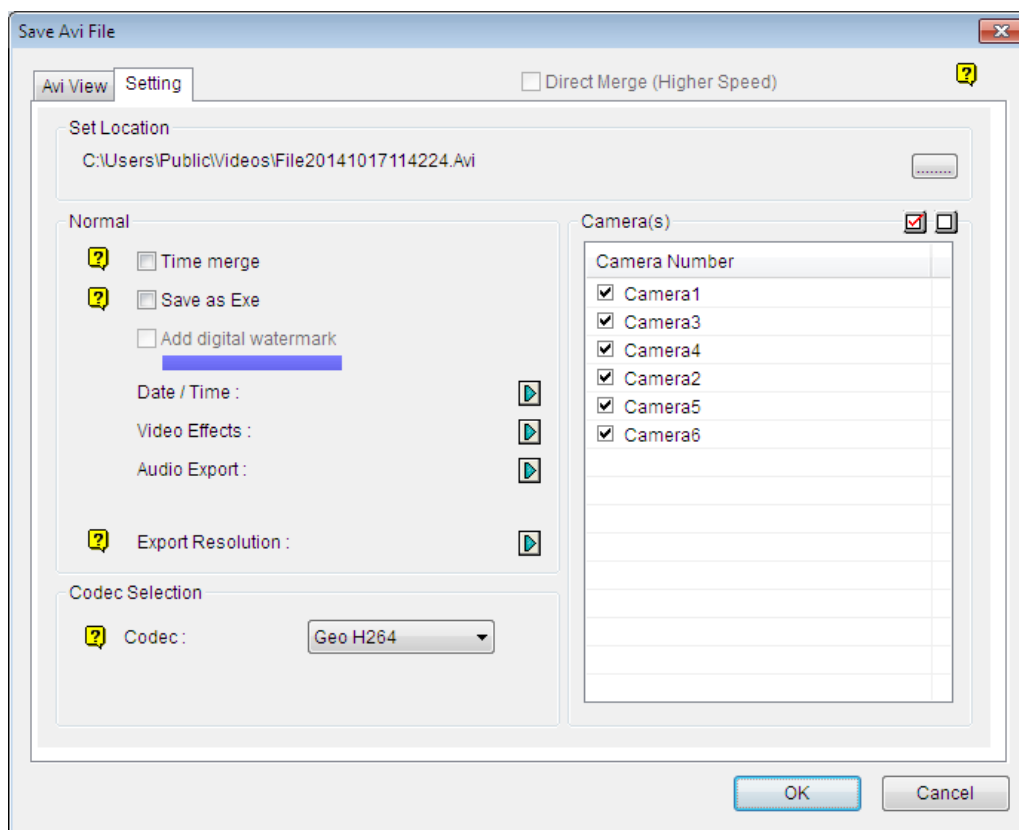


Figure 4-11

[Set Location] Click the [...] button to assign a saving path.

[Normal]

- **Time Merge:** Select whether to save a full-length video with recorded and non-recorded periods. A blank blue screen will be displayed during the non-recorded periods. This option is designed to accurately reflect your recording status.
- **Save as EXE:** Select whether to save files in EXE format. Enable this feature if you want to play back video at the computer without installing GeoVision codec. This format allows you

to auto-play the files with any third-party player.


- **Add digital watermark:** Select whether to include the watermark in the exported video. This option is only available when the watermark has been applied on the recorded video.
- **Date/Time:** Select whether to include date and/or time stamps. You can also select the font type and size, stamp position and color on the images.
- **Video Effects:** Select whether to combine special effects, including De-Interlace, Defog, Stabilizer, and Overlay's camera name and time to the exported video. You must have already applied these functions to the recorded video for this function to take effect.
- **Audio Export:** Select **Denoise** to remove audio noises from the video, or select **Channel** for audio exporting.
- **Export Resolution:** Select the resolution for the exported video.

[Codec Selection]

- **Geo H264:** This codec is created by GeoVision. It provides better image quality, higher frame rates and smaller files size than any other. If the codec is selected, you must play the exported files on the computer with the GeoVision codec installed. Otherwise you can export the files in EXE format in order to play the video at any computer.
- **WMV9:** This code is created by Microsoft. It allows you to play the video with Windows Media Player directly without using GeoVision codec. If the codec is selected, the Privacy Mask you created using the ViewLog will be disabled.

[Cameras]

Select the cameras to merge and export.

7. Click **OK** to export and save the file. The files will be merged and shown in this window. Click  and select **Play** to play back the merged file. Select **Preview** to view a still image of the merged file.

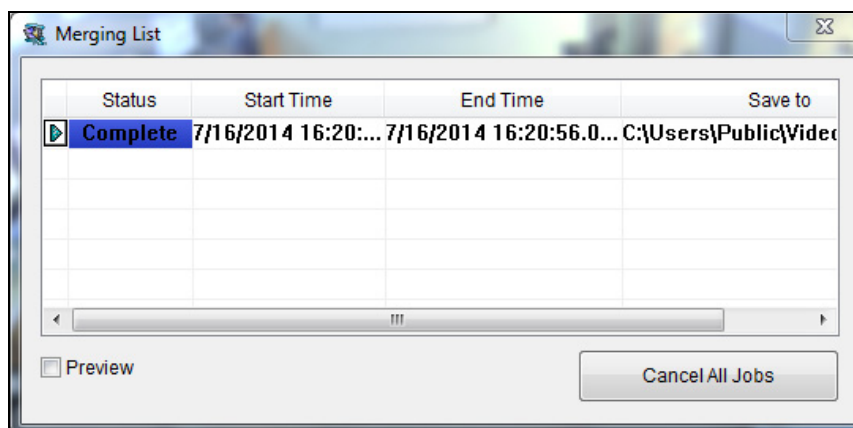


Figure 4-12

4.1.5 Saving Images

You can snapshot and save the current camera view as an image file while the recording is being played back.

1. Click  from a camera channel on ViewLog (Figure 4-3). This dialog box appears.

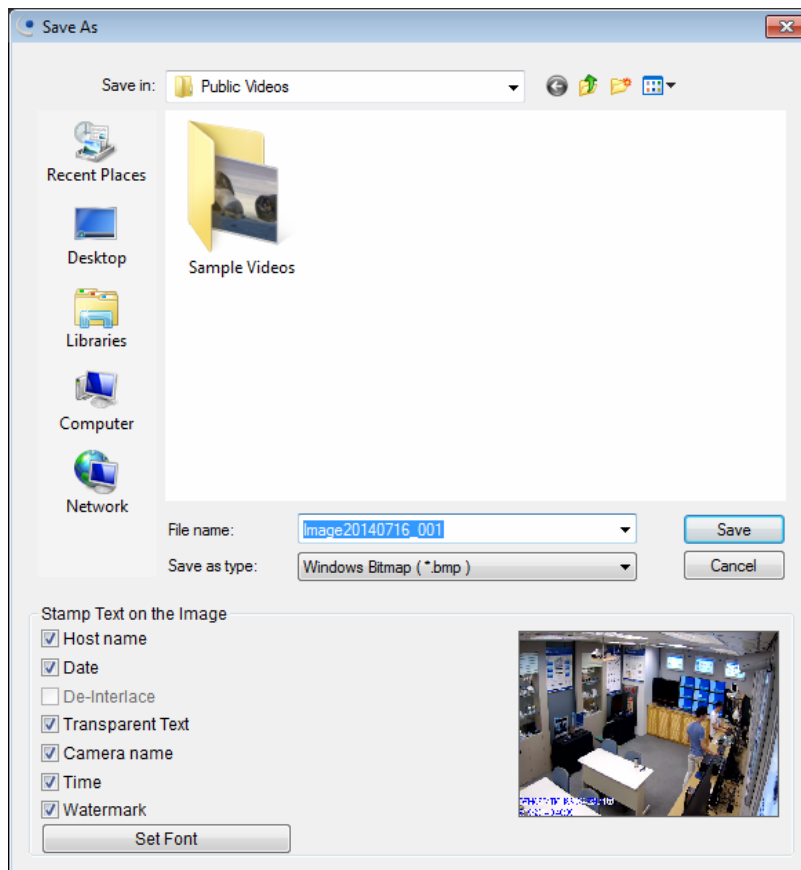


Figure 4-13

[Stamp Text on the Image]

Select whether to include host name, camera name, date and/or time stamp on the image.

Selecting **Transparent Text** will create the stamp on the transparent background.

Selecting **Watermark** and **Deinterlace** will include the two features in the saved image.

[The image] Click on the image at the bottom to preview the stamp text. Click on the image again to close the preview window.

2. Name the file, select a file format, and then assign the location to save the image file.

4.1.6 Printing Images

You can print camera images.

1. Right-click a camera channel on ViewLog (Figure 4-3) and select **Print**. This window appears.

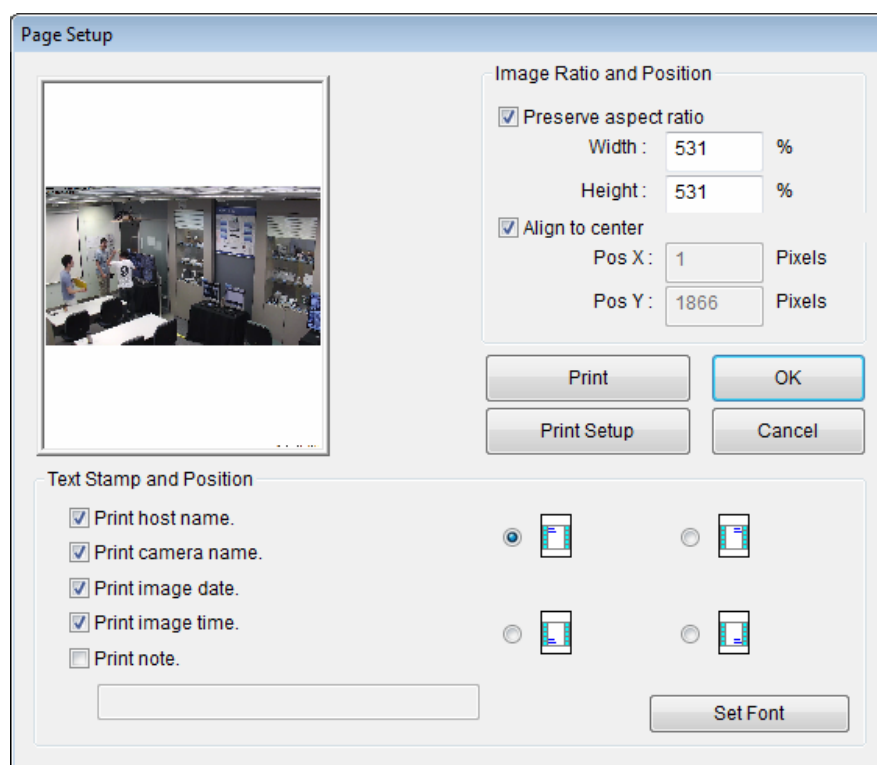


Figure 4-14

[Image Ratio and Position] Changes the size of the image and its position on the page.

- **Preserve aspect ratio:** Select this option to maintain the aspect ratio when resizing an image.
- **Align to center:** Select this option to change the position of the image on the page.

[Text Stamp and Position]




Select whether to include the host name, camera name, date and/or time stamp on the printed image. To include a note below the image, select **Print note** and type a note in the blank below. The text can only be 64 characters at most.

- **Stamp position icons:** Sets the position where the stamp is printed.
- **Set Font tab:** Click to select the font type for the stamp.

2. Click **OK** to save the settings or **Print** to print out the page.

4.1.7 Adjusting Distorted Views

When viewing videos on the ViewLog player, images may be curved near the corners. Correct this distortion using the Wide Angle Lens Dewarping feature.

1. Click **ViewLog** , click **Toolbar** , select **Configure** , select **Effect**, and then select **Wide Angle Lens Dewarping**. This dialog box appears.

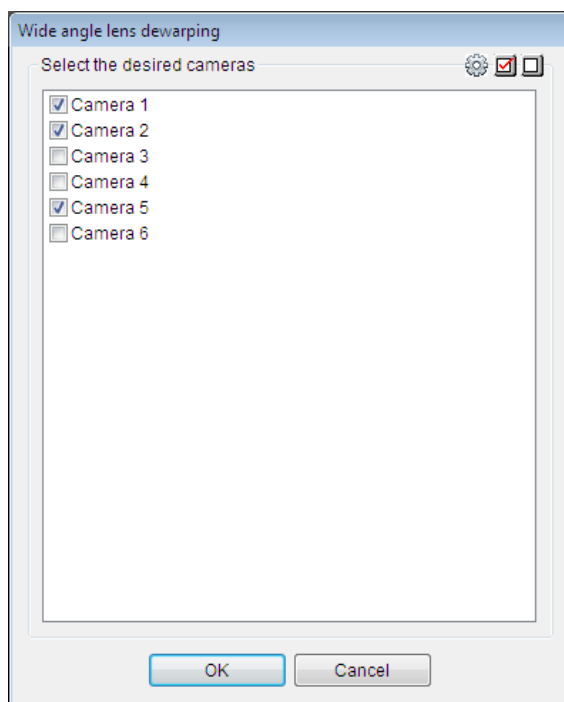


Figure 4-15

2. Select the cameras to apply Wide Angle Lens Dewarping.

3. To adjust the degree of adjustment, click the  button. This dialog box appears.






Figure 4-16

4. Move the slider at the bottom to adjust the degree of warping. The adjusted view is shown on the right.
5. Select **Apply All** to apply the setting to all the cameras selected.
6. Click **OK**. The cameras are immediately dewarped.

4.2 Object Search

Object Search allows you to perform two functions: 1. Detect motion, missing objects or unattended objects to the recordings of a camera within a selected day. 2. Perform the counting function to the recordings of a camera within a selected day. The following instruction is an example of how to detect motion events in the recorded files.

1. Select **ViewLog** , click the desired channel, select **Toolbar** , select **Tools**  and then select **Object Search**. This window appears.

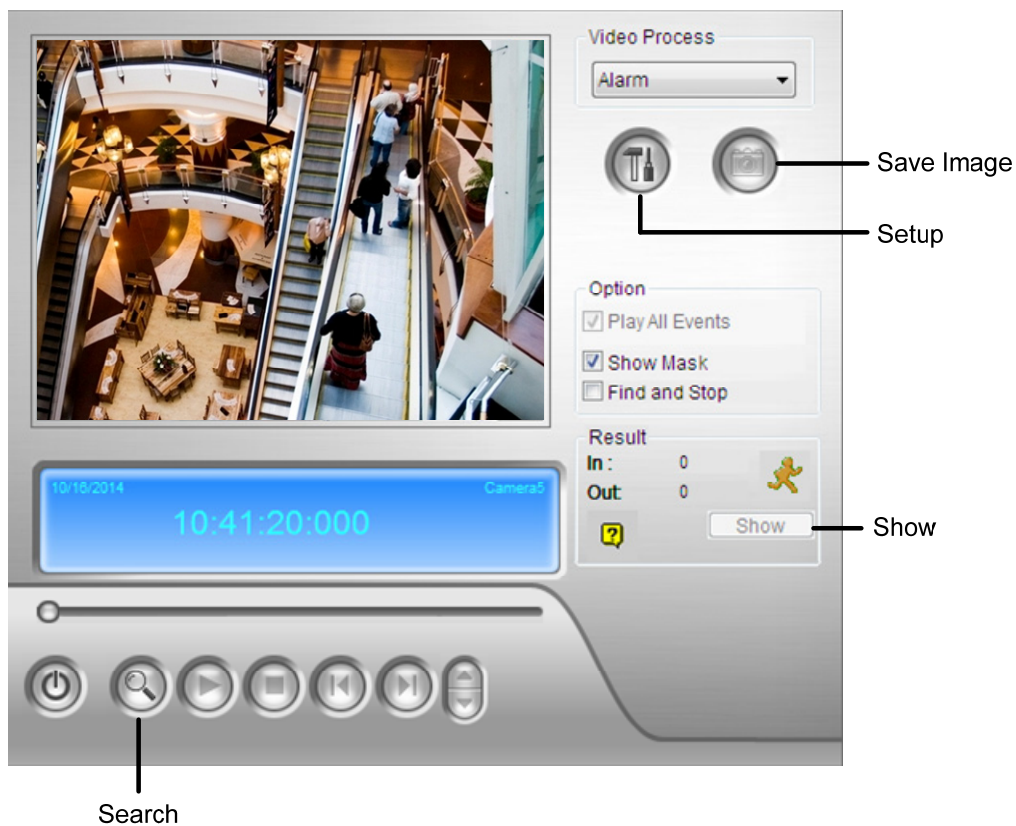


Figure 4-17 Object Search

2. In the Video Process drop-down list, select **Alarm**.

- Click the **Setup** button for further settings. The following window will appear.

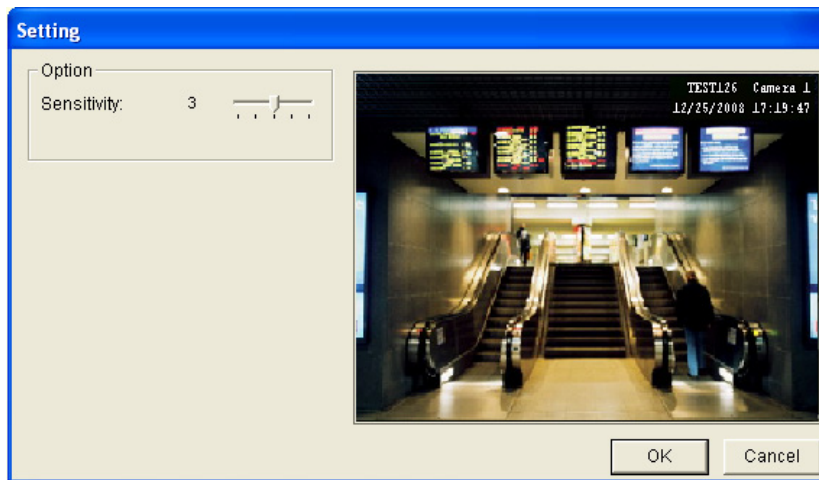


Figure 4-18

- Use the mouse to outline a region for motion detection. You will be prompted to enter **Alarm Region**.
- Adjust the detection Sensitivity if needed.
- Click **OK** to finish the settings and close the window.
- In the Option section, you have several options:
 - **Play All Events:** Plays back the video segments found as a continuous series of images.
 - **Show Mask:** Shows masks on the detection regions.
 - **Find and Stop:** (recommended) Pauses the search process when motion is detected.
- In the control panel, click the **Search** button to play back the video with the motion detection applied.
- When the desired image or the motion event is found, click the **Stop** button and then the **Show** button will become available. Click **Show** to display the Event List window.

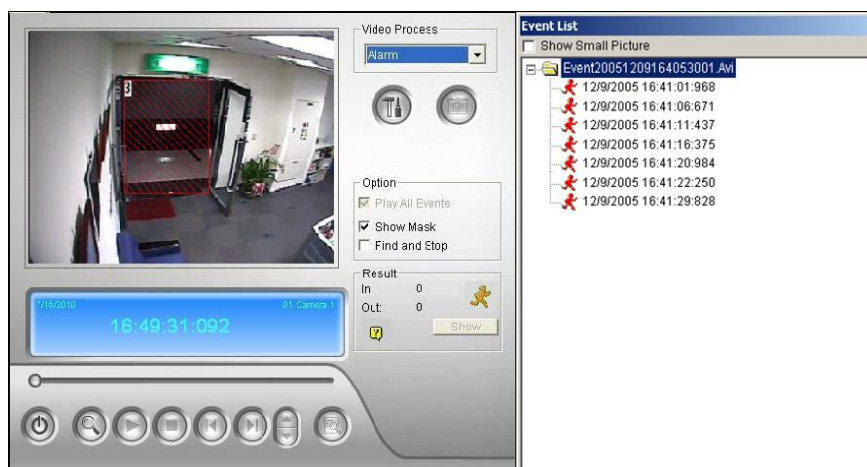





Figure 4-19

10. Expand the event folders to see the video segments inside. Or, enable **Show Small Pictures** at the upper of window to access the thumbnail view.
11. Select one video segment, and click the **Play** button in the Object Search window to play it back.

Note: For details on setting up Counter, Unattended Object or Missing Object in Steps 5 and 6, refer to similar setup steps in *Object Counting and Intrusion Alarm* and *Unattended and Missing Object Detection* in Chapter 3.

4.3 Advanced Log Browser

With the Advanced Log Browser, you can search for log data of monitored events, system activities, user activities, Object Counting events and POS events. For details on the log types, see *System Log* in Chapter 1.

1. Click **ViewLog** , click **Toolbar** , select **Tools** , select **System Log** and select **Advanced**. This dialog box appears.

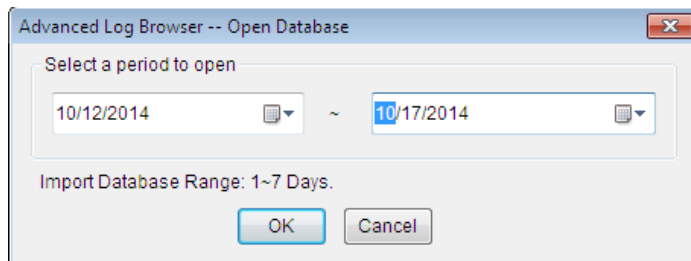


Figure 4-20

2. Specify a time range and click **OK**. All events within the specified range are displayed on the Advanced Log Browser window.

Controls on the Advanced Log Browser

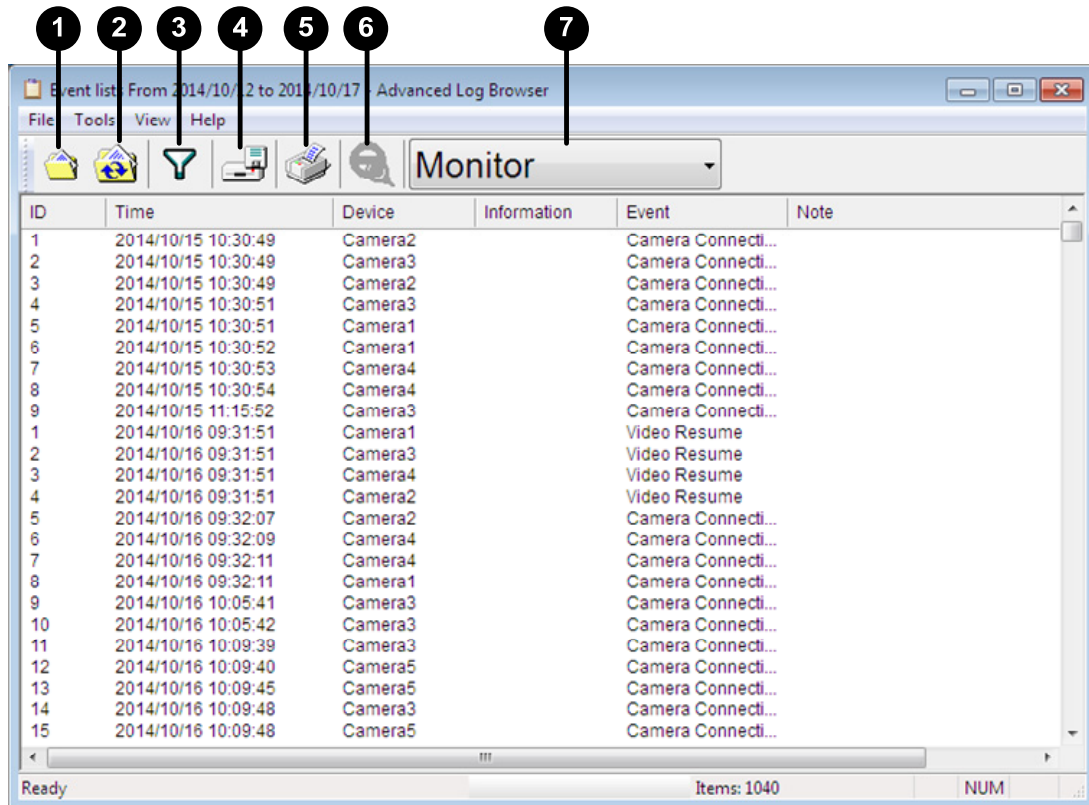


Figure 4-21 Advanced Log Browser

| No. | Name | Description |
|-----|---------------------------------|--|
| 1 | Open | Opens an event log. |
| 2 | Reload | Select Reload All Table or Reload Current Table to refresh loaded data. |
| 3 | Filter | Defines the search criteria. See <i>Filter Settings</i> later in this chapter. |
| 4 | Backup | Select All Tables to back up all log data, or selects Current Table to back up the current log table you are at. By default, audio and video are enabled for backup. |
| 5 | Print | Prints the current log table. |
| 6 | Filtering / Cancel Filtering | This button is only available when filtering starts. Click this button to cancel the filtering. After the filtering is complete, this icon appears dimmed. |
| 7 | Log Type | Select to display log of the following type: monitor, login, system, counter, merge, delete, backup, I/O, notifications and playback. |

4.3.1 Filter Settings

You can define filter criteria to search the desired log data. You can also import pre-defined filter settings for log search, or save current filter settings for future use.

1. On the toolbar, click the desired log table button (Monitor, System, Login or Counter), click the **Filter** button (No. 3, Figure 4-21), and select **Default Filter**. This dialog box appears.

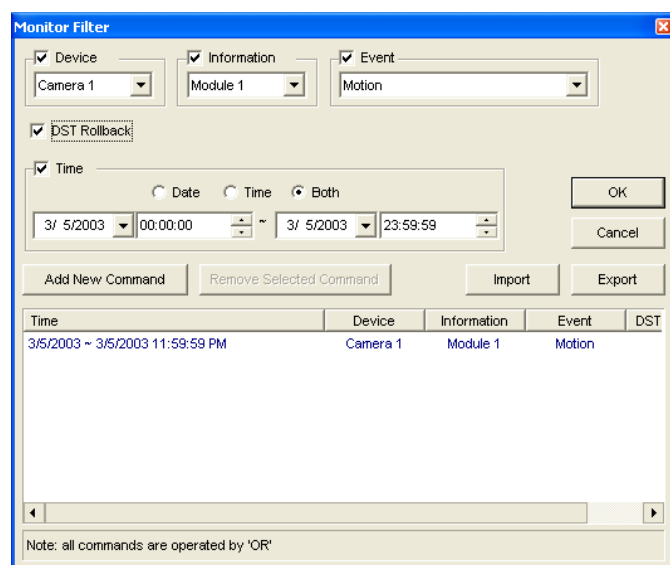


Figure 4-22

2. Define the filter criteria, such as a specific camera and a period of time.
3. If you want to search the log data recorded during the Daylight Saving Time period, select **DST Rollback**.
4. To add more filter criteria, click **Add New Command** and repeat Step 2.
5. You can click **Export** to save the current settings to another location, or **Import** to apply other filter settings.
6. Click **OK** to display the filter results.

Tip: Next time when you want to use the same exported settings, just click the **Filter** button, select **Favorites**, and select the name of the export file.




Note: The default Export path is `:\\GV folder\\Syslog_Favorites\\Monitor`. If you change the saving path, the name of the export file will not be listed in the **Favorites** option.

4.4 Remote ViewLog Service

You can retrieve the files from a remote GV-VMS through the network using the Remote ViewLog Service. The Remote ViewLog Service software:

- supports most functions provided by ViewLog, such as Backup, Save as AVI, Object Search, Database Files Backup, and so on.
- is capable of disabling camera connections under heavy network load
- resumes file transfers for backup

4.4.1 Retrieving Recordings from GV-VMS

1. On GV-VMS, click **Home** , click **Toolbar** , click **Network** , click **Control Center Server** and then select **Remote ViewLog Service** to allow remote access.
2. Download the GV-Remote ViewLog installer to a computer.
 - A. Visit the GeoVision Website http://www.geovision.com.tw/english/5_8.asp
 - B. From the **Supplemental Utilities** section, click the **Download** icon  of **GV-Remote ViewLog**.



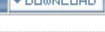

| Supplemental Utilities | | |
|--|---------|---|
| Product | Version | Link |
| GV-E-Map Server Allows you to create multiple e-maps for GV IP devices and DVR/NVR systems. | V8590 |  |
| GV-Multi View A multi-channel viewer for watching up to 32 live cameras simultaneously. | V8590 |  |
| GV-Remote E-Map Allows you to activate and view E-Maps remotely. | V8590 |  |
| GV-Remote ViewLog Retrieves and plays recordings from remote GV IP devices or DVR/NVR systems. | V8590 |  |

Figure 4-23

- C. Execute the installer and follow the on-screen instruction to install GV-Remote ViewLog.

3. Execute GV-Remote ViewLog and press **F10**. This dialog box appears.

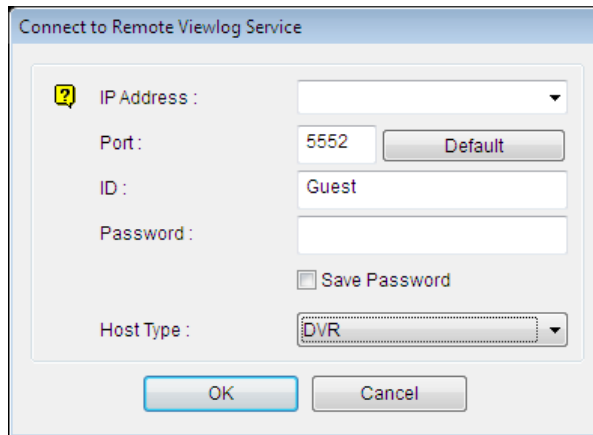


Figure 4-24

4. Type the IP Address, ID and Password of the GV-VMS. Only modify the default port **5552** if necessary.
5. In the Host Type, select **DVR** using the drop-down list.
6. Click the **Connect** button.

When the connection is established, you will see the events from the remote GV-VMS appearing on the Event List. Then you can use all ViewLog features for playback.

4.4.2 Retrieving Images of Object Index

The images of Object Index include the **Object Index**, **Face Detection** and **Video Snapshot**. Through the Remote ViewLog Service, you can retrieve all the Object Index images from a GV-VMS on the network.

1. Build the connection to a GV-VMS on the network using the Remote ViewLog Service. See *Retrieving Recordings from a Single Host* earlier in this chapter.
2. Click the **Advanced** button and select **Object Index**.

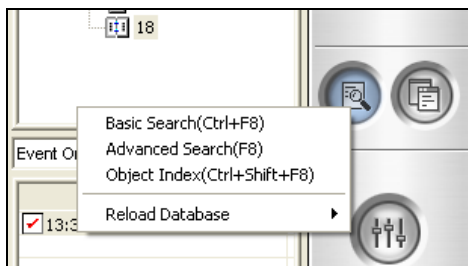


Figure 4-25

3. On the Object Index Search window, select the desired camera and file date for playback.
4. To play images with the ViewLog player, double-click the desired frame on **Object Index List**.

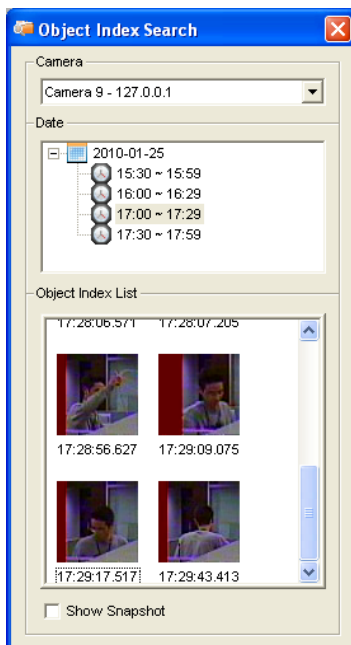


Figure 4-26

5. If you retrieve the images of **Video Snapshot**, you can select **Show Snapshot** at the bottom of the dialog box and double-click the desired frame to display it with the default image viewer of Windows, e.g. Paint.

4.4.3 Resuming Backup

Using the Remote ViewLog Service, you can back up files from a remote GV-VMS. When the file transfer is interrupted by a network error, you can even resume backup.

1. When the backup is interrupted, this message will appear: *There are x file(s) couldn't be backup. Do you want to keep a log file and backup them later?*
2. Click **Yes**. You will be prompted to save the partial backup file as *.lv format.
3. To resume backup, click the **Resume** button in the Backup dialog box, and then locate the partial backup file to continue.

For details on backing up files, see *Backing Up Recorded Files* in Chapter 5.

4.5 Single Player

When backing up the recorded files, you can choose to include the player of ViewLog or Single Player (see *Backing up Recorded Files* in Chapter 5). Compared to ViewLog, the Single Player provides simple and easy playback functions. To play back the recordings using the Single Player, open the backup folder and run **GVSinglePlayer.exe**.

4.5.1 Single Player Window

To play back a recoded file, click **Files** and click **Open File** to select the file you wish to play back. To play back multiple recorded files together in up to 16 screen divisions, click **Files** and click **Open Folder** to select the folder that collects several camera recordings.

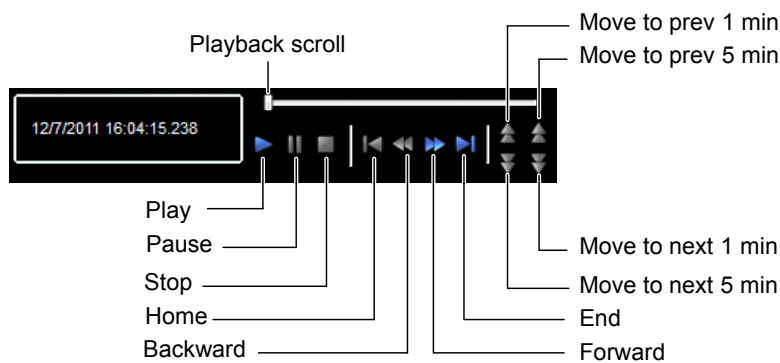
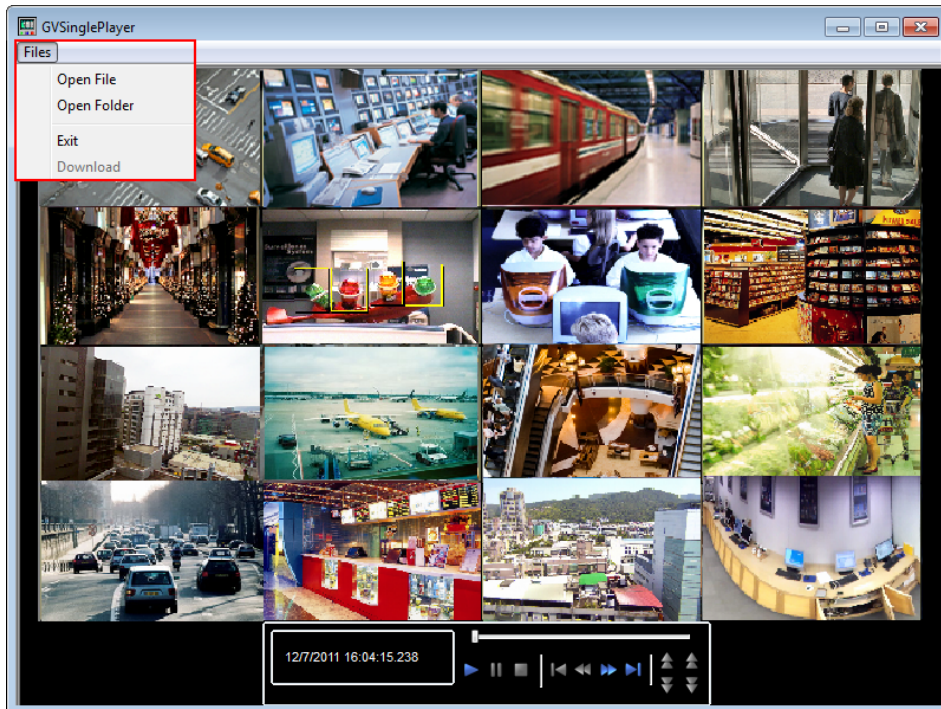


Figure 4-27

Right-clicking the playback window can change the play mode and create special effects when you play video back.

| Name | Functions |
|-----------|---|
| Play Mode | Includes these options: |
| | <ul style="list-style-type: none"> ■ Frame by Frame: Plays back video frame by frame. ■ Real Time: Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback. ■ Key Frame: Plays back video with key frames only. ■ Smooth Playbacks: Evenly distributes 30 frames per second. When the playback appears choppy, select this option to enhance the smoothness. ■ Auto Play Next 5 Minutes: Plays back video up to 5 minutes. ■ Audio: Turns on or off the video sound; audio denoise. |
| Render | Includes these options: |
| | <ul style="list-style-type: none"> ■ Deinterlace: Converts the interlaced video into non-interlaced video. ■ Scaling: Smoothens mosaic squares when enlarging a playback video. ■ Deblocking: Removes the block-like artifacts from low-quality and highly compressed video. ■ Defog: Enhances image visibility. ■ Stabilizer: Reduces camera shake. ■ Text overlay's camera name and time: Overlays camera name and time onto the video. ■ Text overlay's POS/GV-Wiegand: Overlays POS or GV-Wiegand Capture data onto the video. ■ Wide angle lens dewarping: Corrects distortion toward the corner of the camera view. ■ Fisheye: Select Geo Fisheye to choose a camera mode. ■ Mega Pixel View: Enables PIP or PAP view. ■ Display GPS: Shows the location on the map where the video is taken through GPS. ■ Select GPS Map (Apply after restart): Select a type of GPS map to apply. ■ Full Screen: Switches to the full screen view. |
| Tools | <ul style="list-style-type: none"> ■ Snapshot: Saves a video image. ■ Save as AVI: Saves a video as avi format. ■ Download: Downloads the video clip from the DVR or video server to the local computer. |

4.6 Specifications

| Feature | Notes |
|-------------------------------|--------------------------------|
| Support for Defogging | Yes (64 channels) |
| Support for Stabilizer | Yes (64 channels) |
| Support for PIP View | Yes |
| Support for PAP View | Yes |
| Support for Panorama View | Yes (4 sets of Panorama View) |
| Videos Exported as .AVE Files | Yes |
| Object Search | Yes |
| Support for Fisheye View | Yes |

Chapter 5

Backup, Deletion and Repair 204

| | |
|---|------------|
| 5.1 Backing Up Log Data..... | 204 |
| 5.2 Backing Up Recorded Files..... | 206 |
| 5.3 Deleting Recorded Files..... | 209 |
| 5.4 Repairing Damaged File Paths..... | 211 |
| 5.5 Repairing Damaged Video Files..... | 213 |

Backup, Deletion and Repair

This chapter explains how to back up and delete video/audio files. Video files can be copied from the hard disk to external storage media, such as CD-R, DVD, MO, or ZIP drives. Video files saved on the hard disk can be deleted as well.

5.1 Backing Up Log Data

Using the System Log, you can back up all log data or filtered data based on criteria.

1. Click **ViewLog** , click **Toolbar** , select **Tools** , select **System Log** and then select **Advanced**. This dialog box appears.

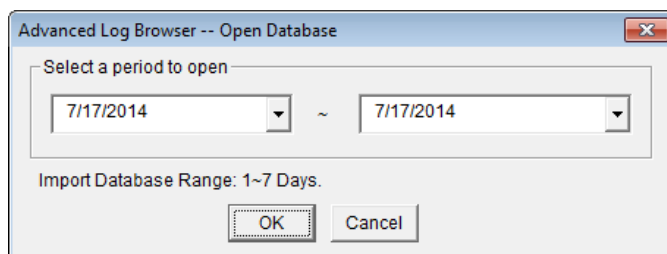



Figure 5-1

2. Specify a time range and click **OK**. Events recorded during the specified range are displayed on the Advanced Log Browser window (Figure 4-19).
3. Click the **Backup** button  on the toolbar. This dialog box appears.

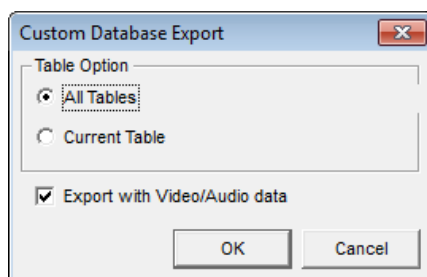


Figure 5-2

[Table Option]

- **All Tables:** Backs up all log data.
- **Current Table:** Backs up only the log table you are currently at.

[Export with Video/Audio data] Backs up video/audio attachments with log data.

4. Click **OK**. The Backup dialog box (Figure 5-3) appears.
5. In the Media section, select the method and destination to back up the log files.
6. Click **OK** to back up.

Note:




1. To back up the filtered data, use the **Filter** function to define search criteria first. See *Filter Settings, Advanced Log Browser* in Chapter 4.
 2. To open the backup data, run **EZSysLog.exe** from the backup file.
-

5.2 Backing Up Recorded Files

Using ViewLog, you have three backup options:

- Back up to hard disk
- Create CD/DVD/BD using third-party software, e.g. Nero, Roxio, etc.
- Create CD/DVD/BD using Windows XP / Vista / Windows 7 / 8 / Windows Server 2012 inbuilt burning software.

To back up files:

1. Click **ViewLog** , click **Toolbar** , select **Tools** , and then select **Backup**. This dialog box appears.

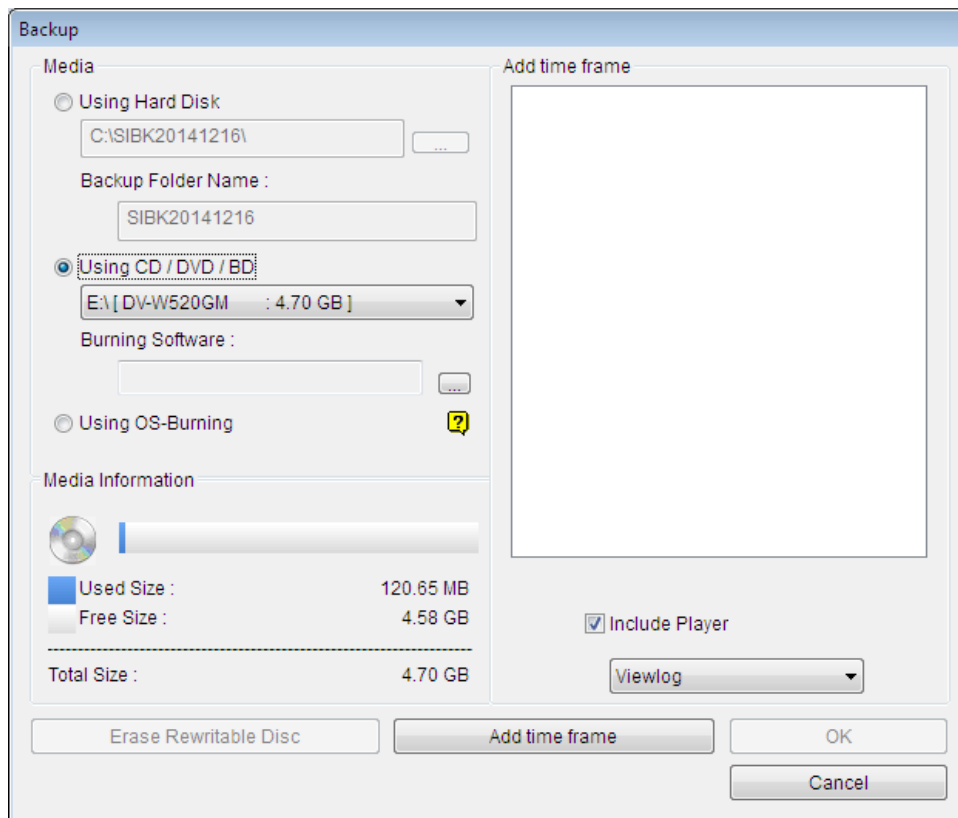


Figure 5-3

2. Select a destination media to back up files.

[Media]

- **Using Hard Disk:** Backs up files to the hard disk you select. Click the [...] button to select the desired hard disk.
- **Backup Folder Name:** Type a desired name for the backup folder.
- **Using CD/DVD/BD:** Click to back up files to the CD or DVD media using the third-party

[Time Period] Specify the time periods for backup.

[Select Camera(s)] Select the camera(s) for backup. The number of video and audio files of each camera is indicated respectively, e.g. "Camera 1 1+0" means Camera 1 has 1 video file and 0 audio file.

- **Video + Audio drop-down list:** Select the types of video events for backup.

[Information]

- **Database Files:** Backs up the files from System Log.
 - **Object Index Files:** Backs up the Object Index files.
 - **Never-Recycle Events only:** Only backs up the never-recycle events.
 - **Unmark these events to be recycled after the backup is complete:** After the backup is complete, the never-recycle events will be unmarked for recycling. Please note if the first file in the database has been marked and then unmarked in this condition, the first file will be deleted automatically.
 - **Include daylight saving rollback events:** Backs up the events recorded during Daylight Saving Time.
 - **The Status and Search End section:** Indicates the number of backup files and their total size. (Total MDB refers to the System Log files.)
4. Click **OK** to add the schedule. You can repeat step 3 to create up to 10 periods of time.
 5. To include the player to the backup files, select **Include Player** at the right bottom of the Backup dialog box and select **ViewLog** or **Single Player**. By default, **ViewLog** is selected. If no player is selected, you can only play the backup files at the computer installed with GeoVision codec.
 6. Click **OK** on the Backup dialog box to start the backup.

Note:

1. If you are unable to record a CD, make sure the CD recording is enabled in your CD burner: open **My Computer**, right-click the CD Drive icon, click **Properties**, click the **Recording** tab, and check **Enable CD recording on this drive**.
 2. For details on ViewLog and Single Player, see *Chapter 4 Video Playback*.
-

5.3 Deleting Recorded Files

To delete files using ViewLog, follow these steps:

1. Click **ViewLog** , click **Toolbar** , select **Tools** , and then select **Delete**. This dialog box appears.

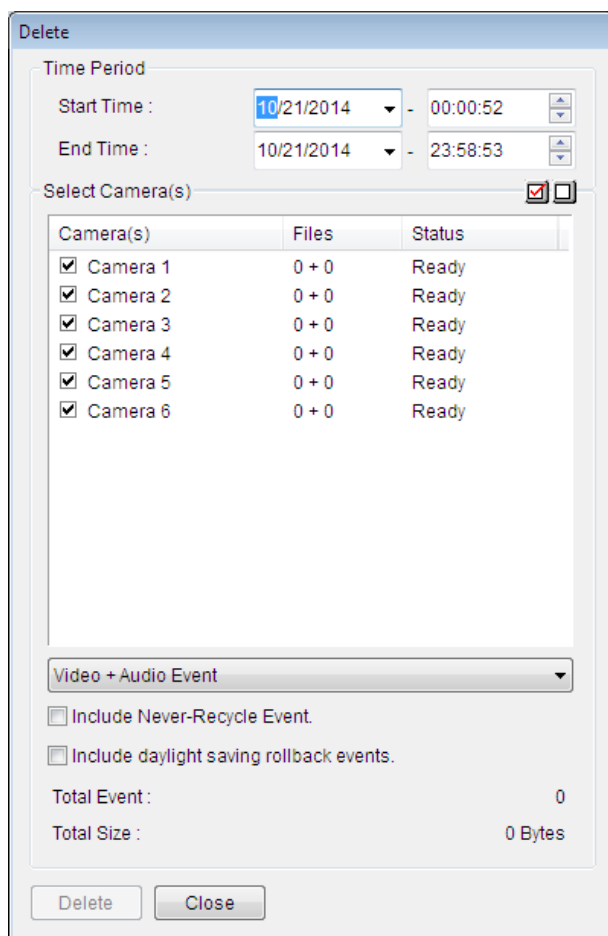




Figure 5-5

2. Define the time period for file deletion.
3. Uncheck the cameras, which you don't want to delete the files of.
4. Use the drop-down list to select the types of events to be deleted, e.g. video, audio or both together.
5. If you want to delete the never-recycle events, select **Include Never-Recycle Event**.
6. If you want to delete the events recorded during the Daylight Saving Time period, select **Include Day Light Saving Time Rollback Event**.
7. Click the **Delete** button.

Note:

1. To view the history of file deletion, click **ViewLog** , click **Toolbar** , select **Tools** , select **System Log**, select **Monitor Table**, and then click the **Delete** tab.
 2. To view the storage path and total file size of a camera, right-click the camera and select **Event View** on the Delete dialog box.
-

5.4 Repairing Damaged File Paths

Use GV-VMS' Delete function (see *Deleting Recorded Files* earlier in this chapter) to correctly delete video and audio files. If you move or delete a video file using Windows Explorer or Windows File Manager, GV-VMS will not be able to detect this change. In this case, use Repair Database Utility to repair misplaced or missing recorded files that are not identified by the ViewLog player. As long as these files are still stored on the hard drives and are detectable by Windows operating system, the Utility can restore these recorded files back to their default paths and allow them to appear under ViewLog. This Utility comes with the installation of Main System. Follow these steps to repair the paths:

1. Go to the **Windows Start** menu, select **All Programs**, select the GV-VMS folder, and select the **Repair Database Utility**. The valid ID and password are required.
2. When the Select Camera for Repair Database dialog box appears, select the cameras that require database repair.
3. Click **OK**. This dialog box appears.

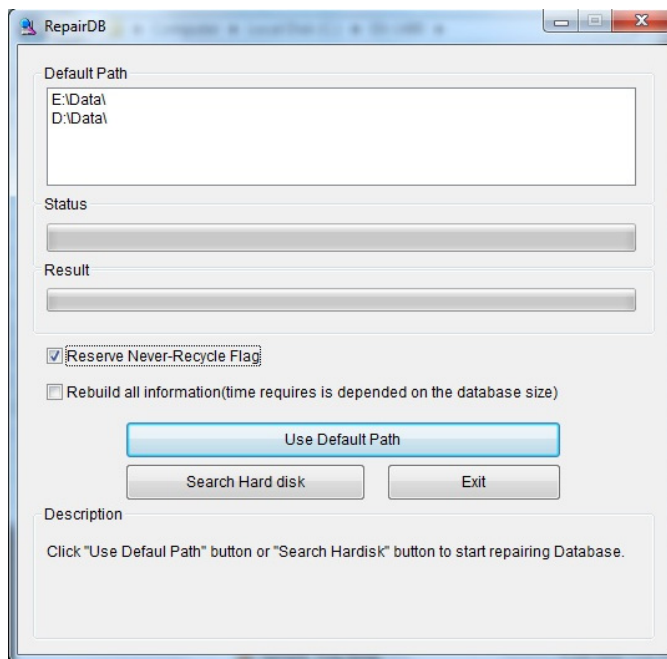


Figure 5-6 The RepairDB Dialog Box

4. If your recorded files exist only in the predefined recording paths, click the **Use Default Path** button. The GV-VMS will rebuild paths for these files in the predefined recording hard drives only.
5. If your recorded files scatter across different hard drives, click the **Search Hard Disk** button. The GV-VMS will rebuild paths for these recorded files in all hard drives connected to the GV-VMS. In this way, more time will be required for building the database.

Note:

1. The repair and the search function will not apply to the files that have been renamed manually.
 2. Use this Utility to repair your database if you encounter any of the following scenarios in ViewLog:
 - a. A question mark appears right before a video file in the Video Event list.
 - b. When you select a file and click the **Playback** button, no video is displayed.
-

5.5 Repairing Damaged Video Files

If the computer has been shut down improperly, e.g. due to power failure, use this function to repair the damaged video files.

Tip: When a computer has been shut down improperly, the first thing you do before starting the GV-VMS is to run **Repair Database Utility**. After running the Utility, go back to ViewLog and view Video Events. You should be able to play back all video files at this step. However, if what you see is a question mark after clicking on the file, the problem may be that the recording process was interrupted. To repair the file, run the AVI Repair Utility and follow the steps below.

1. Double-click **AVIRepairAPI.exe** in the GV folder. This dialog box appears.

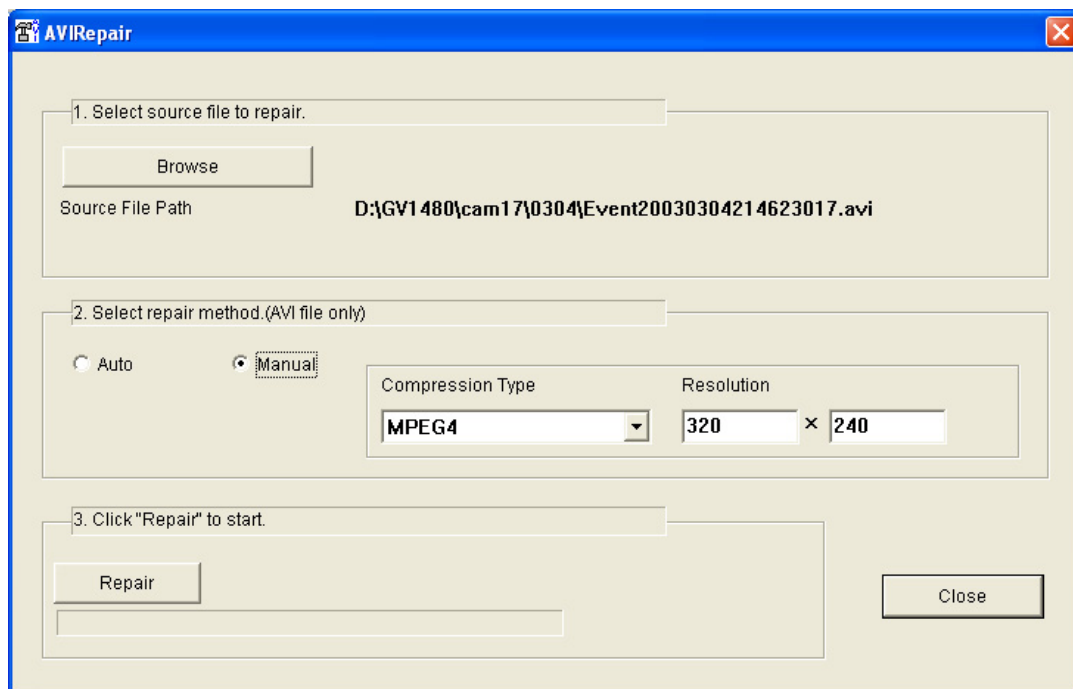


Figure 5-7

2. Click the **Browse** button to find the damaged video file.
3. If you know the codec and resolution of the file, select **Manual**, select **Compression Type** and type **Resolution**. Alternatively, you may select **Auto** and the system will run all combinations for you. Please note it takes longer time to repair with this selection.
4. Click the **Repair** button to start.

5. You may see the distorted image or **No Image** on view screen if an incorrect codec and resolution were chosen. For this, click **No** for the next combination until a complete image appears.

Distorted Image

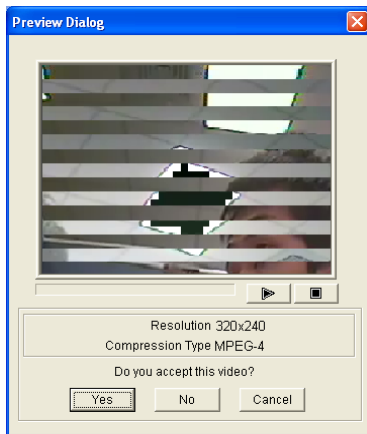


Figure 5-8

No Image

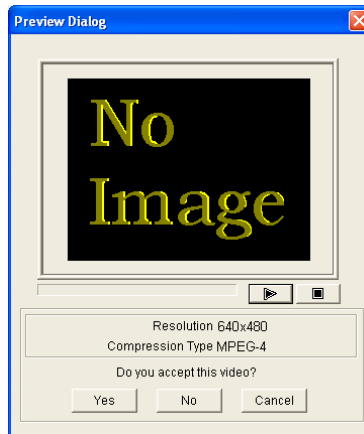


Figure 5-9

Complete Image

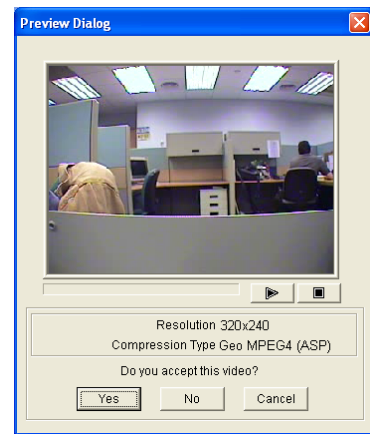


Figure 5-10

6. When a complete image is displayed, click the arrow button to preview the file.
7. Click **Yes** to start the repair.
8. Click **Yes** to overwrite or **No** to save this file to another path. Note if you choose **No** in this step, remember to run **Repair Database Utility** again after exiting this program.

Chapter 6

I/O Applications..... 216

| | | |
|------------|---|------------|
| 6.1 | Setting I/O Devices | 217 |
| 6.1.1 | Adding I/O Devices | 218 |
| 6.1.2 | Setting the Input and Output Devices | 219 |
| 6.1.3 | Latch Trigger..... | 221 |
| 6.1.4 | Keeping Last Toggle Status..... | 223 |
| 6.2 | Advanced I/O Applications..... | 225 |
| 6.2.1 | Setting Up Actions Upon Input Trigger..... | 226 |
| 6.2.2 | Moving PTZ Camera to Preset Points upon Input Trigger | 227 |
| 6.2.3 | Setting Momentary and Maintained Modes | 228 |
| 6.2.4 | Deactivating Alarm and Alert upon Input Trigger | 229 |
| 6.2.5 | Other I/O Application Functions | 230 |
| 6.3 | I/O Devices in Content List | 231 |
| 6.4 | Visual Automation | 232 |




I/O Applications

This chapter discusses how you can set up and control the I/O devices connected to GV-VMS. I/O applications include these features:

- Record video, send e-mail notification and trigger output upon input trigger
- Move PTZ camera to a preset location on input trigger
- Support access control systems of Momentary and Maintained modes
- Visual automation to intuitively trigger an output by clicking on the camera view

6.1 Setting I/O Devices

To connect the I/O device to the computer of GV-VMS, you may need additional devices: GV-Net, GV-Net Card, GV-NET/IO Card or GV-I/O Box. For details on these devices, visit http://www.geovision.com.tw/english/3_1_Accessory.asp.

To set up I/O devices on the GV-VMS, click **Home** , select **Toolbar** , click **Configure** , click **Accessories** (if available), click **I/O Device** (if available) and then select **I/O Device Setup**. This window appears.

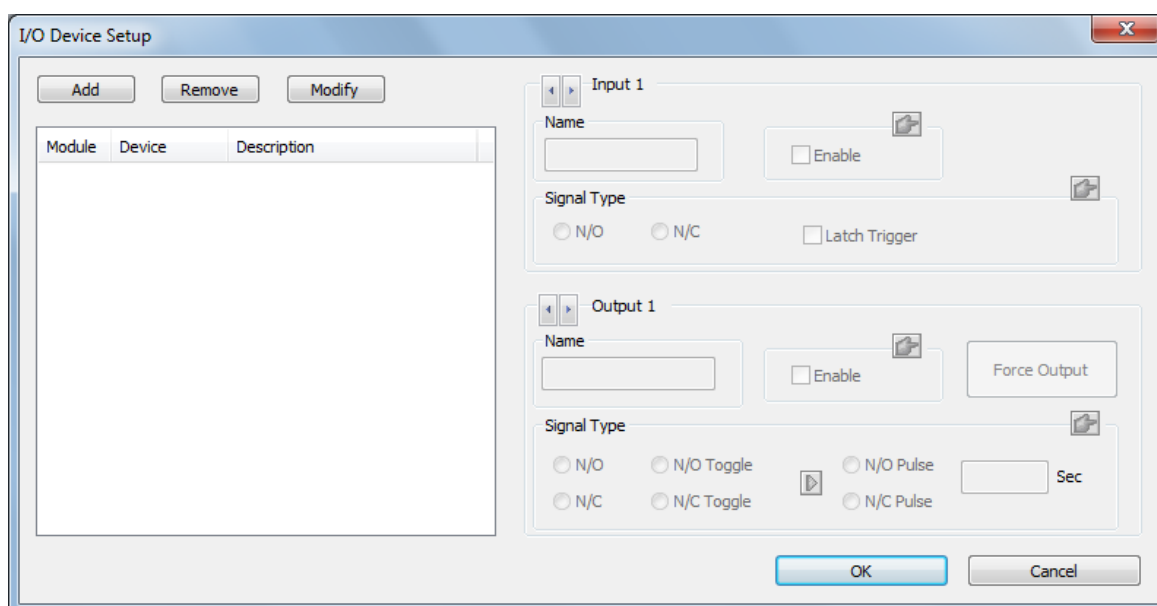


Figure 6-1 I/O Settings

Note: The **Accessories** option only appears when GV-Keyboard or GV-Joystick has been set up on the GV-VMS. The **I/O Device** option only appears after at least one I/O device has been added.

6.1.1 Adding I/O Devices

To add an I/O device to GV-VMS, click the **Add** button in I/O Device Setup dialog box (Figure 6-1).

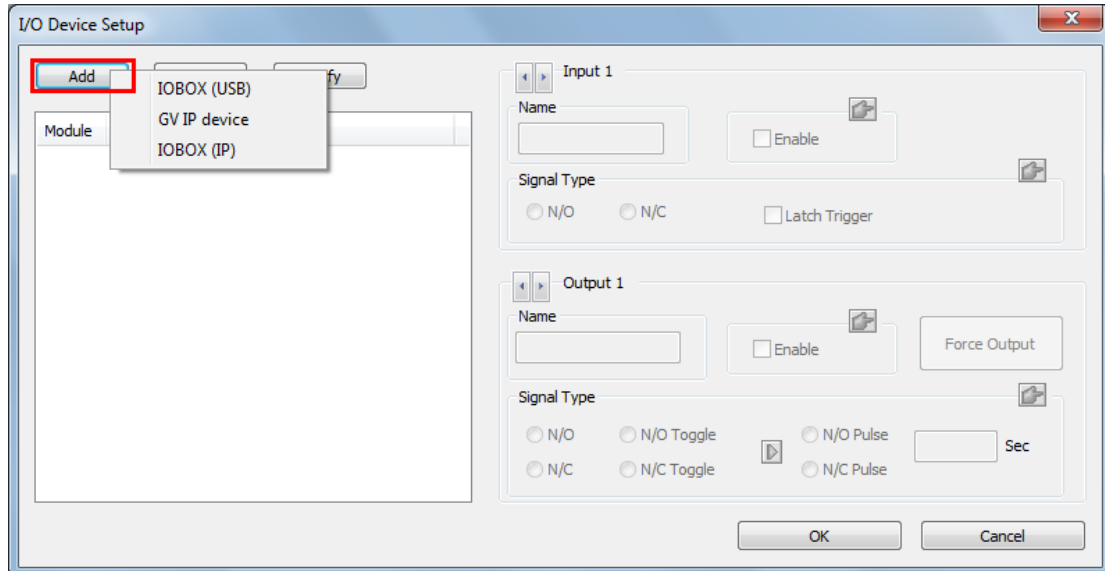




Figure 6-2

There are three ways to add an I/O device:

- **IO Box (USB):** Select if GV-VMS is connected to the GV-I/O Box through USB connection.
 1. Select the type of **Device** connected.
 2. Select the **COM port** used to connect the device.
 3. Assign an **Addr.** number to the device. Start by setting the first device to 1, and then assign a different address for every new device added.
 4. Click **OK**.
- **GV IP Device:** GV-VMS can remotely control the I/O devices connected to GV-IP Devices through TCP/IP connection.
 1. Select the GV-IP Device with I/O devices installed and click the  button.
 2. Click **OK**.
- **IO Box (IP):** GV-VMS can remotely control the I/O devices connected to GV-I/O Box through TCP/IP connection.
 1. Click the **Search** button to search for available devices under LAN or click the **Add** button to manually type the connection information of the device.
 2. Select the device and click the  button. Type the **User Name** and **Password** if needed.
 3. Click **OK**.

6.1.2 Setting the Input and Output Devices

After adding the I/O device, enable the input and output device. For GV-I/O Boxes connected through USB, you can configure the signal type on GV-VMS. For GV-IP Devices and GV-I/O Boxes connected through TCP/IP, you will have to configure the signal type on the device's Web interface.

[Input X] Click the **Arrow** buttons to select the input device you want to set up and click **Enable**.

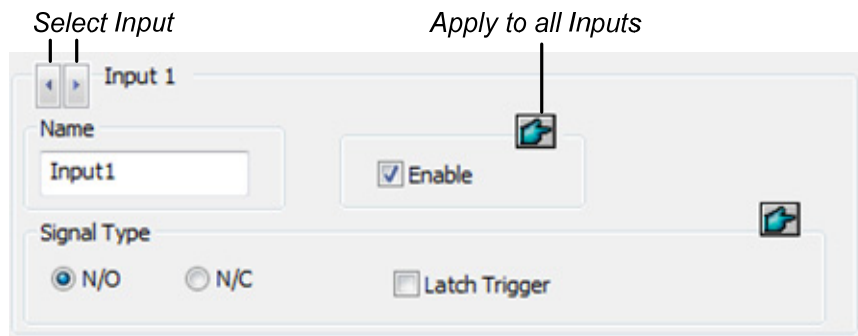


Figure 6-3

- **Name:** Specifies a name for the input device.
- **Signal Type:** Select a signal type for your input device: NO (normally open), NC (normally close) or Latch Trigger. Clicking the finger button to apply the same settings to all input devices. For details on Latch Trigger, see *Latch Trigger* later in this chapter.

[Output X] Click the **Arrow** buttons to select the output device you want to set up and click **Enable**.

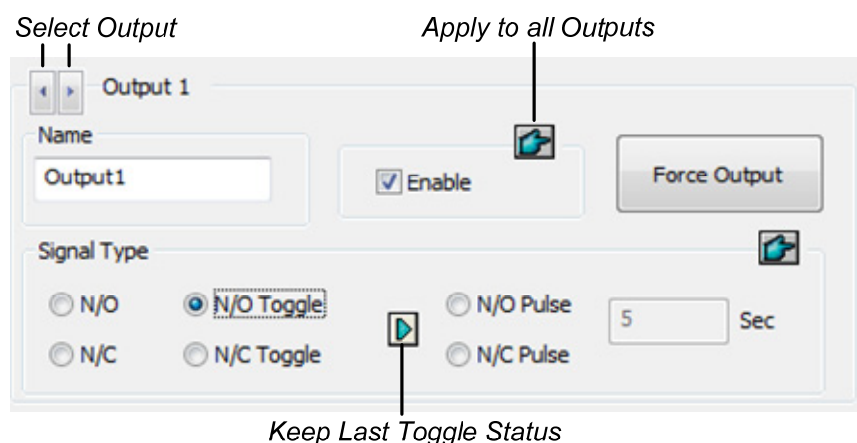


Figure 6-4

- **Name:** Specifies a name for the output device.
- **Force Output:** Click to test signal to the selected device.

- **Signal Type:** Select a signal type: N/O (Normal Open), N/O Toggle, N/O Pulse, N/C (Normal Closed), N/C Toggle, and N/C Pulse. For **Toggle** output type, the output continues to be triggered until a new input trigger ends the output. For **Pulse** output type, the output is triggered for the amount of time you specify in Sec field.
- **Keep Last Toggle Status:** See *Keeping Last Toggle Status* later in this chapter.

Note: PTZ camera and I/O devices cannot be assigned to the same port at the same time.

6.1.3 Latch Trigger

Instead of constant output alarm in N/O and N/C during the input trigger, the Latch Trigger option provides a momentary output trigger.

Setting up Latch Trigger

In the I/O Device dialog box (Figure 6-1), select **Latch Trigger**.

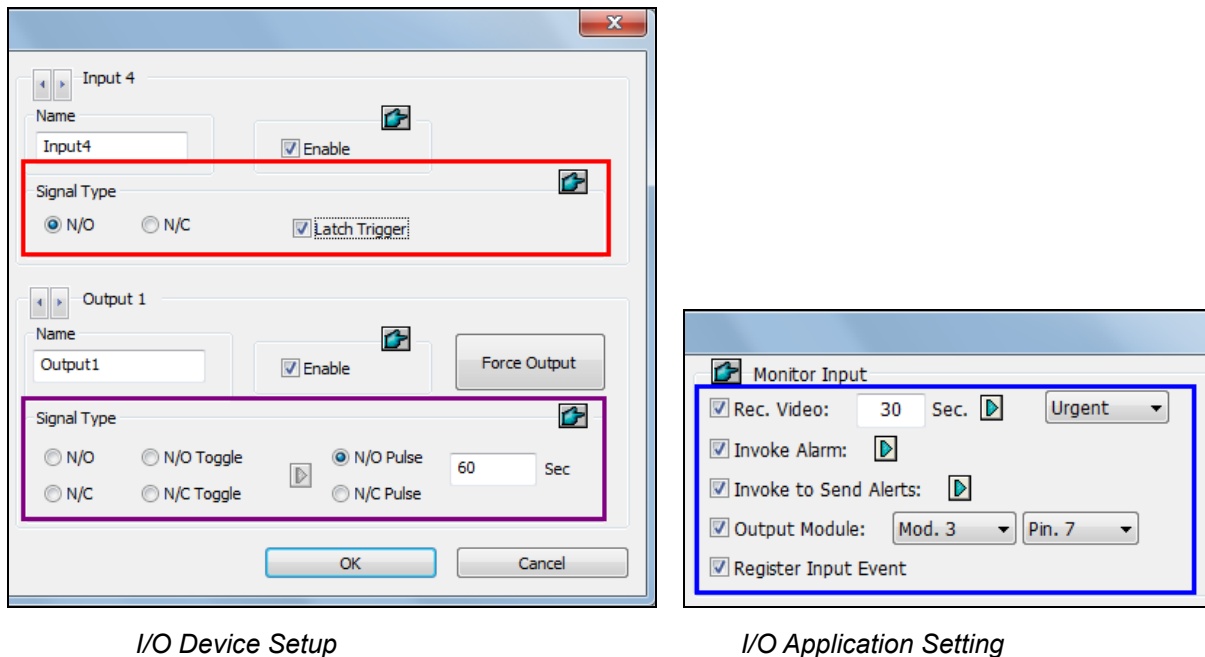


Figure 6-5

Application Example

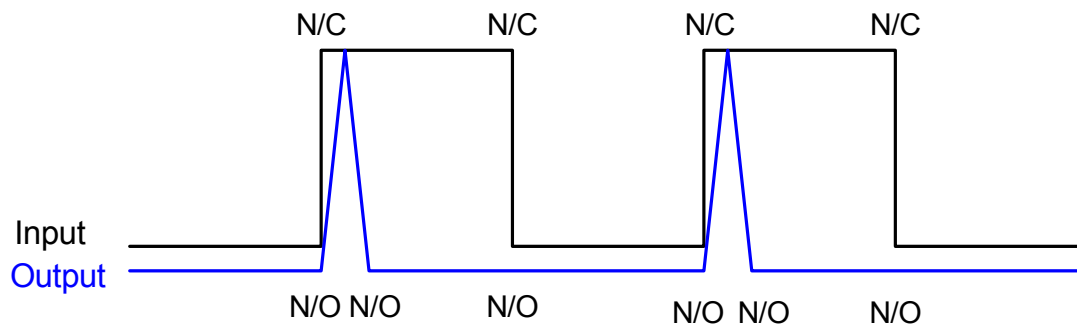
In the above scenario, Input 4 is set to N/O and Latch Trigger. When Input 4 is triggered:

- The camera starts recording for 30 seconds using the frame rate settings for Urgent Event and stops itself when the next input trigger (see the Rec Video option in the blue box).
- Computer Alarm sounds once (see the Invoke Alarm option).
- The output (Module 3, Pin 7) is triggered simultaneously based on the Latch Trigger mode (see the illustrations below).

The following illustrations can help you understand different output signals (see purple square in the above dialog box) working with the Latch Trigger option.

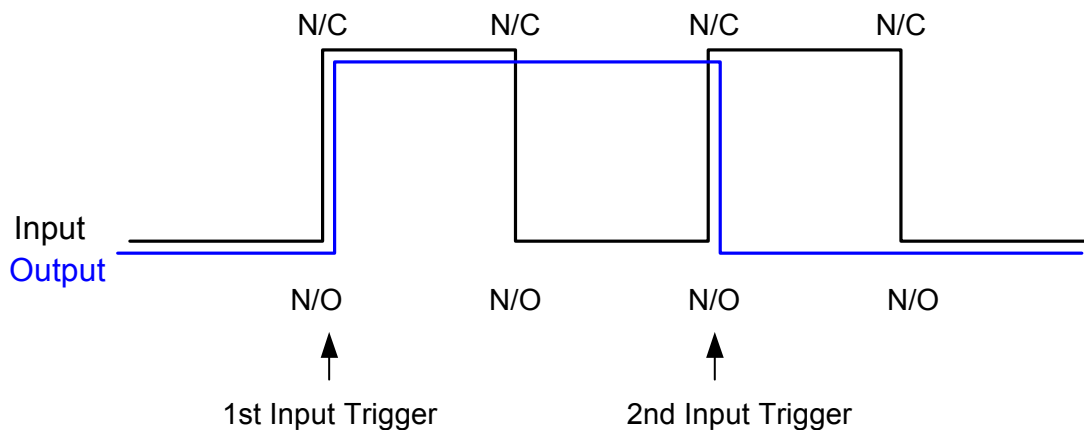
1. N/O (Normal Open) + Latch Trigger

Once the input triggers the output, the output will be triggered for a short moment and then turn off itself.



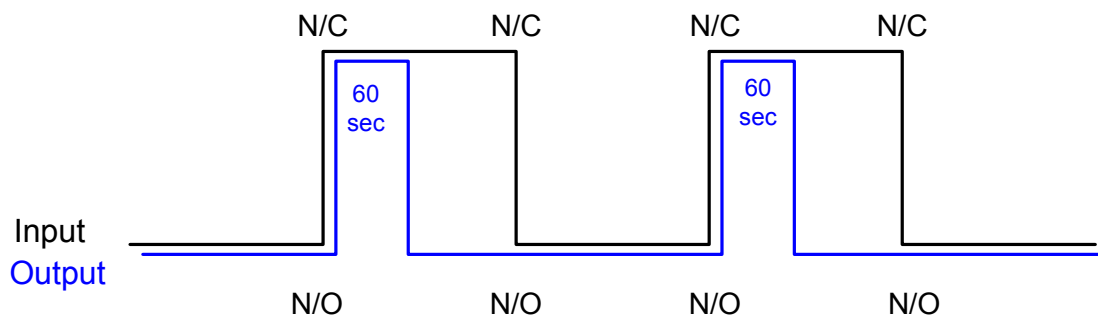
2. N/O Toggle + Latch Trigger

Once the input triggers the output, the output will keep triggering until a new input trigger.



3. N/O Pulse + Latch Trigger

Suppose you set the Pulse time to 60 seconds. Once the input triggers the output, the output will remain ON for 60 seconds before turning off itself.



6.1.4 Keeping Last Toggle Status

This feature can memorize the current output state when the monitoring is stopped or the system is restarted. For example, if the output device is a light, the triggered light will remain ON when you stop monitoring.

Setting up “Keep Last Toggle Status”

In the I/O Device dialog box (Figure 6-1), select **N/O Toggle** or **N/C Toggle**, and click the **Arrow** button on the right to select **Keep Last Toggle Status**.

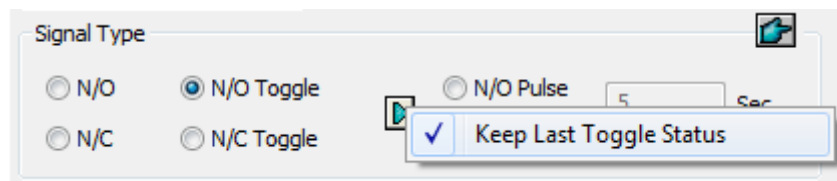


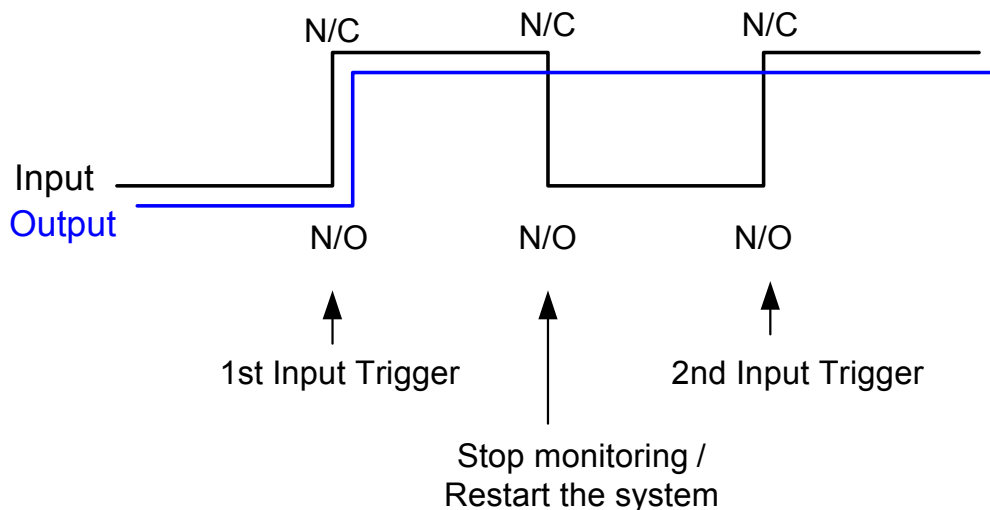
Figure 6-6

Application Example

The following two illustrations explain how the input works with the output set to **Keep Last Toggle Status**.

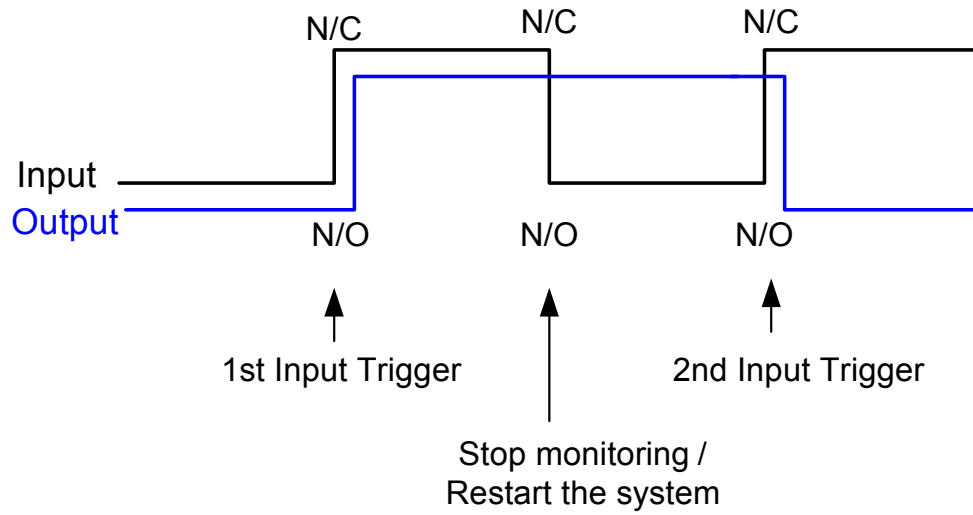
1. Input (N/O) + Output (N/O Toggle + Keep Last Toggle Status)

The triggered output remains ON even when you stop monitoring or restart the system.





2. Input (N/O + Latch Trigger) + Output (N/O Toggle + Keep Last Toggle Status)

When “Latch Trigger” works with “Keep Last Toggle Status”, the output only has a momentary trigger but also needs to remain ON even when you stop monitoring or restart the system. Therefore under the two conditions, the output turns off when a new input triggers.



6.2 Advanced I/O Applications

After adding I/O devices to GV-VMS, you can configure advanced I/O applications, such as setting alarm notification, defining a PTZ camera movement upon input trigger, setting momentary or maintained mode, and deactivating alarm and alert settings.

Click **Home** , select **Toolbar** , click **Configure** , click **Accessories** (if available), click **I/O Device** (if available) and then select **I/O Application Setting**. This dialog box appears.

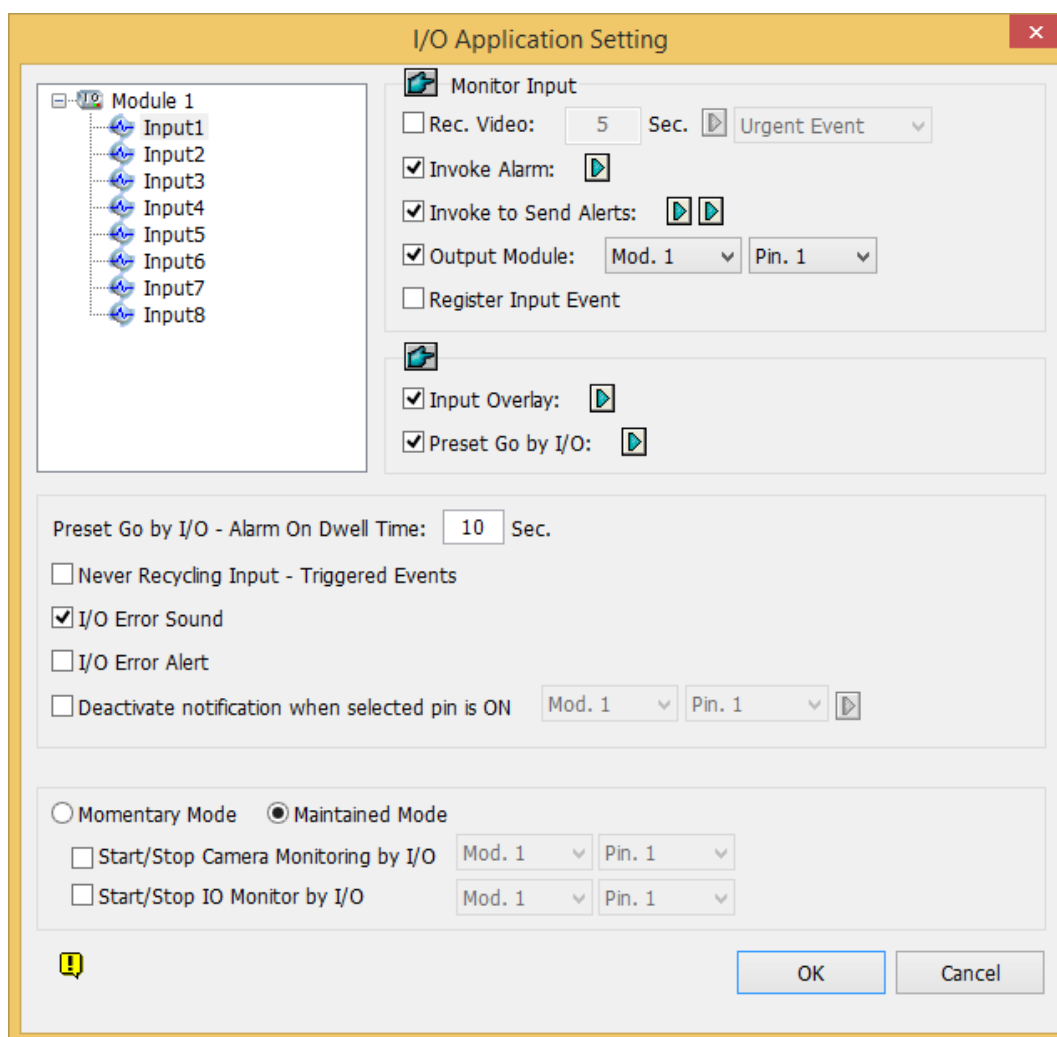



Figure 6-7 I/O Application

Note: The **Accessories** option only appears when GV-Keyboard or GV-Joystick has been set up on the GV-VMS. The **I/O Device** option only appears after at least one I/O device has been added.

6.2.1 Setting Up Actions Upon Input Trigger

This section helps you set up the actions to take after the input device is triggered. Select an input on the left to set it up. Clicking the Finger button  will apply the same settings to all inputs.

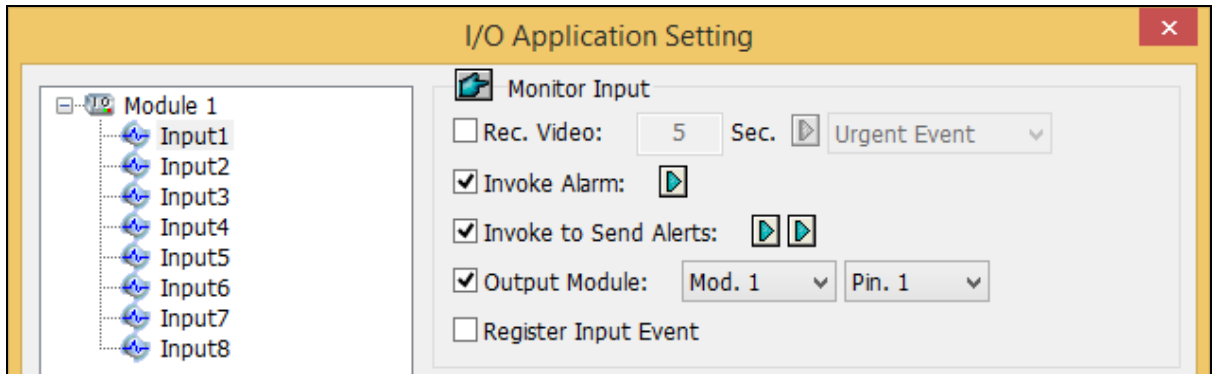


Figure 6-8

[Monitor Input]

- **Rec Video:** Select to record one or multiple cameras upon input trigger. Specify the recording duration and click the **Arrow** button to select which camera to record upon input trigger. Use the drop-down list to select whether to use the frame rate settings for Urgent Event or General Event. For details on setting up Urgent and General Event, see *Configuring General Setting* in Chapter 2.
- **Invoke Alarm:** Select to activate computer alarm when the input is triggered. You can select the alarm sound from the drop-down list.
- **Invoke to Send Alerts:** Select to send out E-mail notification when the input is triggered. Click the **First Arrow** button to select the camera(s). Click the **Second Arrow** button to specify the recipient's email address. For e-mail alerts, see *E-Mail Notification* in Chapter 1.
- **Output Module:** Triggers the specified output module when the input is activated. Use the drop-down lists to select the output module and pin number.
- **Register Input Event:** Registers the I/O trigger events into System Log. Each event is labeled with ID, time, device name (camera or I/O input), corresponding module of the device, and event for later retrieval. For details on System Log, see *System Log* in Chapter 1.

6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger

This feature allows you to move the PTZ camera to preset points when an input is triggered. Select an input number to be set up.

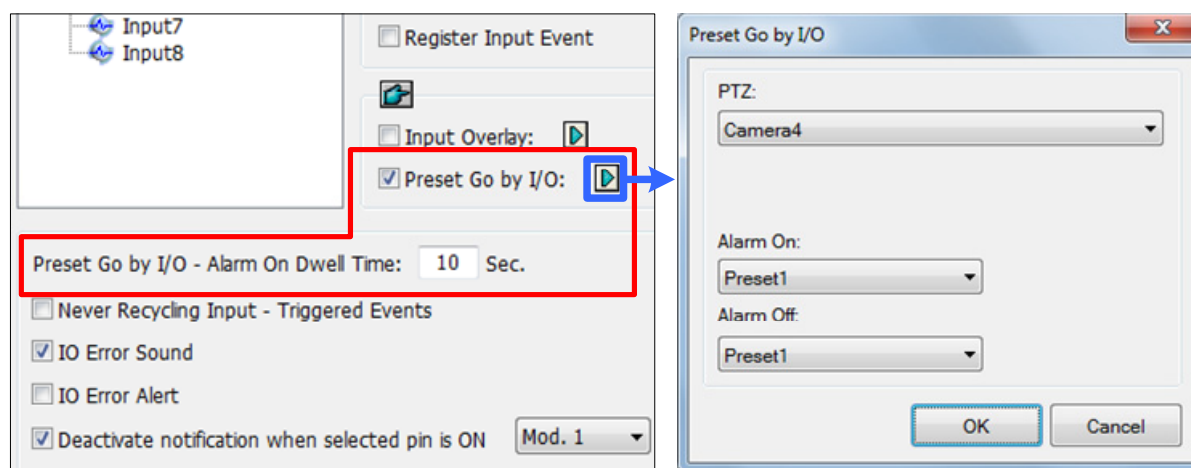



Figure 6-9

- **Preset Go by I/O:** Enable the option and click the Arrow button to select your PTZ camera from the drop-down list. Clicking the Finger button can apply the same settings to all inputs.
- **Alarm On:** Moves the PTZ camera to a preset point when the input is triggered.
- **Alarm Off:** Moves the PTZ camera to a preset point when the triggered input is off.
- **Preset Go by I/O - Alarm On Dwell Time:** Specify the amount of time the PTZ camera stays at “Alarm On” preset point, before returning to the “Alarm Off” preset point.

Note: Depending on the capability of the PTZ camera, up to 256 PTZ preset points (ranging from 1 to 256) and addresses (ranging from 0 to 255) can be programmed.

6.2.3 Setting Momentary and Maintained Modes

This section introduces the momentary and maintained modes.



The screenshot shows a configuration window with two radio buttons at the top: 'Momentary Mode' (unselected) and 'Maintained Mode' (selected). Below these are two rows of settings, each with a checked checkbox and two dropdown menus. The first row is 'Start/Stop Camera Monitoring by I/O' with 'Mod. 1' and 'Pin. 1' selected. The second row is 'Start/Stop IO Monitor by I/O' with 'Mod. 1' and 'Pin. 1' selected.

Figure 6-10

[Momentary Mode] Push button switches that are normally open and stay closed as long as the button is pressed. Momentary switches allow turn-on or turn-off from multiple locations. For example, certain premises have a designated entry/exit door. When the staff enters the entry door, the system starts monitoring. When the staff leaves from the exit door, the system stops monitoring.

[Maintained Mode] Push-on/push off button switches that stay open until thrown, and then stay closed until thrown again. Maintained switches are convenient for only one switch location.

For example, in the business hour when the door is opened, the system stops monitoring; in the non-business hour when the door is closed, the system starts monitoring.

6.2.4 Deactivating Alarm and Alert upon Input Trigger

The option lets you instantly deactivate all the prior alarm and alert settings (Output, Wave Alarm, Send Alerts), when an assigned input module is triggered.

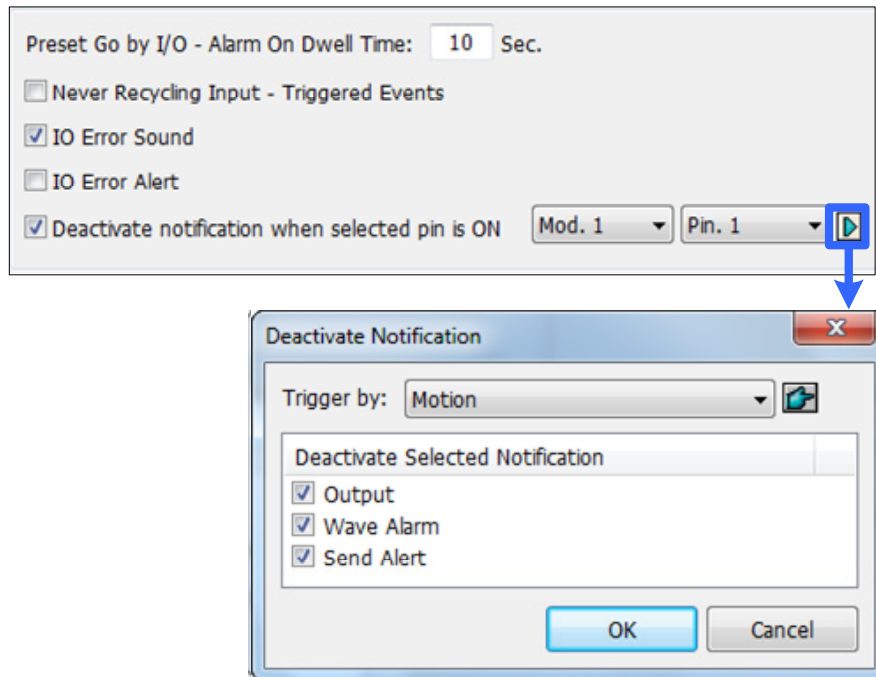


Figure 6-11

[Deactivate notification when selected pin is ON] When an assigned input module is activated, all designated alarms and alerts will be disabled. Assign an installed input module and a pin number for the application.

[Deactivate Notification] Click the **Arrow** button to select the alert to deactivate.

- **Triggered by:** Select an alert condition from the drop-down list for the application. For example, if you choose Motion, all designated alarms and alerts upon motion detection will be deactivated when the assigned input module is activated.
- **Deactivate Selected Notification:** Select the alarms and alerts you want to be deactivated, such as Output, Wave Alarm and/or Send Alert, when the assigned input module is activated.

6.2.5 Other I/O Application Functions

In the I/O Device Application dialog box, you can also set up Input Overlay on live view, alert for I/O errors, and whether to recycle input-triggered events or not. Select an Input number to be set up.

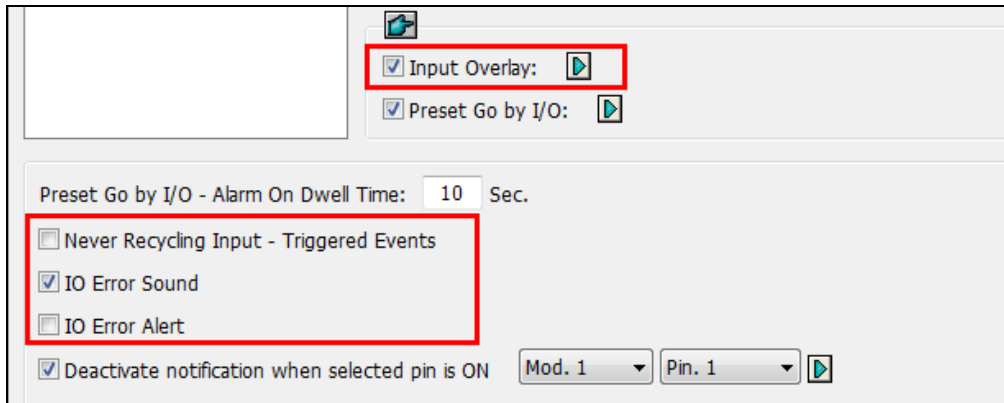




Figure 6-12

[Input Overlay] Select to overlay the name of input device on live video for alert or save it to video files whenever the input is triggered. Click the Arrow button to select the camera to overlay input name. You can click the Finger button to apply the same settings to all inputs.

To overlay the name of triggered input on live video, click **Home** , select **Toolbar**, click **Configure**  and click **Video Process**. In the dialog box that appears, select **Text Overlay** in the Video Analysis drop-down list, select the camera, and click **Setting**. Click **Print on screen (Only for I/O alarm)** or **Print on video file**. You can also select the position of the name stamp on the screen. For details, see *Text Overlay* in Chapter 3




[Never Recycling Input-Triggered Events] When selected, the files recorded upon input trigger won't be recycled by the system when disk space is full.

[IO Error Sound] When enabled, the computer alarm will sound when GV-VMS fails to detect the connected I/O device.

[IO Error Alert] When enabled, an e-mail notification will be sent when GV-VMS fails to detect the connected I/O device. Remember to set up e-mail notifications. See *Email Notification* in Chapter 1.

6.3 I/O Devices in Content List

When an I/O device is added to the system, the I/O device will appear in the Content List.

1. To display the Content List, click **Home** , select **Toolbar** , and click **Content List** .
2. Click **I/O Device** to see the I/O devices added to GV-VMS.

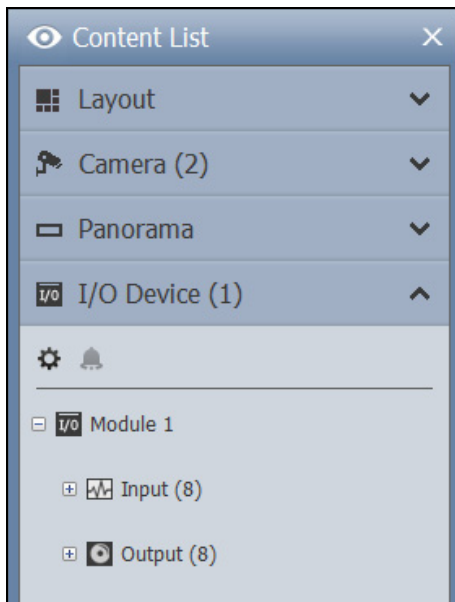


Figure 6-13

When an input or output is triggered, its icon will light up in the I/O Device list.

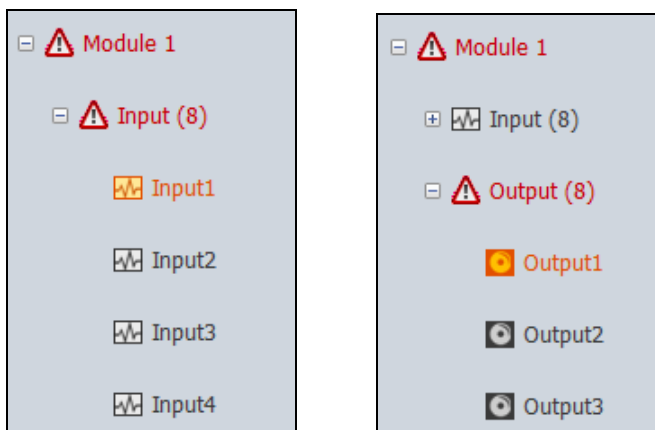







Figure 6-14

3. You can force the output device to be triggered by clicking its icon . Another way to trigger an output is to select an output and click the **Force Output** button .
4. To manually turn off a triggered output, right-click the triggered output in the list and click **Reset**.

6.4 Visual Automation

The Visual Automation helps you automate any electronic device by triggering the connected output. On the camera view, draw the visual automation region where the electronic device is located in the camera view. You can then intuitively click on the image of the electronic device, a light for example, to change its current state, e.g. turning the light on.

1. On the main screen, click **Home** , select **Toolbar** , click **Configure** , click **Accessories** (if available), click **I/O Device** (if available) and select **Visual Automation Setting**. This dialog box appears.

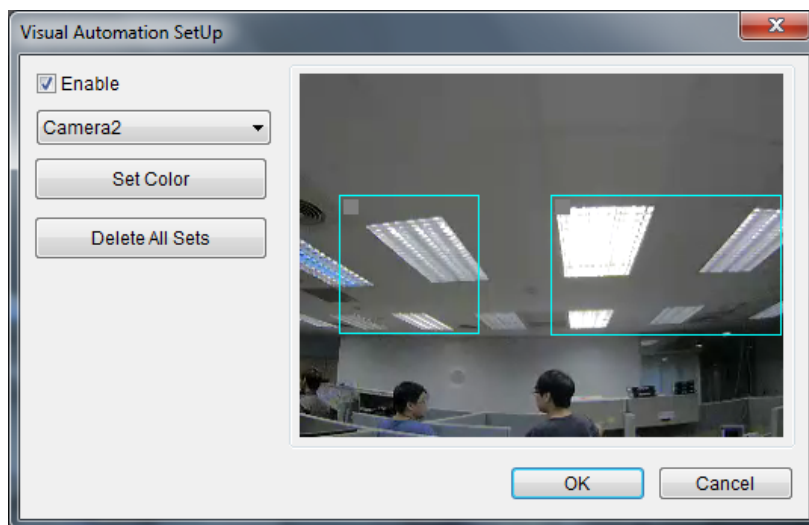


Figure 6-15

Note: The **Accessories** option only appears when GV-KeyBoard or GV-Joystick has been set up on the GV-VMS. The **I/O Device** option only appears after at least one I/O device has been added.

2. Select a camera from the drop-down list, and check **Enable**.
3. Drag the region on the camera view. This dialog box appears.

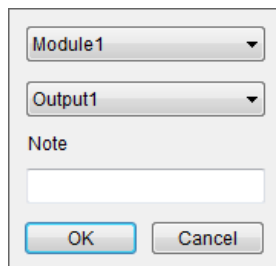



Figure 6-16

4. Select the connected module and output device. You can type a **Note** to help you identify the device. Click **OK**.
5. To change the frame color of the set region, click the **Set Color** button.
6. To test the output trigger, click the region on the camera view drawn in step 3.

To use Visual Automation, on the main screen, move the cursor to the camera view with Visual Automation, click **Tools**  and select **I/O Automation**.

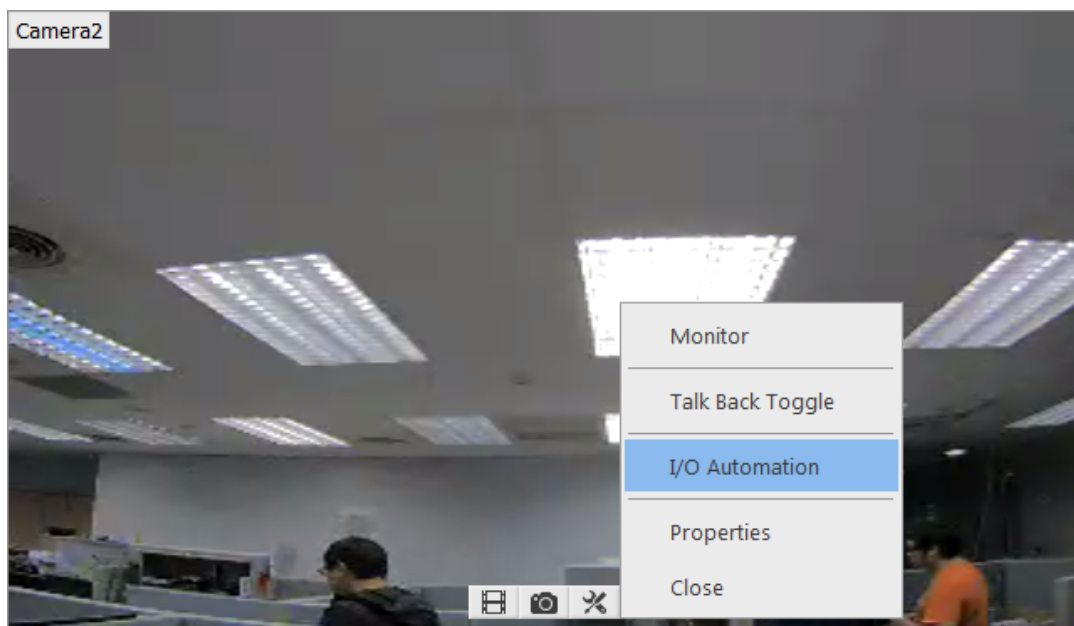


Figure 6-17

Next, click the regions you set to trigger the connected output device. You can right-click the camera view and select **Show all** to see all Visual Automation regions if needed.

Chapter 7

Remote Viewing.....236

| | |
|--|------------|
| 7.1 Remote Viewing Using a Web Browser..... | 237 |
| 7.2 WebCam Server Settings | 240 |
| 7.2.1 General Settings | 240 |
| 7.2.2 Server Settings | 241 |
| 7.2.3 Video Settings..... | 242 |
| 7.2.4 Audio Settings..... | 243 |
| 7.2.5 JPG Settings | 244 |
| 7.2.5 JPG Settings | 244 |
| 7.2.6 UPnP Settings | 245 |
| 7.2.7 Network Port Information | 246 |
| 7.3 Single View Viewer | 247 |
| 7.3.1 Adjusting Video Quality and Recording Videos | 249 |
| 7.3.2 Control Panel..... | 250 |
| 7.3.3 Configuring Single View Viewer Options..... | 251 |
| 7.3.4 PTZ Control Panel..... | 256 |
| 7.3.8 Visual PTZ Control | 257 |
| 7.3.5 I/O Control | 258 |
| 7.3.6 Visual Automation | 259 |
| 7.3.7 Picture-in-Picture View..... | 260 |
| 7.3.8 Picture-and-Picture View | 261 |
| 7.4 2-Window Viewer..... | 262 |
| 7.5 Multi-Window Viewer | 263 |
| 7.6 JPEG Image Viewer..... | 264 |
| 7.7 Playing Back Events..... | 265 |
| 7.7.1 Event List Query..... | 265 |
| 7.7.2 Remote Playback | 267 |
| 7.8 Remote ViewLog | 268 |
| 7.9 Download Center | 269 |
| 7.10 Mobile Phone Applications | 270 |
| 7.10.1 Activating Mobile Functions on GV-VMS..... | 270 |
| 7.10.2 Installing GV-Eye | 271 |
| 7.10.3 Connecting to GV-VMS | 272 |

| | | |
|-------------|--|------------|
| 7.11 | Web Browsers on Smartphones | 274 |
|-------------|--|------------|

Remote Viewing

With Microsoft Internet Explorer, you can remotely view live video, download and play back video files, manage systems within the security network, control PTZ camera and I/O devices through the WebCam server.

The remote computer used to access live video must meet the following minimum requirements:

| | | |
|--------------|--|--|
| OS | 32-bit | Windows XP / Vista / 7 / 8 / 8.1, Windows Server 2008 |
| | 64-bit | Windows 7 / 8 / 8.1, Windows Server 2008 / 2012 |
| CPU | | Pentium 4, 2.0 GHz |
| Memory | Windows XP | 2 x 512 MB Dual Channels |
| | Windows Vista / 7 / 8 / 8.1 / Server 2008 / 2012 | 2 x 1 GB Dual Channels |
| Hard Disk | | 80 GB |
| Graphic Card | | AGP or PCI-Express, 800 x 600 (1280 x 1024 recommended), 32-bit color AGP or PCI-Express, 1024 x 768, 32-bit color (for Multi View Viewer only) |
| Network | | TCP/IP |
| Web Browser | | IE 7.0 or later |
| DirectX | | 9.0c |

With non-IE browsers, the below browsers are supported for remotely viewing live view, playing back videos and listing the event query only:




| | |
|-----------------|---------------------------|
| Google Chrome | V38.0.2125.111 or earlier |
| Mozilla Firefox | V30.0 or earlier |
| Apple Safari | V5.1.7 or earlier |

7.1 Remote Viewing Using a Web Browser

The GV-VMS has a built-in a WebCam server that allows you to remotely view and manage the camera images from the GV-VMS using Internet Explorer, Google Chrome, Apple Safari, or Mozilla Firefox.

Note:

1. For Internet connection, the GV-VMS must have an IP address or domain name from ISP. If the IP address is dynamic, you may use the DDNS service to direct changing IP addresses to the GV-VMS. For the service, see *Dynamic DNS* in Chapter 9.
 2. Make sure the remote PC is going to access the GV-VMS meets the minimum system requirements mentioned above.
 3. If a router or firewall is installed with the GV-VMS server, ensure the following communication ports required by WebCam Server are open: Command Port (4550), Data Port (5550), Audio Port (6550) and HTTP Port (80).
-

1. To enable the WebCam Server on GV-VMS, click **Home** , click **Toolbar** , click **Network**  and click **WebCam Server**. The Server Setup dialog box appears. You can click **OK** to close the dialog box for now and modify the default configurations later.
2. On any remote computer, open a Web browser and type the IP address or domain name of the GV-VMS. This dialog box appears.

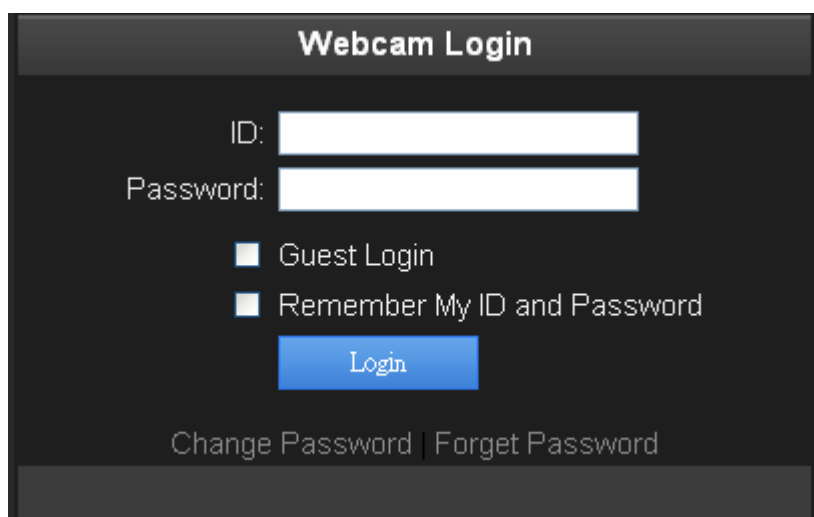


Figure 7-1

Note: If the default HTTP port 80 has been changed, type a colon and the port number after the IP address, for example, **Http://192.168.3.199:81/**.

3. Type a user ID and a password created on the GV-VMS.
4. Click **Login**. When logging in for the first time, click the bar at the top of the browser and install Add-on and ActiveX components. After connection is established, this Single View page appears.

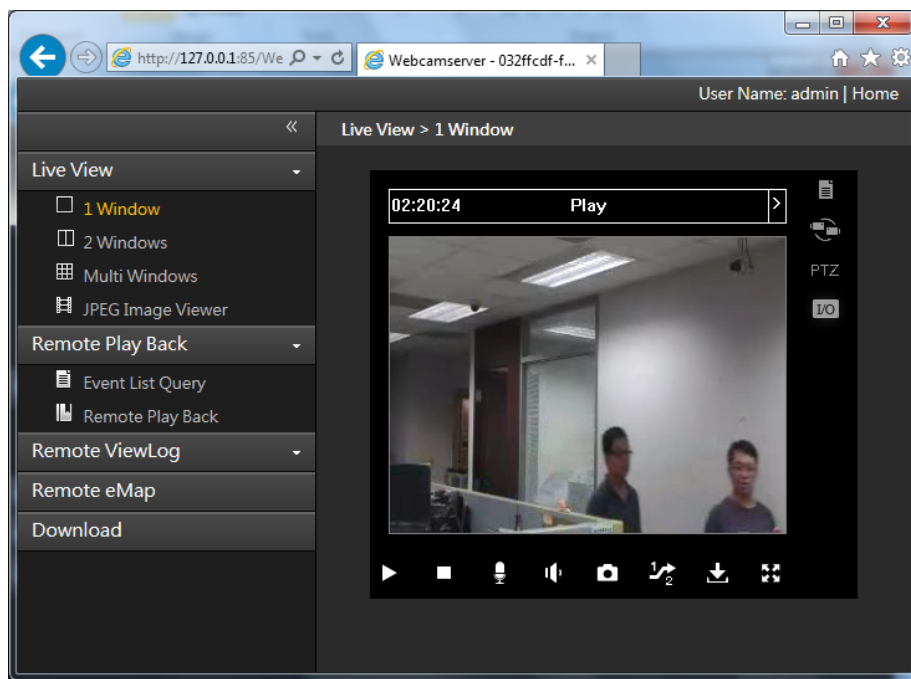


Figure 7-2 Live View on IE Browser

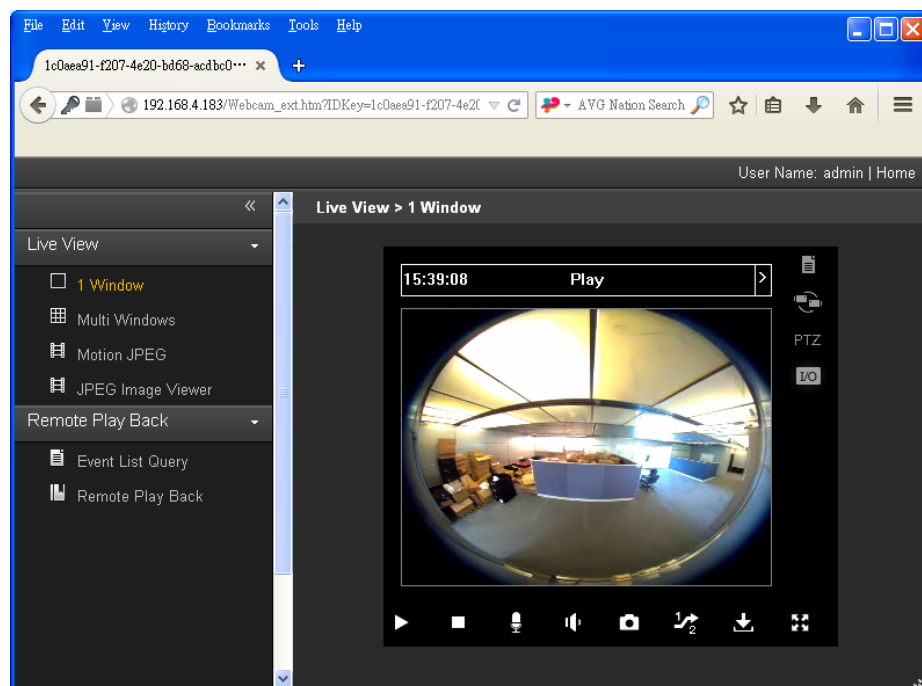


Figure 7-3 Live View on Non-IE Browser

The following WebCam server features will be introduced later in this chapter:




IE Browser's WebCam Server Features

| Name | Description |
|------------------|---|
| Live View | Accesses different types of live view viewers. See <i>Single View Viewer</i> , <i>2-Window Viewer</i> , <i>Multi-Window Viewer</i> , and <i>JPEG Image Viewer</i> later in this chapter. |
| Remote Play Back | Accesses remote playback options. See <i>Event List Query</i> later in this chapter. |
| Remote ViewLog | Accesses the Remote ViewLog. See <i>Remote ViewLog</i> later in this chapter. |
| Remote E-Map | Accesses E-Maps remotely set up at the GV-VMS. See <i>E-Map Application</i> in Chapter 8. |
| Download | Accesses the Download Center. This function offers optional viewing programs to be downloaded to the local PC. See <i>Download Center</i> later in this chapter. |

Non-IE Browsers' WebCam Server Features

| Name | Description |
|------------------|---|
| Live View | Accesses different types of live view viewers. See <i>Single View Viewer</i> , <i>Multi-Window Viewer</i> , and <i>JPEG Image Viewer</i> later in this chapter. |
| Remote Play Back | Accesses remote playback options. See <i>Event List Query</i> and <i>Remote Playback</i> later in this chapter. |

7.2 WebCam Server Settings

To enable and configure GV-VMS's built-in web sever, click **Home** , click **Toolbar** , click **Network**  and click **WebCam Server**. The Server Setup dialog box that appears contains these tabs: (1) General, (2) Server, (3) Video, (4) Audio, (5) JPG, (6) Mobile.

7.2.1 General Settings

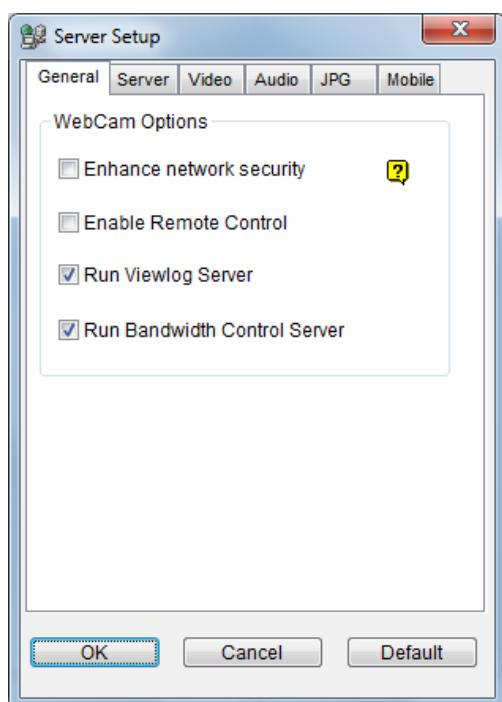


Figure 7-4

[WebCam Options]

- **Enhance network security:** When this option is enabled, it is required to complete a word verification step every time when you log on to the WebCam server.
- **Enable Remote Control:** Select this option to remotely configure the I/O devices through the WebCam server.
- **Run Viewlog Server:** Select to remotely play back video files through the WebCam server.
- **Run Bandwidth Control Server:** Select this option to enable the **Bandwidth Control Server**. For details, see *Bandwidth Control Application* in Chapter 9.

Note: When **Enhance network security** is enabled, JPEG/Mobile applications will be disabled.

7.2.2 Server Settings

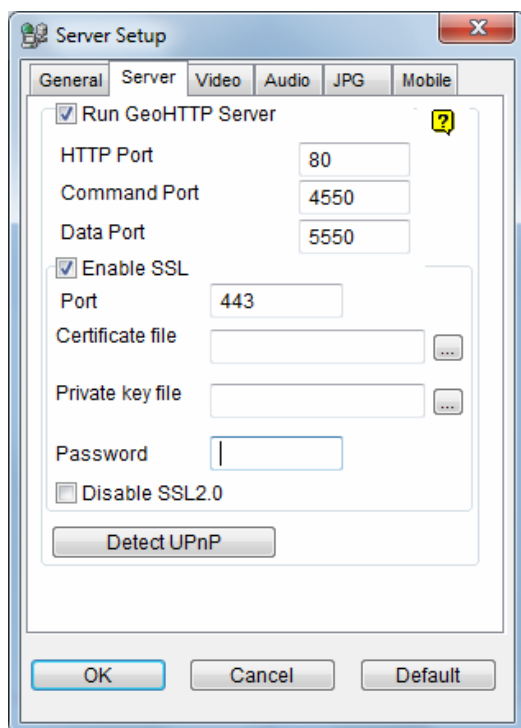


Figure 7-5

[Run GeoHTTP Server] Enable GeoVision HTTP server or use your own HTTP server. Command Port is the port used to access WebCam, and Data Port is the port used to transfer data over Internet.

[Enable SSL] Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of Internet connection. To use your own generated Certificate and Private Key or ones verified by SSL authority, click the [...] buttons and select the files stored at your computer. Note that the system will enable both SSL 2.0 and SSL 3.0 as its default; to disable SSL 2.0 protocol when using SSL 3.0, select **Disable SSL2.0**.

[Detect UPnP] For details, see *UPnP Settings* later in this chapter.

Note: If you want to enable SSL 3.0 on a computer running Windows Vista, it is required to upgrade your system to Service Pack 1 or Service Pack 2.

7.2.3 Video Settings



Figure 7-6

- **Max. Channel(s):** Specify the number of channels allowed to access the WebCam server, with the upper limit of 200 channels.
- **Max Image size:** Select a maximum resolution allowed for remote access. The default resolution on the WebCam is **Normal** (320 x 240). The other options are **Middle** (640 x 480 (De-interlace), 704 x 480 (De-interlace)), **Large** (640 x 480 or 704 x 480) and the **Actual Size** of that IP camera.
- **Allowed PTZ camera:** Allows you to control selected PTZ cameras at a remote computer. Click the button and select the desired PTZ cameras to allow for remote access.

Note: To specify the time length allowed for a guest user to access the WebCam server, click the account ID at the top of the main page, click **Password Setup**, and select **Local Account Edit**. In the WebCam tab, select the **Limit Connection Time** option and specify the time length. The time range is between 10 and 3600 seconds.

7.2.4 Audio Settings

Connecting Audio Devices

Through the WebCam server, you can access live audio at a remote site and talk to the server site.

This feature is useful when the remote site requires speaking to the personnel at the server site in case of emergency. Before using this feature, make sure all the necessary hardware are in place:

1. To record audio, make sure the connected IP camera has built-in audio function or an external microphone connected.
2. Make sure your sound card is already inside the computer. Connect a multimedia speaker to the audio output of your computer's sound card. This is for receiving audio from the remote site.
3. Connect a desktop microphone to the input of the audio extension card (or cable line). This is for sending audio to the remote site.

Audio Setup

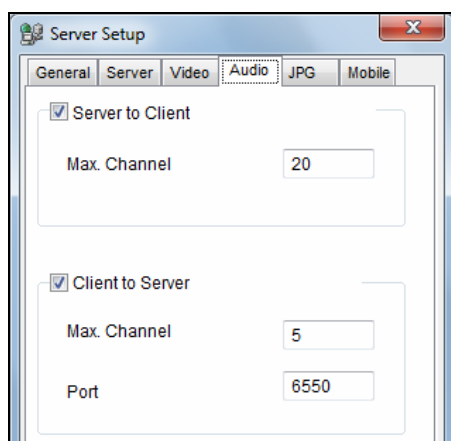


Figure 7-7

[Server to Client] Allows a remote computer to access live audio from the GV-VMS server.

- **Max. Channel(s):** Enter the maximum number of channels allowed to access live audio, with the upper limit of 40 channels.

[Client to Server] Allows a remote computer to speak to the GV-VMS server.

- **Max. Channel(s):** Enter the maximum number of channels allowed to speak to the server site, with the upper limit of 20 channels.
- **Port:** The default audio port is 6550.

7.2.5 JPG Settings

These settings allow you to send JPEG or GIF files over Internet.

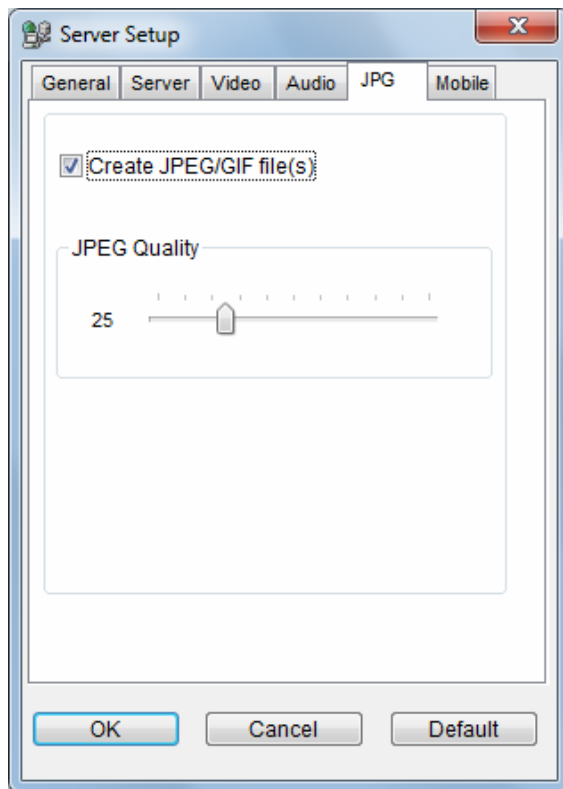





Figure 7-8

- **Create JPEG/GIF file(s):** Allows you to view the JPEG/GIF images remotely. You can use the JPEG Image Viewer feature of the WebCam server to access the JPEG images over Internet. After the feature is enabled, use the slider to adjust JPEG image quality. Bigger number results in better image quality and bigger image file size.

7.2.6 UPnP Settings

WebCam Server supports UPnP technology (Universal Plug and Play) to allow automatic port configuration to your router. UPnP must be enabled both on your operating system and your router.

Enabling UPnP on the WebCam Server:

1. On the main screen, click **Home** , click **Toolbar** , click **Network**  and click **WebCam Server**. The Server Setup dialog box appears.
2. Click the **Server** tab and click **Detect UPnP**. This dialog box appears.

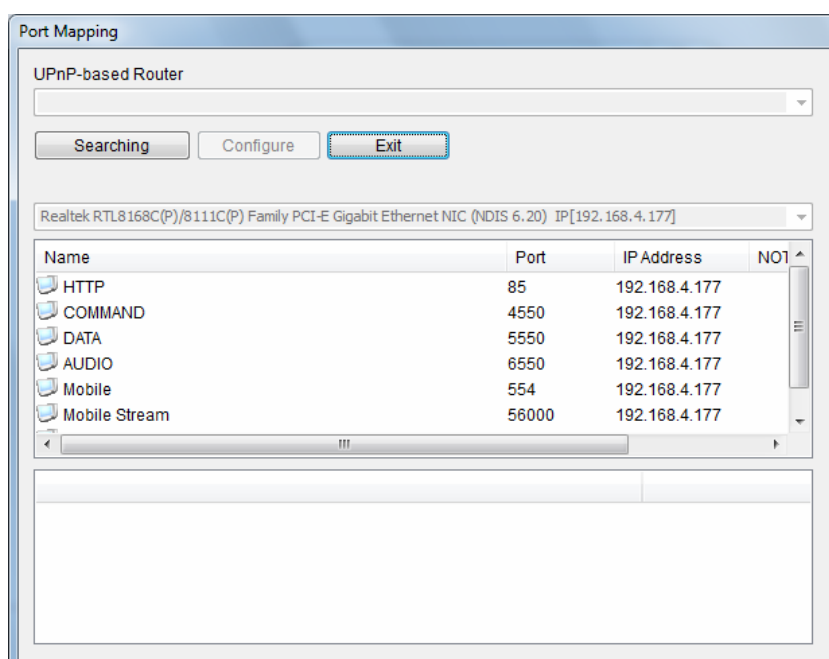


Figure 7-9

3. Click **Searching** to search the UPnP-enabled routers.
4. If your server is installed with multiple routers, select one from the UPnP Router drop-down list.
5. If you server is installed with multiple network adapters, select one from the drop-down list under the Searching button.
6. Click **Configure** to automatically configure the communication ports on the router.

Note:

1. If you don't use the default ports, modify the related ports in the Server Setup dialog box (Figure 7-5) and then click **OK**. Re-open the dialog box and follow above steps to configure your router.
 2. UPnP technology is also available in other remote applications: Control Center, Center V2, Remote Playback, Authentication Server, Vital Sign Monitor and TwinDVR.
-

7.2.7 Network Port Information

The Network Port Information is designed for users to view and manage all network ports of remote applications.

On the main screen, click **Home** , click **Toolbar** , click **Network**  and select **Network Port Information**. This dialog box appears.

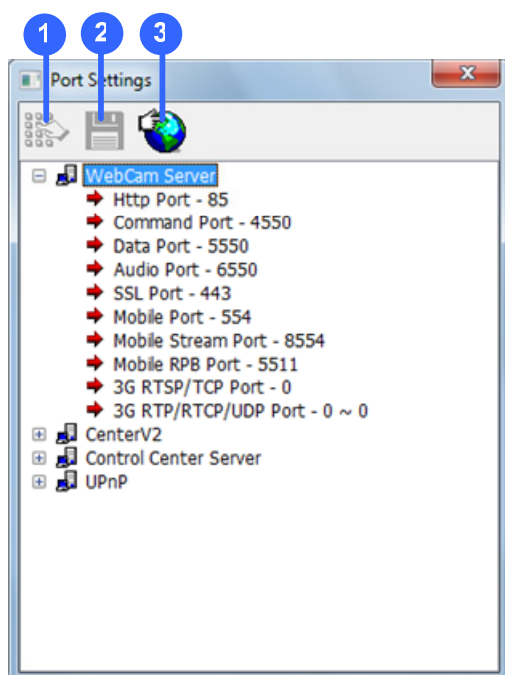


Figure 7-10

The controls on the Port Settings:

| No. | Name | Description |
|-----|--------------|--|
| 1 | Modify | Changes the port settings. |
| 2 | Save | Saves the port settings. |
| 3 | Port Mapping | Employs UPnP technology (Universal Plug and Play) to allow automatic port configuration to the router. |

7.3 Single View Viewer

After you log into the WebCam server successfully, you can see the single live view from the GV-VMS.

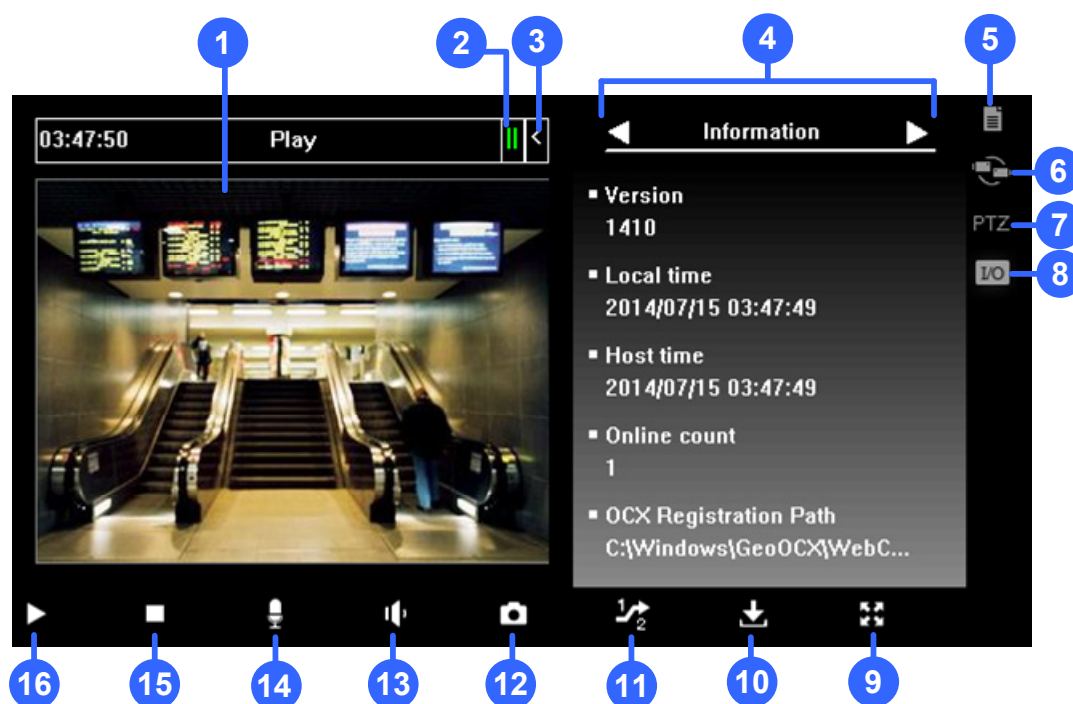


Figure 7-11 Single View MPEG4 Encoder Viewer

The controls in the Single View Viewer:

| No. | Name | Description |
|-----|----------------|--|
| 1 | Live Video | Right-clicking on live video allows you to instantly access some useful functions. The Resolution option can display a resolution indicator at the bottom right corner of the video. |
| 2 | Menu | Opens the menu of Control Panel. See <i>Control Panel</i> later in this chapter. |
| 3 | Expand / Close | Expands or closes the Control Panel. |
| 4 | Control Panel | See <i>Control Panel</i> later in this chapter. |
| 5 | Options | Brings up these options: Alarm Notify, Video and Audio Configuration, Change Server, Show Camera Name and Image Enhance. See <i>Alarm Notification</i> , <i>Video and Audio Configuration</i> , <i>Server List</i> , and <i>Image Enhancement</i> later in this chapter. |
| 6 | Change Camera | Selects the desired camera for display. |

| | | |
|----|----------------|--|
| 7 | PTZ Control | Displays the PTZ control panel. See <i>PTZ Control</i> and <i>Visual PTZ Control Panel</i> later in this chapter. |
| 8 | I/O Control | Displays the I/O control panel. See <i>I/O Control</i> later in this chapter. |
| 9 | Full Screen | Switches to full screen view. The maximum video resolution configured on the GV-VMS will be applied. See <i>Video Settings</i> in <i>WebCam Server Settings</i> earlier in this chapter. |
| 10 | File Save | Saves live video in the local computer. See <i>Video Recording</i> later in this chapter. |
| 11 | Change Quality | Adjusts video quality with two options: Geo H264 and Geo MPEG4 . |
| 12 | Snapshot | Takes a snapshot of the displayed live video. |
| 13 | Speaker | Enables live audio from the remote GV-VMS. See <i>Video and Audio Configuration</i> later in this chapter. |
| 14 | Microphone | Enables speaking to the remote GV-VMS. See <i>Video and Audio Configuration</i> later in this chapter. |
| 15 | Stop | Terminates the connection to the remote GV-VMS. |
| 16 | Play | Connects to the remote GV-VMS. |

Displaying Full Screen Live View on Another Monitors

Using the IE browser, you can display up to 10 full-screen channels with multiple monitors installed. Right-click the live view and select a designated monitor to bring full screen live view. The full screen live view appears on the designated monitor immediately.




Note: The full-screen display closes at the designated monitor if its Web interface window is minimized.

7.3.1 Adjusting Video Quality and Recording Videos

Video Quality

To adjust the live view quality in the Single View Viewer:

1. Select **Actual Size** on the GV-VMS.

Click **Home** , click **Toolbar** , click **Network** , click **WebCam Server**, click the **Video** tab and select **Actual Size** in the Max Image Size option. Refer to *Video Settings* in *WebCam Server Settings* earlier in this chapter.

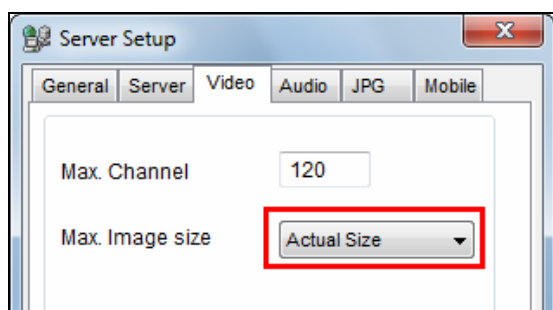


Figure 7-12

2. On the Single View, click the **Change Quality** button (No. 11, Figure 7-20). You will have the option of megapixel resolution now.

Note:

1. Streaming live view in Actual Size requires a lot of bandwidth. It is highly recommended to enable this function in a LAN environment.
 2. To have fisheye dewarping view, you must first follow the steps above to set fisheye camera to megapixel resolution. Next, right-click the camera view and select **Geo Fisheye** to see the fisheye settings. For more details on the fisheye settings, see *Fisheye View* in chapter 3.
-

Video Recording

Click the **File Save** button (No. 10, Figure 7-20) to save video in a local computer. Files saved in AVI format are playable at third-party viewers. Use the slider to adjust the time length of each saved clip.

7.3.2 Control Panel

A control panel can be opened next to the live view by clicking the **Expand / Close** button on top of the Single View viewer. To change the pages of the control panel, click the **Menu** button. You can also use the right and left arrow buttons on the panel to change the pages.

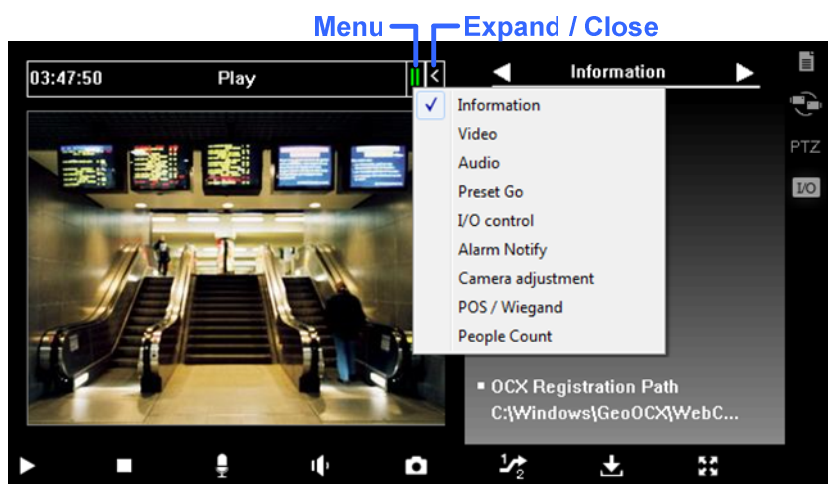


Figure 7-13

| Name | Description |
|-------------------|---|
| Information | Displays the current version, local time, host time and number of channels currently accessing WebCam. |
| Video | Displays the current video codec, resolution and data rate. |
| Audio | Displays audio data rates when the microphone and speaker devices are enabled. |
| Preset Go | Allows you to remotely move the PTZ to the preset points. |
| I/O Control | Provides a graphic display of the input and output devices from the GV-VMS. |
| Alarm Notify | Displays the captured images by sensor triggers and/or motion detection. <i>See Alarm Notification later.</i> |
| Camera Adjustment | Allows you to remotely adjust image quality by moving the slider to the desired values. |
| POS/Wiegand | Not functional. |
| People Count | Allows you to view the counts of Object Counting along with live view. Once the counts are logged into the GV-VMS, In and Out counts will become zero and the system will start counting those numbers again. |

7.3.3 Configuring Single View Viewer Options

To access the Single View Viewer options, click the **Options** button located on the right of the live view.

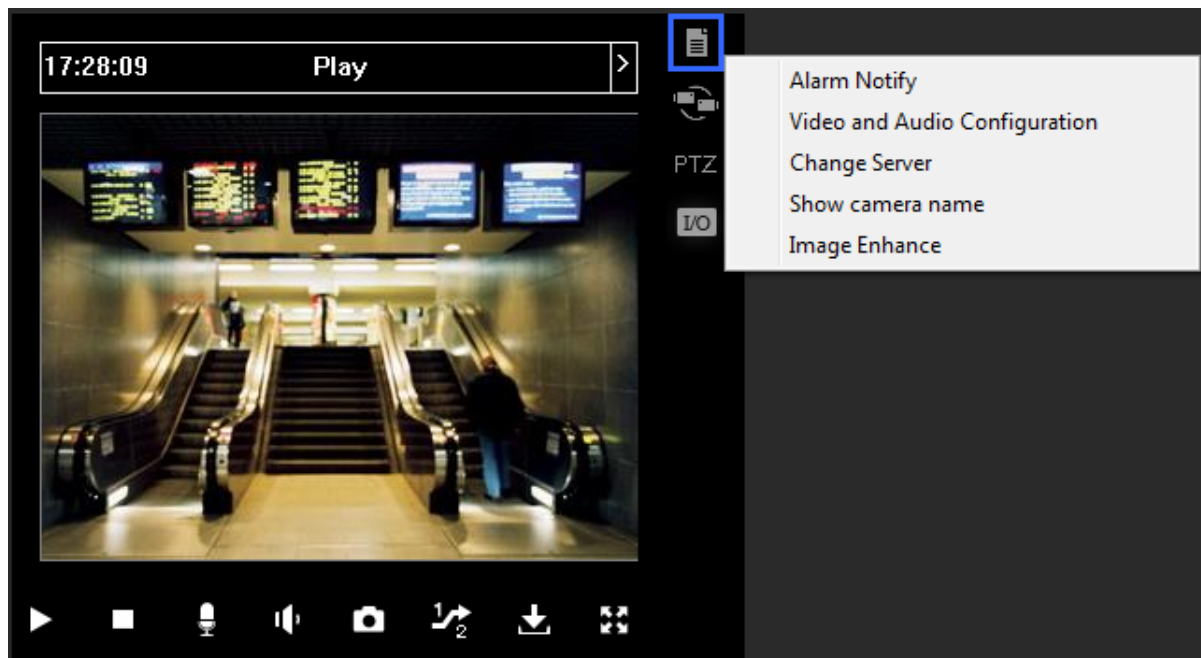


Figure 7-14

Alarm Notification

Up to four captured images can be shown in the control panel upon motion detection or input trigger.

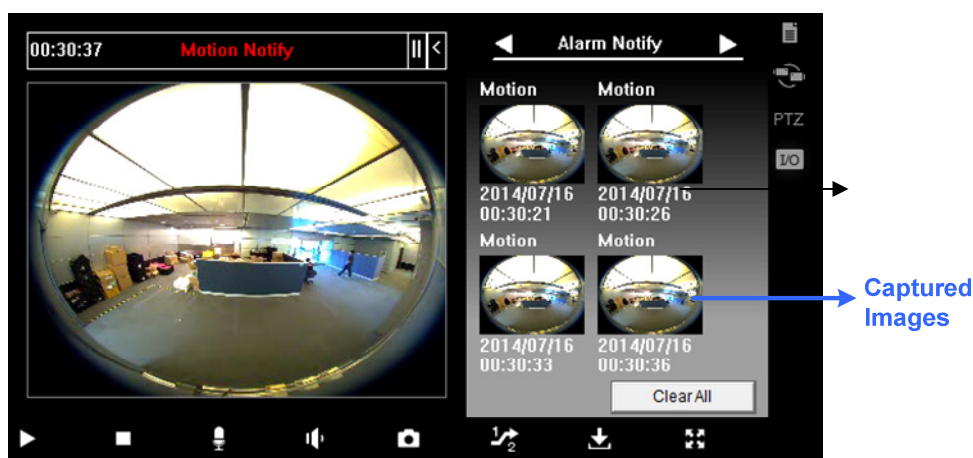


Figure 7-15

1. Click the **Option** button, and select **Alarm Notify**. This dialog box appears.

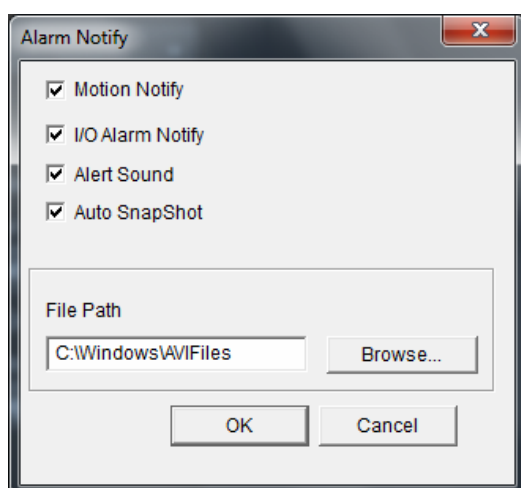


Figure 7-16 Alarm Notification

- **Motion Notify:** Once motion is detected, the captured images are displayed in the control panel of the Single View.
 - **I/O Alarm Notify:** Once the input device is triggered, the captured images are displayed in the control panel of the Single View.
 - **Alert Sound:** Activates the computer noise alarm on motion and input-triggered detection.
 - **Auto Snapshot:** The program will take a snapshot every 5 seconds on motion and input-triggered detection.
 - **File Path:** Assigns a path to save the snapshots.
2. Click **OK** to apply the above settings.

Video and Audio Configuration

To change the video and audio configurations of the connected camera, click the **Option** button, and select **Video and Audio Configuration**.

[Camera] In this tab, you can change the video codec, quality and frame rate. The resolution options depend on the maximum image size set on the connected GV-VMS. For details, see *Video Settings* in *WebCam Server Settings* earlier in this chapter.

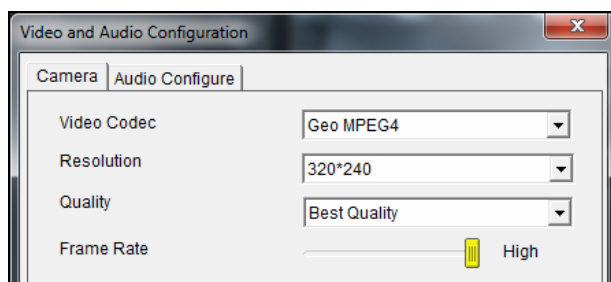


Figure 7-17

[Audio Configure] In this tab, you can enable the microphone and speaker for two-way audio communication. Select **Speaker** to access live audio from the server site, and select **Microphone** to speak to the server site. Ensure the speaker and microphone are properly installed in the local computer, and the audio settings (Figure 7-8) are activated on the WebCam server too. There are three options for audio quality:

- **Real Time:** Transmits simultaneously audio and video but may create sound interruption depending on your network condition.
- **Smooth:** Has a smooth sound quality but without audio and video synchronization.
- **Normal:** The default value which has the audio and video effects between Real-Time and Smooth.

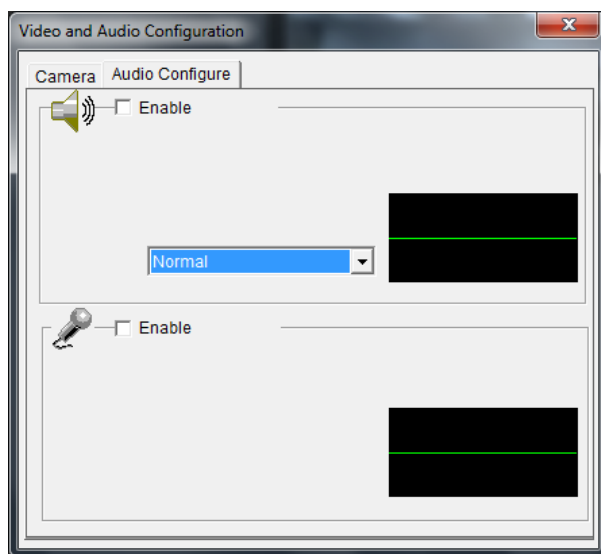
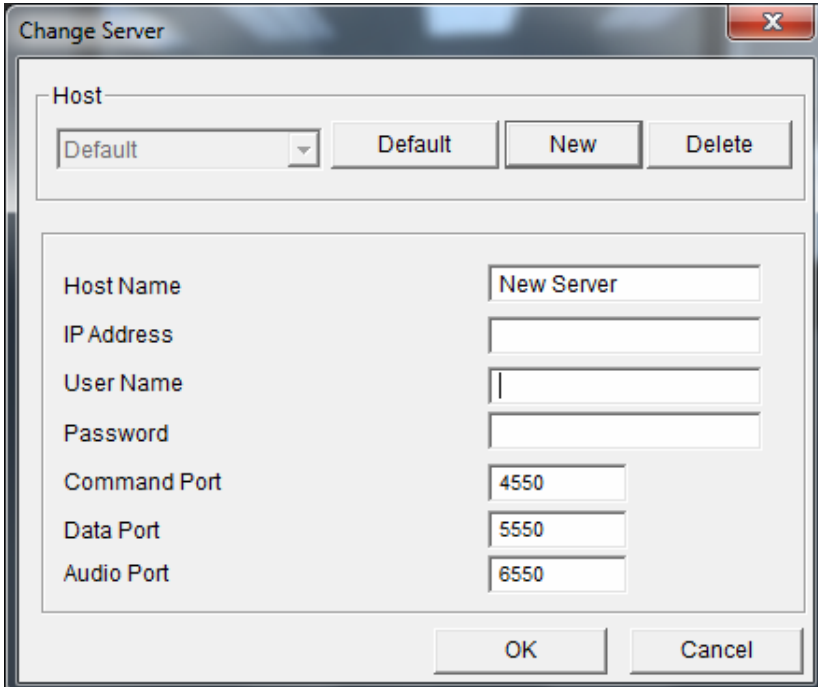


Figure 7-18

Server List

You can add the connection information of multiple GV-VMS to the WebCam server for quick access later. Click the **Option** button, and select **Change Server** to display the following dialog box.



The 'Change Server' dialog box contains the following fields and buttons:

- Host:** A drop-down menu currently showing 'Default', with 'Default', 'New', and 'Delete' buttons next to it.
- Host Name:** A text field containing 'New Server'.
- IP Address:** An empty text field.
- User Name:** An empty text field.
- Password:** An empty text field.
- Command Port:** A text field containing '4550'.
- Data Port:** A text field containing '5550'.
- Audio Port:** A text field containing '6550'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Figure 7-19 Change Server

To add a server to the drop-down list, click the **New** button. In Host Name field, type a name to identify the GV-VMS. Type the IP address or domain name of the GV-VMS. Type a valid username and password to log in to the GV-VMS. Leave all port settings as defaults at **4550**, **5550**, and **6550** respectively unless otherwise necessary. Click the **OK** button. Then the created GV-VMS will appear in the Host drop-down list.

Show Camera Name

To show camera name on the live view, click the **Option** button and select **Show Camera Name**. The camera name appears in the top-left corner.



Figure 7-20

Image Enhancement

To enhance the image quality of live video, click the **Option** button and select **Image Enhance**. This dialog box appears.

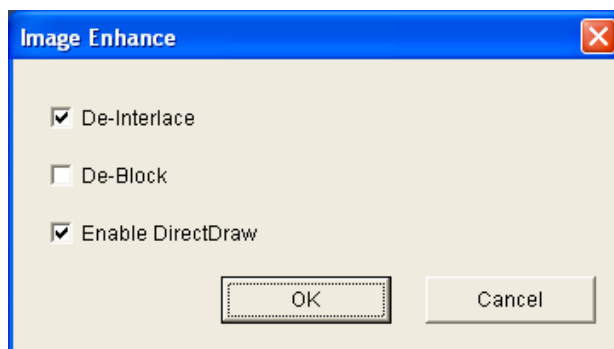


Figure 7-21

- **De-Interlace:** Converts the interlaced video into non-interlaced video.
- **De-Block:** Removes the block-like artifacts from low-quality and highly compressed video.
- **Enable DirectDraw:** The DirectDraw setting is enabled by default. Some VGA cards might not support DirectDraw and can produce distorted frames. Uncheck this option to disable the DirectDraw function.

7.3.4 PTZ Control Panel

Click the **Camera Select** button to select one PTZ camera, and click the **PTZ Control** button (No. 7, Figure 7-20) to bring up the PTZ control panel.

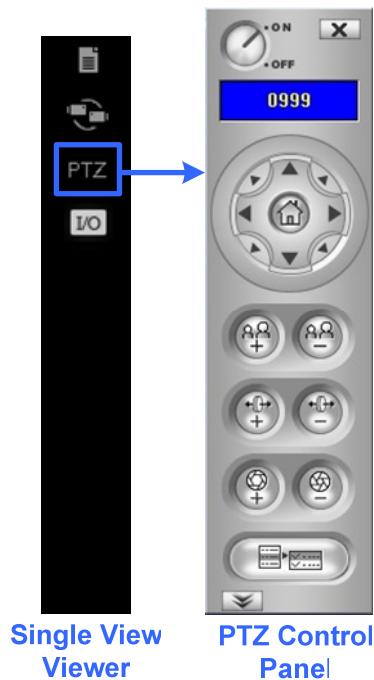



Figure 7-22 PTZ control panel

One PTZ camera can only be controlled by one user at a time. If several users are trying to control the same PTZ camera at the same time, the Single View viewer will give the priority to the first login user and then to the next user in queue.

Each user will be given 60 seconds to control the PTZ camera. The Timer at the upper right corner informs the user of the remaining time of control or the total waiting time. The supervisor is given the highest priority to control the PTZ camera and won't be restrained by 60-second time limit. When the supervisor logs on the WebCam server, the Timer shows 999.

Click the  button to access additional PTZ functions such as changing PTZ speed, starting Auto Scan and setting preset points. The functions available vary depending on the PTZ models.

7.3.8 Visual PTZ Control

Other than the PTZ control panel, you can enable the Visual PTZ Control functions. Right-click the live view and select **Visual PTZ**. Next, click the green **PTZ** button on the top left corner of the PTZ control window to have these options:

[PTZ Control Type]

- **Random Move:** In this mode, you can move the camera view to any direction by clicking on a desired direction. When you place the mouse cursor on the live view, a circular PTZ control panel appears. Refer to *PTZ Control Panel and Auto Functions* in Chapter 1 for details on the circular PTZ control panel.



Figure 7-23 PTZ control panel

- **Center Move:** In this mode, you can zoom in and out using the mouse scroll or by drawing a block directly on the live view.

Note: The **Center Move** mode is only for GV-SD220.

7.3.5 I/O Control

The I/O control panel shows the I/O status and alarm event. Additionally, you can force output, as well as enable and disable I/O devices to the remote GV-VMS. Click the **I/O Control** button at the right of the live view to bring out the I/O control panel.

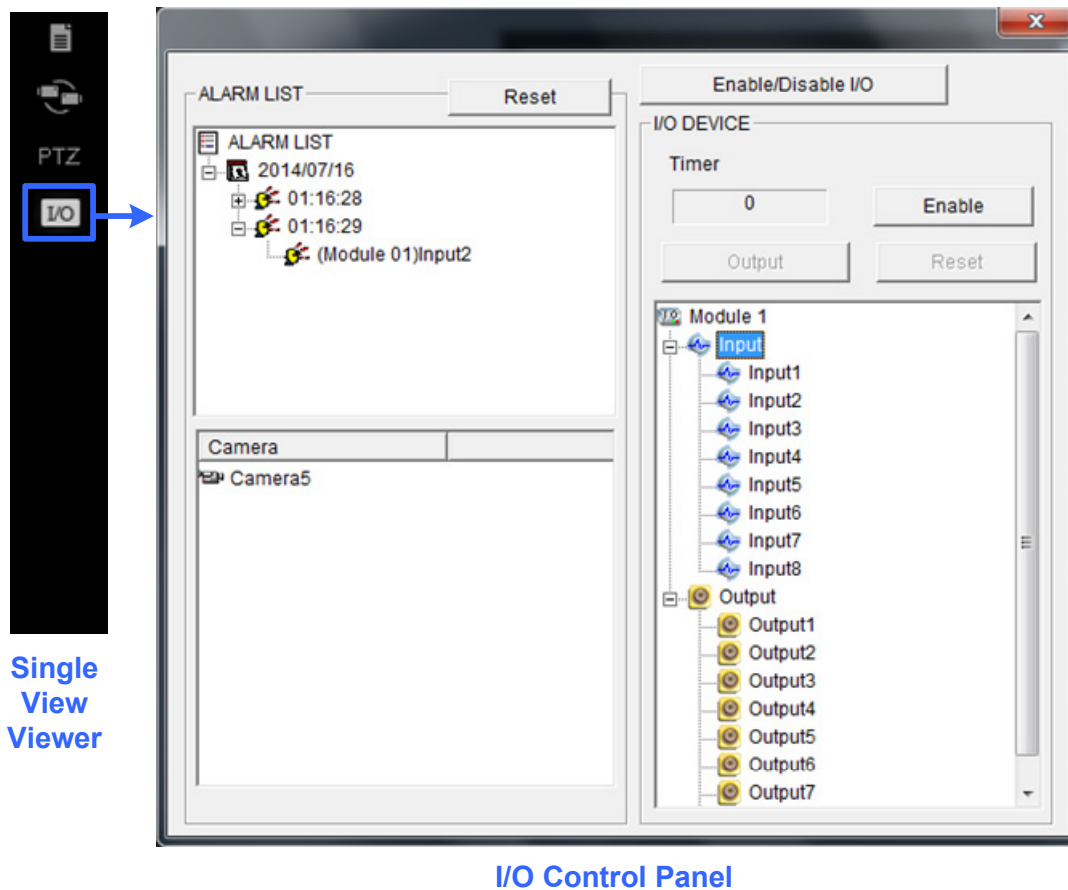


Figure 7-24 I/O Control

The alarm status is shows the triggered inputs. Clicking the **Reset** button will clear the alarm list.

To force trigger an output device, click the **Enable** button, highlight an output and then click the **Output** button. The Timer functions the same as in the PTZ control panel. Each user will be given 60 seconds of control time while the supervisor has 999 seconds. Clicking the **Stop** button will stop the operation and turn over the control privilege to the next user waiting online.

If you want to enable or disable I/O devices to the remote GV-VMS, click the **Enable/Disable I/O** button. Note that the **Enable Remote Control** option must be enabled in the WebCam Server Setup dialog box (Figure 7-4)

7.3.6 Visual Automation

If you have enabled the Visual Automation function on GV-VMS, you can remotely trigger the connected output by simply clicking on a designated spot on the live view. For details on setting up Visual Automation, see *Visual Automation* in Chapter 6.

1. To access this feature, right-click the live view and select **Visual Automation**. A green I/O icon appears in the corner.
2. To see where the designated visual automation spots are located, right-click the live view again, select **Visual Automation** and select **Show All**.
3. Click the alert areas on the image to force the outputs to be triggered remotely.

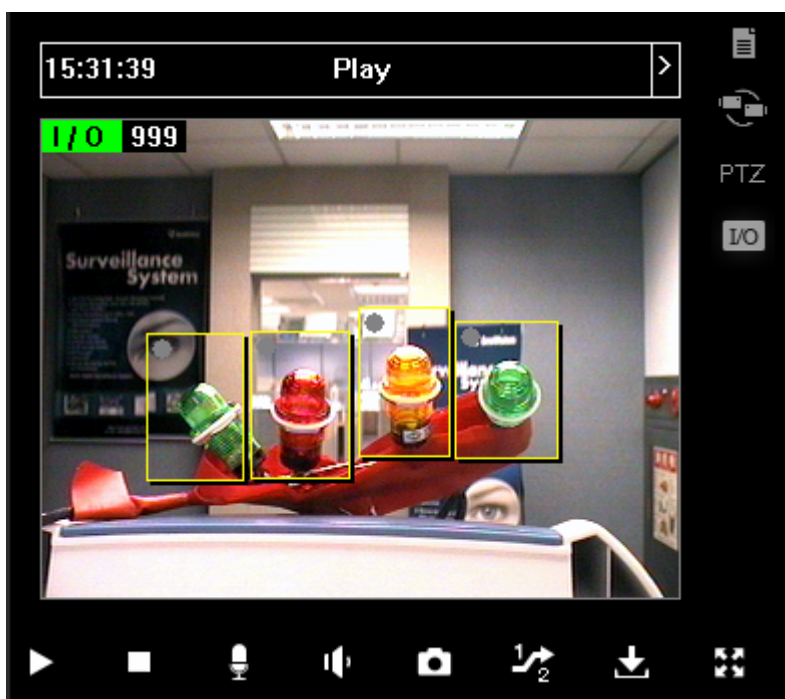


Figure 7-25

7.3.7 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. This function is useful in providing clear and detailed images of the surveillance area.

1. Right-click on the screen and then select **PIP**. An inset window of the camera view appears in the live view.



Figure 7-26

2. Move the navigation box around in the inset window to have a close-up view of the selected area. You can adjust the size of the navigation box if needed.
3. Drag the inset window to adjust its location on the live view if needed.
4. To exit the PIP view, click the camera name and click **PIP View** again.

7.3.8 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. This function is useful for megapixel resolution that provides clear and detailed images of the surveillance area.

1. Right-click on the live view and then select **PAP**. A row of three inset windows appears on the bottom of the screen.
2. Draw a navigation box on the image, and this selected area is displayed in one inset window. Up to seven navigation boxes can be drawn on the image. You can adjust the size and the location of the navigation box if needed.



Figure 7-27

3. To exit the PAP view, right-click the live view and select **PAP** again.

7.4 2-Window Viewer

To access the 2-Window Viewer, click **Live View** on the left panel of WebCam Viewer, and then select **2 Windows**.

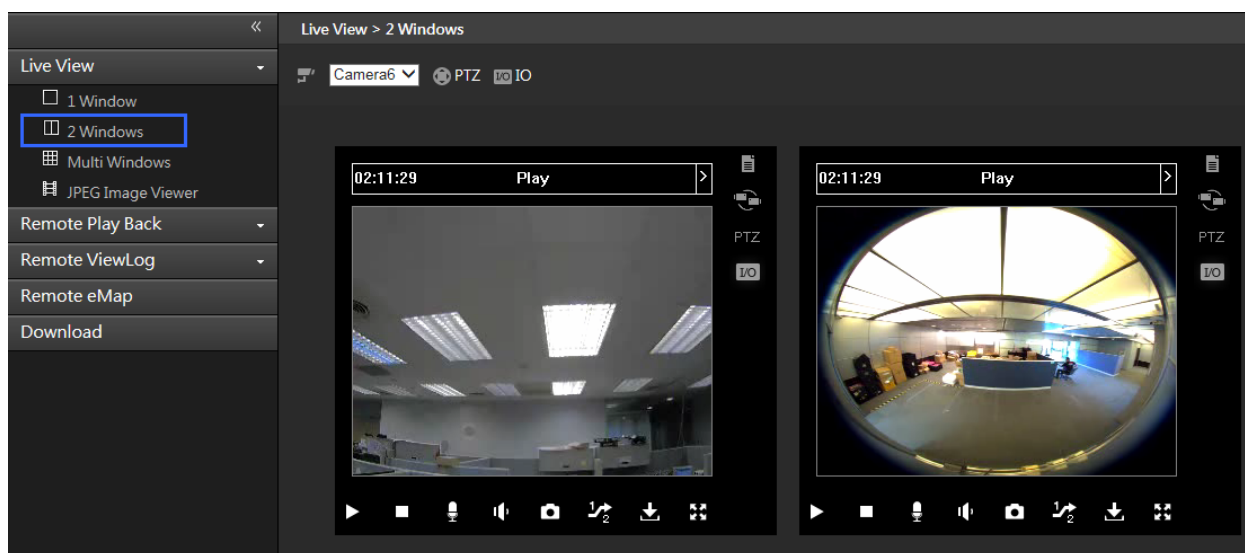


Figure 7-28

In the 2-Window Viewer, select the camera you want to access, and drag the **camera** icon to the viewer windows. You can also drag and drop the **PTZ** and **I/O** icons to the viewer windows for the following functions:

- **PTZ:** activates the Visual PTZ Control Panel on the image
- **I/O:** activates the Visual Automation function

7.5 Multi-Window Viewer

The Multi Windows displays up to 16 channels at a time and supports up to 64 channels.

To access the Multi Windows, click **Live View** on the left panel of the Webcam Viewer page, and select **Multi Windows**. You can also access Multi Windows directly if you select **Simple Version** at the Login page (Figure 7-1).

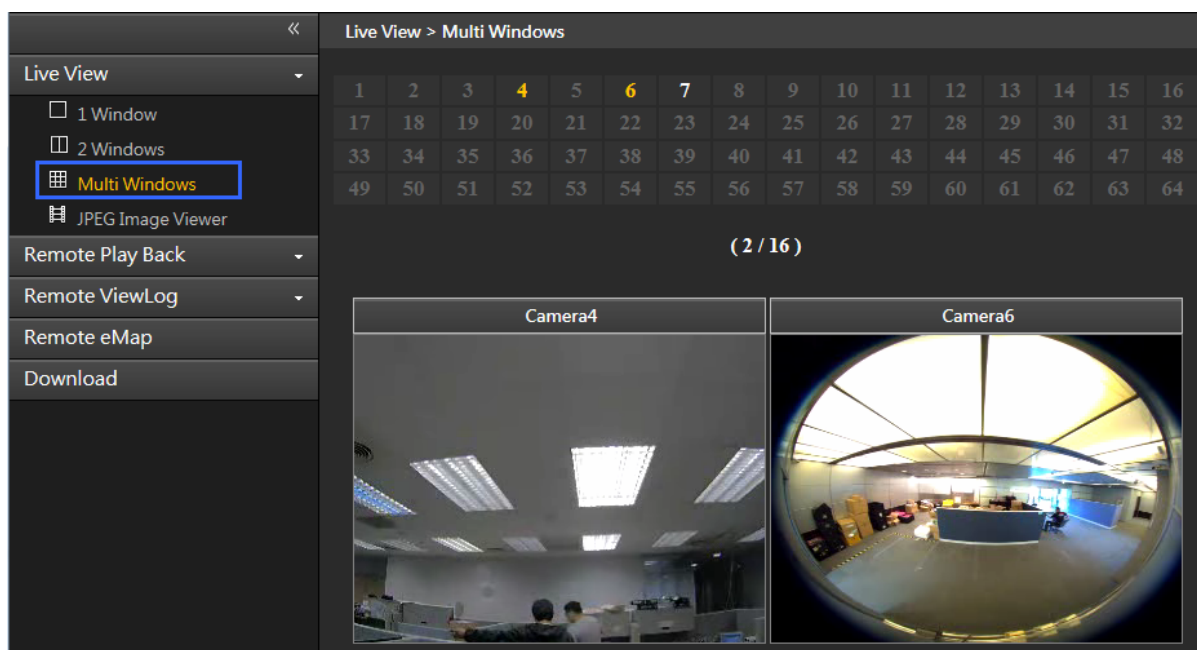





Figure 7-29

7.6 JPEG Image Viewer

JPEG Image Viewer is a cross-platform viewer, compatible with Mac OS and Microsoft IE browsers. Continuously receiving JPEG images from GV-VMS and limited to the single camera view, the viewer is an ideal tool for the users with limited Internet bandwidth.

Note: To enable the JPEG Image Viewer, Java needs to be installed on the local PC.

To enable the function on the WebCam server, click **Home** , click **Toolbar** , click **Network**  and click **WebCam Server**. Disable **Enhance Network Security** under the General tab (Figure 7-4), and enable **Create JPEG/GIF File(s)** under the JPG tab (Figure 7-8).

On the left panel of WebCam Viewer, click **Live View** and select **JPEG Image Viewer**. The JPEG Image Viewer appears.

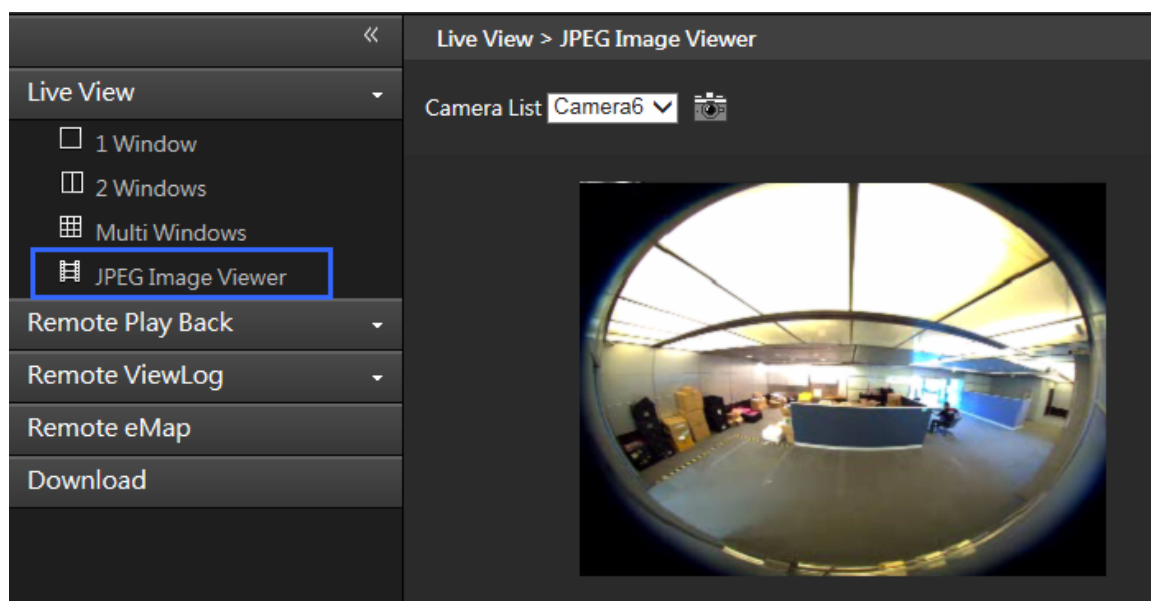


Figure 7-30

7.7 Playing Back Events

7.7.1 Event List Query

The Event List Query function on the WebCam server allows you to remotely search for an event by defining event type and time. The search results can be displayed in text form or in a chart. You can also play back events instantly from the search results.

To allow remote access to GV-VMS and remotely play back events,

- Ensure the WebCam server with the **Run ViewLog Server** function (Figure 7-4) is activated on GV-VMS.
- Ensure that the **Register Event** options are selected under the events you want to access. For example, the Register Motion Event option needs to be selected to access motion events.

Figure 7-31

1. On the left panel of the Single View page (Figure 7-2), click **Remote Play Back** and select **Event List Query**. The Query window appears.
2. On the top, select one of the following search categories: **Monitor**, **System**, **Login**, **Counter**, **Merge**, **Backup** and **Delete**. Note that the above categories are based on those of System Log in the Main System, so you can also locate the same event recorded in System Log.
3. Define the search criteria such as Event Type, Device, Information, Date and etc. The selection of search criteria may vary depended on search categories.

- Click **Submit Query**. The search results will be displayed in the text form.

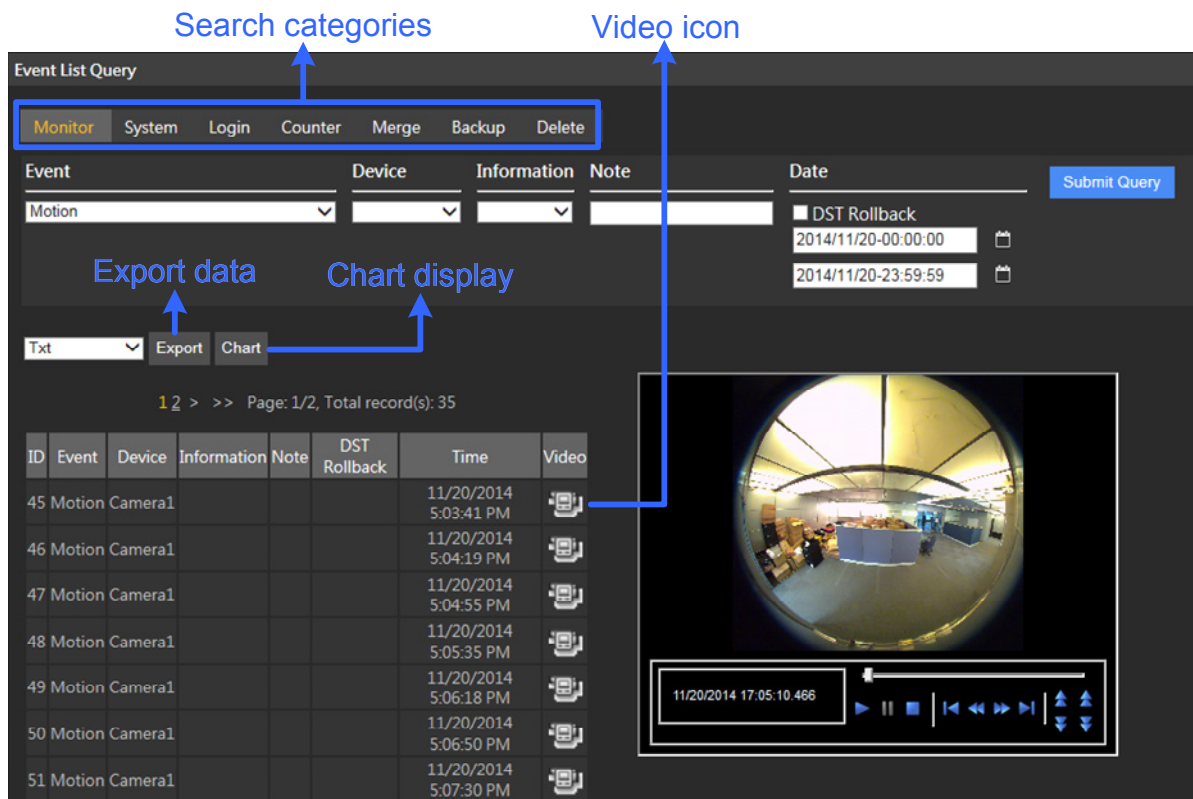


Figure 7-33

- To play back the attached video, click the **Video** icon.
Right-click on the video image gives you more playback features, such as changing playback mode and turning on audio if available.
- To graph the search results, click the **Chart** button.
- To export the search results, select one of formats Txt, Html or Excel and then click the **Export** button.

7.7.2 Remote Playback

With the Remote Playback (RPB) function on the WebCam server, you can play back the recorded files of the connected GV-VMS.

To allow remote access to GV-VMS, ensure the WebCam server with the **Run ViewLog Server** function (Figure 7-4) is activated on GV-VMS.

1. In the left panel of the Single View page, click **Remote Play Back** and select **Remote Play Back**. This window appears.

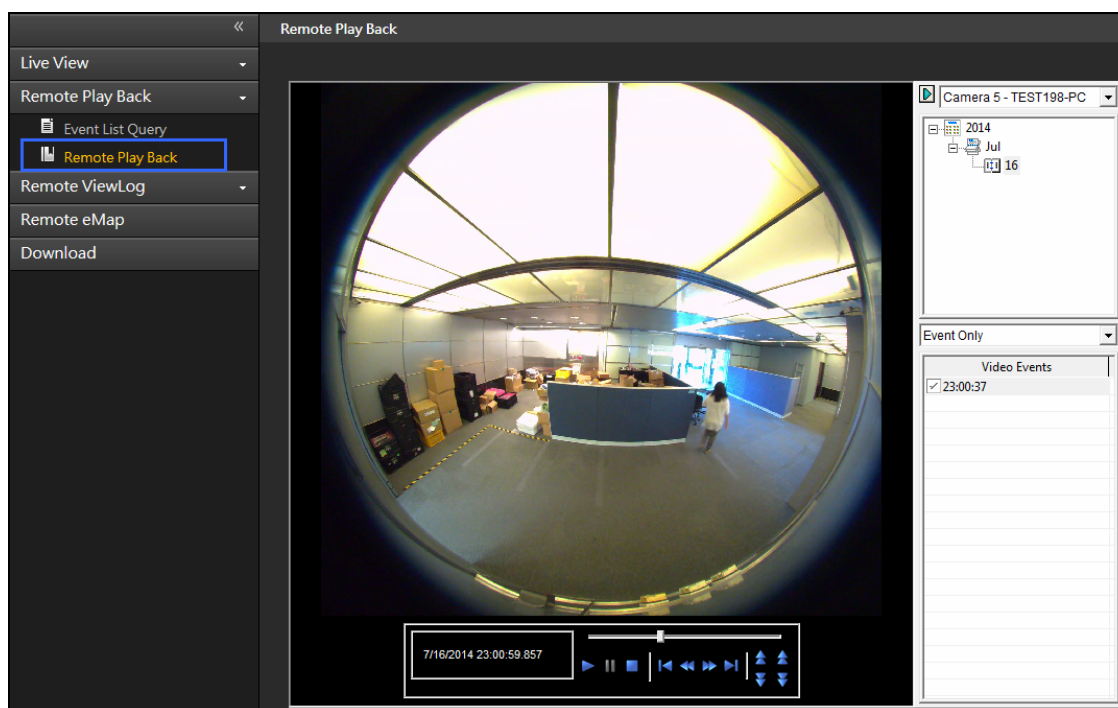


Figure 7-34

2. Select the desired camera, date and time-segment file.
3. Click the **Play** button to start.
4. For additional playback features, right-click on the image to have the options of **Play Mode**, **Render** and **Tools**.

7.8 Remote ViewLog

Through WebCam Server, you can remotely play back the recorded files by using the video player ViewLog.

To allow remote access to GV-VMS, ensure the WebCam server with the **Run ViewLog Server** function (Figure 7-5) is activated on GV-VMS.

1. On the left panel of the Single View page (Figure 7-20), click **Remote Play Back** and select a resolution. Remote ViewLog will be installed on your PC if it is not already. The Remote ViewLog window appears.
2. Select **Remote ViewLog Service**. This dialog box appears.

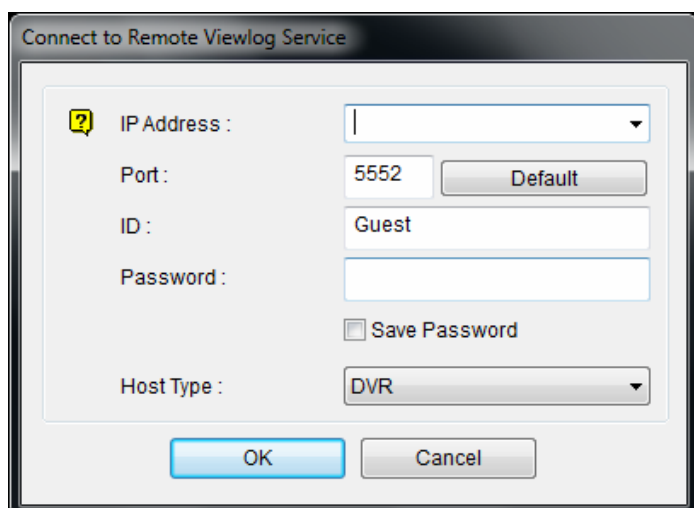


Figure 7-35

3. Type the IP Address, ID and Password of the GV-VMS. Select **DVR** to be the host type. Keep the default port as **5552**, or modify it if necessary.
4. Click **OK**. The events available will be listed in the Event List.

For details on ViewLog player functions, see Chapter 4.

7.9 Download Center

The Download Center allows you to download Remote eMap and Remote ViewLog based on screen resolution required.

1. Click **Download** in the left panel of the Single View page (Figure 7-20). This page appears.

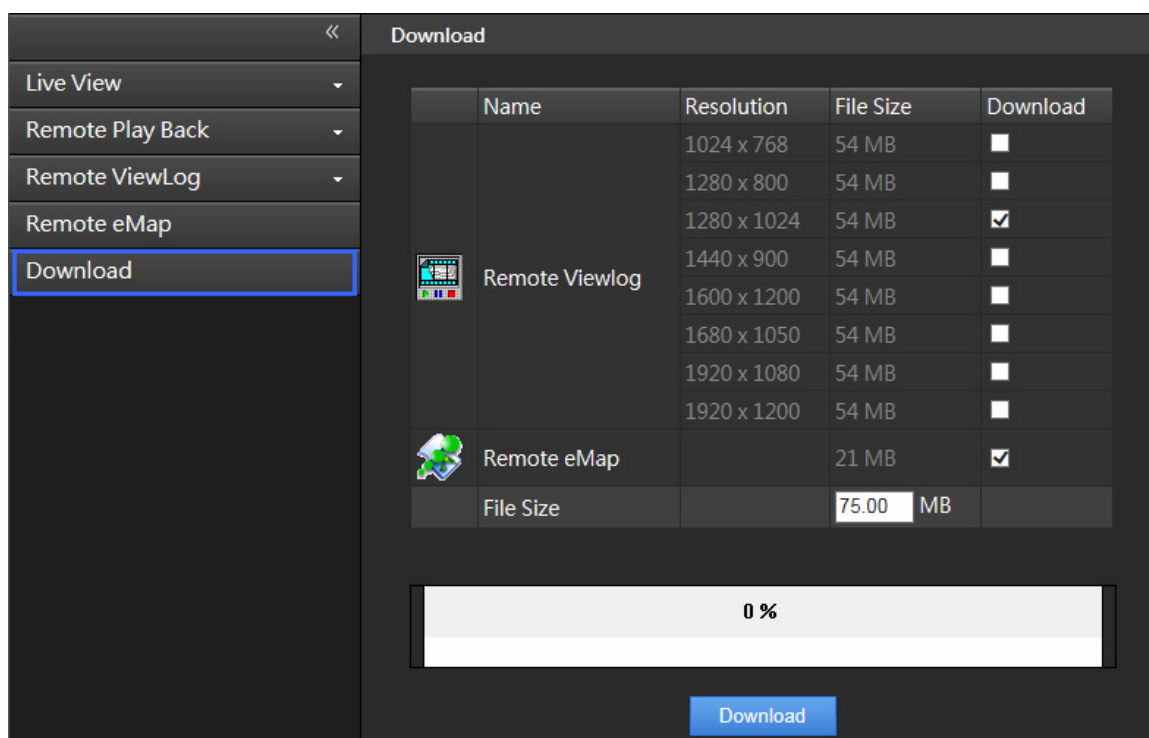


Figure 7-36

2. Check the desired programs. The **File Size** field will display the total file size of the selected programs.
3. Click **Download** and follow the on-screen instructions to install the programs. When the installation is complete, the message “*Install Complete*” will be displayed.

7.10 Mobile Phone Applications

With the mobile phone capable of GPRS, 3G and Wi-Fi, you can receive live videos from your GV-VMS using GV-Eye V2.0 or later. To download the latest GV-Eye or see the full installation guide, visit http://www.geovision.com.tw/english/5_8_App.asp.

Note:

1. Hardware decoding is only supported by devices using Android 4.1 or later and that contain a GPU (graphic processing unit).
 2. Access is only allowed for **Admin** users.
 3. By default, GV-Eye connects to stream 2 of any GV-IP device, which is in H.264 codec and CIF resolution.
 4. Fisheye Dewarp is an optional and a paid service.
-

7.10.1 Activating Mobile Functions on GV-VMS

To access the GV-VMS from GV-Eye, you need to first activate the ViewLog Server and the mobile function on the GV-VMS.

1. On the main screen, click **Home** , click **Toolbar**  and click **Network** .
2. In the dialog box that appears, select **Run ViewLog Server** under the **General** tab.

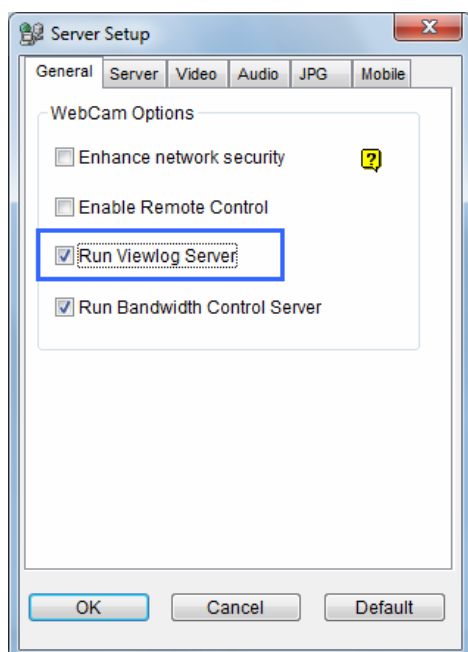


Figure 7-37

3. Click the **Mobile** tab and select the checkbox to enable the mobile function.

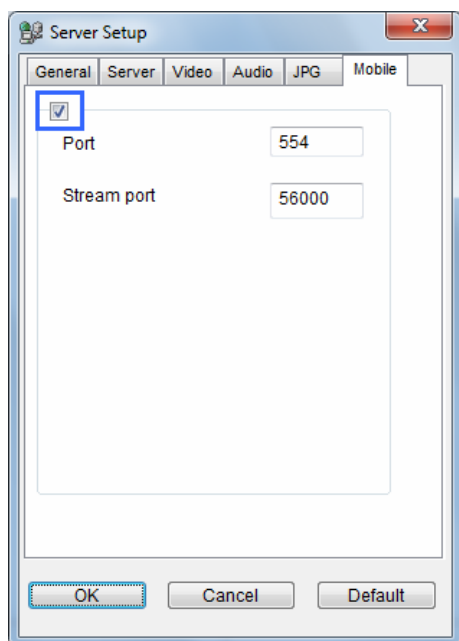


Figure 7-38

7.10.2 Installing GV-Eye

You can download GV-Eye from the **App Store** or **Android Market** and install the application. The GV-Eye icon will appear on the desktop of your mobile device.

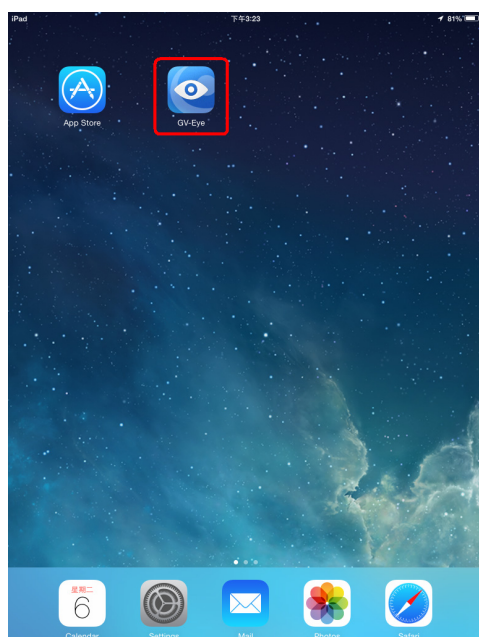


Figure 7-39 GV-Eye icon on iPad

7.10.3 Connecting to GV-VMS

1. On your mobile phone, tap the **GV-Eye** icon  on the main screen. This page appears.

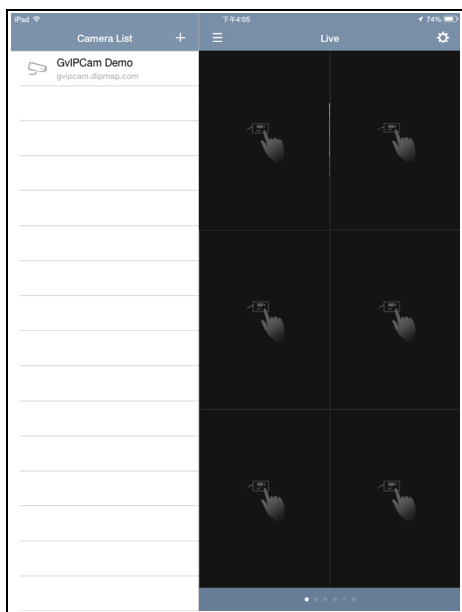


Figure 7-40

2. Tap the **Add** button . This page appears.



Figure 7-41

3. Enter the IP address, port number, username and password of the GV-VMS. The default port for GV-VMS is 56000.

For details on accessing live view, playing back recording and other functions, visit the link below and click **Installation Guide** under GV-Eye: http://www.geovision.com.tw/english/5_8_App.asp

7.11 Web Browsers on Smartphones

Using the browser on your smartphone, you can watch live view, control PTZ live views, and play back recordings from a GV-VMS. By connecting to the WebCam server, no extra application is required.

Note:

1. Make sure the Mobile function is enabled at the WebCam server.
 2. Live view control is only available for supported PTZ cameras.
-

In the following steps, we use the Android smartphone as an example to log in the GV-VMS:

1. Open the browser on your Android device and type the IP address of the GV-VMS to log in.

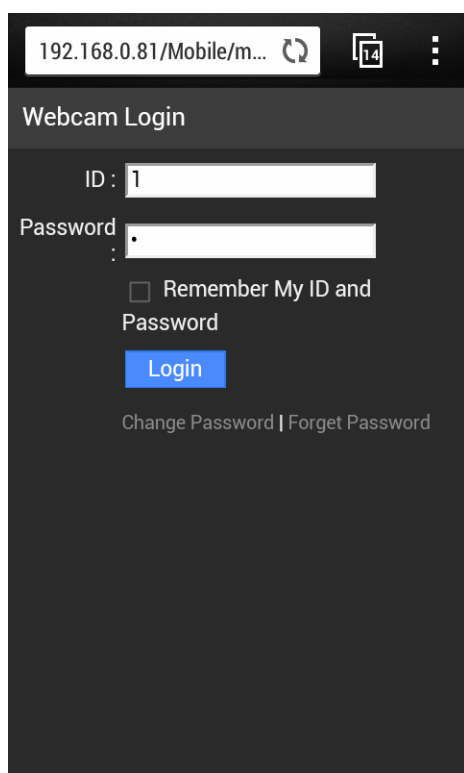


Figure 7-42

- Click **Login**. The cameras on the GV-VMS appear.

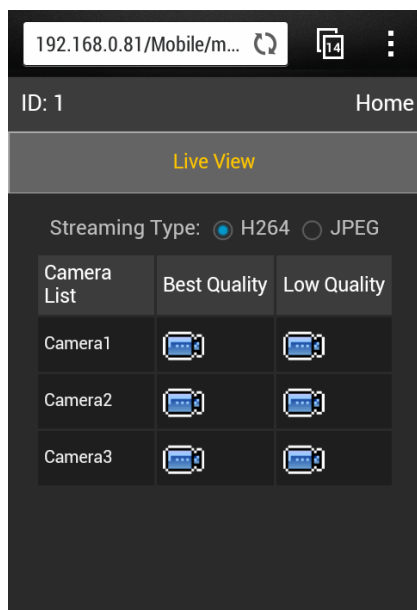



Figure 7-43

- To watch live view, keep the **H.264** option for **Streaming Type**, and then tap a **video** icon . Stream 1 will be displayed if Best Quality is selected and Stream 2 will be displayed if Low Quality is selected.
- To access the PTZ functions, tap the **JPEG** option for **Streaming Type**. This page appears. Tap the live view to see direction arrows. You can control the live view with the direction arrows, zoom in/out and home position buttons.

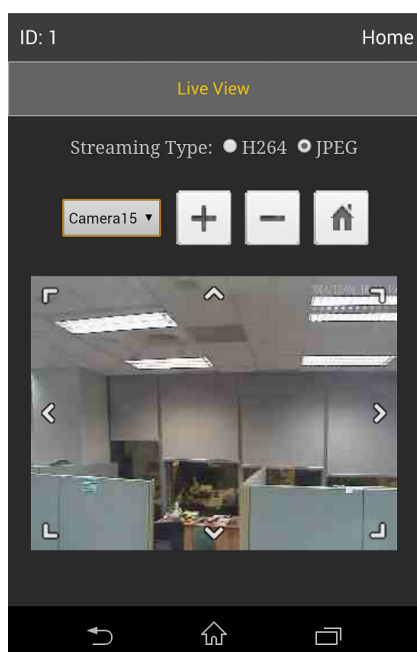


Figure 7-44

Chapter 8

| | |
|--|------------|
| E-Map Application..... | 277 |
| 8.1 The E-Map Editor | 277 |
| 8.1.1 The E-Map Editor Window | 278 |
| 8.1.2 Creating an E-Map | 279 |
| 8.1.3 Creating an E-Map for a Remote Host | 284 |
| 8.2 Starting E-Map..... | 285 |
| 8.2.1 Setting Up the Pop-up Map | 287 |
| 8.3 Remotely Accessing E-Map..... | 289 |
| 8.3.1 The Remote E-Map Window..... | 290 |
| 8.3.2 Accessing E-Maps of Multiple Hosts | 292 |
| 8.3.3 Configuring the Remote E-Map | 293 |
| 8.3.4 Viewing Event List and Playing Back Videos | 295 |
| 8.4 E-Map Server..... | 296 |
| 8.4.1 Installing E-Map Server..... | 296 |
| 8.4.2 The E-Map Server Window | 297 |
| 8.4.3 Setting up E-Map Server..... | 298 |
| 8.4.4 Connecting to E-Map Server | 298 |

E-Map Application

The E-Map displays the monitoring area on an electronic map, by which the operator can easily locate the cameras, sensors and alarms triggered by motion or I/O devices.

The application is available through two programs: **E-Map Editor** which comes with the installation of GV-VMS, and **E-Map Server** applicable on a designed server.

8.1 The E-Map Editor

The E-Map Editor allows you to import a floor plan in BMP, GIF or JPEG formats, and use the icons of cameras and I/O devices to customize a map.

8.1.1 The E-Map Editor Window

The E-Map Editor comes with the installation of GV-VMS. Click the Windows **Start** menu, find **Programs**, select **GV folder** and click **E-Map Editor**. The E-Map Editor window appears.

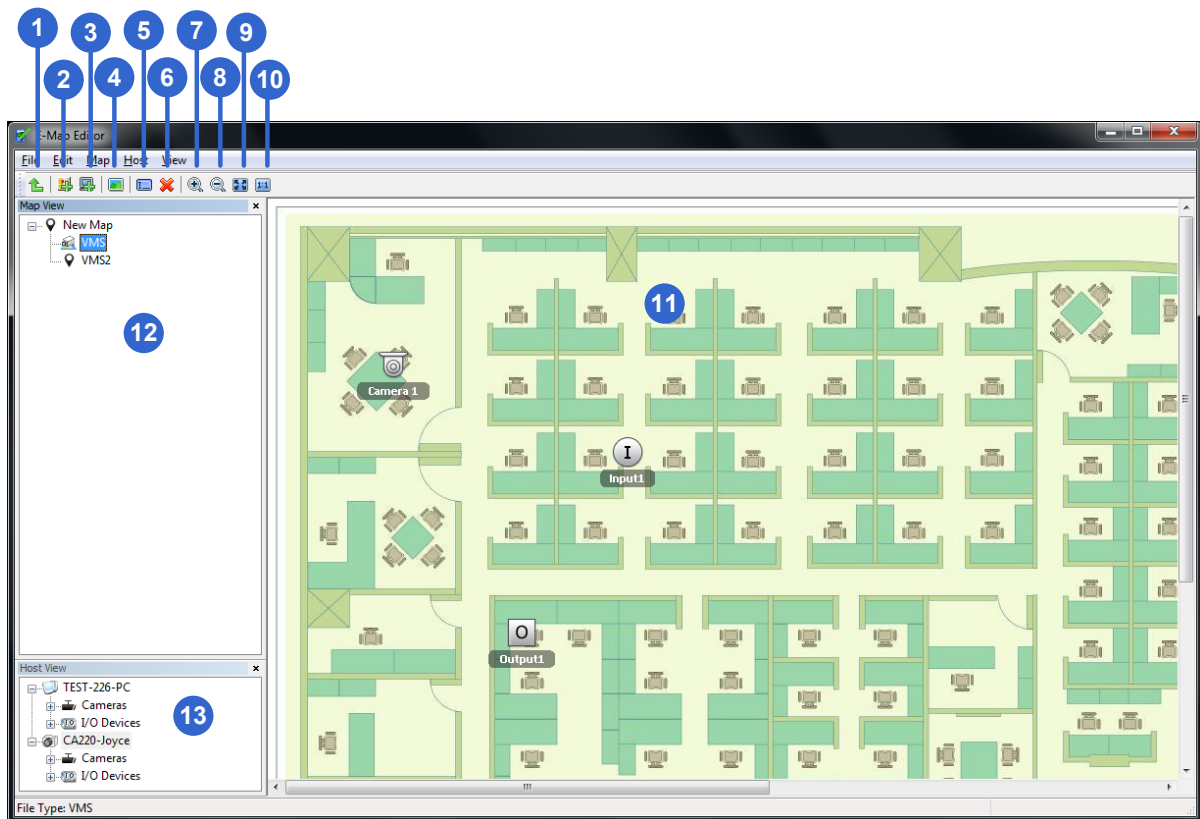


Figure 8-1


The controls in the E-Map Editor window:

| No. | Name | Description |
|-----|----------|--------------------------------------|
| 1 | Up | Returns to the previous E-Map file. |
| 2 | Add Map | Adds an E-Map file. |
| 3 | Add Host | Adds a host folder in the Host View. |
| 4 | Load Map | Imports a floor map. |
| 5 | Rename | Renames an E-Map file and/or folder. |
| 6 | Delete | Deletes an E-Map file and/or folder. |

| No. | Name | Description |
|-----|---------------|---|
| 7 | Zoom In | Enlarges the Map View. |
| 8 | Zoom Out | Diminishes the Map View. |
| 9 | Fit to Screen | Adjusts the Map View to fit the current size of the window. |
| 10 | Actual Size | Displays the actual size of imported graphic file. |
| 11 | Floor Plan | The view of imported graphic file. |
| 12 | Map View | Tree view of E-Map files. |
| 13 | Host View | Tree view of hosts |

8.1.2 Creating an E-Map

To create an E-Map, follow the steps below.

1. Click the **Add Map** button  on the toolbar. A New Map file is created.

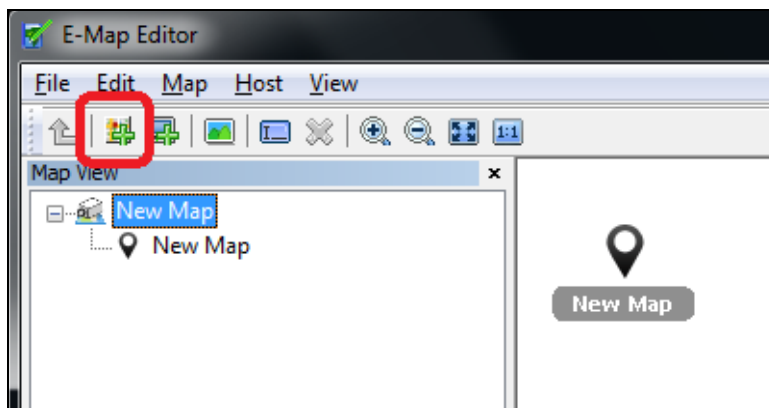


Figure 8-2

2. Select and right-click **New Map** under Map View, and select **Load Map** to import a graphic file. The file opens in the Floor Plan window (No. 11, Figure 8-1).

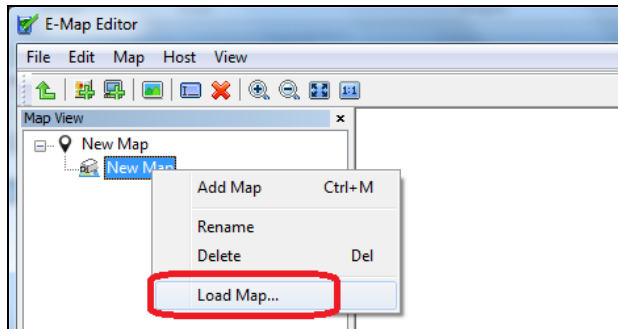


Figure 8-3

3. Double-click the local server folder in Host View (No. 13, Figure 8-1). The program will automatically detect the number of cameras and I/O devices installed at the server, and display their icons.

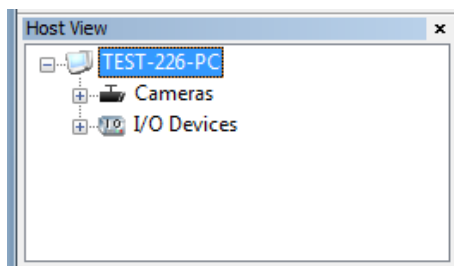


Figure 8-4

4. Drag and drop these icons from Host View to the map in the Floor Plan window.
5. To save the created file, click **File** in the window menu. Select **Save to VMS** to save the file to GV-VMS folder, or select **Save to File** to save the file to a specified path.

Advanced Settings

Optionally, you can have the following settings on your created E-Map.

A. Camera Icons

1. You can set the orientation of camera icons. Select any camera icon which will be highlighted in yellow, right-click the icon to bring up a menu, and select the direction where you want the camera to point to.

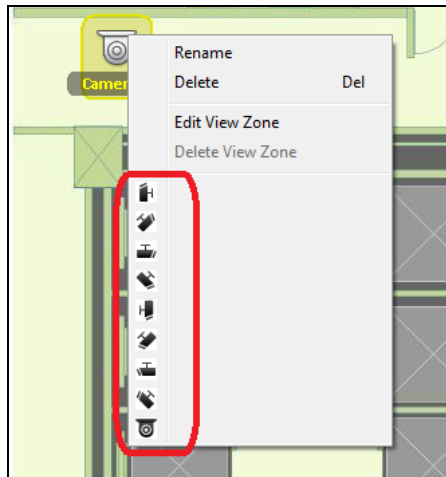


Figure 8-5

2. You can set up a view zone to help recognize the area monitored by the camera:
 - A. Select any camera icon which will be highlighted in yellow, right-click the icon to bring up a menu, and select **Edit View Zone**. A fan-shaped section appears on the map.
 - B. Move the mouse to adjust the length and direction of the view zone.
 - C. Scroll the mouse to adjust the width of the view zone.
 - D. Right-click the map and select **Finish** to finalize the zone.



Figure 8-6

B. I/O and Camera Icons

3. You can change the icons for cameras and I/O devices.
 - A. Select any I/O device or camera icon which will be highlighted in yellow, right-click the icon and select **Change Icon**. The dialog box appears.

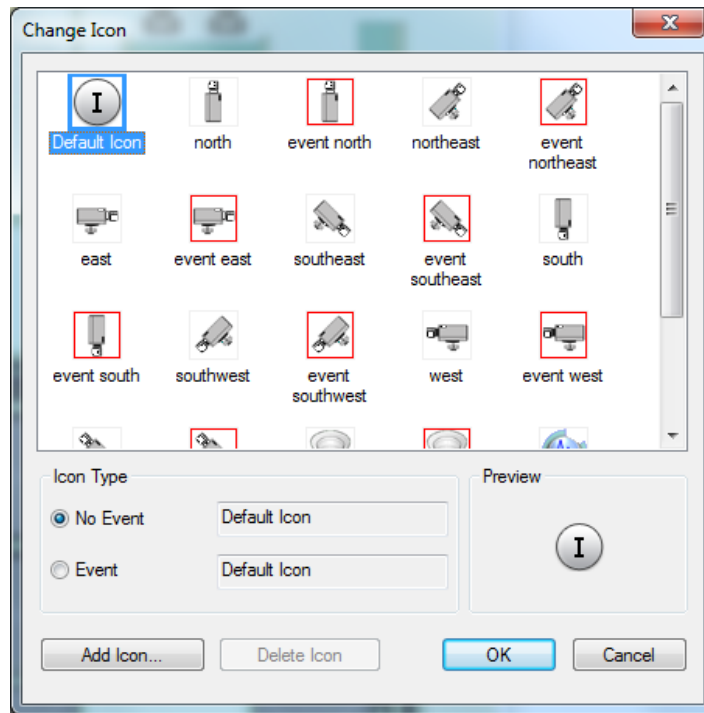


Figure 8-7

- B. Select **No Event** and click **Add Icon** to import your own icon. The icon will display when the I/O device or the camera is not triggered.
 - C. Select **Event** and click **Add Icon** to import your own icon. The icon will display when the I/O device or the camera is triggered.

Note: The size of imported icon must be 32 x 32 pixels.

C. Polygonal Map

4. You can create the Polygonal Map to help you quickly locate the location of a triggered I/O device or a camera detecting motion. Draw an area on the map and it will flash when any device within the area is triggered.
 - A. In E-Map, select a map icon.
 - B. Right-click the map icon and select Edit Polygonal Map.
 - C. Click on the map to start drawing a polygonal area with the yellow dotted line.

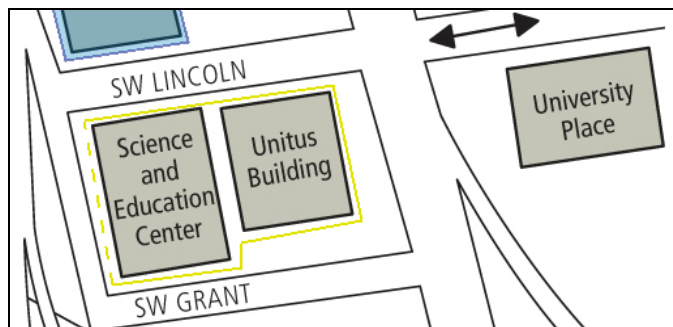


Figure 8-8

- D. After completing the drawing, right-click the map and select **Finish**.

The enclosed area will be colored in blue. When a device placed within the area is triggered, the blue area will flash in red.

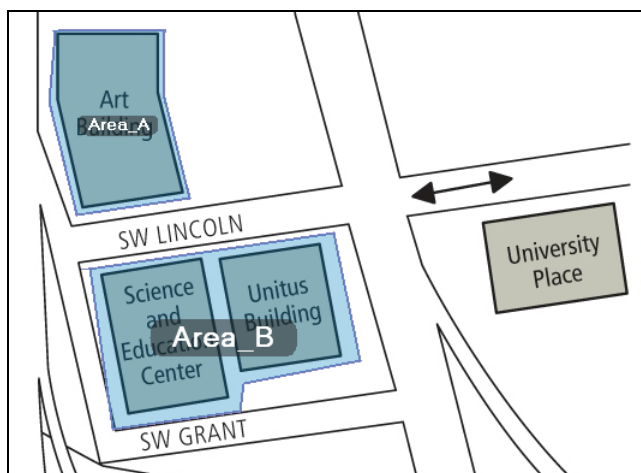



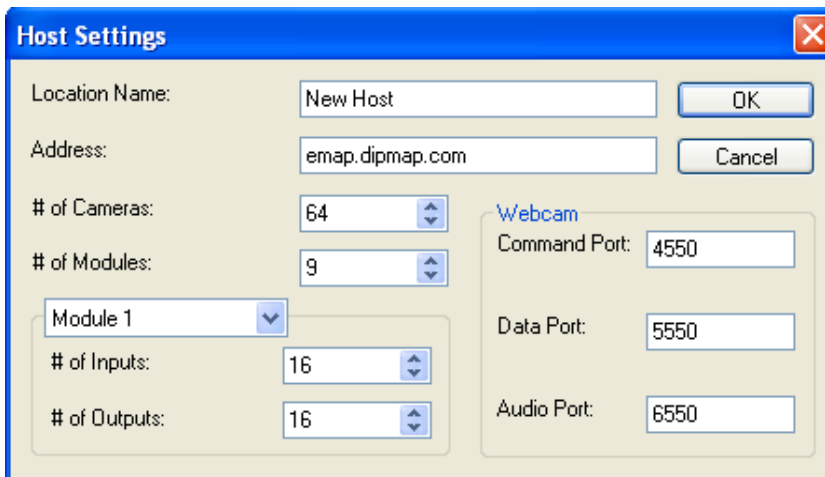
Figure 8-9

8.1.3 Creating an E-Map for a Remote Host

With E-Map Editor, you can create E-Maps for remote hosts in addition to your local host (GV-VMS). Through the Remote E-Map function, these E-Maps can be accessed and monitored through a Web browser. For how to remotely access E-Maps, see *Accessing E-Maps of Multiple Hosts* later in this chapter.

Note: The supported hosts for E-Map include GV-System, GV-VMS, GV-IP Devices, GV-Video Server and GV-Compact DVR.

1. Click the **Add Host** button  on the toolbar and select the type of host. A new host is added in Host View.
2. Right-click the created host and select **Host Settings**. This dialog box appears. The dialog box varies based on the type of host you select.



The **Host Settings** dialog box is shown with the following fields and values:

| Field | Value |
|----------------------|-----------------|
| Location Name: | New Host |
| Address: | emap.dipmap.com |
| # of Cameras: | 64 |
| # of Modules: | 9 |
| Module 1 (selected): | Module 1 |
| # of Inputs: | 16 |
| # of Outputs: | 16 |
| Webcam Command Port: | 4550 |
| Data Port: | 5550 |
| Audio Port: | 6550 |




Buttons: OK, Cancel

Figure 8-10

3. Type the location name, IP address, the number of cameras, I/O modules, inputs, outputs installed at the remote host and port information, and then click **OK**.
4. Follow the instructions in *Creating an E-Map* earlier in this chapter to create an E-Map file for the remote host. Note you need to drag and drop the icons under the remote host to the map on the Floor Plan.

8.2 Starting E-Map

After creating an E-Map with E-Map Editor, you can start the E-Map on GV-VMS and monitor the surveillance area in the electronic map. When any camera or I/O device is triggered, its corresponding icon on the map will blink as an alert.

1. Click **Home** , select **Toolbar**  and click **Content List** . The Content List appears.
2. Expand the **E-Map** folder, drag and drop the created E-Map to the live view grid. The E-Map is displayed.

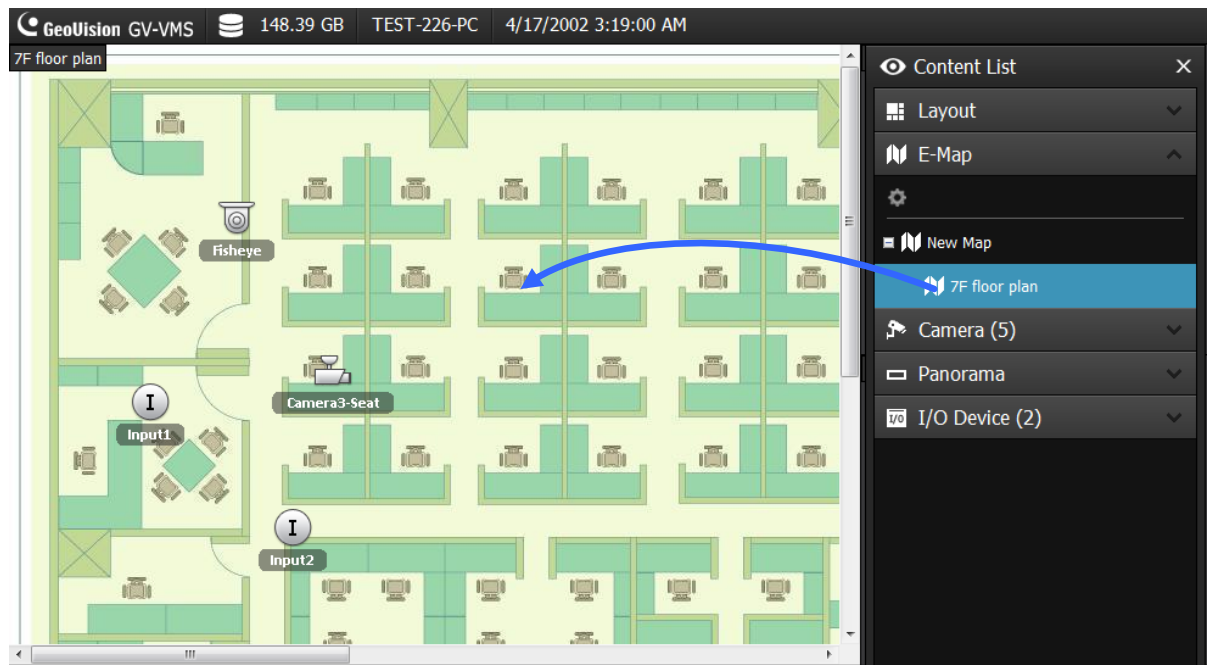


Figure 8-11

3. When any camera or I/O device is triggered, its corresponding icon will start blinking in red. You can move the cursor on the icon to have an image or click the icon to bring the camera view to full view.

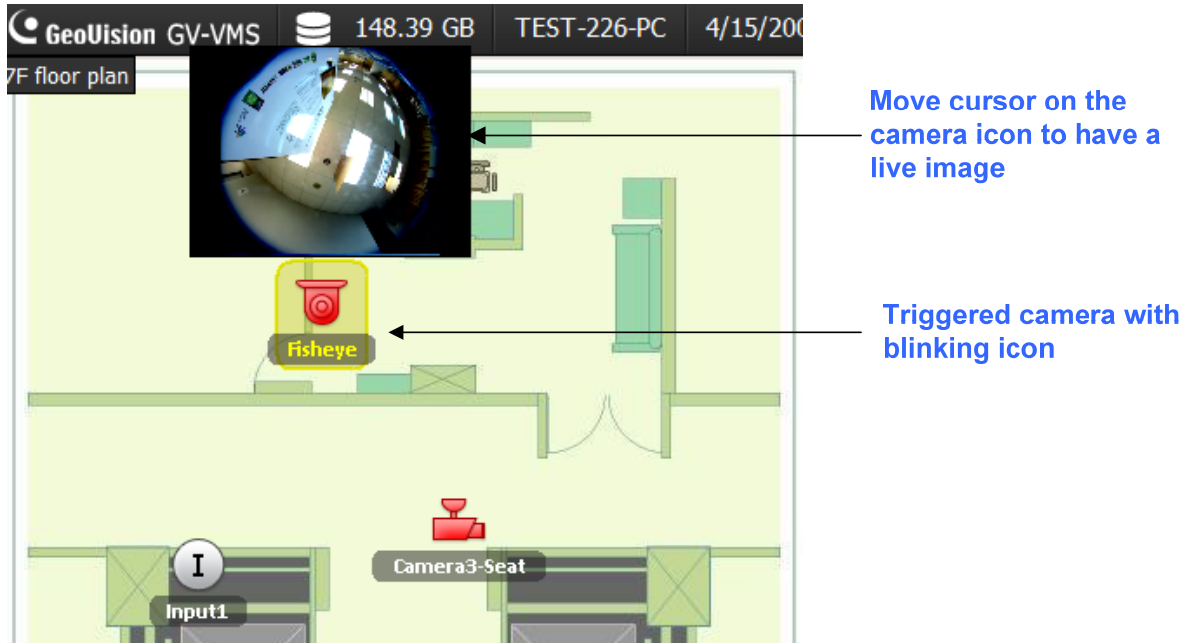


Figure 8-12

Note: If you have created the E-Maps for multiple hosts, you can also see these map files in the Content List. However, these map files won't function on the GV-VMS and only work on the Remote WebCam through a Web browser. For details, see *Accessing E-Maps of Multiple Hosts* later in this chapter.

8.2.1 Setting Up the Pop-up Map

When multiple E-Maps are monitored at one time, you can enable the pop-up function for monitoring convenience. Once any camera or I/O device is triggered, its corresponding E-Map will pop up, replacing the current E-Map, as an alert. To set up the function, follow the steps below.

1. In the Content List, click the **Configure** button under the E-Map.

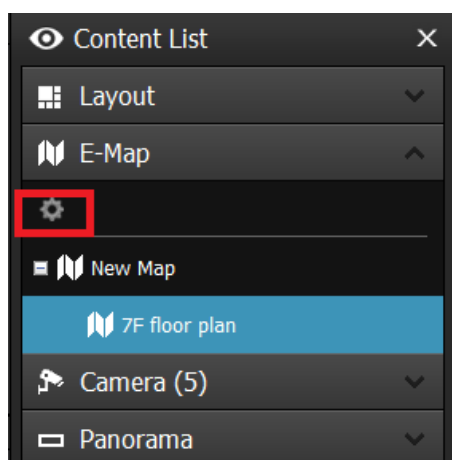


Figure 8-13

2. Select desired cameras and input devices for the application, and specify **Interrupt Interval** for the duration between event triggers. Any event trigger will be ignored by the system during the interval to avoid frequent map pop-up.

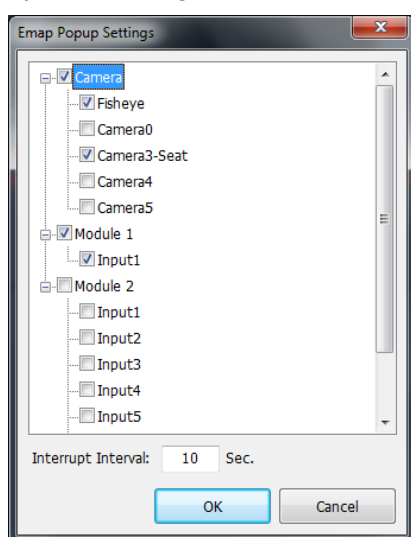


Figure 8-14





- At the bottom of the E-Map grid, click the **E-Map Auto Pop-up** button  to enable the function. In this example, two floor plans (7F and 9F) are under monitoring. When you are observing 9F floor plan but one event is triggered on 7F floor plan, the 7F floor plan will pop up replacing the current 9F floor plan as a warning.



Figure 8-15

8.3 Remotely Accessing E-Map

You can remotely access and view E-Maps over a Web browser.

1. Click **Home** , select **Toolbar** , click **Network**  and select **WebCam Server**. The Server Setup dialog box appears.

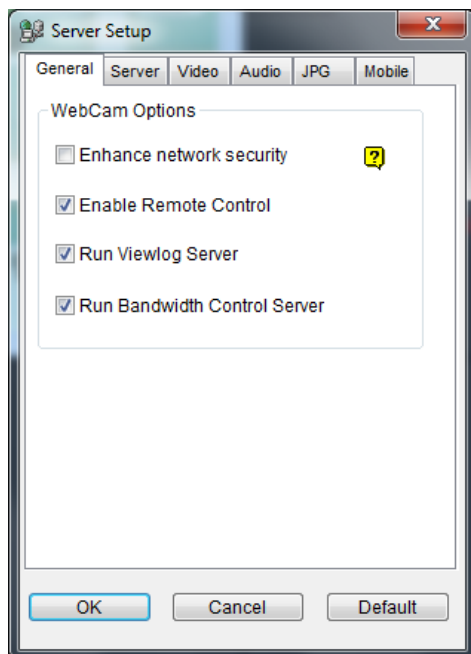


Figure 8-16

2. Click **OK** to start the WebCam server.
3. Open the Web browser and type the address of the GV-VMS. Once the connection is established, the Single View page will appear.
4. On the left panel, click **Remote E-Map**. The Login dialog box appears.

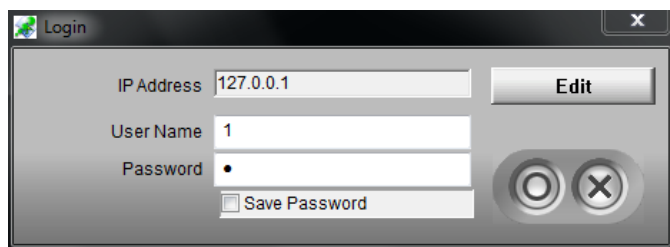



Figure 8-17

5. Type the login user name and password assigned on the GV-VMS and click . The Remote E-Map window is displayed.

8.3.1 The Remote E-Map Window

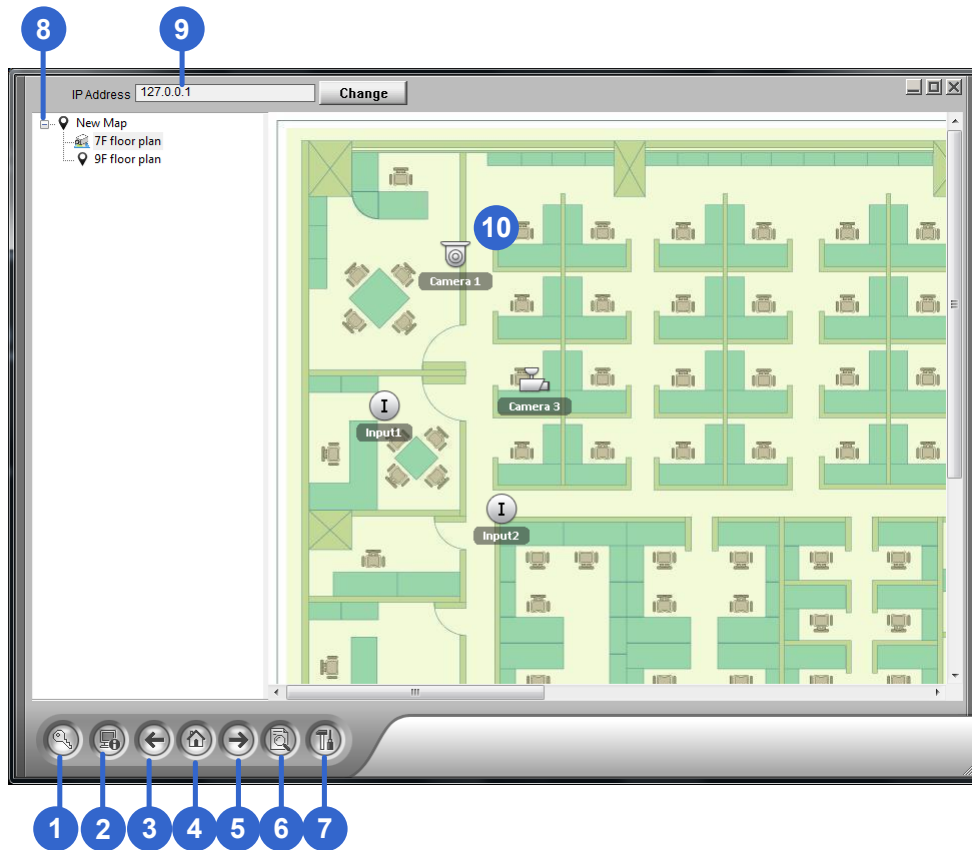


Figure 8-18

The controls in the Remote E-Map window:

| No. | Name | Description |
|-----|------------------|--|
| 1 | Login | Logs into 500 hosts at most. |
| 2 | Host Information | Views the information of incoming events upon motion detected and I/O devices triggered. |
| 3 | Previous | Goes to the last selected E-Map file. |
| 4 | Home | Goes back to the top of the tree view. |
| 5 | Next | Goes to the next E-Map file. |
| 6 | ViewLog | Accesses the Remote ViewLog function. For details, see <i>Remote ViewLog Service</i> in Chapter 4. |
| 7 | Configure | Configures the advanced settings. |
| 8 | Tree List | Displays all created E-Map files and folders. |

| No. | Name | Description |
|-----|--------------------------|---|
| 9 | IP Address | Displays the IP Address of the connected host. |
| 10 | Camera/Input/Output Icon | <p>When the events occur, the corresponding icons will blink in red as an alert.</p> <p>Camera icon: Move the cursor on the icon to have a live image. Click the icon to open a control panel for the camera.</p> <p>Output Icon: Click the icon to manually trigger the output device. .</p> |

The control in the Camera Icon

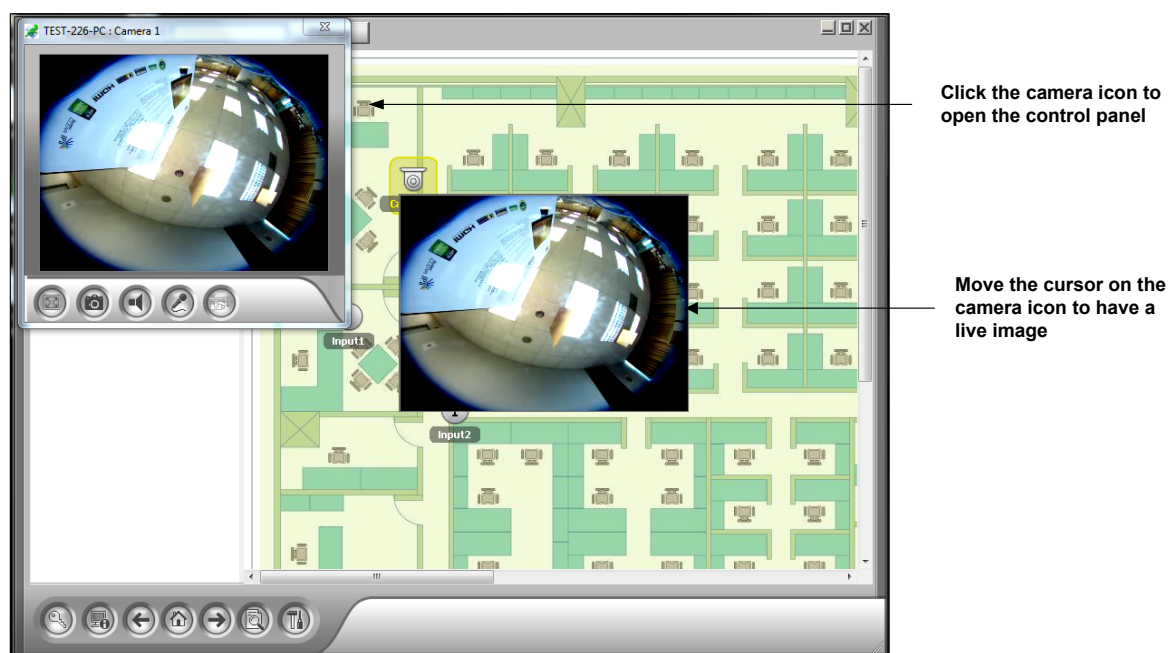



Figure 8-19

8.3.2 Accessing E-Maps of Multiple Hosts

If you have created E-Maps for multiple hosts (see *Creating an E-Map for a Remote Host* earlier in this chapter), you can monitor these E-Maps remotely through a Web browser. The E-Maps of up to 500 hosts can be accessed at one time. To log in a host, follow the steps below.

1. Click the **Login** button  on the Remote E-Map window. The Login window appears.
2. Select a host on the right panel and click the **Login** button. You will be prompted for a username and password for login to the host.

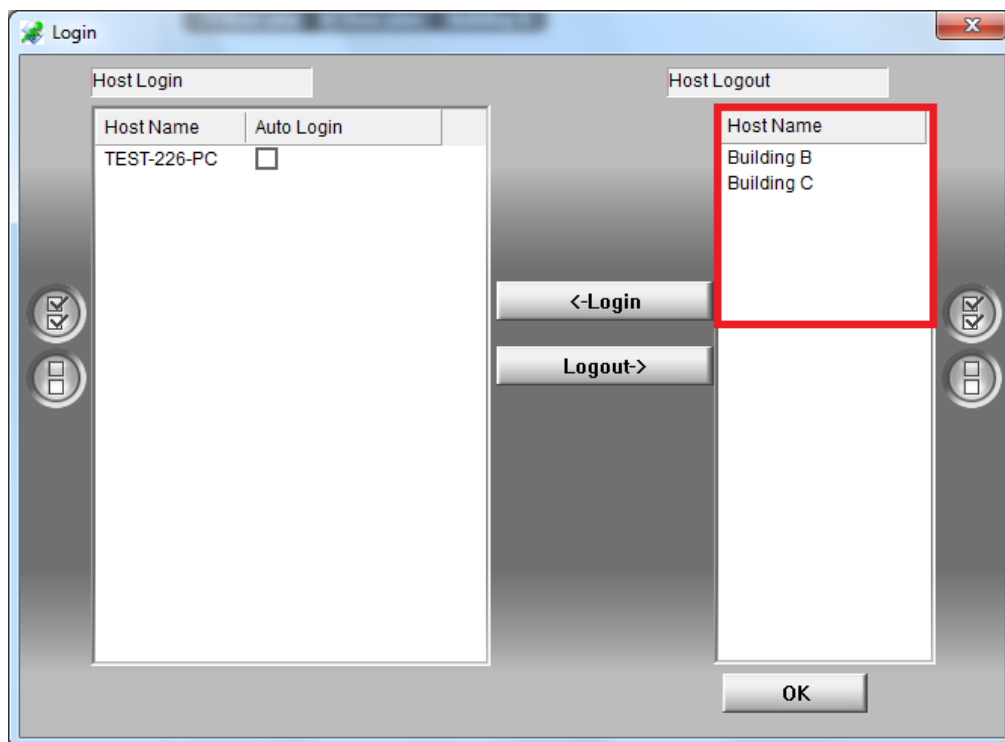



Figure 8-20

3. Click **OK** to return to the Remote E-Map window. Now you can select the corresponding E-Map for the new host for monitoring.

8.3.3 Configuring the Remote E-Map

Click the **Configure** button  on the Remote E-Map window. The Configure window appears.

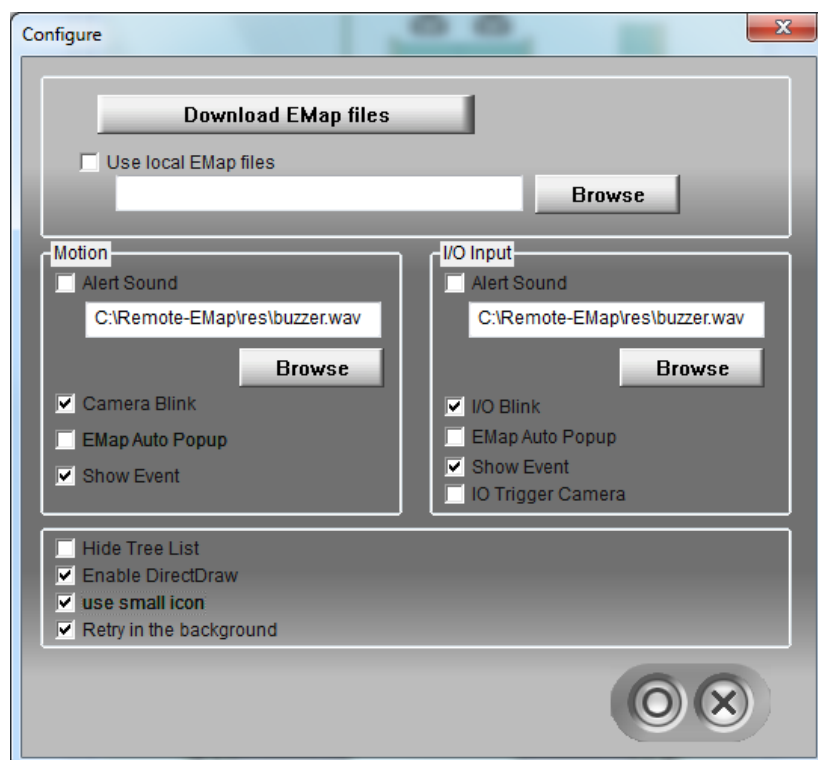


Figure 8-21

[Download E-Map files] Download E-Map files from the local server to the client PC. This option can reduce network loading if you wish to view the E-Maps of multiple hosts.

- **Use local E-Map files:** After downloading E-Map files to the client PC, you can select and use these E-Map files for connection.

[Motion] / [I/O Input]

- **Alert Sound:** Assign a .wav file to alert the operator when cameras or I/O devices are triggered.
- **Camera Blink, I/O Blink:** When cameras or I/O devices are triggered, their icons on the E-Map flash. Unselect this option if you do not want to see the blinking icons.
- **E-Map Auto Popup:** When cameras or I/O devices are triggered, the related map will pop up on the screen instantly when the Remote-E-Map window is minimized.

- **Show Event:** Display motion or I/O triggered events on the Host Information window.
- **I/O Trigger Camera:** When the input devices are triggered, the related camera views will pop up on the screen instantly. To enable this function, you must map input devices to cameras on the GV-VMS first. See *Setting Live View Pop-up Video* in Chapter 1.
- **Hide Tree List:** Check to hide the tree list.
- **Enable DirectDraw:** By default, DirectDraw is enabled to speed up the graphics rendering. Some VGA cards might not support DirectDraw and can produce distorted frames. In this case, disable the option.
- **Use Small Icon:** By default, the large icons of cameras and I/O devices are used. Enable this option if you want to use small icons.
- **Retry in the Background:** When the Remote E-Map is disconnected with GV-VMS, a warning message will pop up every 30 seconds. Select this option to always hide the message and retry the connection in the background.

8.3.4 Viewing Event List and Playing Back Videos

You can see a list of triggered events on the Host Information window and play back any video of interest.



1. Click the **Host Information** button on the Remote E-Map window. The Host Information window appears.

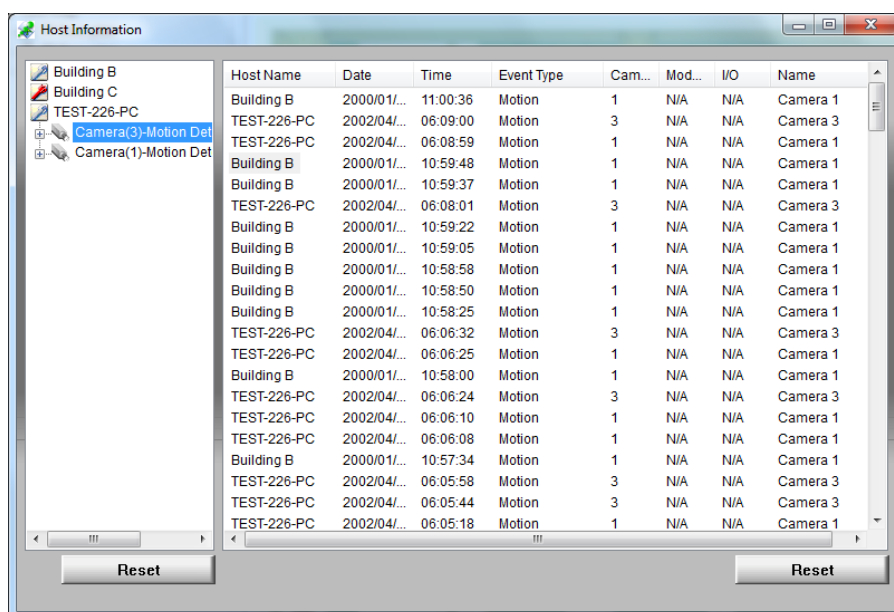


Figure 8-22

2. For event playback, double-click any motion event on the left panel. The player appears.

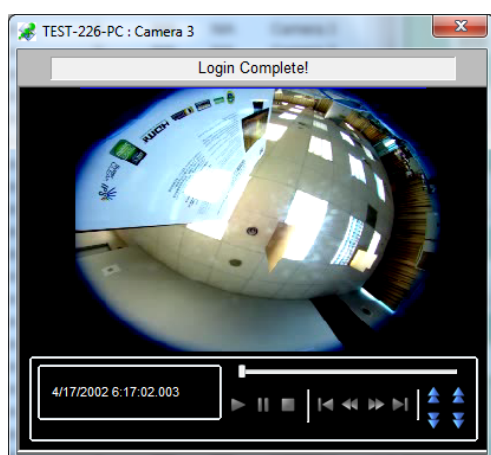


Figure 8-23

3. Right-click the image to access the advance functions of the player.

8.4 E-Map Server

The E-Map Server is an independent program designed to create E-Maps for different hosts. With E-Map Server, you can monitor different sites on electronic maps through any computer accessible to the network.


8.4.1 Installing E-Map Server

You can install the Dynamic DNS from Software DVD or GeoVision Website.

Downloading from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-E-Map Server** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-E-Map Server**.

8.4.2 The E-Map Server Window

Go to Windows **Start**, find **Programs**, select **eMapServer** and click **E-Map Server**. This window appears.

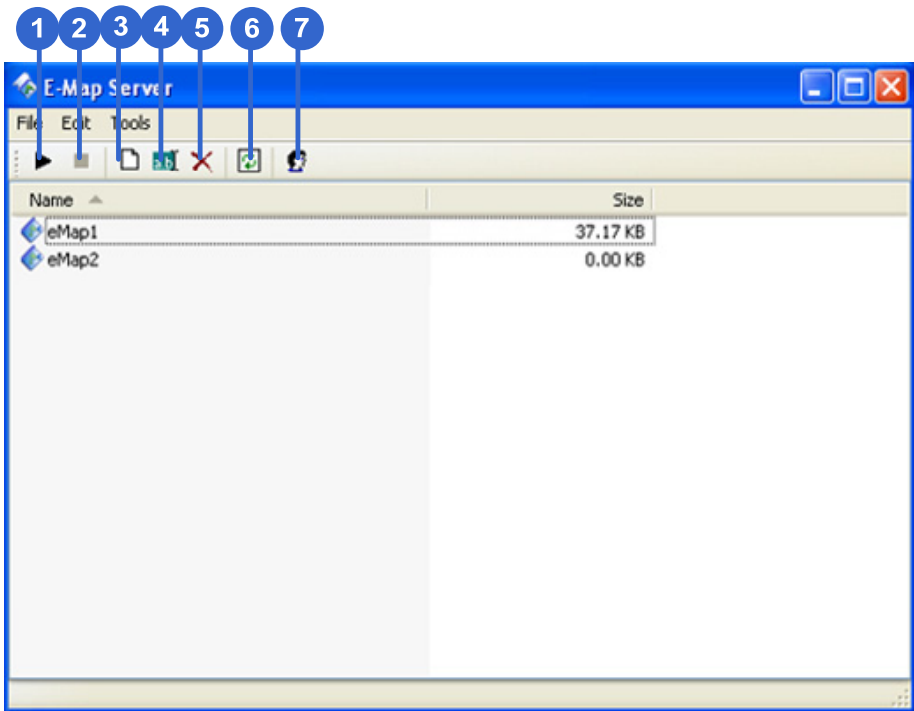


Figure 8-24

The controls on the E-Map Server window:

| No. | Name | Description |
|-----|---------------|--|
| 1 | Start Service | Starts the E-Map Server. |
| 2 | Stop Service | Stops the E-Map Server. |
| 3 | New | Creates a new E-Map file. |
| 4 | Rename | Renames the E-Map file. |
| 5 | Delete | Deletes the E-Map file. |
| 6 | Refresh | Refreshes the E-Map Server window. |
| 7 | Accounts | Creates user accounts of the E-Map Server. |


8.4.3 Setting up E-Map Server

Before starting the E-Map server, you must create E-Map files and user accounts.

- To create E-Map(s), click the **New** button (No.3, Figure 8-24). For details, see *Creating an E-Map* earlier in this chapter.
- To create a user account for the server, click the **Accounts** button (No. 7, Figure 8-24).

8.4.4 Connecting to E-Map Server

With E-Map Server, you can monitor different sites on electronic maps through any computer accessible to the network.

1. Open the Web browser and type the IP address of the E-Map server.
2. Type a user name and password created on the E-Map Server. You will be prompted to select an E-Map file (.emp file).
3. Click **OK**. The Remote E-Map window appears (Figure 8-18).
4. Click the **Login** button  and log in the desired host(s). For details, see *Accessing E-Maps of Multiple Hosts* earlier in this chapter.

Note: To log in the GV-VMS, make sure the WebCam Server is enabled.

Chapter 9

Useful Utilities301

| | |
|---|------------|
| 9.1 Dynamic DNS | 301 |
| 9.1.1 Running Dynamic DNS..... | 302 |
| 9.1.2 Registering Domain Name with DDNS..... | 303 |
| 9.1.3 Starting Dynamic DNS..... | 305 |
| 9.2 Watermark Viewer | 307 |
| 9.2.1 Activating Watermark Protection | 307 |
| 9.2.2 Running the Watermark Proof | 308 |
| 9.2.3 The Main Window | 309 |
| 9.3 Windows Lockup..... | 310 |
| 9.3.1 The GV-Desktop Screen..... | 310 |
| 9.3.2 GV-Desktop Features | 311 |
| 9.3.3 Token File for Safe Mode..... | 314 |
| 9.4 Authentication Server..... | 315 |
| 9.4.1 Installing the Server | 315 |
| 9.4.2 The Main Window | 316 |
| 9.4.3 Creating Clients..... | 318 |
| 9.4.4 Creating User Accounts | 319 |
| 9.4.5 Importing Groups and Users from Active Directory | 323 |
| 9.4.6 Starting the Server..... | 325 |
| 9.4.7 Connecting GV-VMS to the Server | 327 |
| 9.4.8 Remote Access from Control Center and Remote E-Map..... | 330 |
| 9.5 Fast Backup and Restore..... | 333 |
| 9.5.1 Running the FBR Program..... | 333 |
| 9.5.2 Plugin Component..... | 334 |
| 9.5.3 Customizing the Features | 335 |
| 9.5.4 Backing up and Restoring Settings | 336 |
| 9.6 Bandwidth Control Application..... | 338 |
| 9.6.1 Installing the Bandwidth Control | 339 |
| 9.6.2 The Main Window | 340 |
| 9.6.3 Allowing Remote Control | 341 |
| 9.6.4 Connecting to a WebCam Server..... | 342 |
| 9.6.5 Controlling Specific WebCam Server | 343 |

| | |
|--|------------|
| 9.6.6 Setting up the Bandwidth | 344 |
| 9.6.7 Block List Setup | 345 |
| 9.6.8 General Setup | 346 |
| 9.7 Language Setting | 347 |
| 9.7.1 Installing the MultiLang Tool | 347 |
| 9.7.2 Revising the Translated Text | 348 |
| 9.7.3 Setting Up the UI Language to English | 352 |
| 9.8 Skype Video Utility | 354 |
| 9.8.1 Installing GV-Skype Video Utility | 355 |
| 9.8.2 Setting Up Notifications Upon Motion or I/O Trigger | 356 |
| 9.8.3 Requesting Live View | 361 |
| 9.9 GV-SDSyncCard Utility | 362 |
| 9.9.1 Installing GV-SDCardSync Utility | 362 |
| 9.9.2 Setting Up GV-SDCardSync Utility | 363 |
| 9.9.3 The Main Window | 366 |

Useful Utilities

GV-VMS support the advanced utilities, such as Authentication Server, Fast Backup and Restore program, Bandwidth Control Application and GV-IP Device Utility to enhance the system performance in a security network.

9.1 Dynamic DNS

GV-Dynamic DNS allows you to register domain names that always point to your GV-VMS server. This application is only necessary when your server is using a dynamic IP address. The GV-Dynamic DNS will update the server's IP address to DNS Server every 10 minutes. Therefore, even if your server's IP address changes, you can still locate it by using the registered domain name.

Note: GV-Dynamic DNS uploads IP addresses over the Internet through ports 80 and 81. If your GV-VMS server is connected behind a router or firewall, make sure ports 80 and 81 are enabled. GV-Dynamic DNS will only upload global IP addresses. If your GV-VMS server is using virtual IP, NAT port mapping should be done first.

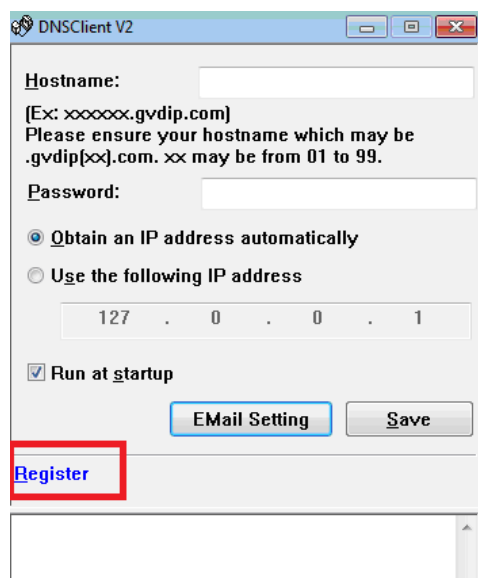
IMPORTANT: The DDNS service is provided purely as a favor to you. We hope it simplifies the process of trying to connect an IP video device to the network. GeoVision does not and cannot warrant that the DDNS service will be uninterrupted or error free. Please read Terms of Service carefully before using the service. Besides GeoVision, you can also obtain the free DDNS service from these providers: DynDNS.org and No-IP.com.

9.1.1 Running Dynamic DNS

GV-Dynamic DNS Service is included in the installation of GV-VMS. Go to Windows **Start**, point to **Programs**, select **GV-VMS**, and click **DNS Client V2**. The DNSClient V2 dialog box appears.

9.1.2 Registering Domain Name with DDNS

1. Click **Register** on the DNSClient V2 dialog box (Figure 9-1). The register page appears.



DNSClient V2 dialog box

 A screenshot of the 'GV-Dynamic DNS Service V2' Register page. The page title is 'GV-Dynamic DNS Service V2'. Under the 'Register' heading, there are input fields for 'Username: jula', 'Password:,', and 'Re-type Password:,'. To the right of these fields are instructions: 'Username is 16-character maximum; username may not start with spaces or minus signs ('-'). Username will be your hostname.' and 'Password' instructions: 'The password is case-sensitive.' Below the input fields, there is a CAPTCHA section titled 'Word Verification' with the instruction 'Enter the characters as they are shown in the box below.' and a CAPTCHA image showing the characters 'aevm'. At the bottom of the page are 'Send' and 'Refresh' buttons.

Register page

Figure 9-2

2. Type a username. The username can be up to 16 characters. The username accepts “a ~ z”, “0~9”, and “-”, but does not accept space or “-” as the first character.
3. Type a password. The password is case-sensitive and must be at least 6 characters. Re-type the password for confirmation.
4. In the Word Verification section, type the code within the box. The Word Verification is not case-sensitive.
5. Click the **Send** button. The following message appears.

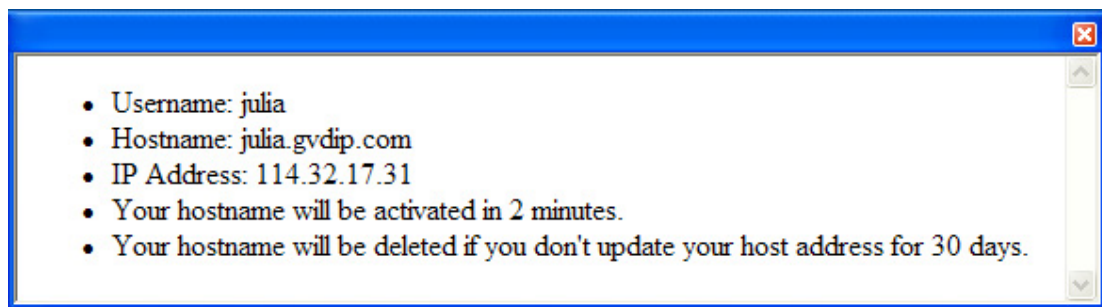


Figure 9-3

- **Username:** The username you registered. In this example, the username is “julia”.
- **Hostname:** The hostname you created. Hostname is made by registered username and “gvdip.com”. In this example, the hostname is “http://julia.gvdip.com”. This will be the domain name used to log into your server.
- **IP Address:** Your server’s current IP address. This IP address is updated every 10 minutes.

Note: The domain name .gvdip(xx).com may vary with xx from 01 to 99.

9.1.3 Starting Dynamic DNS

After registering a domain name with GV-Dynamic DNS, you can enable the DDNS function on your server. Run **DDNS Client V2** and make sure GeoVision software is also enabled at the background.

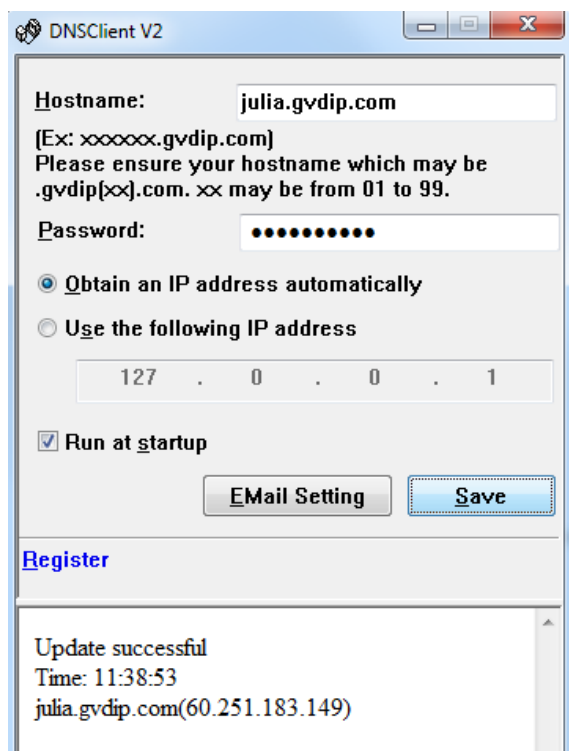


Figure 9-4

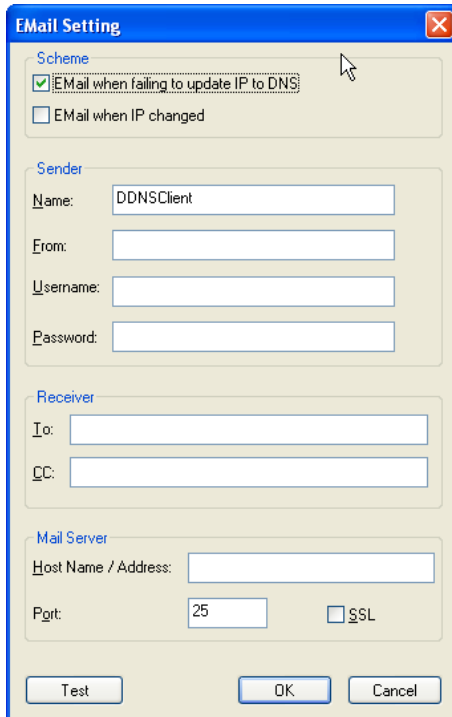
- **Hostname:** Type the hostname used to enable the service from the DDNS.
- **Password:** Type the password used to enable the service from the DDNS.
- **Obtain an IP address automatically:** The DDNS server will use any available IP address from the server or the router.
- **Use the following IP address:** If your server or router has more than one IP address, you can assign one IP address for the connection between the DDNS server and GV-VMS. It is highly suggested to assign a fixed IP address instead of a dynamic IP address, which will not be accessible for the DDNS when the IP address is changed.
- **Run at startup:** Select this option to automatically run the DDNS service at Windows startup.
- **E-mail Setting:** See *Setting up E-mail Notification* later in this chapter.

After completing the settings above, click **Save**. The connection information will be displayed.

Note: The DNS Client will not upload the IP address unless the compatible GeoVision software is running such as GV-VMS. If the IP address of your server is not updated for more than 30 days, your host name will be deleted automatically.

Setting up E-mail Notification

You can set up E-mail settings to receive e-mail notification. In the DNS Client dialog box (Figure 9-4), click **E-mail Setting**. The E-mail Setting dialog box appears.



The E-mail Setting dialog box is shown with the following fields and options:

- Scheme:**
 - ☒ EMail when failing to update IP to DNS
 - ☐ EMail when IP changed
- Sender:**
 - Name: DDNSClient
 - From: [Empty text box]
 - Username: [Empty text box]
 - Password: [Empty text box]
- Receiver:**
 - To: [Empty text box]
 - CC: [Empty text box]
- Mail Server:**
 - Host Name / Address: [Empty text box]
 - Port: 25
 - ☐ SSL

Buttons at the bottom: Test, OK, Cancel.

Figure 9-5

[Scheme] Select to receive e-mail notification when the server fails to update IP to DNS or the IP has changed.

[Sender] Type the name, e-mail address, username and password of the sender.

[Receiver] Type the recipient's e-mail address(es). For multiple recipients, add a semicolon between each e-mail address.




[Mail Server] Type the host name or address of your mail server. Keep the default port 25 or modify if the mail server uses a different port. Select **SSL** if your e-mail server requires the SSL authentication for connection.

Click the **Test** button to send a test e-mail to confirm if the settings are correct.

9.2 Watermark Viewer

The GV-VMS can embed digital watermarks in video streams for the purpose of authentication. The watermarks are encrypted with digital signatures in video streams during the compression stage, ensuring that images are not edited or damaged after they are recorded. In addition, you can apply the **Watermark Proof**, a watermark-checking program included in the installation of the GV-VMS, to further verify the authenticity of the recording.

9.2.1 Activating Watermark Protection

1. To enable the watermark protection, click **Home** , select **Toolbar** , click **Configure** , select **System Configure** and click **Record Setting**.
2. In the Record Setting dialog box, select **Use Digital Watermark Protection** and click **OK**. The GV-VMS will digitally sign videos during the recording.

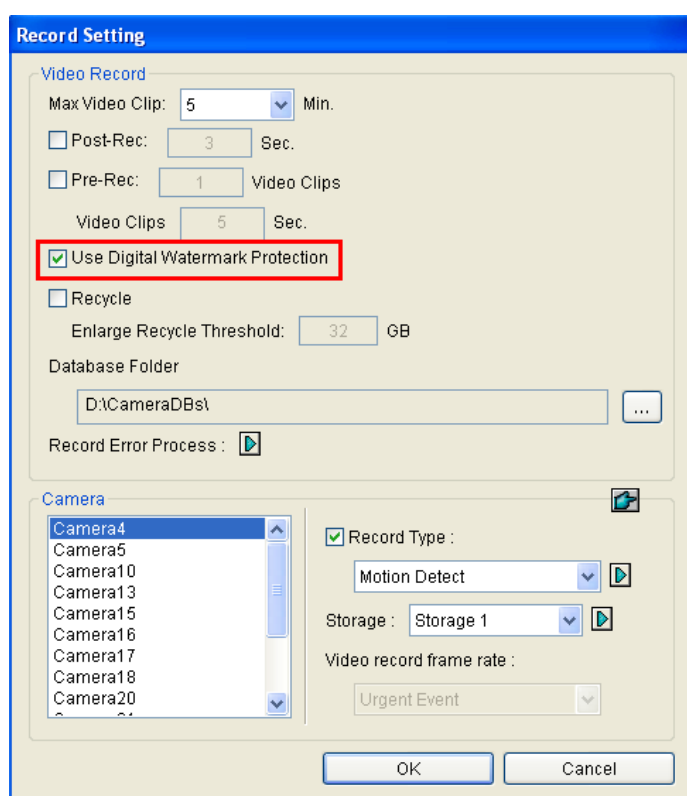


Figure 9-6

9.2.2 Running the Watermark Proof

To apply the Watermark Proof program for verifying the authenticity of the recording, follow the steps below.

1. Go to the GV-VMS folder and run **WMProof.exe**. The Watermark Proof window appears.
2. Click **File** from the menu bar, select **Open**, locate the recorded file (.avi) and click **Open**. The selected file is listed on File List (No. 9, Figure 9-7). Alternatively, you can directly drag the file from the storage folder to the window.
 - If the recording is unmodified, a check mark will appear in the **Pass** column.
 - If the recording is modified or does not contain watermark during recording, a check mark will appear in the **Failed** column.
2. To play the recording, double-click the listed file on the window.

9.2.3 The Main Window

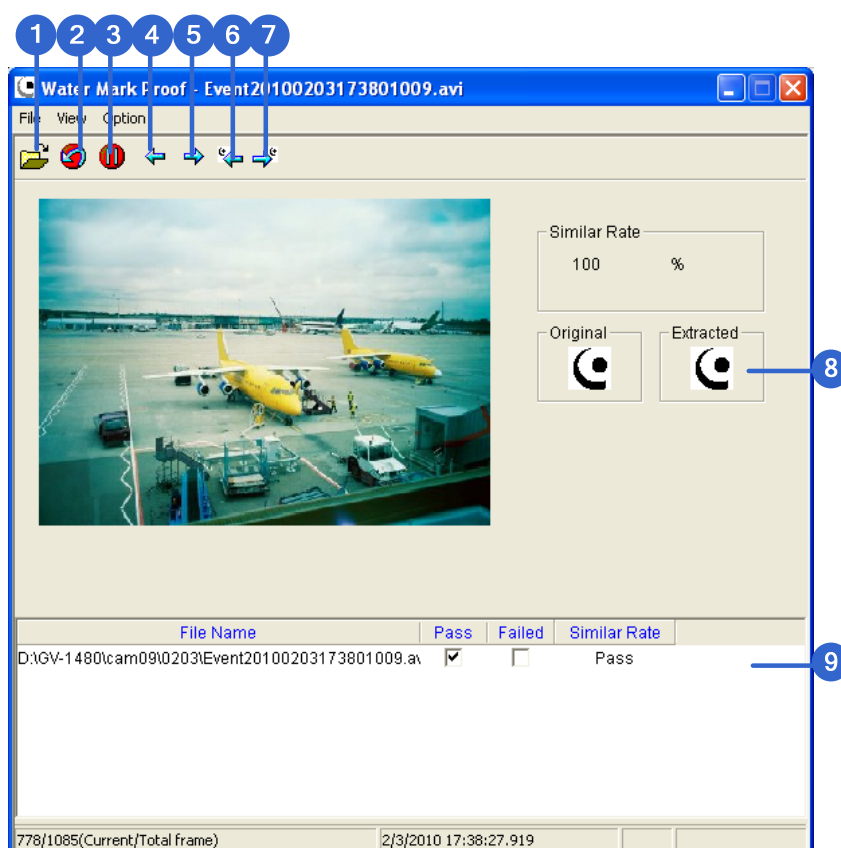


Figure 9-7

| No. | Name | Description |
|-----|--------------------------|--|
| 1 | Open File | Opens the recorded file. |
| 2 | First Frame | Goes to the first frame of the file. |
| 3 | Play | Plays the file. |
| 4 | Previous Frame | Goes to the previous frame of the file. |
| 5 | Next Frame | Goes to the next frame of the file. |
| 6 | Previous Watermark Frame | Goes to the previous frame that contains watermark. |
| 7 | Next Watermark 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. |

9.3 Windows Lockup

The GV-Desktop helps you secure your computer while away from your workstation. You may lock up the Windows desktop while launching a customized GV-Desktop. In the GV-Desktop, users are limited to run the GV-VMS and selected programs.

9.3.1 The GV-Desktop Screen

The GV-Desktop is included in the installation of GV-VMS. Go to Windows **Start**, point to **Programs**, select **GV-VMS3**, and click **Key Lock Utility**. The GV-Desktop screen appears.

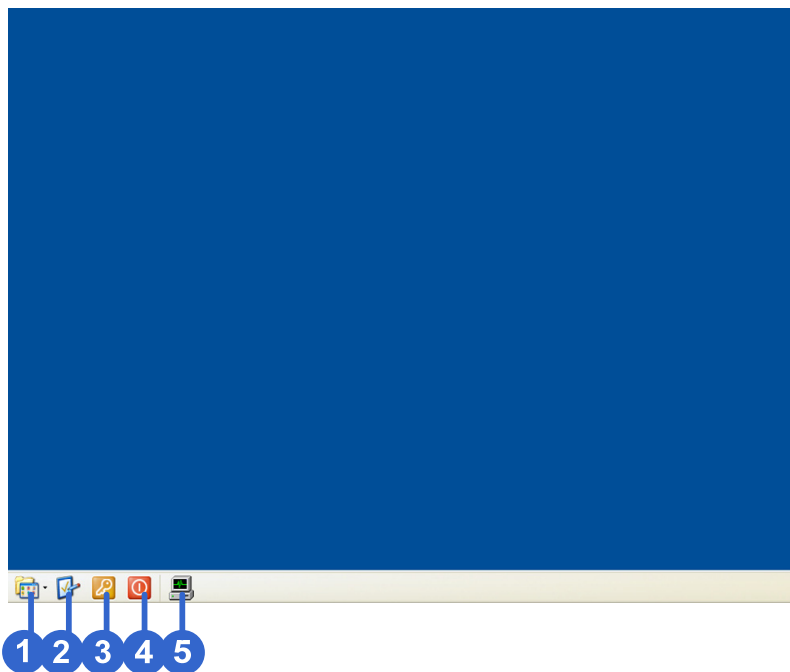


Figure 9-8

The controls in the GV-Desktop screen:

| No. | Name | Description |
|-----|--------------|---|
| 1 | Programs | Accesses programs. |
| 2 | Settings | Adds programs to the programs menu. |
| 3 | Log Off | Logs off GV-Desktop. |
| 4 | Shut Down | Shuts down the computer. |
| 5 | Task Manager | Views the tasks currently running on your computer. |

9.3.2 GV-Desktop Features

The five buttons on GV-Desktop are introduced below.

Programs

Click the **Programs** button (No.1, Figure 9-8) to see the program menu. The default programs are Video Management System (GV-VMS), Repair Database Utility, eMap Editor and Control Center Service. To add or remove new programs to the menu, see the *Settings* section later in this chapter. In the example below, Paint is a new program added to the menu.

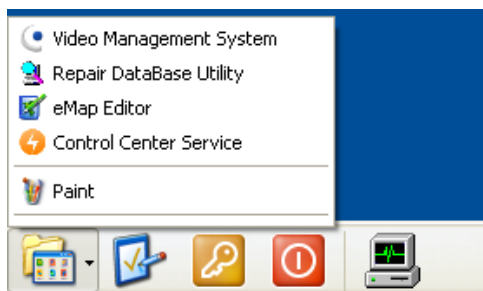


Figure 9-9

Settings

Click the **Settings** button (No.2, Figure 9-8) and type the valid ID and password. This window appears.

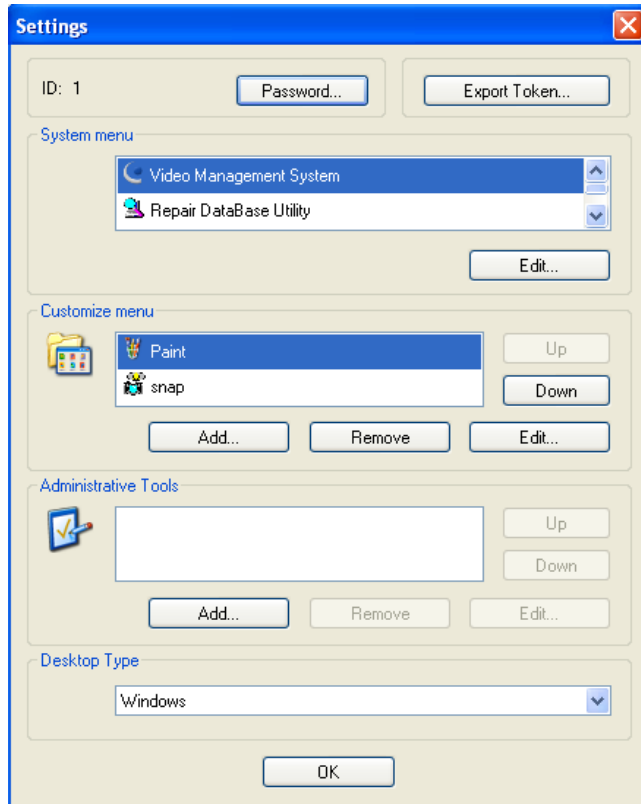


Figure 9-10

[Password] Click the button to change the password. For the **Allow Removing Password System** option, see *Account and Password* in Chapter 1.

[Export Token] This option is introduced in *Token File for Save Mode* later in this chapter.

[System Menu] Select a desired program and click the **Edit** button to change its name.

[Customize Menu] Set up the Programs menu as desired. To add a program, click the **Add** button. In the Shortcut dialog box, type the program name, click the button next to the field to assign a path and click **OK**.

[Administrative Tools] Set up the Programs menu as instructed In *Customized Menu* option. To run the added programs configured in the Administrative Tools field, the administrative ID and Password are required.

[Desktop Type] Select Windows or GV-VMS from the drop-down menu. The selected desktop will launch the next time when you log into the computer.

Log Off

Click the **Log off** button (No.3, Figure 9-8) to log off GV-Desktop. A valid ID and password are required.

Shut Down

Click the **Shut Down** button (No. 4, Figure 9-8) to shut down your computer. A valid ID and password are required.

Task Manager

Click the **Task Manager** button (No. 5, Figure 9-8) to view the programs which are currently running on your computer. When you minimize a program, it will be hidden and under operation in the background. To bring the program back to desktop, double-click the program listed in Task Manager.

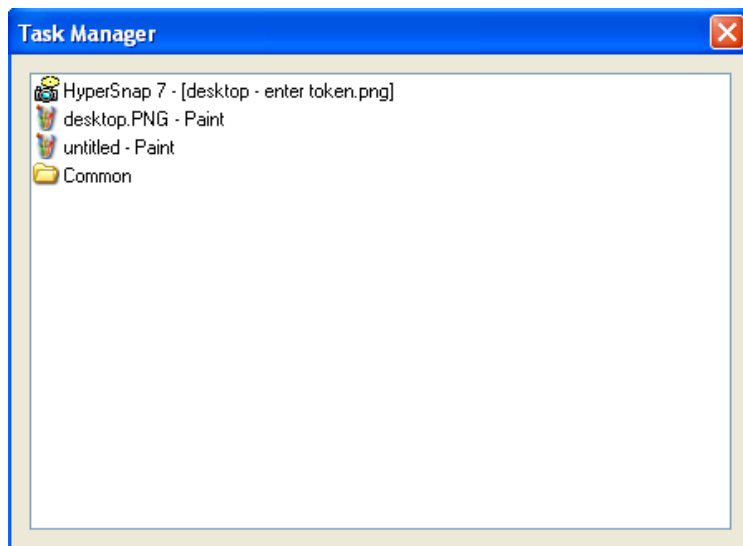


Figure 9-11

9.3.3 Token File for Safe Mode

This option in the Settings section lets you export a token file. In case you enter safe mode and are in the status of the GV-Desktop, this token file allows you to exit from the GV-Desktop and enter the Windows desktop. To export a token file, follow the steps below.

Exporting the Token File

1. Click the **Export Token** button (Figure 9-10). This dialog box appears.

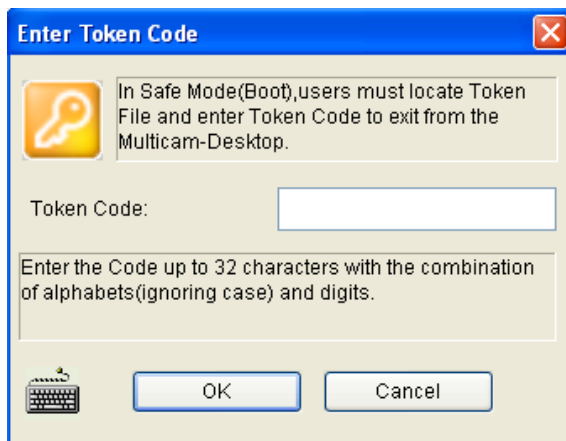


Figure 9-12

2. Type a code in the Token Code field and click **OK**.
3. In the Save As dialog box, locate a path, type a desired name in the File Name field and click **Save** to save the file.

Switching from GV-Desktop to Windows Desktop

1. Click the **Settings** button on the GV-Desktop. You will be prompted to locate the stored token file and type the configured token code.
2. When the Settings window (Figure 9-10) appears, select **Windows** in the Desktop Type field and exit from the window.
3. Click the **Log Off** button to log off the GV-Desktop and run the Windows desktop. You need to locate the stored token file and type the configured token code again.

9.4 Authentication Server

The Authentication Server is a password and account management system for multiple GV-VMS. Through the Authentication Server, the administrator can create the accounts with different access rights to a group of GV-VMS. Once any GV-VMS is connected to the Authentication Server, the previous password settings in local GV-VMS will be invalid. Local GV-VMS will submit to the full control of the Authentication Server.

Note: In addition to the GV-VMS, the Authentication Server also supports GV-System, E-Map Server and GV-Control Center V3.1.2.0 or earlier for central credential management. Up to 1000 client accounts in total can be created.


9.4.1 Installing the Server

You can install the Authentication Server from Software DVD or GeoVision Website.

Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-Authentication Server** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-Authentication Server**.

| Supplemental Utilities | |
|--|--|
| Product | |
| Content Designer (for GV-3D People Counter) | Creates a scenario for GV-3D People Counter. |
| Dbsync2 | Sends people counting data from GV-System to GV-Web Report. |
| GV-Audio Broadcast | Allows a host to speak to other hosts using the same broadcast IP address within LAN. |
| GV-Authentication Server | Manages the account and password of multiple DVR/NVR systems. |
| GV-Backup Viewer | Accesses the recordings and log data backed up at the storage system from a remote PC. |

Figure 9-13

9.4.2 The Main Window

Go to Windows **Start**, click **Programs**, select **AuthServer** and click **AuthServer**. This window appears.

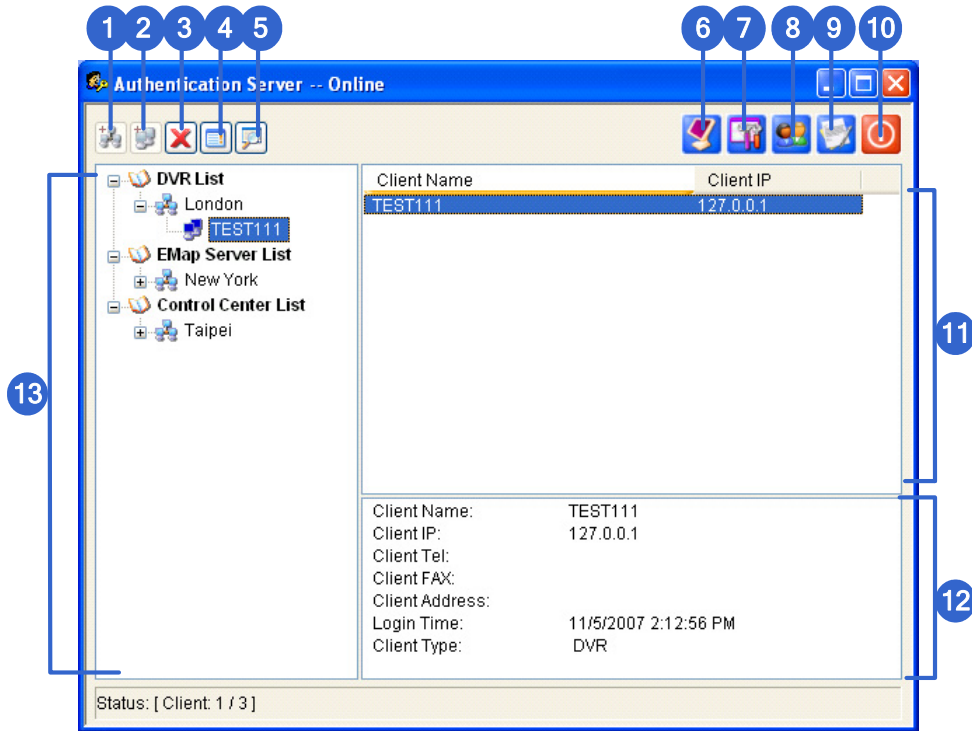


Figure 9-14

The controls in this window:

| No. | Button | Description |
|-----|-------------------------|--|
| 1 | Add An Area | Creates an Area group. |
| 2 | Add A Client | Creates a client account. |
| 3 | Delete An Area / Client | Deletes an existing group or client. |
| 4 | View/Edit A Client | Select a client from the Client List, and click to view / edit it. |
| 5 | Find A Client | Finds an existing client. |
| 6 | Start/Stop Service | Starts/Stops the Authentication Server. |
| 7 | Server Setup | Configures the Authentication Server. |
| 8 | Account Setup | Configures passwords and grants permissions to clients. Imports groups from Active Directory. |

| No. Button | | Description |
|------------|-----------------------|--|
| 9 | Log | Sets up the Authentication Server Log and opens the log browser. |
| 10 | Exit | Exits this window; Logs out Administrator; Changes Password, imports or exports account information. |
| 11 | Connected Client List | Lists the connected GV-VMS, GV-System, E-Map Server or GV-Control Center. |
| 12 | Client Information | Lists the information of the selected GV-VMS, GV-System, E-Map Server or Control Center. |
| 13 | Client List | Lists the created clients and area groups. |

9.4.3 Creating Clients

You must create and arrange the clients first which user credentials will be centrally managed by the Authentication Server. To create a list of GV-VMS clients, follow the steps below.

1. To create a GV-VMS client, highlight the **DVR List** from the left panel and click the **Add A Client** button (No. 2, Figure 9-14).

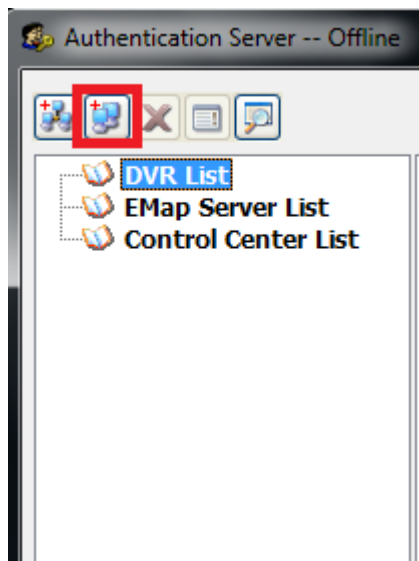
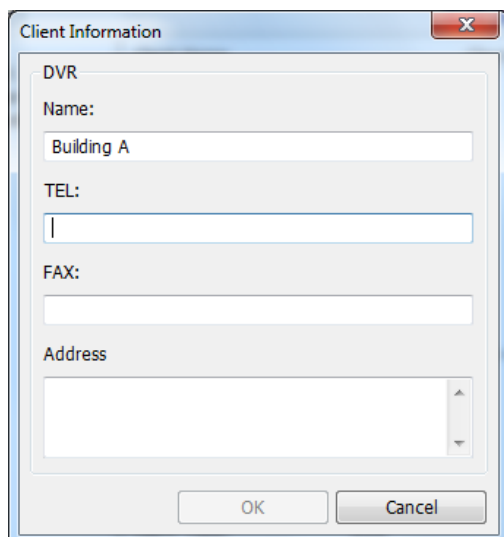


Figure 9-15

2. Type the client's information and click **OK**. The **Name** must match that of local GV-VMS.





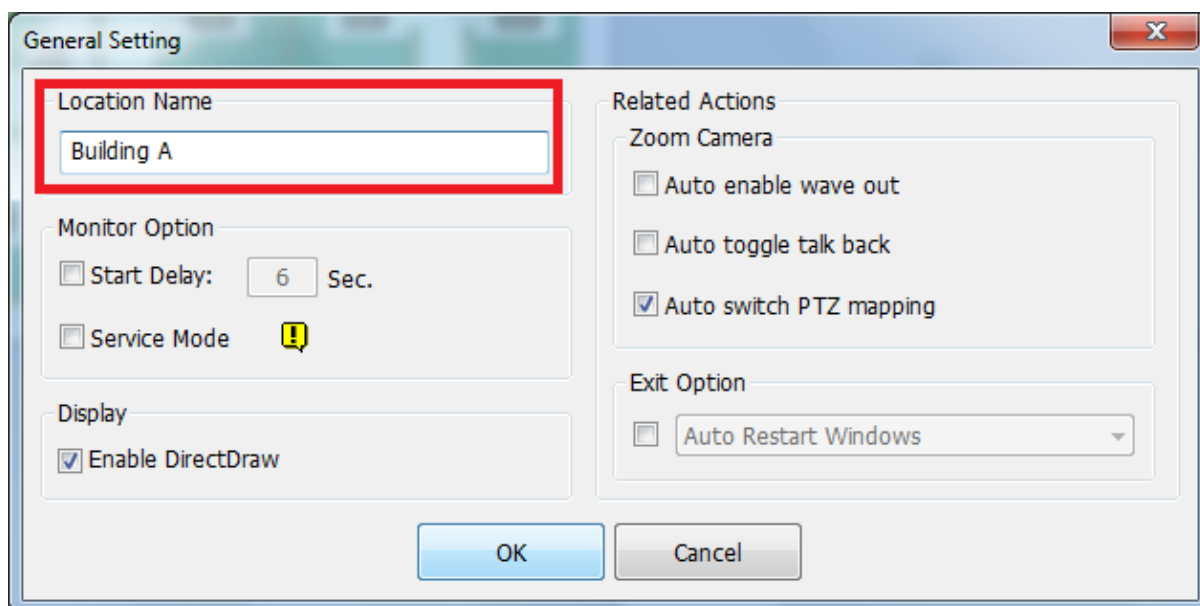
The image shows a 'Client Information' dialog box. It has a title bar with a close button (X). The dialog contains the following fields:

- DVR**: A section header.
- Name:** A text input field containing 'Building A'.
- TEL:** A text input field.
- FAX:** A text input field.
- Address**: A multi-line text area.

 At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel'.

Figure 9-16

Tip: To view the name of your GV-VMS server, select **Toolbar** , click **Configure** , select **System Configure** and click **General Setting**.



3. To create another client, repeat the steps above.
4. You can also arrange multiple clients under a group by highlighting a list and clicking the **Add An Area** button (No. 1, Figure 9-14). The created group appears under the selected List.

9.4.4 Creating User Accounts

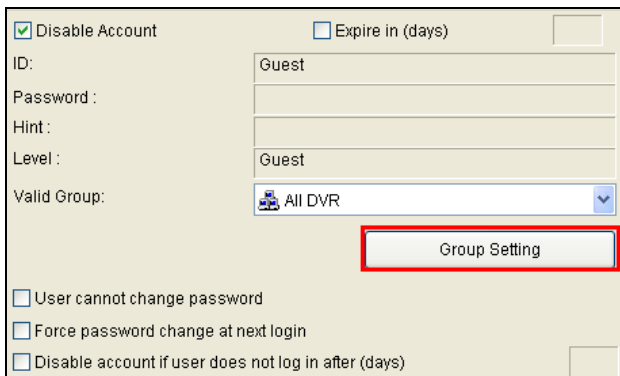
To create user accounts with different access rights and assign the user accounts to a group of GV-VMS clients, follow the steps below.

1. Click the **Account Setup** button (No.8, Figure 9-14) and select **Password Setup**. The Password Setup dialog box appears .
2. To create and edit a user account, refer to *Account and Password* in Chapter 1.

Note: The Administrator has the authority of changing the password of any accounts.

3. To assign the created user to a group of GV-VMS clients:

A. Click the **Group Setting** button.



A dialog box for user configuration. It contains the following fields and options:

- ☒ Disable Account
- ☐ Expire in (days) [text box]
- ID: [text box containing "Guest"]
- Password: [text box]
- Hint: [text box]
- Level: [text box containing "Guest"]
- Valid Group: [dropdown menu showing "All DVR"]
- Group Setting** button (highlighted with a red rectangle)
- ☐ User cannot change password
- ☐ Force password change at next login
- ☐ Disable account if user does not log in after (days) [text box]

Figure 9-17

B. In the Valid Group List window, click the **New Group** button.

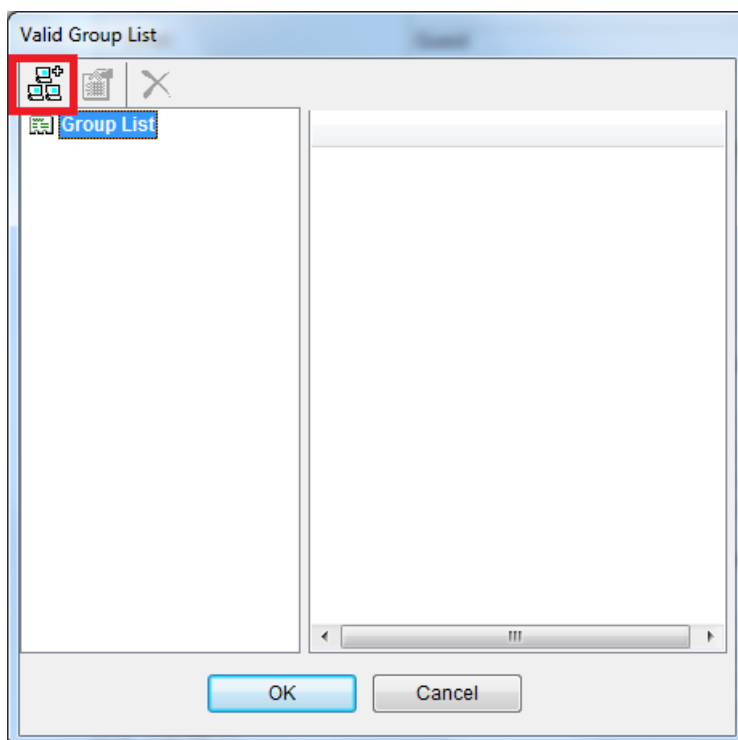


Figure 9-18

- C. In the DVR Group Information window, give a name to the group, select the desired GV-VMS clients to be added to the group. Click **OK**.

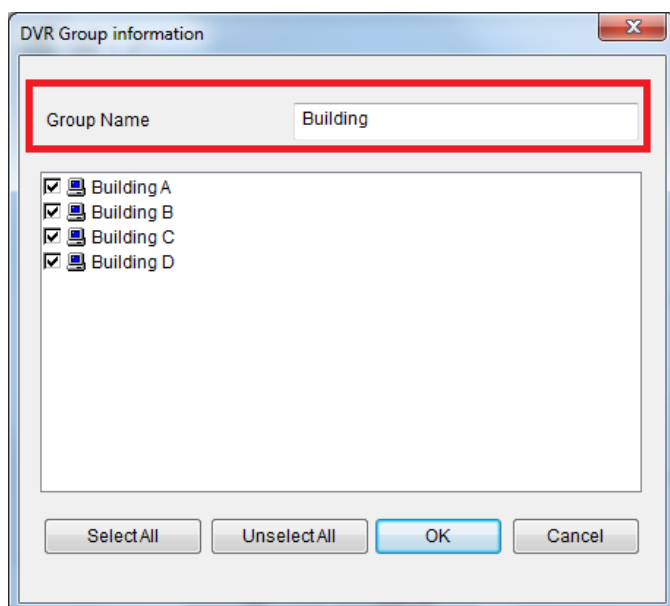


Figure 9-19

- D. Click **OK** again to go back to the Password Setup window.
- E. Use the **Valid Group** drop-down list to select the created group. The user will be able to log in the assigned GV-VMS clients.

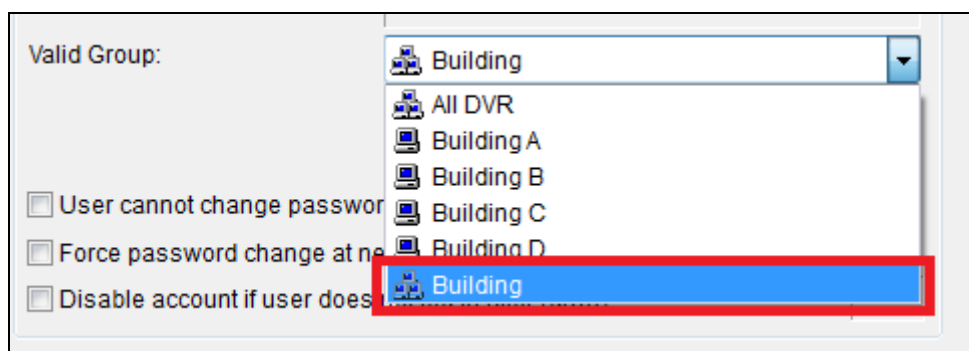


Figure 9-20

4. Optionally, you can use the following functions to arrange the user and client accounts.
 - A. Right-click a user account to have two options. The **Apply setting to** option allows you to apply the same settings to a specific user account. The **Apply setting to group** option allows you to apply the same settings to all user accounts under the same account level.

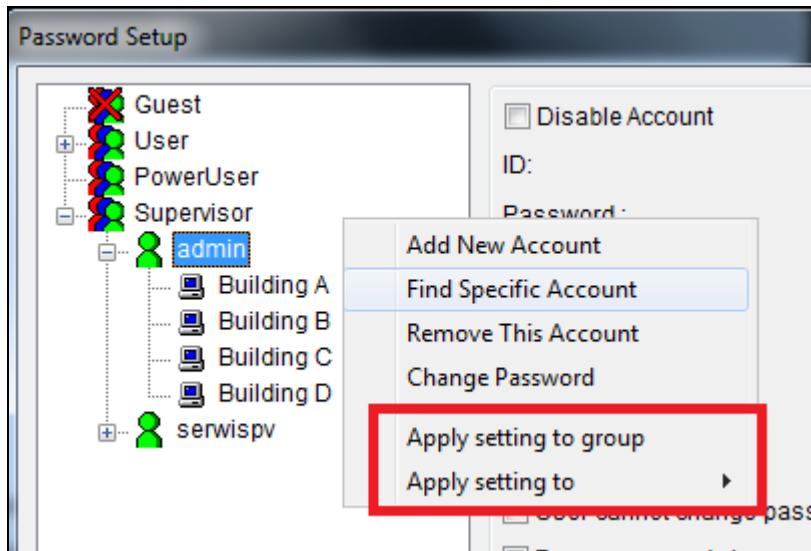


Figure 9-21

- B. Right-click a client account to have two options. The **Apply setting to other DVR(s)** option allows you to apply the same settings to all clients under the same user account. For this example, the settings of Building A client will be applied to all Building B, C and D clients. The **Copy** option allows you to copy and paste one client's settings and any client.

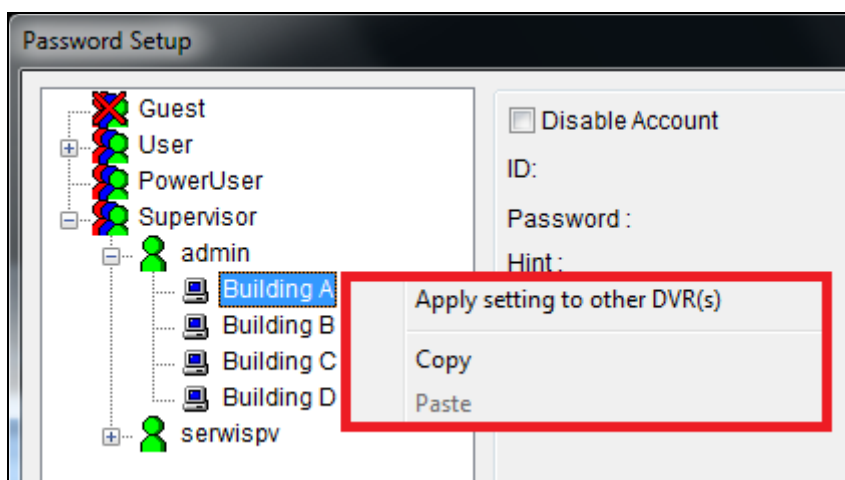


Figure 9-22

9.4.5 Importing Groups and Users from Active Directory

To create user accounts efficiently, you can import groups and users from Microsoft's Active Directory to Authentication Server. You will need to install Active Directory on Windows operating system and set up users into groups before following the steps below.

Note: User accounts in Active Directory need to be grouped into Groups settings first as only groups can be imported into Authentication Server.

1. Click the **Account Setup** button (No.8, Figure 9-14) and select **Active Directory Setup**. This page appears.

The screenshot shows a 'Configure' window with the following sections:

- Source Database:** Two radio buttons, 'Default Database' and 'Active Directory' (selected).
- Active Directory Setup:**
 - 'Server IP Address' and 'Port' (389) text boxes.
 - Two radio buttons: 'Connect with current login information' and 'Connect with administrator login information' (selected).
 - 'User Name' and 'Password' text boxes.
 - 'Test Connection' button.
- Group Mapping Setup:** 'Assign Authority Level' button.
- Auto Update Setup:**
 - 'Auto update' checkbox (checked).
 - '5' in a text box, followed by 'Minute(s)[1~9999]'.

At the bottom, a message reads: 'Please restart Authentication Server for changes to take effect.' Below this are 'OK' and 'Cancel' buttons.

Figure 9-23

2. Under Source Database, select **Active Directory** to enable the function.
3. To connect to the server with Active Directory:
 - A. Type the **Server IP Address** and the **Port** number of the server.
 - B. To log into the server using your current login information, select **Connect with the current login information**. To log into the server using the login information of its administrator, select **Connect with administrator login information** and type the user name and password.
 - C. Click **Test Connection** to see if you can connect to the server with Active Directory.

4. To assign groups in Active Directory to User, Power User or Supervisor authority levels:
 - A. Click the **Assign Authority Level** button. This dialog box appears.

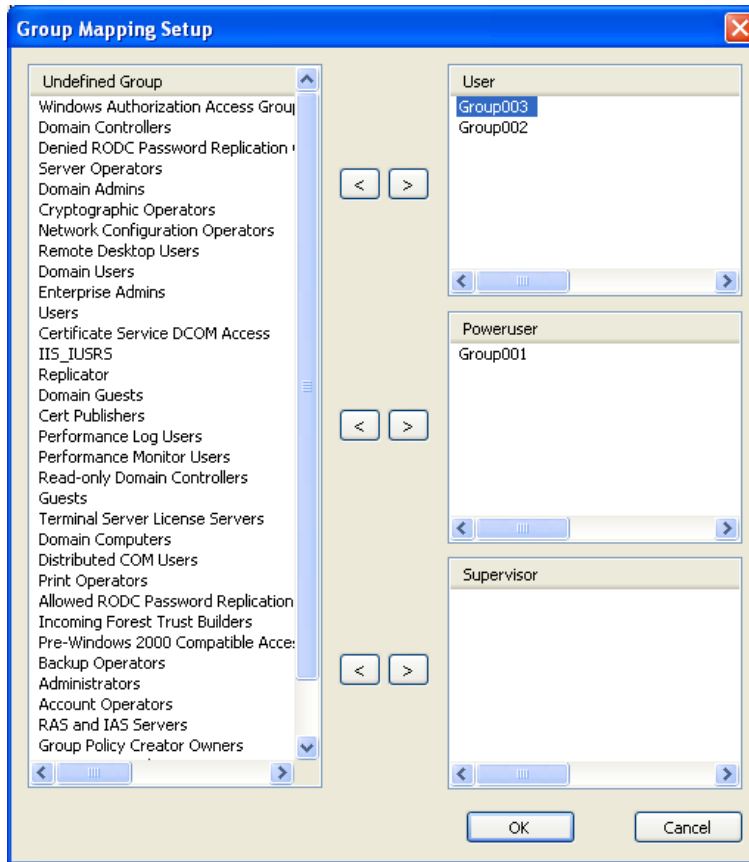




Figure 9-24

- B. Select the groups detected in Active Directory from the Undefined Group list and use the arrow buttons   to assign the groups to User, Power User or Supervisor level.
 - C. Click **OK** to import the user data into the Password Setup window.
5. To automatically update changes to user data in Active Directory, click **Auto Update** and specify the update frequency in minutes.
6. Click **OK** and restart Authentication Server to apply the settings.

9.4.6 Starting the Server

To configure the server and start the service, follow the steps below.

1. Click the **Server Setup** button (No. 7, Figure 9-14). This dialog box appears.

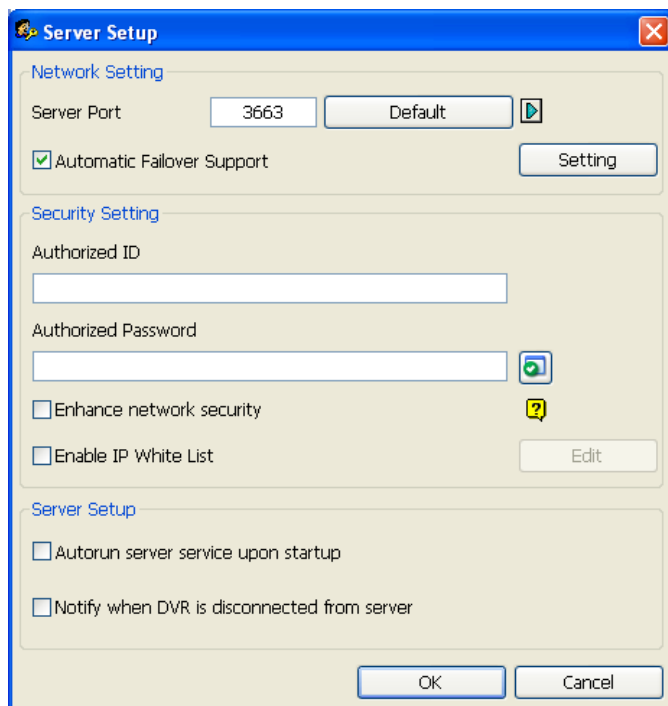


Figure 9-25

2. Under Security Setting, type the **Authorized ID** and **Authorized Password** which will be used for the client GV-VMS to log into the Authentication Server.
3. Click **OK** to apply the settings.
4. Click the **Start/Stop Service** button (No. 6, Figure 9-14) to start the services.

Optionally, you can configure the following settings before starting the Authentication Server:

[Network Setting]

- **Server Port:** The default port number is **3663**. To use UPnP for automatic port configuration to your router, click the **Arrow** button. For details, see *UPnP Settings* in Chapter 7.

- **Automatic Failover Support:** Select and click the **Setting** button to configure up to 2 Authentication Servers in case the primary Authentication Server fails. Once the primary server fails, the second or the third server will take over the connection from clients and provide uninterrupted services. Note the settings of Authorized ID and Authorized Password on the failover server must match those of the primary server.

Tip: To set up the failover Authentication Server, you can export the current settings by using the **Export Account** and **Import Account** functions in the **Exit** button.

Note: Once the primary Authentication Server is ready to resume the services, it is required to close the failover Authentication Server so the connection from clients can move back to the primary.

[Security Setting]

- **Enhance network security:** Strengthen network security on Authentication Server.
- **Enable IP White List:** Click **Edit** to create a list of IP addresses only which are allowed to establish connection with Authentication Server.

[Server Setting]

- **Auto run server service upon startup:** Allow the server to automatically start service upon Windows startup.
- **Notify when DVR is disconnected from server:** Notify the Authentication Server with a pop-up window when the GV-VMS is disconnected with the Authentication Server.

9.4.7 Connecting GV-VMS to the Server

To configure the GV-VMS in order to access the Authentication Server remotely through a network connection, follow the steps below.

1. On the main screen of GV-VMS, click **User** 1, select **Password Setup** and click **Remote Authentication Setup**. The Setup Remote Authentication Server dialog box appears.

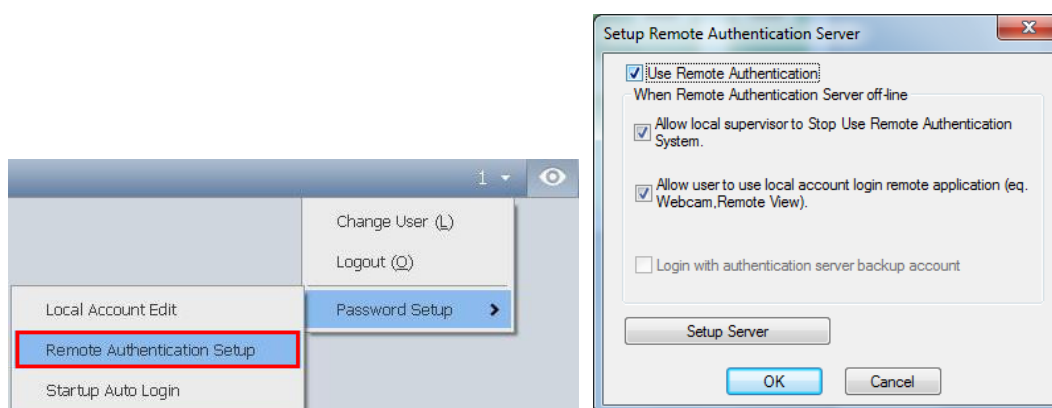


Figure 9-26

2. Select **Use Remote Authentication** and select any of the following options.

[When Remote Authentication Server Off-line]

- **Allow local supervisor to stop use Remote Authentication System:** Allow the local supervisor to stop the Authentication application when the connection with the Authentication Server fails. Note if the option is disabled and the connection with the Authentication Server fails, the local supervisor will not be able to log into the GV-VMS, and the dialog box will not be accessible until the connection resumes.
- **Allow user to use local account login remote application:** Allow local users to access remote applications with their previous password and ID settings when the connection with the Authentication Server fails.
- **Login with authentication server backup account:** Keep using password settings created on the Authentication Server even though the connection with the server fails.

3. Click **Setup Server**. This dialog box appears.

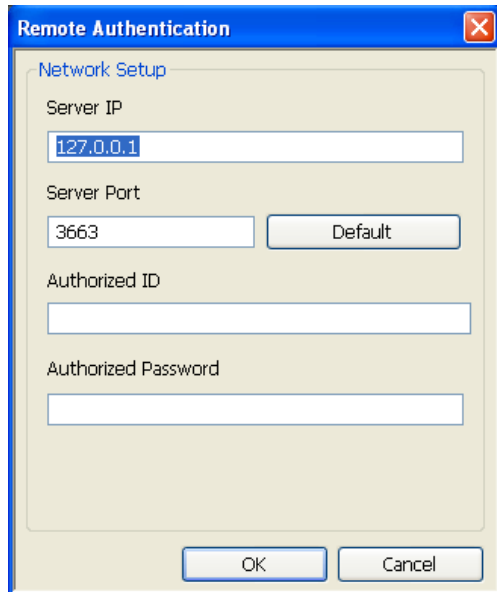


Figure 9-27



4. Type the IP address and port of the Authentication Server.
5. Type the **Authorized ID** and **Authorized Password** of the Authentication Server.
6. Click **OK** to start the connection. When the connection is established, the previous password settings in the GV-VMS will be invalid.
7. Press **[L]** on the keyboard to call up the Login dialog box. The icon  indicates that the connection is established.



Figure 9-28

As long as the Authentication Server is working, every time when you start the GV-VMS, the Login dialog box will appear. Type the user account created on the Authentication Server to log into the GV-VMS.

Note: The disconnection icon  will appear on the Login dialog box (Figure 9-28) when one of the following situations occurs:

1. The login ID and Password do not match any of the user IDs and Passwords created on the Authentication Server.
 2. The client name (Figure 9-16) does not match the location name of GV-VMS.
 3. The network connection encounters traffic problem.
-

9.4.8 Remote Access from Control Center and Remote E-Map

The Authentication Server allows you to restrict users of E-Map Server and GV-Control Center to access specific GV-VMS hosts and cameras only. Instead of connecting to GV-VMS hosts directly, the user of E-Map Server and Control Center will connect to the Authentication Server using the user account you created on the Authentication Server.

You must first set up remote authentication on E-Map Server and GV-Control Center. After the E-Map Server and GV-Control Center are connected to the Authentication Server, the user will be prompted to log in with the user ID and password you created on the Authentication Server. Once the user logs in, a list of GV-VMS hosts authorized to the user account will be displayed, and the user will be able to view the assigned cameras.

Setting up Authentication Server

You need to create and arrange E-Map Servers and Control Servers under their separate lists on the Authentication Server window (Figure 9-14).

1. In the Client List field, click the E-Map Server List or Control Center List and click the **Add A Client** button (No. 2, Figure 9-14). The Client Information dialog box appears.
2. Type the name and information of the E-Map Server or Control Center. The name does not need to match the location name of the E-Map Server or Control Center.
3. Click **OK** to add the E-Map Server or Control Center.

Accessing from E-Map Server

The E-Map Server can access the user account setting of the Authentication Server.

1. Run the **E-Map Server**. For details, see *E-Map Sever* in Chapter 8.

- In the E-Map Server window, click **Tools** on the menu bar, and select **Options**. This dialog box appears.

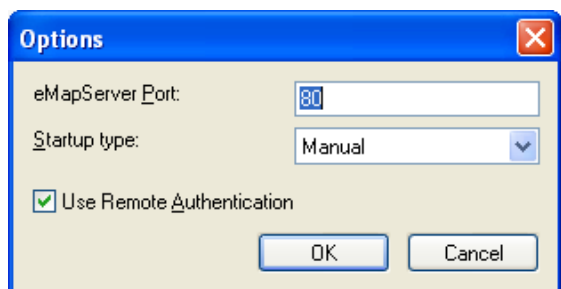


Figure 9-29

- Select **Use Remote Authentication**.
- To enable the Authentication Server service to start automatically at Windows startup, select **Automatic**. Keep the E-Map Server Port **80** as default or modify if necessary.
- Click **OK** to apply the settings.
- In the E-Map Server window, click **Tools** on the menu bar and select **Remote Authentication**. This dialog box appears.

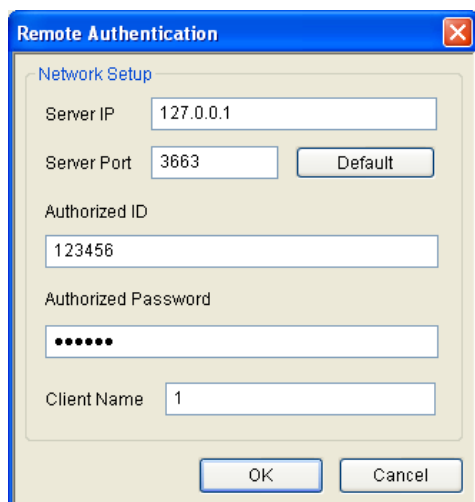


Figure 9-30

- Type the IP address, authorized ID and authorized password of the Authentication Server, as well as the E-Map Server's client name created on the Authentication Server, and then click **OK**.
- In the E-Map Server window, click **Tools** on the menu bar and select **Start Service** to start the E-Map Server.
- When you log into the E-Map Server, type the user ID and password created on the Authentication Server. A list of assigned GV-VMS clients to the user will be displayed.

Accessing from GV-Control Center

The GV-Control Center can access account settings of the Authentication Server.

Note: The Authentication Server only supports GV-Control Center V3.1.2.0 or earlier.

1. Run the **GV-Control Center**. For details, see *GV-Control Center User's Manual*.
2. On the Host List, right-click **Host List by ID** and select **Remote Authentication Setup**. A dialog box appears (Figure 11-27).
3. Type the IP address, authorized ID and authorized password of the Authentication Server, as well as Control Center's client name created on the Authentication Server, and then click **OK** to enable connecting to the Authentication Server.
4. To access the Authentication Server account settings, on the Host List, right-click **Host List by ID** and select **Get Host List by ID**. A dialog box prompts you for ID and password.
5. Type a user ID and password created on the Authentication Server, and click **OK**. A list of assigned GV-VMS hosts to the user will be displayed.

9.5 Fast Backup and Restore

With the Fast Backup and Restore (FBR) solution, you can change interface skin and customize features to suit personal preference, as well as back up and restore your configurations in GV-VMS.

9.5.1 Running the FBR Program

The Fast Backup & Restore program is included in the installation of GV-VMS. Go to Windows **Start**, point to **Programs**, select **GV-VMS**, and click **Fast Backup & Restore Main System**. You will be prompted to enter a valid ID and Password of GV-VMS, and then this window will appear.

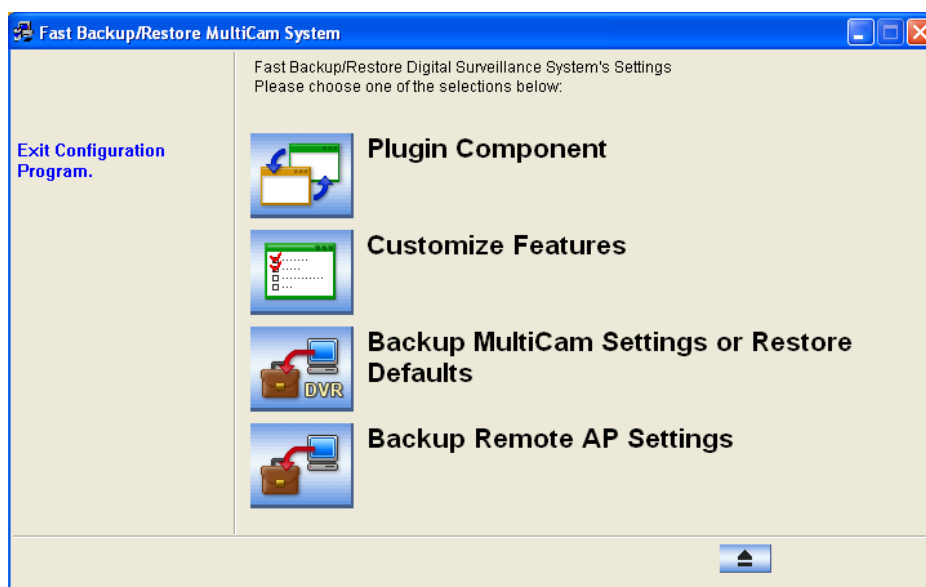


Figure 9-31

9.5.2 Plugin Component

You can add programs to your GV-VMS to expand the applications. To add programs, follow the steps below.

1. In the FBR window (Figure 9-31), click the **Plugin Component** icon. The User Define dialog box appears.

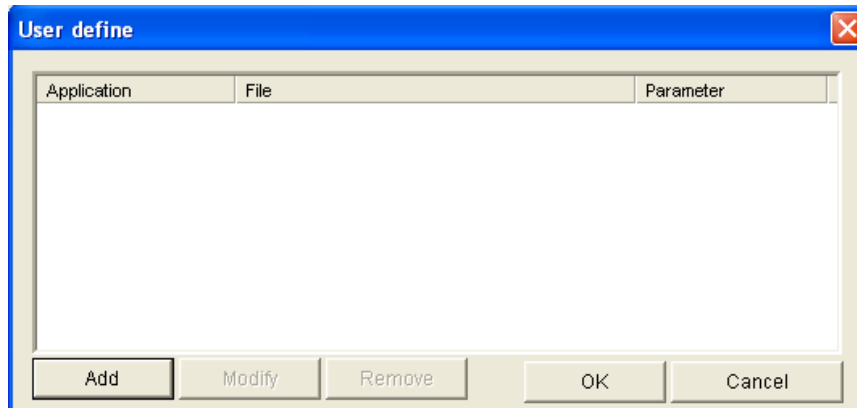


Figure 9-32

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

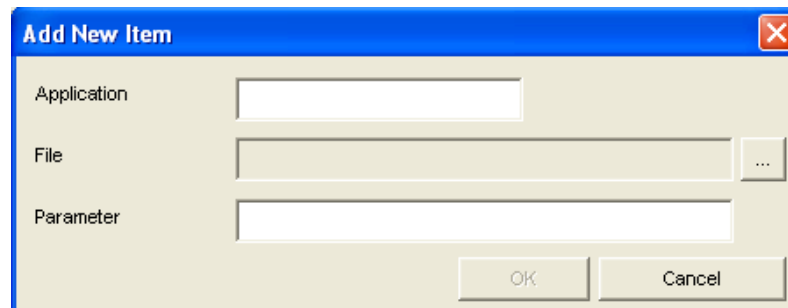





Figure 9-33

Note: For some applications, type **/FBR** in the Parameter column if necessary.

3. Type the name of the desired application, locate its path and click **OK**.
4. To add more applications, repeat steps 1 to 3 and click **OK** in the User Define dialog box.
5. To access the added applications, run the GV-VMS, click **Home** , select **Toolbar** , click **Tools** , point to **Plugin** and select desired application.

9.5.3 Customizing the Features

Not every feature may be of equal interest to you. You can specify which features are to be displayed at system startup.

1. In the FBR Window (Figure 9-31), click **Customize Features**. This dialog box appears.

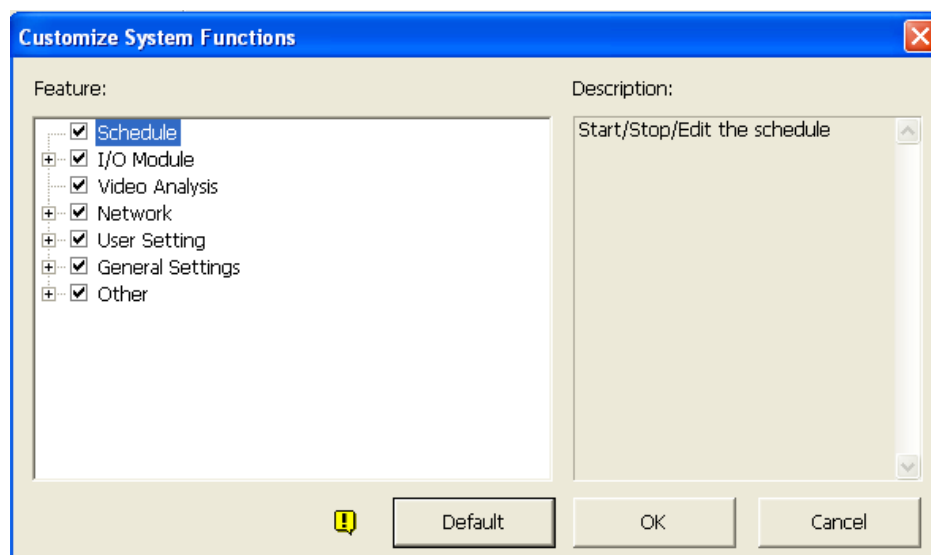


Figure 9-34

2. Expand the folder(s) and click the function(s) you want to disable in the GV-VMS.
3. Click **OK** to save the settings.

Note: You need to restart the GV-VMS to activate the settings.

9.5.4 Backing up and Restoring Settings

You can back up the configurations you made in the GV-VMS, and restore the backup data to the current system or import it to another GV-VMS.

Backing up the settings

1. In the FBR window (Figure 9-31), click the **Backup MultiCam Settings or Restore Defaults** icon, and select **Backup Current System**. This dialog box appears.

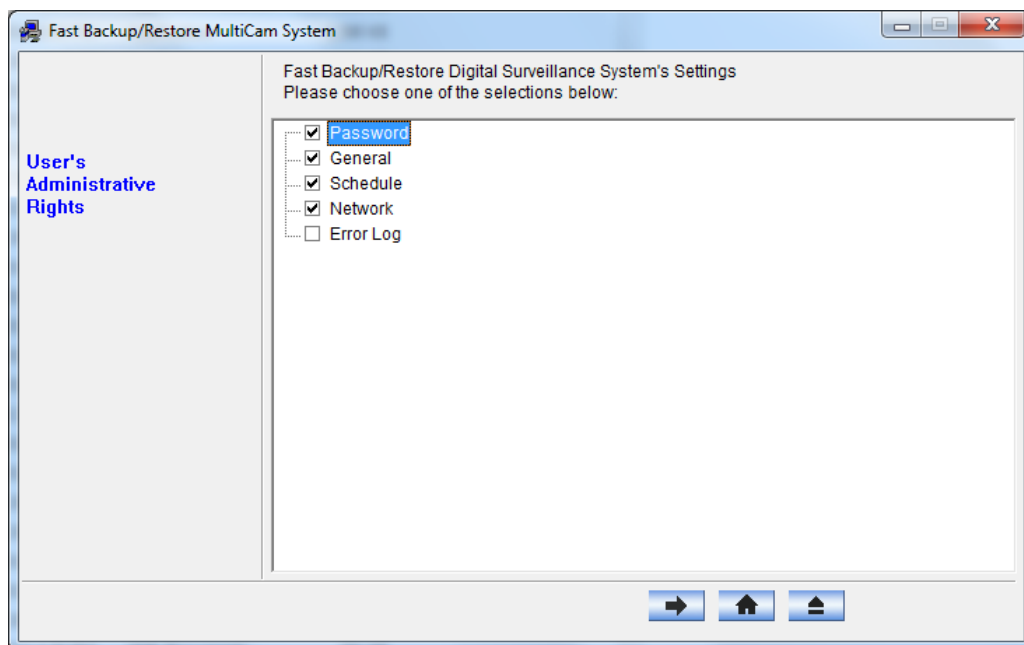



Figure 9-35

2. Select which settings you want to back up and click the **Next Step** button .
3. In the Save As dialog box, select the destination to store the backup file. When the backup is complete, the “Successfully Backup MultiCam System Settings” message will appear:

Restoring the System

You can restore the current system with the backup of configuration file. Also, you can copy this backup file to configure another system with the same settings as the current system.

1. Open the backup file (*.exe) you previously stored. A valid ID and password are required to display this window.

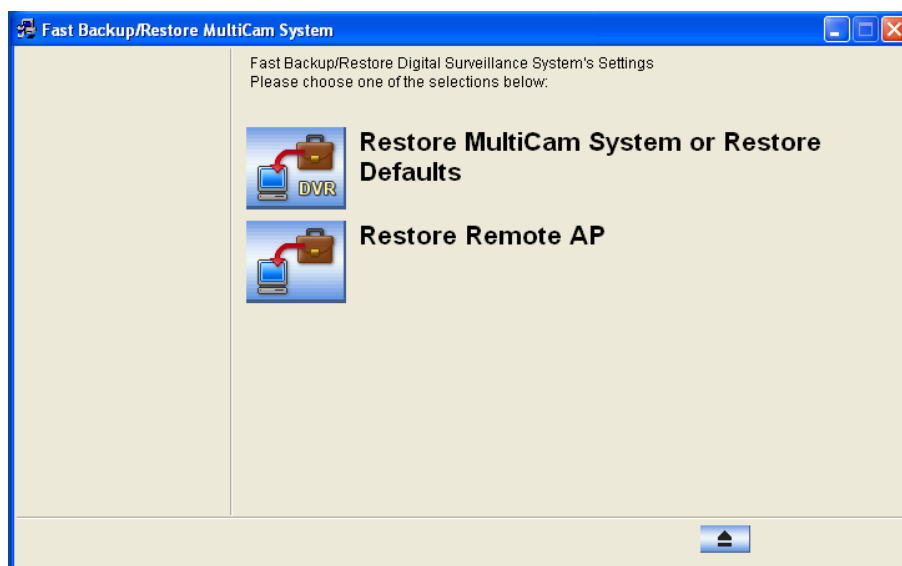



Figure 9-36

2. Click the **Restore Multicam System** icon and then select which backup settings you want to restore.
3. Click the **Next Step** button  to start restoring.
4. When the restoration is complete, the “Successfully Restore MultiCam System Settings” message will appear.

Restoring Defaults

To restore the system default, click the **Backup MultiCam Settings or Restore Defaults** icon (Figure 9-36), select **Restore Defaults** and follow the on-screen instructions to complete the process.

9.6 Bandwidth Control Application

The Bandwidth Control is an independent application that controls and monitors the network traffic of the WebCam servers. Its features include:

- Manage up to 5 GV-VMS systems
- Get bandwidth usages of every Webcam server and every user
- Set bandwidth thresholds for specific users and IP addresses
- IP black and white list
- Kick unwanted users


9.6.1 Installing the Bandwidth Control

You can install the Bandwidth Control program from Software DVD or GeoVision Website.

Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-Bandwidth Control Client Site** and follow the on-screen instructions.

Downloading from GeoVision Website

1. On the computer you want to install the Bandwidth Control program, go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-Bandwidth Control Client Site**.

9.6.2 The Main Window

After the installation is complete, double-click the **Bandwidth Remote Control** icon created on the desktop. The Bandwidth Control window appears.

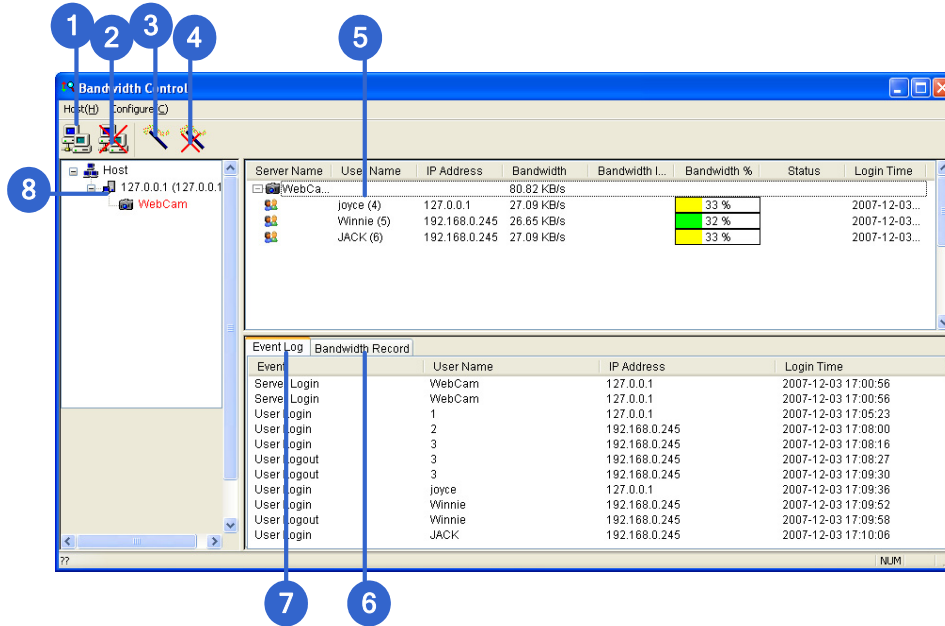


Figure 9-37

| No. | Name | Description |
|-----|------------------|---|
| 1 | Connection | Builds the connection to a WebCam server. |
| 2 | Disconnect | Stops the connection to a WebCam server. |
| 3 | Get Control | Obtains the right to remotely control the WebCam servers. |
| 4 | Give Up Control | Ceases controlling the WebCam servers and users. |
| 5 | User List | Displays the connected users and their status |
| 6 | Bandwidth Record | Displays the network traffic in graph display. |
| 7 | Event Log | Records activities of WebCam servers and users. |
| 8 | Host List | Displays all WebCam servers to be connected. |

9.6.3 Allowing Remote Control

The network traffic of WebCam server can be controlled when the GV-VMS permits the remote control from the Bandwidth Control program by the following steps:

1. On the main screen of GV-VMS, click **Home** , select **Toolbar** , click **Configure** , select **Network**  and click **WebCam Server**. This dialog box appears.

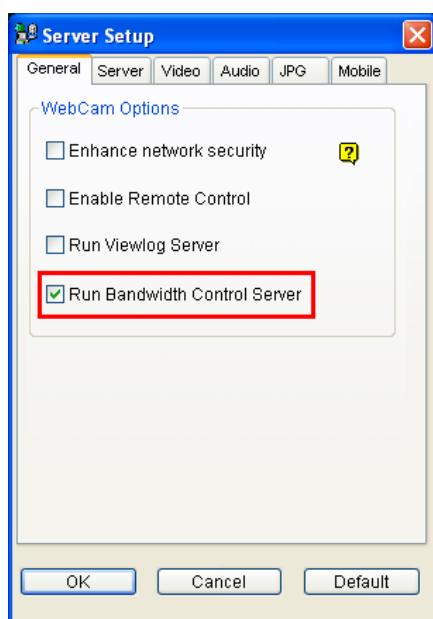


Figure 9-38

2. Under the **General** tab, select **Run Bandwidth Control server**. After this option is enabled, on the Control Center Server option list, the **Bandwidth Control Service** is marked with a check.

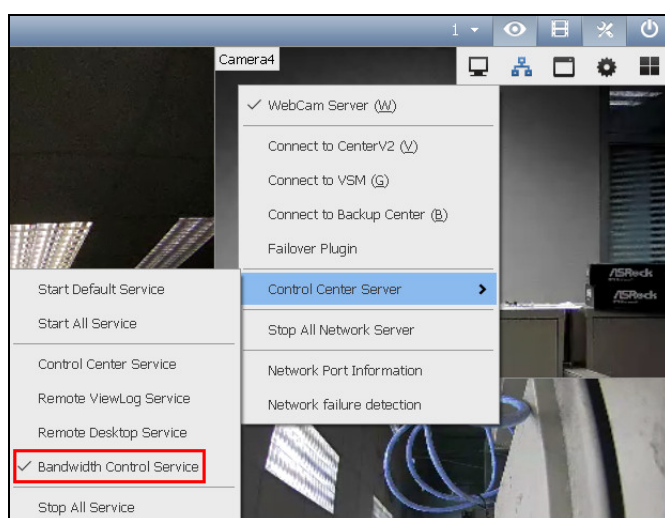


Figure 9-39

9.6.4 Connecting to a WebCam Server

1. Click **Host** on the menu bar, and select **Connection**. Or you can click the **Connection** button (No. 1, Figure 9-37) on the toolbar. This dialog box appears.

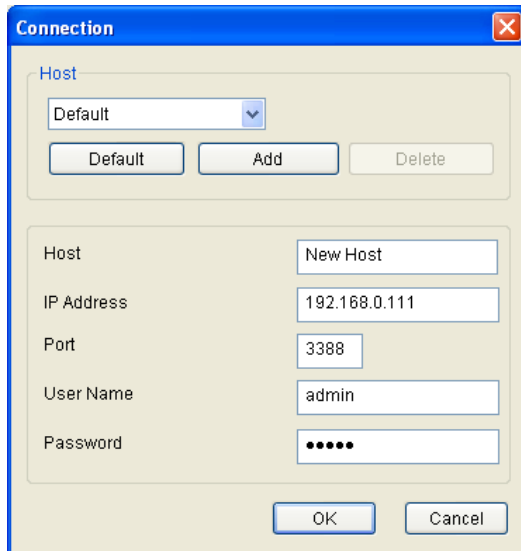


Figure 9-40

2. To add a WebCam server to be connected to, click **Add**.
3. Type the host name, IP address, user name and password of the WebCam server. Modify the port if necessary.
4. Click **OK**. After the connection is established, the WebCam server shows up in the Host List.
5. You can add up to 10 WebCam servers by repeating above steps.
6. To stop the connection, select the host and click the **Disconnect** button (No. 2, Figure 9-37). The host will be deleted from the host list.
7. Up to 5 users of the Bandwidth Control programs can connect to a single WebCam server for network traffic monitoring. However, only one user has the access to bandwidth settings. When this user clicks the **Give Up Control** button (No. 4, Figure 9-37), the user no longer controls the WebCam server. Whoever clicks the **Get Control** button (No. 3, Figure 9-37) first has access to bandwidth settings. For bandwidth settings, see *Controlling a WebCam Server* later in this chapter.

9.6.5 Controlling Specific WebCam Server

To disconnect a login user or set the bandwidth limit for a specific user, right-click the user to have the options below:

| Server Na... | User Name | IP Address | Bandwidth | Bandwidt... | Bandwidt... | Status | Login Time |
|--------------|-----------|------------|------------|-------------|-------------|--------|--------------|
| WebC... | | | 736.00 B/s | | | | |
| | Joyce (4) | 192.1... | | | 50 % | | 2021-04-1... |
| | Peter (5) | 192.1... | | | 50 % | | 2021-04-1... |

Figure 9-41

- **Kick:** Disconnect the user from the WebCam server.
- **Block IP:** Prohibit the user from connecting to the WebCam server. To use the function, the **Enable IP Black List** option (Figure 9-44) must be selected first.
- **Bandwidth Setup:** Select **By Username** to specify a bandwidth limit for the user, or select **By IP** to limit the bandwidth used by the IP address. This setup dialog box will appear. In this example, an IP address is selected for bandwidth limit setup. Select **Bandwidth Setup**, specify a bandwidth limit and click **OK**.

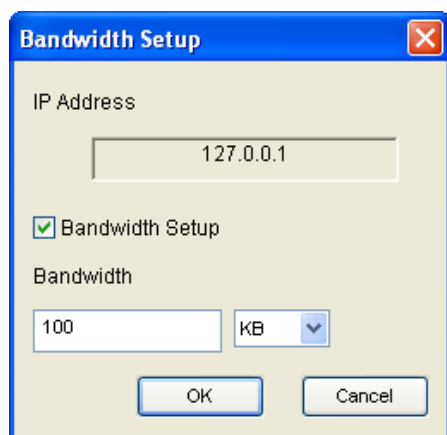


Figure 9-42

9.6.6 Setting up the Bandwidth

You can manage the bandwidth of multiple hosts allocated to a WebCam server by specifying certain users and IP addresses when your network is busy or heavily loaded.

1. Click **Configure** on the menu bar and select **Bandwidth Setup**.
2. In the Bandwidth Setup dialog box, select the desired WebCam server and click **OK**. This dialog box appears.

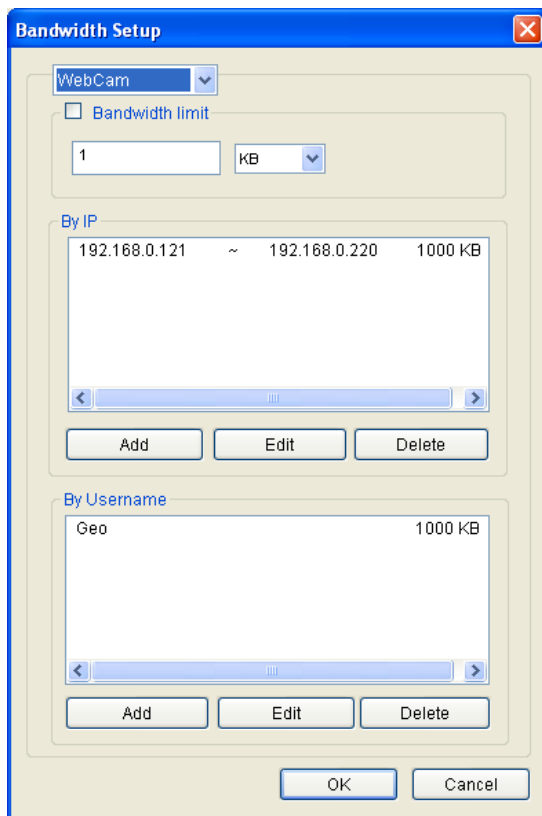


Figure 9-43

- **Bandwidth limit:** Select this option and define the total bandwidth that the WebCam server will be allowed to use on your network.
- **By IP:** Click **Add** and specify a IP address or a range of IP addresses and its bandwidth limit.
- **By Username:** Click **Add** and specify the user name and its bandwidth limit.

Note: If you have already specified the total bandwidth to a WebCam server, it is prioritized before the bandwidth limits set to user names and IP addresses.

9.6.7 Block List Setup

Two types of block lists are provided to restrict the access to a WebCam server: permitting and denying a specified range of IP address to establish the connection. Note that only one type of block list can be used at a time.

1. Click **Configure** on the menu bar and select **IP White / Black List Setup**. A dialog box prompts for you to select a host.
2. In the IP White / Black List Setup dialog box, select the desired WebCam server and click **OK**. This dialog box appears.

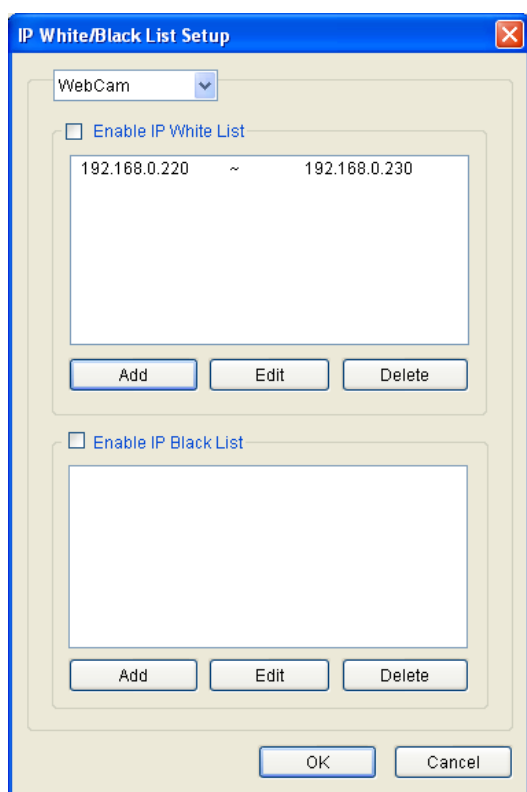


Figure 9-44

3. Select a desired type of block list and click **Add** to define the IP addresses.
 - **Enable IP White list:** Allow the defined range of IP addresses to establish the connection to the WebCam Server.
 - **Enable IP Black list:** Prohibit the defined range of IP addresses from establishing the connection to the WebCam Server.
4. Click **OK** to apply the settings.

9.6.8 General Setup

You can set up sound alarm for user log-in, or change the real-time graph display of network traffic. Click **Configure** on the menu bar and select **General Setup**. This dialog box appears.

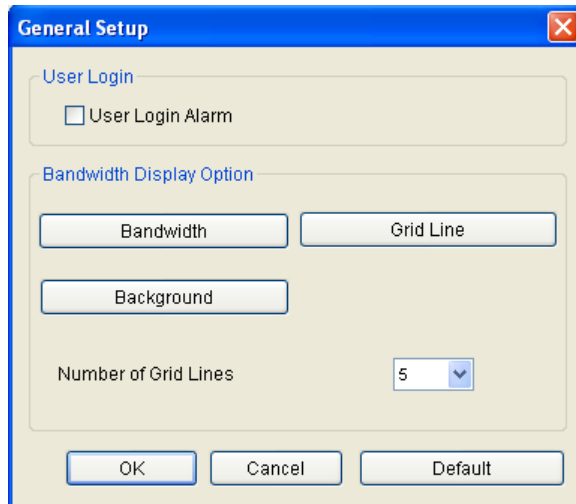


Figure 9-45

- **User Login Alarm:** Enable the computer alarm on when a user logs in.
- **Bandwidth:** Set the color of bandwidth wave.
- **Grid Line:** Set the color of grid lines of the graph.
- **Background:** Set the background color of the graph.
- **Number of Grid Line:** Set up the number of grid lines to be displayed on the graph.

Click **OK** to apply the settings. To set the bandwidth display at default, click **Default**.

When you click the Bandwidth Record tab in the Bandwidth Control window, you can view the network traffic in graph.

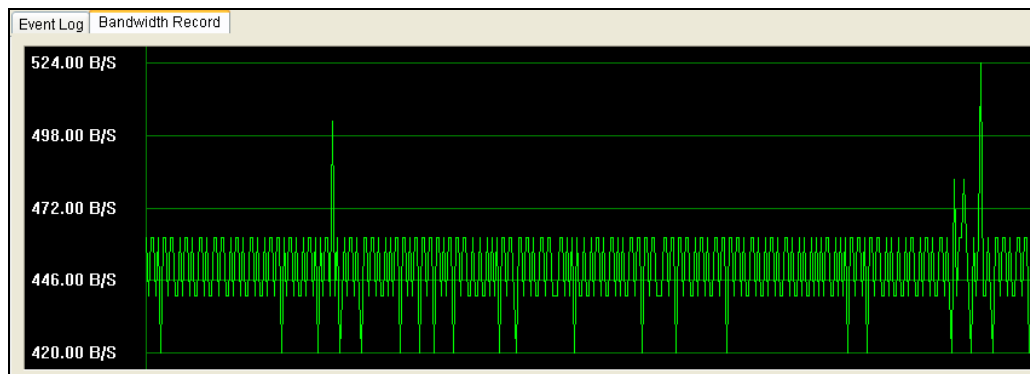


Figure 9-46

9.7 Language Setting

The user interface has been translated from English into 30 other languages. If you find the translation to be unsuitable and would like to correct it, you can use the **MultiLang Tool** to revise the translation. Next, you can apply the revised text to the applications and export a **MRevise.exe** file to make the same revision on another computer. You can also send the revision back to GeoVision to have the revision included in future software release.


9.7.1 Installing the MultiLang Tool

You can install the MultiLang Tool from Software DVD or GeoVision Website.

Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-MultiLang Tool** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-MultiLang Tool**.

9.7.2 Revising the Translated Text

Revising the Translated Text

1. After completing the installation, close all GeoVision applications, go to Windows **Start**, find **programs** and click **MultilingualConfig**. This dialog box appears.

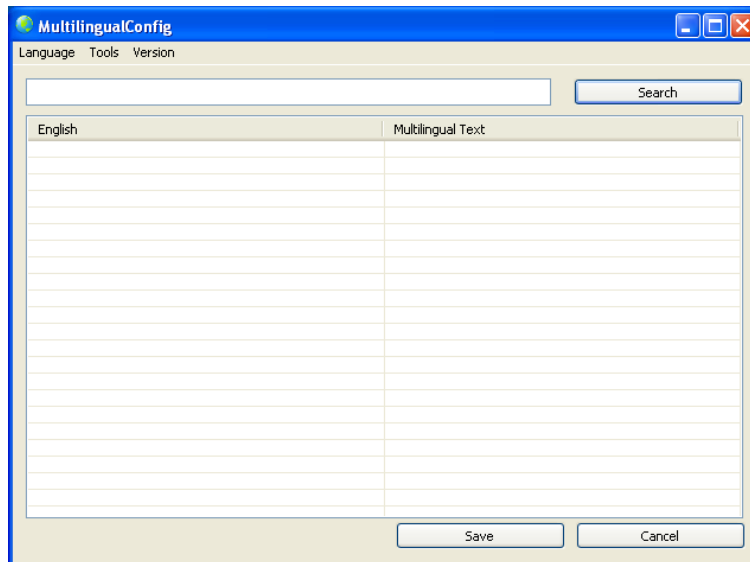


Figure 9-47

2. Click **Language** and select the language of the text you want to revise.
3. Click **Version** to select the version of the GV-VMS that you want to revise.

4. In the **Search** field, type all or part of the text in English or the target language and click **Search**. The results are displayed.

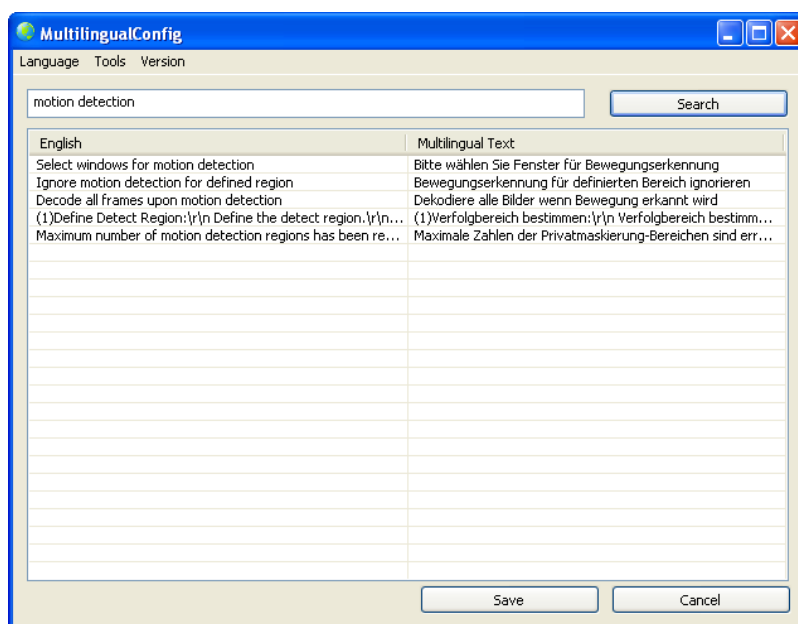


Figure 9-48

Note: The search is case sensitive.

5. Double-click the text you want to revise. This dialog box appears.

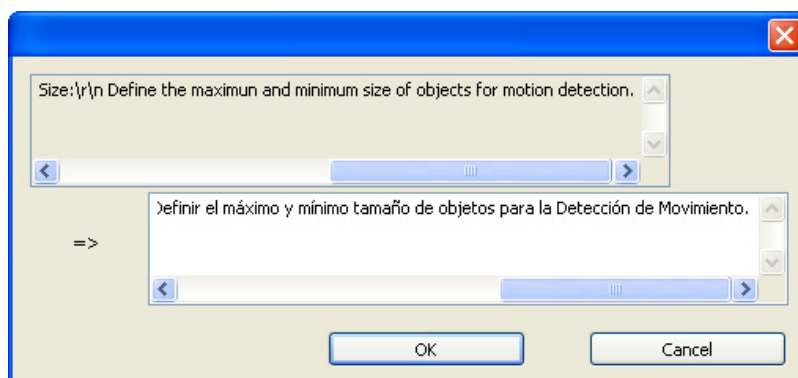


Figure 9-49

6. Revise the translated text and click **OK**.

Note:

1. It is recommended to revise an entire sentence at a time instead of simply searching a single word and replacing the word in all other strings.
 2. The text may contain symbols such as **%d** or **\n** that instruct the application to perform certain functions. Be careful not to change the symbols in the translated text.
 3. Before making any revision, click **Tools** and select **Revision Note** to read the revision instructions.
-

Applying the Revised Text

1. To apply the revised translation to the applications, click **Save**. This dialog box appears.

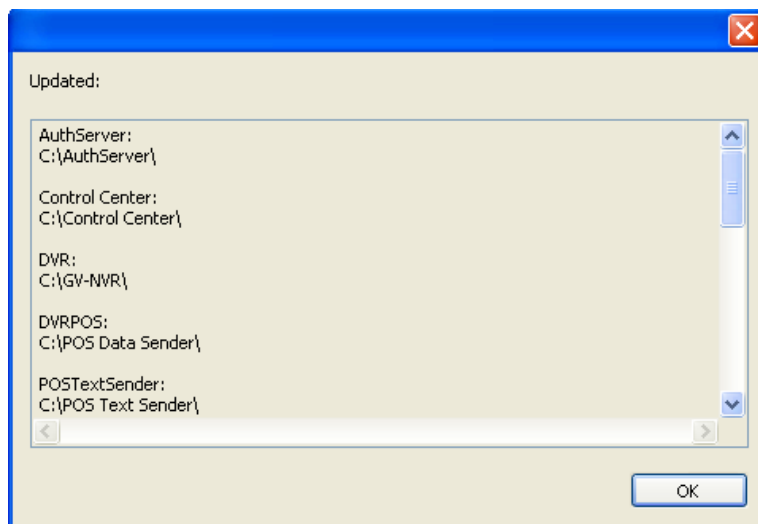


Figure 9-50

Note: The system will automatically locate the corresponding files on your computer and replace with the revised translation for the following applications: GV-VMS, Authentication Server, Bandwidth Control Client Site, Center V2, Dispatch Server, Fast Backup and Restore (FBR), GV-IP Device Utility, MCamCtrl Utility, Remote E-Map and Remote ViewLog.

2. Click **OK**. The message “Do you want to apply the revised multilingual texts to another folder?” appears. If the storage path for the application has been changed or if the associated application is not listed in the dialog box, click **Yes** and select the folder of the application.

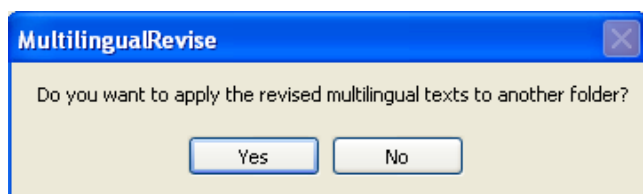


Figure 9-51

Exporting the Revised Text

1. To export the revision as an executable file, click **Tools**, select **Export** and click **Export executable file**. You can copy the .exe file to another computer and apply the same translation revision by running the .exe file.
2. To report the translation revision back to GeoVision:
 - If your default mail client is Outlook, Outlook Express or Mozilla Thunderbird, click **Tools**, **Export** and **Send Report** to send the revision.
 - If your default mail client is not set up or supported, click **Tools**, **Export** and **Export text file**, and email the exported text file to gvlocalize@geovision.com.tw.
3. For the distributors to duplicate Software DVD with the translation revision,
 - Copy and paste all the contents of Software DVD to your computer.
 - Export the revised translation file and rename the file as **MRevise.exe**.
 - Move **MRevise.exe** to the location you saved the contents of Software DVD :**\Software\Translation Revision**.
 - Duplicate the Software DVD with the **MRevise.exe** file.
 - Test the Software DVD by clicking **10. Import Translation Revision** from the Install Program window to apply the translation revision.

9.7.3 Setting Up the UI Language to English

The default user interface (UI) language of the following GeoVision software and applications is set according to the region detected. You can install the **Set Language** tool to set the UI language to English.


- GV-VMS
- GV-Fast Backup and Restore Multicam System
- ViewLog
- GV-Remote ViewLog
- GV-IP Device Utility
- GV-Center V2
- GV-Dispatch Server
- GV-Control Center
- GV-Remote E-Map

You can install the Set Language tool from Software DVD or GeoVision Website.

Downloading from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-SetLanguage** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-Set Language**.
3. After completing the installation, close all Geovision software or applications.
4. Go to Windows **Start**, find **Programs** and select **SetLanguage**.

5. In the Configure window, select **English** from the Language drop-down list.

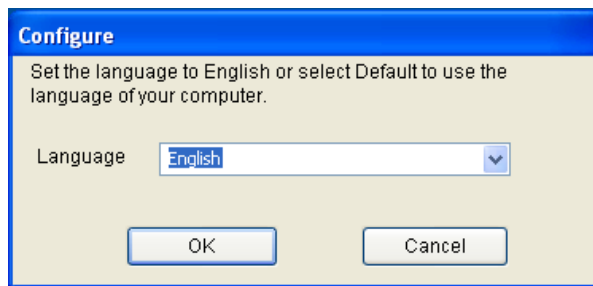


Figure 9-52

6. Click **OK** and restart your GeoVision software or application to enable the English UI.

9.8 Skype Video Utility

The GeoVision Skype Video Utility allows you to receive live view or text notifications through a Skype account using a PC or mobile device upon motion detection or input trigger. You will need to install Skype on the computer of the GV-VMS, and the notifications can be sent to other Skype accounts.

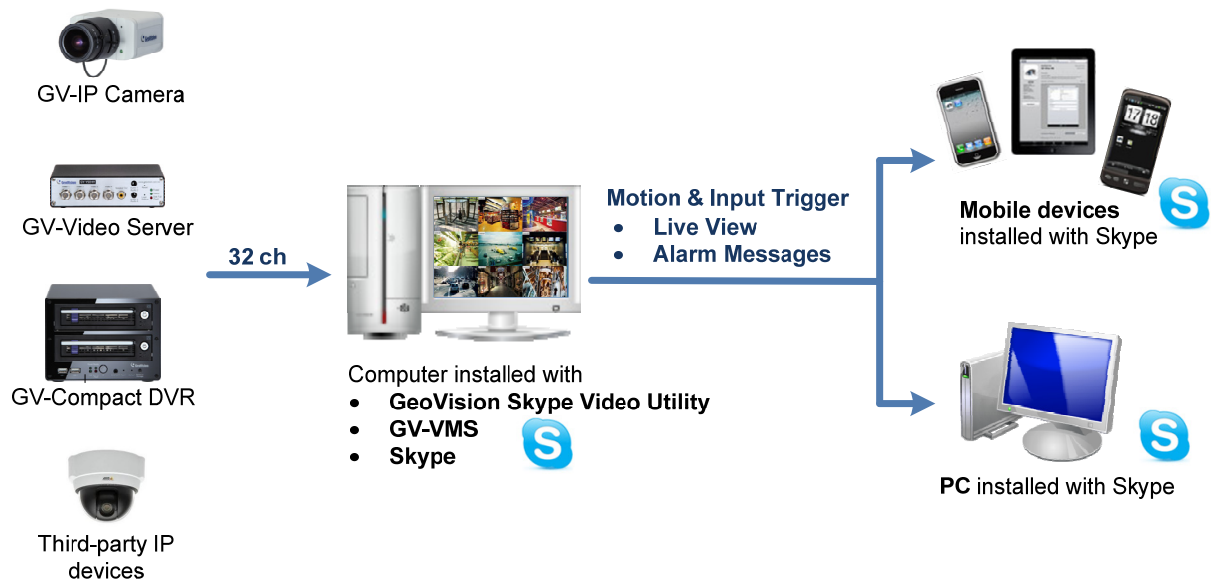


Figure 9-53

Note: Audio function is not supported in GV-Skype Video Utility.


9.8.1 Installing GV-Skype Video Utility

You can install the GV-Skype Video Utility from Software DVD or GeoVision Website.

Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-Skype Video Utility** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-Skype Video Utility**.

Note: Before running the utility, make sure you have logged in your Skype account and GV-VMS.

3. To run the utility, double-click the **GV-Skype Video Utility.exe** icon on the desktop. After connecting with Skype successfully, the GV-Skype Video Utility minimizes itself to system tray.



9.8.2 Setting Up Notifications Upon Motion or I/O Trigger

General Setting

1. Right-click the **GV-Skype Video Utility** icon in the system tray and click **Settings**. This dialog box appears.

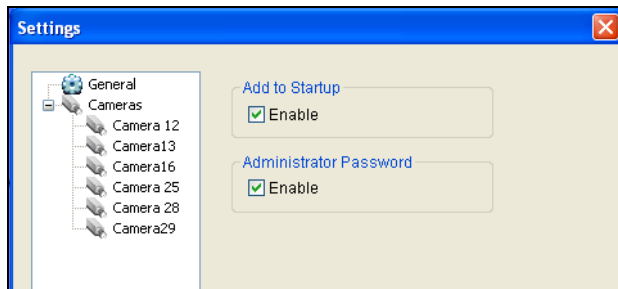


Figure 9-54

2. The General setting page offers the following options:
 - **Add to Startup:** Click **Enable** to automatically run GV-Skype Video Utility at Windows startup.
 - **Administrator Password:** Click **Enable** to require password to log in and out of GV-Skype Video Utility.

Camera Setting

To send camera live view or notification message to Skype accounts upon motion detection, expand the Cameras list and select a camera. This dialog box appears.

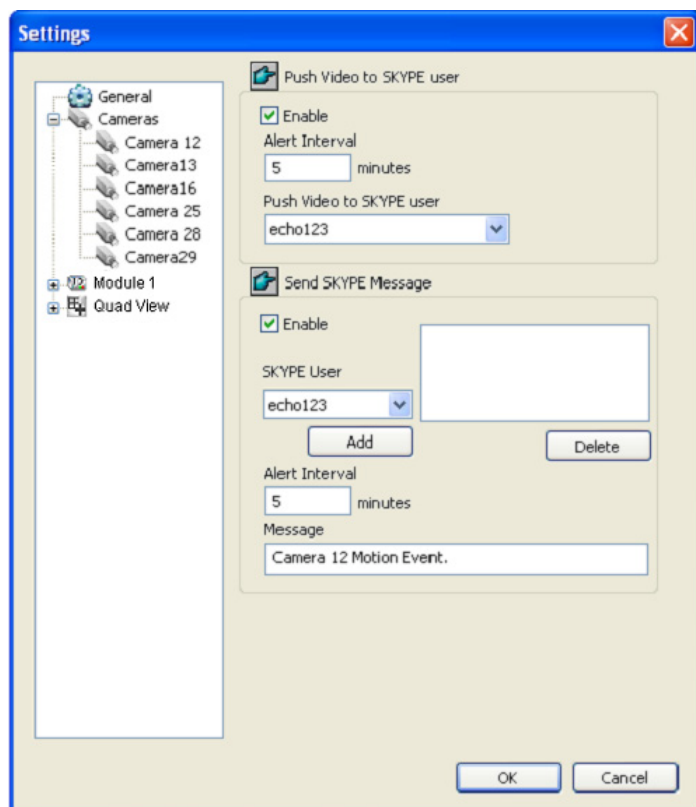


Figure 9-55

To Send the Live View

You can send live view from the selected camera or quad view to a Skype account upon motion.

1. Select **Enable** under Push Video to Skype User.
2. Set an **Alert Interval** to specify the minimum time between each notification.
3. Select a desired camera or a quad view from the **Push Camera** drop-down list. (See *To Create a Quad View* in this chapter later.)
4. Use the **Push Video to SKYPE user** drop-down list to select a Skype user to send live view.

Note:

1. GV-Skype Video Utility can only send camera live view to one Skype account at a time.
 2. The received camera live view will be displayed in Skype's default resolution.
-

To Create the Quad View

1. Click **Quad View** and select a quad view. This dialog box appears.

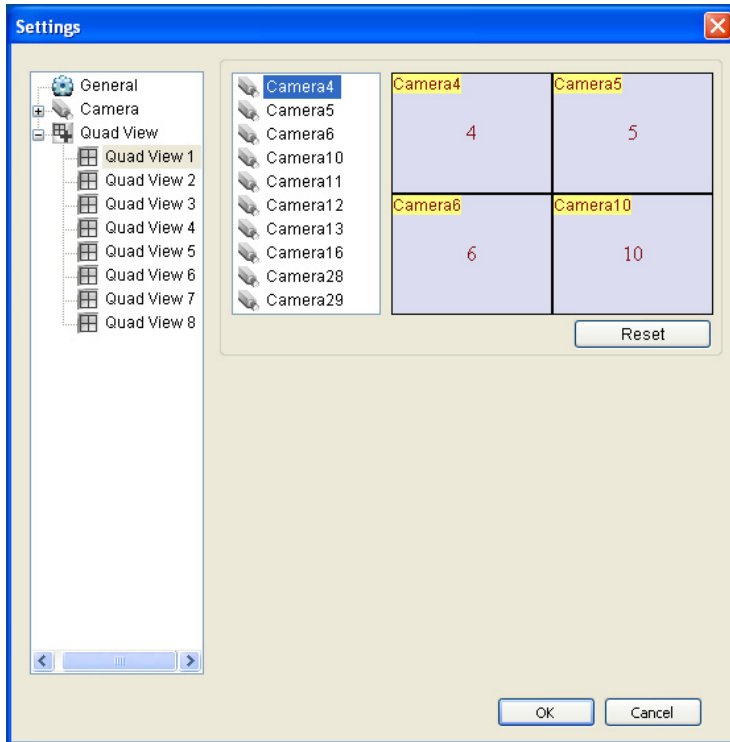


Figure 9-56

2. Drag and drop up to four cameras to the quad view on the right.
3. Click **OK**.

To Send a Notification Message

You can send notifications to multiple Skype accounts upon motion.

1. Select **Enable** under Send Skype Message (Figure 9-55).
2. Use the **Skype User** drop-down list to select the recipient of the message and click the **Add** button. Repeat for any additional recipient.
3. Set an **Alert Interval** to specify the minimum time between each notification.
4. Type a notification message up to 255 characters.

Input Module Setting

To send camera live view or notification message to Skype accounts upon input trigger, expand the **Module** list and select an input device. This dialog box appears.

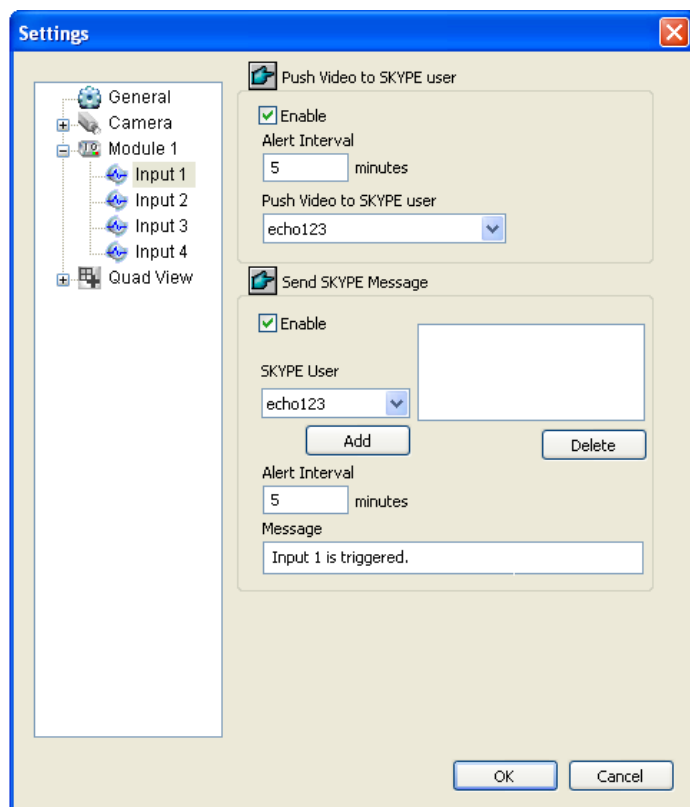


Figure 9-57

1. To send live view to a Skype account of a camera upon input trigger, follow the steps from *To Send the Live View* in the previous *Camera Setting* section.
2. To send a notification message to multiple Skype accounts upon input trigger, follow the steps from *To Send a Notification Messages* in the previous *Camera Setting* section.
3. Click **OK** to apply the setting.

Note: You can back up the settings on the utility by using Fast Backup and Restore. See *Fast Backup and Restore* earlier in this chapter.

Receiving Notification Messages and Live View

After setup is completed, upon motion detection or input trigger, the designated Skype user will see a notification message, as well as an incoming call to receive live view.

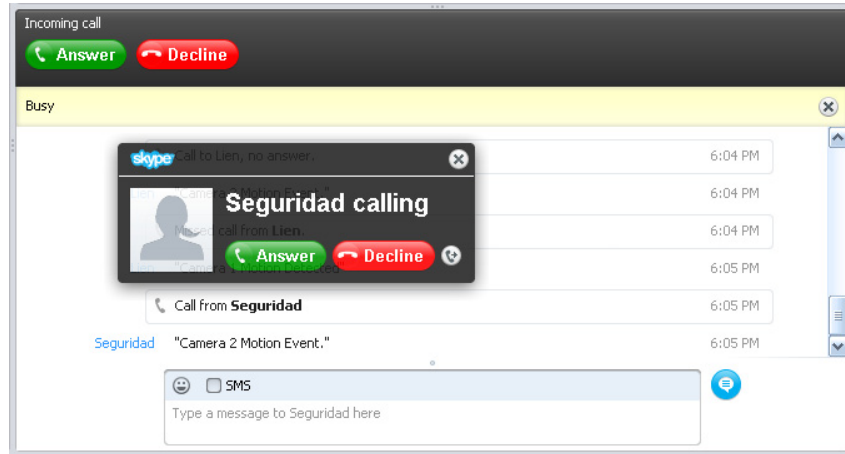


Figure 9-58

Click the **Answer** button to receive camera live view. When you finish watching the live view, click the red phone button to end the video call.

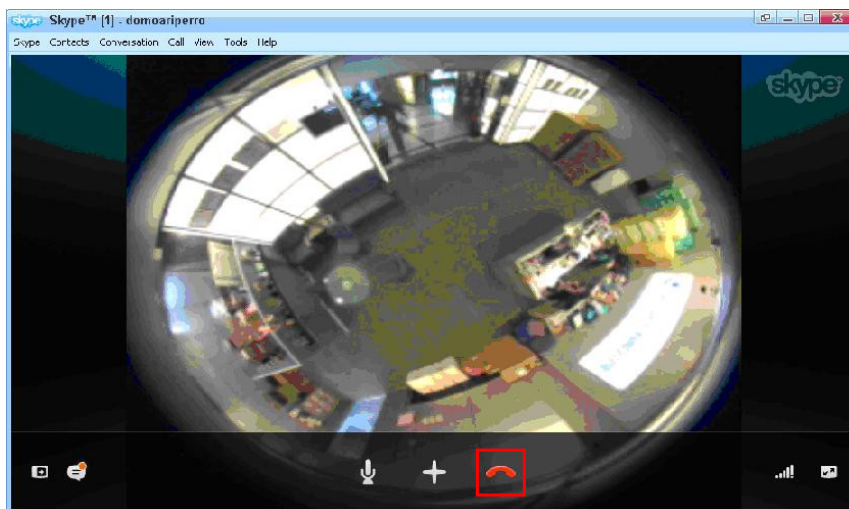



Figure 9-59

Note: If the incoming call is not picked up, the Skype user will see a missed call record in the call history.

9.8.3 Requesting Live View

1. Log in your Skype and select the Skype account of the GV-Skype Video Utility from the Contacts list.
2. Click the **IM** button  and type **Cam 1** to view the channel 1 or type other channel numbers. To view single channel live view, type channels 1 to 32. To view one of the 8 quad views, use channels 33 to 40.

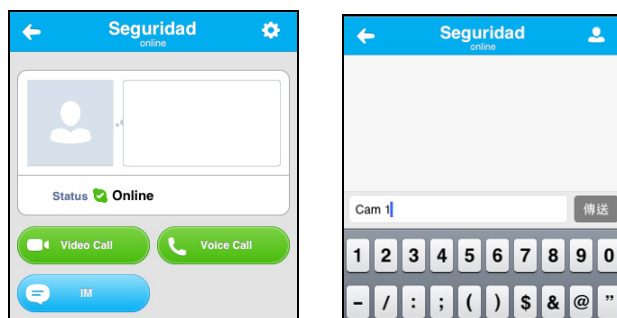


Figure 9-60

3. Click **Send** and an incoming call will appear momentarily.

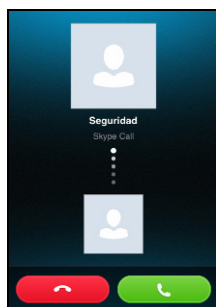


Figure 9-61

4. Click the green **Answer** button to watch the live view.



Figure 9-62

9.9 GV-SDCardSync Utility

The GV-SDCardSync Utility allows you to download videos from the Micro SD card inserted in the GV-IP Camera. When the connection between the GV-IP Camera and the GV-VMS is lost, recordings are automatically saved to the memory cards inserted in the GV-IP Cameras. To automatically synchronize and download recordings from the micro SD cards to a local folder, install and execute the program on the GV-VMS.

Note:

1. GV-SDCardSync Utility is only supported by GV-IPCam H.264 V1.11 or later.
 2. It is recommended to keep the GV-SDCardSync Utility running in the background to automatically synchronize and download videos.
-


9.9.1 Installing GV-SDCardSync Utility

You can install the GV-SDCardSync Utility from Software DVD or GeoVision Website.


Installing from Software DVD

1. Insert Software DVD to the computer. It runs automatically and a window appears.
2. Click **Install GeoVision Supplemental Utilities**.
3. Select **GV-SDCardSync Utility** and follow the on-screen instructions.

Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:
http://www.geovision.com.tw/english/5_8_VMS.asp.
2. Select the **Video Management Software** tab, find the **Supplemental Utilities** section and click the **Download** icon  of **GV-SDCardSync Utility**.

9.9.2 Setting Up GV-SDCardSync Utility

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

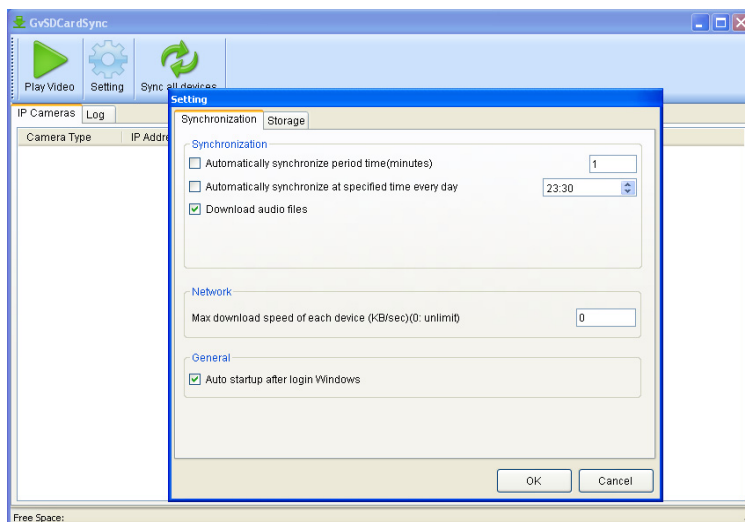


Figure 9-63

2. To configure synchronization, network and startup settings, select the **Synchronization** tab on the Setting window. This page appears.

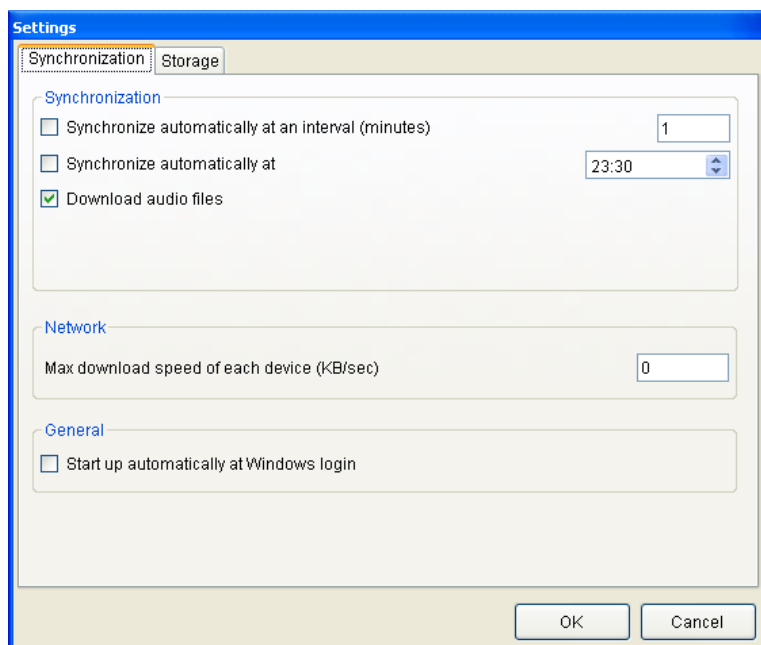


Figure 9-64

[Synchronization]

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

[Network]

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

[General]

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

3. To configure the storage and recycling settings, select the **Storage** tab on the Setting window. This page appears.

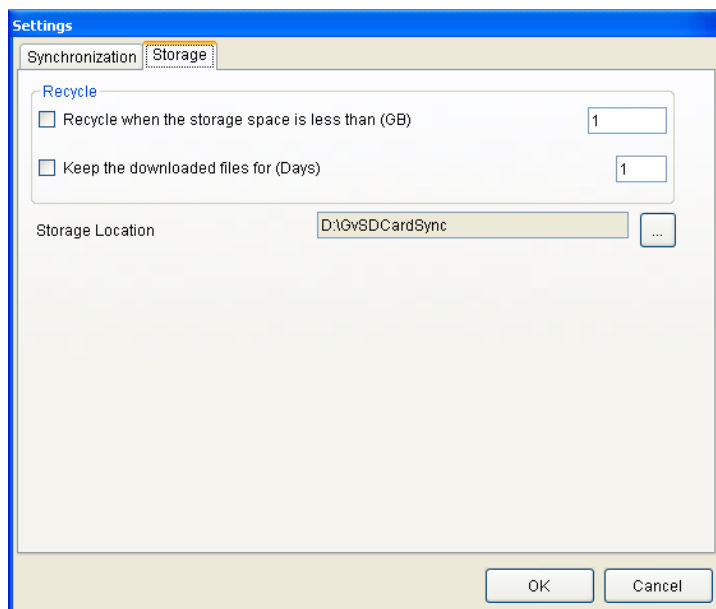


Figure 9-65

Note: By default, downloads are saved to **:\GvSDCardSync** and are not recycled automatically.

[Recycle]


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

[Storage Location]

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

4. Click **OK** to save the configuration and exit the Setting window.

9.9.3 The Main Window

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

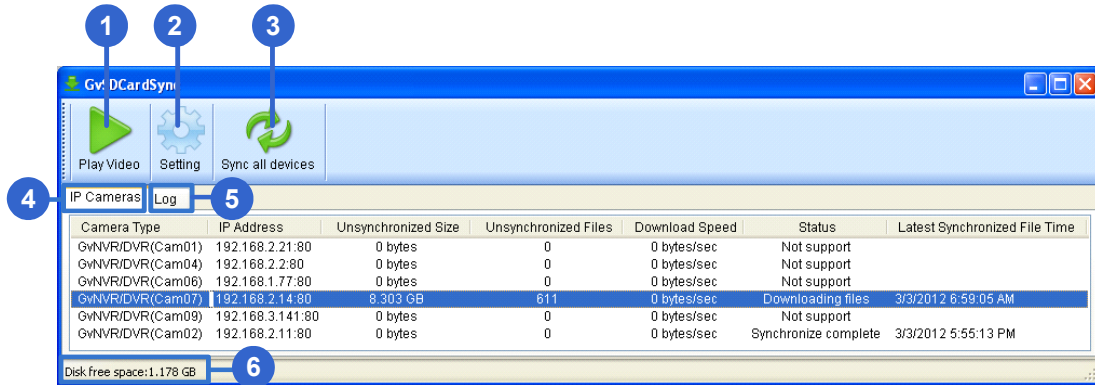


Figure 9-66

| No. | Name | Description |
|-----|------------------|---|
| 1 | Play Video | Plays downloaded recordings of the selected GV-IP Cameras using the ViewLog player. For details, see <i>Chapter 4 Video Playback</i> . |
| 2 | Setting | Configures settings of synchronization, network, storage location and recycling criteria. See step 4 in <i>Installing the GV-SDCardSync Utility</i> earlier in this chapter. |
| 3 | Sync all devices | Manually synchronizes and downloads the recording files saved in GV-IP Camera. |
| 4 | IP Camera Tab | Shows information of GV-IP Camera connected to the GV-VMS, including channel number, IP address, size and number of unsynchronized files, download speed, status and the last synchronization time. |
| 5 | Log Tab | Displays up to 100 event entries of the GV-SDCardSync Utility. Once the entries are full, recycling will start from the oldest file. |
| 6 | Storage Space | Shows the storage space of the designated hard drive. |

Note:

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