GeoVision inc
The Vision of Security

GV-AI Guard

User's Manual



GUARDV22-UM-A

© 2025 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* is the registered trademark of Microsoft Corporation.

November 2025

Scan the following QR codes for product warranty and technical support policy:

[Warranty]

[Technical Support Policy]

Before Installing

For optimal performance, please refer to the following recommendations before installing GV-AI Guard:

- It is highly recommended to use separate hard disks; one for installing Windows OS and GV-AI Guard software, while the other for storing recorded files and system logs.
- When formatting the hard disks, select NTFS as the file system.
- When GV-AI Guard is running, it is not recommended to perform disk defragmentation at the same time.
- 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 notice the total of recording frame rates that you can assign, as listed below:

Frame rate limit in a single hard disk

Video Resolution	H.264		H.265	
	Frame Rate (fps)	Bitrate (Mbps)	Frame Rate (fps)	Bitrate (Mbps)
1.3 MP (1280 x 1024)	660	5.05	N/A	N/A
2 MP (1920 x 1080)	660	7.01	660	5.90
3 MP (2048 x 1536)	440	10.48	660	5.35
4 MP (2048 x 1944)	330	11.65	550	7.74
5 MP (2560 x 1920)	220	16.48	660	6.73
8 MP (3840 x 2120)	550	14.13	440	9.83
12 MP (4000 x 3000)	330	14.47	440	9.85
Note: The data above was determined using the bitrate listed above, 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 the resolutions, the lower the frame rates you can assign to a single hard disk. In other words, the higher the frame rates you wish to record, the more hard disks you'll need. For detailed information of recording frame rates, refer to the user's manual of the IP camera that you wish to connect to.

V2.2 New Features

GV-AI Guard V2.2 supports the following new features. For details, refer to related sections.

- **Vehicle Attribute Recognition** to provide vehicle information, including license plate numbers, eTag details, and key attributes such as vehicle type, brand, and color, for the following applications: (Plugin required)
  - Entrance
  - Exit
  - Zone Monitor
  - Queued Traffic
  - Vehicle Attribute Event Search

  See *1.4.9 Vehicle Attribute Recognition* for details.

- **Fall Down Detection** for identifying incidents of people failing (Plugin required). See *1.3.10 Fall Down Detection* for details.

- **AI Query** to filter AI and PVD events by cameras, time range, facial recognition, event types, person attributes, and vehicle attributes. See *1.6.1 AI Query* for details.

- **Transmission of metadata** from the following cameras to the local GV-AI Guard or GV-Cloud VMS for AI Event Search, enabling event searches based on people or vehicle attributes: GV-GBL4900, GBL4911, GBL12811, GDR4900, GEB4900, GEBF4911, and GVD4910.

  See *3.7 Video Analysis by Camera* for details.

- Support for **GV-IP Speaker** for broadcasting and active deterrence.
  - See *GV-IP Speaker User's Guide* to add a IP speaker to GV-AI Guard.
  - Activate the connected GV-IP Speaker to play audio files when an input or output is triggered. See *6.2.1 Setting up Actions upon Input / Output Trigger* for details.

GPU Decoding

GPU (Graphics Processing Unit) decoding can lower the CPU loading and increase the total frame rate supported by your system. **GV-AI Guard only supports Intel onboard GPU.**

- 11th - 14th Generation Intel Core i7 / i9 Desktop Processors
- Intel Core Ultra 7 / Ultra 9 Desktop Processors (Series 2)

IMPORTANT: The LPR recognition feature is currently not supported on systems using Intel Core Ultra Series 2 Desktop processors (Arrow Lake) due to compatibility concerns. Support for this feature is planned for GV-AI Guard V2.3 or later.

Multi-Channel Playback

Playing back multiple channels at high resolution can increase the CPU loading especially if the GV-AI Guard is processing other tasks simultaneously. As a result of the high CPU loading, dropped frames may sometimes occur in the recorded video when playing back multiple megapixel channels. To avoid the problem, **it is recommended to play back megapixel video in single view.**

GDPR Practice

For details on how GeoVision Inc. is committed to helping users become GDPR (General Data Protection Regulation) compliant, visit the GDPR Consent Request.

Naming and Definition

- **System:** refers to the **GV-AI Guard** system in the manual.
- **AI Event**: refers to **Video Analytics Event** in the manual.
- **PVD Motion Detection**: refers to people and vehicle motion detection in the manual.

Supported Software

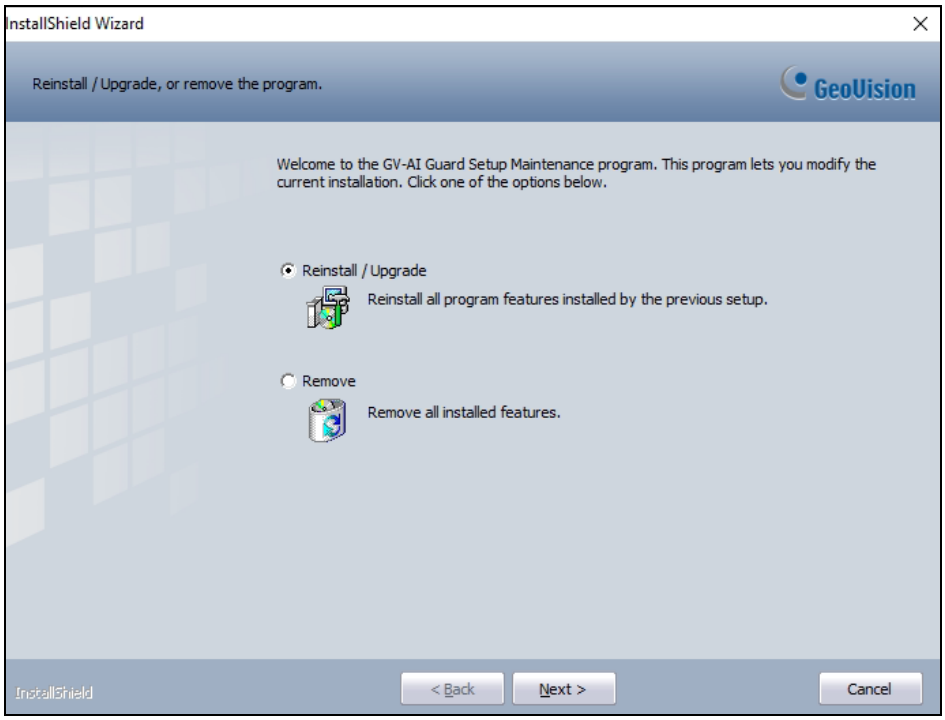
GV-AI Guard can be integrated with the following software/program. **Except for GV-Center V2 and GV-Dispatch Server (AI versions)** and **GV-Cloud VMS**, the listed software/program only supports live streaming and camera motion events from GV-AI Guard.

- GV-Center V2 and GV-Dispatch Server (AI versions) in V20
- GV-Center V2 V18.4.1 or later
- GV-Vital Sign Monitor V18.4.1 or later
- GV-Edge Recording Manager (for Windows) V2.2.4 or later
- GV-Remote ViewLog V2 V17.4.5 or later
- GV-Eye V3.0.0 or later
- GV-Control Center V4.1 or later
- GV-Cloud VMS

Note: Non-AI versions of GV-Center V2 (V18) are limited to receive system and camera motion events only.

Upgrading GV-AI Guard

To upgrade GV-AI Guard, run the **Installer** (setup.exe) included in the latest software downloads from the GeoVision Website. Select **Reinstall / Upgrade** to start.



Contents

Before Installing i

V2.2 New Features ii

GPU Decoding iii

Multi-Channel Playback iii

GDPR Practice iii

Naming and Definition iv

Supported Software iv

Upgrading GV-AI Guard v

Contents vi

1 AI Video Analytics 4

1.1 Introduction 5

1.1.1 Key Features 5

1.1.2 System Requirements 6

1.1.3 Specifications 7

1.2 Getting Started 9

1.2.1 Installing GV-AI Guard 9

1.2.2 Running GV-AI Guard 10

1.2.3 Automatically Adding IP Cameras 11

1.3 Basic AI Video Analytics 13

1.3.1 Starting Basic AI Video Analytics 13
1.3.2 Intrusion 15
1.3.3 Loitering 19
1.3.4 Personal Protective Equipment Detection 22
1.3.5 Social Distancing Detection 24
1.3.6 Face Mask Detection 27
1.3.7 Crowd Detection 29
1.3.8 LPR Setting 31
1.3.9 Average Speed Detection 34
1.3.10 Smoke/Flame Detection 36
1.3.11 Fall Down Detection 38
1.4 Advanced AI Video Analytics 40
1.4.1 Starting Advanced AI Video Analytics 40
1.4.2 Intrusion (Advanced) 42
1.4.3 Loitering (Advanced) 45
1.4.4 Cross Line 48
1.4.5 Enter / Leave Area 50
1.4.6 Counter 52
1.4.7 Mandatory Crossroad Stopping 54
1.4.8 Wrong-way Detection 57
1.4.9 Vehicle Attributes Recognition 59
1.5 Live AI Events 72
1.5.1 Live Event Lists 72
1.5.2 Popup AI Events 73
1.5.3 AI Event Logs 74
1.5.4 AI Event Detection Schedule 75
1.6 AI Event Playback and Search 76
1.6.1 AI Query 76
1.6.2 Advanced Log Browser 80
1.7 Telegram Notify 81
1.8 Getting Started on Video Surveillance 83
1.8.1 Main Screen 83
1.8.2 Adding Cameras 84
1.8.3 Accessing Live View 85
1.8.4 Enabling Recording 85

1.8.5 Playing Back Video 86
1.9 Recording Settings 87
1.9.1 Setting up Global Recording Settings for All Cameras 87
1.9.2 Setting up Recording Settings for Individual Cameras 89
1.9.3 Setting up Video Storage Locations 90
1.9.4 Setting up Motion Detection 92
1.10 Live View and Layouts 97
1.10.1 Utilizing Live View Functions 97
1.10.2 Arranging Live View Layouts 99
1.10.3 Setting up Zoom Window 100
1.10.4 Setting up Scan Window 100
1.10.5 Setting up Popup Window 102
1.10.6 Setting up Focus View 103
1.10.7 Automatic Switch among Different Live View Layouts 104
1.10.8 Adding GV-IP Decoder Box for Remote Monitor Display 104
1.10.9 Adding GV-IP Speaker for Broadcasting 104
1.10.10 Setting up SIP Audio Communication for Dial-out 104
1.11 Start Monitoring 106
1.12 System Configuration 107
1.12.1 Configuring General Settings 107
1.12.2 Customizing Startup Settings 109
1.12.3 Customizing Display Position and Panel Resolution 110
1.12.4 Setting up E-mail Notifications 111
1.12.5 System Idle Protection 112
1.12.6 Configuring Fast Key Locks 114
1.13 Account and Password 114
1.13.1 Creating an Account 115
1.13.2 Configuring Account Settings 116
1.13.3 Changing or Retrieving Password at Login 118
1.13.4 Preventing Unauthorized System Termination 118
1.13.5 Setting up a Startup Auto Login User 119
1.13.6 Setting up Limits on Playback Time 119
1.14 Schedule 120
1.14.1 Creating a Schedule with Setup Wizard 121
1.14.2 Creating a Schedule Manually 123

1.14.3 Exporting and Importing Schedule Settings 124
1.15 System Log 124
1.15.1 Setting up System Log 124
1.15.2 Viewing System Log 126
1.16 Other Functions 128
1.16.1 Setting up Popup Live View 128
1.16.2 Adjusting to Daylight Saving Time 129
1.16.3 Setting up Network Failure Detection 130
1.17 PTZ Camera 131
1.17.1 Accessing PTZ Control Panel and Auto Functions 132
1.17.2 Setting up PTZ Idle Protection and Advanced Functions 134
1.18 QView 135
1.19 Storyline 136
1.19.1 Creating a Storyline in Live View 136
1.19.2 Creating a Storyline in Video Playback 137
1.19.3 Creating a Storyline in QView 137
1.19.4 Accessing a Storyline 138

2 IP Camera Setup 140

2.1 Adding IP Cameras 140
2.1.1 Adding Cameras Manually 142
2.1.2 Scanning for Cameras 144
2.1.3 Mapping GV-IP Cameras using GV-IP Device Utility 144
2.2 Configuring Individual IP Cameras 145
2.2.1 Configuring Video Settings 145
2.2.2 Configuring Audio Settings 147
2.2.3 Configuring Abnormality Settings 149
2.3 Connection through RTSP, ONVIF & PSIA 151
2.4 On Demand Display 153

2.5 Wide Angle Lens Dewarping 155
2.6 Fisheye View 157
2.6.1 Setting up Fisheye View 157
2.6.2 Setting up a Third-Party Fisheye Camera 160
2.6.3 Object Tracking 162
2.6.4 Virtual PTZ Tour 164
2.7 PTZ Object Tracking 166
2.7.1 Dual-Camera Tracking 166
2.7.2 Single Camera Tracking 168
2.8 Panoramic PTZ Object Tracking 170
2.8.1 Accessing the Live View 171
2.8.2 Automatic Object Tracking 172

3 Video Analysis 177

3.1 Face Recognition 177
3.1.1 Enrolling Face Data 178
3.1.2 Setting up Face Groups 181
3.1.3 Synchronizing Face Database 182
3.1.4 Defining Access Schedule 183
3.1.5 Setting up Recognition Alerts 186
3.1.6 Configuring Face Recognition Database 187
3.1.7 Backing up Face Database 188
3.1.8 Face ID — Live Recognition Profiles 188
3.1.9 Viewing and Searching for Face Recognition Events 189
3.1.10 Tracking Recognized Faces 190
3.1.11 Integrating Face Recognition to Access Control 193
3.1.12 Batch Enrolling Faces and Access Cards 196
3.2 Privacy Mask Protection 200
3.2.1 Setting up a Privacy Mask 200
3.2.2 Granting Access Privileges to Recoverable Areas 201

3.3 Advanced Scene Change Detection 202
3.4 Text Overlay 204
3.5 Video Analysis by Camera 205

4 Video Playback 209

4.1 Playing back on ViewLog 210
4.1.1 ViewLog Window 211
4.1.2 ViewLog Control Panel 212
4.1.3 Adjusting the Camera View 216
4.1.4 Bookmarking Video Events in ViewLog 217
4.1.5 Merging and Exporting Video 218
4.1.6 Saving, Printing & Copying Images 223
4.1.7 Adjusting Distorted Views 224
4.2 Object Search 225
4.3 Advanced Log Browser 227
4.3.1 Controls on the Advanced Log Browser 227
4.3.2 Filter Settings 228
4.4 Remote ViewLog V2 230
4.5 Single Player 231
4.5.1 Single Player Window 231
4.6 Specifications 232

5 Backup, Deletion and Repair 234

5.1 Backing up Log Data 234
5.2 Backing up Recorded Files 235

5.3 Deleting Recorded Files 238
5.4 Repairing Damaged File Paths 239
5.5 Repairing Damaged Video Files.. 241

6 I/O Applications 244

6.1 Setting up I/O Devices 244
6.1.1 Adding I/O Devices 245
6.1.2 Setting up the Input and Output Devices 246
6.1.3 Latch Trigger 248
6.1.4 Keeping Last Toggle Status 250
6.1.5 Setting up PLC I/O devices 252
6.2 Advanced I/O Applications 254
6.2.1 Setting up Actions upon Input / Output Trigger 255
6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger 256
6.2.3 Setting up Momentary and Maintained Modes 257
6.2.4 Deactivating Alarm and Alert upon Input Trigger 258
6.2.5 Other I/O Application Functions 259
6.3 I/O Devices in Content List 260
6.4 Visual Automation 261

7 Remote Viewing 263

7.1 Remote Viewing using a Web Browser 264
7.2 WebCam Server Settings 267
7.2.1 General Settings 267
7.2.2 Server Settings 268
7.2.3 Video Settings 269

7.2.4 Audio Settings 270
7.2.5 JPG Settings 271
7.2.6 UPnP Settings 272
7.2.7 Network Port Information 273
7.2.8 Mobile Service 274
7.3 Single View Viewer 275
7.3.1 Adjusting Video Quality 277
7.3.2 Control Panel 278
7.3.3 Configuring Single View Viewer Options 279
7.3.4 PTZ Control Panel 282
7.3.5 Visual PTZ Control 283
7.3.6 I/O Control 284
7.3.7 Visual Automation 285
7.3.8 Picture-in-Picture View 286
7.3.9 Picture-and-Picture View 287
7.4 Multi-Window Viewer 288
7.5 JPEG Image Viewer 289
7.6 Remote Playback and Query 290
7.6.1 Event List Query 290
7.6.2 Remote Playback 291
7.7 Download Center 292
7.8 Remote ViewLog 293
7.9 GV-Cloud 294
7.10 GV-Edge Recording Manager 296
7.11 Mobile Phone Applications 297

8 E-Map Applications 299

8.1 The E-Map Editor 299
8.1.1 The E-Map Editor Window 300
8.1.2 Creating E-Map 301
8.1.3 Creating E-Map for a Remote Host 304

8.2 Starting E-Map 305
8.2.1 Setting up the Popup Map 306
8.3 3D E-Map Display 307
8.3.1 3D E-Map Display 307
8.3.2 Utilizing 3D E-Map Icons 308
8.4 Remotely Accessing E-Map 309
8.4.1 The Remote E-Map Window 310
8.4.2 Accessing E-Maps of Multiple Hosts 311
8.4.3 Configuring the Remote E-Map 312
8.4.4 Viewing Event List and Playing back Videos 314
8.5 E-Map Server 314
8.5.1 Installing E-Map Server 314
8.5.2 The E-Map Server Window 315
8.5.3 Setting up E-Map Server 316
8.5.4 Connecting to E-Map Server 316

9 Useful Utilities 319

9.1 Dynamic DNS 319
9.1.1 Running Dynamic DNS 319
9.1.2 Registering and Starting Dynamic DNS 319
9.2 Watermark Viewer 320
9.2.1 Activating Watermark Protection 320
9.2.2 Running Watermark Proof 320
9.2.3 The Main Window 321
9.3 Windows Lockup 322
9.3.1 The GV-Desktop Screen 322
9.3.2 GV-Desktop Features 323
9.3.3 Token File for Safe Mode 326
9.4 Authentication Server 327
9.4.1 Installing the Server 327
9.4.2 The Main Window 328

9.4.3 Creating Clients 329
9.4.4 Creating User Accounts 331
9.4.5 Importing Groups and Users from Active Directory 334
9.4.6 Starting Authentication Server 337
9.4.7 Connecting to Authentication Server 339
9.4.8 Remote Access from Control Center and Remote E-Map 341
9.5 Fast Backup and Restore 344
9.5.1 Running the FBR Program 344
9.5.2 Plugin Component 345
9.5.3 Customizing the Features 346
9.5.4 Backing up and Restoring Settings 347
9.6 Bandwidth Control Application 350
9.6.1 Installing the Bandwidth Control 350
9.6.2 The Main Window 351
9.6.3 Allowing Remote Control 352
9.6.4 Connecting to WebCam Server 353
9.6.5 Controlling a Specific WebCam Server 354
9.6.6 Setting up the Bandwidth 355
9.6.7 Block List Setup 356
9.6.8 General Setup 357
9.7 Language Setting 358
9.7.1 Installing the MultiLang Tool 358
9.7.2 Revising the Translated Text 359
9.7.3 Setting up the UI Language to English 362
9.8 GV-SD Card Sync Utility 363
9.8.1 Installing the Utility 363
9.8.2 Setting up the Utility 364
9.8.3 The Main Window 367
9.9 The Media Man Tools Window 368
9.9.1 The Media Man Tools Window 368
9.9.2 Viewing Disk Drive Status 369
9.9.3 Adding a Disk Drive 371
9.9.4 Removing a Disk Drive 372
9.9.5 Logging in Automatically at Startup 373
9.9.6 Setting up LED Panel 373
9.10 Alert Notifications through SNMP Protocol 376

9.11 Local and Remote Backup 377
9.11.1 Remote Backup 377
9.11.2 Local Backup 377
9.11.3 Advanced Settings 379
9.11.3.1 Advanced Settings for Local Backup 379
9.11.3.2 File Transfer Settings for Local Backup 381
9.12 Report Generator 383
9.13 GV-Cloud VMS 383

10 Point-Of-Sale (POS) Application 385

10.1 Displaying Transactions on the Screen 386
10.2 Setting up Text Overlay 387
10.3 Filtering Transactions for a Product Item 388
10.4 Triggering Transaction Alarms 390
10.5 Mapping Codepage 392
10.6 Coloring Transactions of a Product Item 393
10.7 Displaying Receipt Details of a Transaction 396
10.7.1 Setting Up Receipt Display Conditions 396
10.8 Filtering Transactions by a Keyword 402
10.9 Searching for POS Events 405
10.9.1 Advanced Search Panel 406

Chapter 1

AI Video Analytics 4

1.1 Introduction 5
1.1.1 Key Features 5
1.1.2 System Requirements 6
1.1.3 Specifications 7
1.2 Getting Started 9
1.2.1 Installing GV-AI Guard 9
1.2.2 Running GV-AI Guard 10
1.2.3 Automatically Adding IP Cameras 11
1.3 Basic AI Video Analytics 13
1.3.1 Starting Basic AI Video Analytics 13
1.3.2 Intrusion 15
1.3.3 Loitering 19
1.3.4 Personal Protective Equipment Detection 22
1.3.5 Social Distancing Detection 24
1.3.6 Face Mask Detection 27
1.3.7 Crowd Detection 29
1.3.8 LPR Setting 31
1.3.9 Average Speed Detection 34
1.3.10 Smoke/Flame Detection 36
1.3.11 Fall Down Detection 38
1.4 Advanced AI Video Analytics 40
1.4.1 Starting Advanced AI Video Analytics 40
1.4.2 Intrusion (Advanced) 42
1.4.3 Loitering (Advanced) 45
1.4.4 Cross Line 48
1.4.5 Enter / Leave Area 50
1.4.6 Counter 52
1.4.7 Mandatory Crossroad Stopping 54
1.4.8 Wrong-way Detection 57
1.4.9 Vehicle Attributes Recognition 59
1.5 Live AI Events 72
1.5.1 Live Event Lists 72
1.5.2 Popup AI Events 73

1.5.3 AI Event Logs 74
1.5.4 AI Event Detection Schedule 75
1.6 AI Event Playback and Search 76
1.6.1 AI Query 76
1.6.2 Advanced Log Browser 80
1.7 Telegram Notify 81
1.8 Getting Started on Video Surveillance 83
1.8.1 Main Screen 83
1.8.2 Adding Cameras 84
1.8.3 Accessing Live View 85
1.8.4 Enabling Recording 85
1.8.5 Playing Back Video 86
1.9 Recording Settings 87
1.9.1 Setting up Global Recording Settings for All Cameras 87
1.9.2 Setting up Recording Settings for Individual Cameras 89
1.9.3 Setting up Video Storage Locations 90
1.9.4 Setting up Motion Detection 92
1.10 Live View and Layouts 97
1.10.1 Utilizing Live View Functions 97
1.10.2 Arranging Live View Layouts 99
1.10.3 Setting up Zoom Window 100
1.10.4 Setting up Scan Window 100
1.10.5 Setting up Popup Window 102
1.10.6 Setting up Focus View 103
1.10.7 Automatic Switch among Different Live View Layouts 104
1.10.8 Adding GV-IP Decoder Box for Remote Monitor Display 104
1.10.9 Adding GV-IP Speaker for Broadcasting 104
1.10.10 Setting up SIP Audio Communication for Dial-out 104
1.11 Start Monitoring 106
1.12 System Configuration 107
1.12.1 Configuring General Settings 107
1.12.2 Customizing Startup Settings 109
1.12.3 Customizing Display Position and Panel Resolution 110
1.12.4 Setting up E-mail Notifications 111
1.12.5 System Idle Protection 112
1.12.6 Configuring Fast Key Locks 114
1.13 Account and Password 114

1.13.1 Creating an Account 115
1.13.2 Configuring Account Settings 116
1.13.3 Changing or Retrieving Password at Login 118
1.13.4 Preventing Unauthorized System Termination 118
1.13.5 Setting up a Startup Auto Login User 119
1.13.6 Setting up Limits on Playback Time 119
1.14 Schedule 120
1.14.1 Creating a Schedule with Setup Wizard 121
1.14.2 Creating a Schedule Manually 123
1.14.3 Exporting and Importing Schedule Settings 124
1.15 System Log 124
1.15.1 Setting up System Log 124
1.15.2 Viewing System Log 126
1.16 Other Functions 128
1.16.1 Setting up Popup Live View 128
1.16.2 Adjusting to Daylight Saving Time 129
1.16.3 Setting up Network Failure Detection 130
1.17 PTZ Camera 131
1.17.1 Accessing PTZ Control Panel and Auto Functions 132
1.17.2 Setting up PTZ Idle Protection and Advanced Functions 134
1.18 QView 135
1.19 Storyline 136
1.19.1 Creating a Storyline in Live View 136
1.19.2 Creating a Storyline in Video Playback 137
1.19.3 Creating a Storyline in QView 137
1.19.4 Accessing a Storyline 138

CHAPTER

1

AI Video Analytics

GV-AI Guard is a full-featured video management software powered by intelligent AI video analytics. It detects specific conditions, triggers alarms for intrusions and violations, and instantly alerts operators to potential risks—making it ideal for securing premises, improving road and construction site safety, and supporting public health through preventive safety measures.

1.1 Introduction

1.1.1 Key Features

- **PVD Motion Detection** for identifying human and vehicle motion from other moving objects
- **Intrusion** for creating virtual fences
- **Loitering** for identifying unauthorized parking and pedestrian violations
- **Social Distancing Detection** for alerting people not keeping a safe distance from each other
- **Personal Protective Equipment Detection** to ensure compliance with safety gear requirements such as hard hats and vests.
- **Social Distancing** and **Face Mask Detection** to support public health and safety protocols
- **Crowd Detection** for detecting overcrowding of people or vehicles
- **Average Speed Detection** for vehicle speed violation
- **Smoke/Flame Detection** for early fire alerts
- **Fall Down Detection** to enhance safety in healthcare environments
- **Cross Line** to monitor movement across preset lines in specific directions
- **Enter & Leave Area** to track entry and exit activities within predefined zones
- **Counter** for people or vehicle counting
- **Mandatory Crossroad Stopping** for identifying vehicles that fail to stop at required points
- **Wrong-Way Detection** to alert on vehicles traveling in the wrong direction
- **Vehicle Attributes Recognition** for providing comprehensive vehicle information to enhance access management and operational efficiency, supporting functions such as Entrance, Exit, Zone Monitor, and Queued Traffic control (Plugin required)
- **LPR recognition** for vehicle loitering, overspeed detection, and vehicle attributes recognition for up to 14 countries/areas
- **AI Query** to filter AI and PVD events by cameras, time range, facial recognition, event types, person attributes, and vehicle attributes

1.1.2 System Requirements

Minimum System Requirements

OS	**64-bit**	Windows 10 / Windows 11 / Server 2016 / Server 2019 / Server 2022 / Server 2025
CPU[1] [2]		Intel Core i7-11700 Processor
Memory	**PVD Motion Detection (Up to 16 ch)**	16 GB (8 GB x 2)
	Basic AI Analytics[7]	16 GB (8 GB x 2)
	Advanced AI Analytics[8]	32 GB (16 GB x 2)
	PVD Motion Detection (Up to 32 ch with GV-AI Accelerator Module)[9]	32 GB (16 GB x 2)
Graphics Card		Intel UHD Graphics 750

IMPORTANT: The LPR recognition feature is currently not supported on systems using Intel Core Ultra Series 2 Desktop processors (Arrow Lake) due to compatibility concerns. Support for this feature is planned for GV-AI Guard V2.3 or later.

Note:

1. For AI analytics and PVD motion detection, 11th Generation Intel Core i7 / i9 processors or above are required, and the function utilizes the integrated GPU, which only works when a monitor is connected to the onboard GPU.
2. Only Intel Core processors are compatible with GV-AI Guard; other brands of CPU do not work with GV-AI Guard.
3. GV-AI Guard does not support virtual machine installation.
4. To use fisheye dewarping, the graphics card must support DirectX 10.1 or above.
5. H.265 decoding and searching of face recognition events by face images requires 6th Generation Intel Desktop Processor (Skylake) or above, which comes with onboard GPU.
6. Basic AI Analytics: Under minimum system requirements, GV-AI Guard supports basic AI analytics for up to **16** channels.
7. Advanced AI Analytics: Under minimum system requirements, GV-AI Guard supports advanced AI analytics for up to **8** channels.
8. PVD Motion Detection: To expand PVD motion detection to **32** channels, ensure your PC has at least 32 GB RAM and GV-AI Accelerator Module installed. Only one unit of GV-AI Accelerator Module is supported. For details, refer to the *Options* section in the *datasheet*.
9. The system requirements are determined in round-the-clock recording settings with live view only, while remote connections and video analysis are disabled.

Recommended Hard Disks

GeoVision software performance tests are conducted using **enterprise-grade 7200 RPM** HDDs with an average read/write speed of **110 MB/s**. If you are using HDDs with different specifications, we recommend conducting performance tests in your actual installation environment to ensure their read/write speed meets your application requirements.

Licenses

GV-AI Guard is a premium software solution that requires a GV-USB Dongle with **at least one AI Analytics channel** for activation. For details, refer to the *Licenses* section in the *datasheet*.

1.1.3 Specifications

- GV-AI Guard supports recording of up to 32 camera channels, with
  - **16 channels for Basic AI Analytics,** or
  - **8 channels for Advanced AI Analytics**.
- The cameras used for AI video analytics should not have **Smart Streaming** enabled, as it may affect analytics accuracy and results.
- It may take about 40 seconds to start AI video analytics after enabling monitoring for the first time.

For detailed specifications, refer to the *datasheet*.

1.1.3.1 Min. Object Size for Detection

The minimum detectable object size (Length × Width) in pixels is listed below. For example, PVD motion detection requires a minimum of 48 × 48 pixels for 8 MP video images. The minimum object size for detection increases in proportion to video resolution.



- **Average Speed Detection:** See the Max. / Min. license plate height (pixels) setting in *1.3.8 LPR Setting* for details.
- **Crowd Detection:** 30 x 30 pixels (for 2 MP video), 40 x 40 pixels (for 4 MP video), 60 x 60 pixels (for 8 MP video), 62 x 62 pixels (for 12 MP video)
- **Face Mask Detection**: 80 x 80 pixels (for 2 MP video), 106 x 106 pixels (for 4 MP video), 160 x 160 pixels (for 8 MP video), 166 x 166 pixels (for 12 MP video)
- **Fall Down Detection** [4]**:** 30 x 30 pixels (for 2 MP video), 40 x 40 pixels (for 4 MP video), 60 x 60 pixels (for 8 MP video), 62 x 62 pixels (for 12 MP video)
- **Flame Detection:** 40 x 40 pixels (for 2 MP video), 52 x 52 pixels (for 4 MP video), 76 x 76 pixels (for 8 MP video), 80 x 80 pixels (for 12 MP video)
- **People/Vehicle Intelligent Analysis (Basic / Advanced)** [1] [2]**:** 24 x 24 pixels (for 2 MP video), 32 x 32 pixels (for 4 MP video), 48 x 48 pixels (for 8 MP video), 50 x 50 pixels (for 12 MP video)
- **Personal Protective Equipment Detection:** 30 x 30 pixels (for 2 MP video), 40 x 40 pixels (for 4 MP video), 60 x 60 pixels (for 8 MP video), 62 x 62 pixels (for 12 MP video)
- **Smoke Detection:** 60 x 60 pixels (for 2 MP video), 76 x 76 pixels (for 4 MP video), 116 x 116 pixels (for 8 MP video), 120 x 120 pixels (for 12 MP video)
- **Social Distancing Detection:** 48 x 48 pixels (for 2 MP video), 64 x 64 pixels (for 4 MP video), 96 x 96 pixels (for 8 MP video), 100 x 100 pixels (for 12 MP video)
- **Vehicle Attributes Recognition** [3]**:** 24 x 24 pixels (for 2 MP video), 32 x 32 pixels (for 4 MP video), 48 x 48 pixels (for 8 MP video), 50 x 50 pixels (for 12 MP video)

Note:

1. The minimum object size required for PVD Motion Detection and People/Vehicle Intelligent Analysis (Basic/Advanced) is **1/80 of the image resolution** (Length × Width). Detection will fail if either the object's length or width falls below this threshold.
2. The people/vehicle detection size is adjustable under the PVD Confidence Setting. See *Step 4* in *1.3.1 Starting Basic AI Video Analytics* for details.
3. If image clarity is poor, detection accuracy for vehicle type, color, and brand may decrease, even when the object meets the minimum size requirement.
4. The minimum object size for Fall Down Detection required is **1/20 of the image resolution** (Length × Width). Detection will fail if either the object's length or width falls below this threshold.

1.2 Getting Started

1.2.1 Installing GV-AI Guard

Installing GV-AI Guard

1. To download GV-AI Guard, selecting **Primary Applications** from the dropdown list and click **Download** of *GV-AI Guard* on the GeoVision Website.
2. Insert GV-USB Dongle to your computer.
3. To install the USB driver, select **Drivers**, **F/W**, **Patch** from the dropdown list, and click **Download** icon of **GV-Series Card Driver / USB Devices Driver**.
   - To verify the driver is installed correctly, go to Windows Device Manager and expand **DVR-Devices**. You should see **GV-Series USB Protector**.



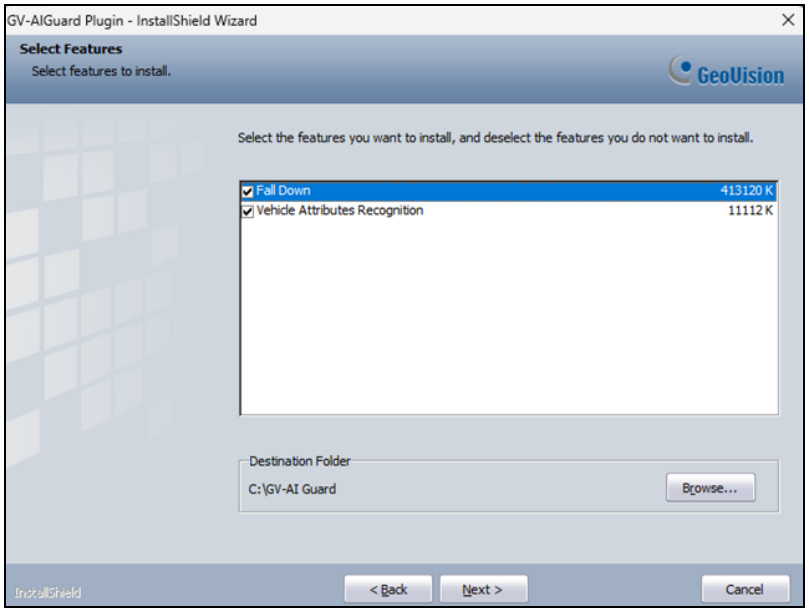
Installing GV-AI Guard Plugin (Optional)

If you plan to use the following GV-AI Guard functions, you must install the **GV-AI Guard Plugin** after installing the main software:

- **Fall Down Detection**
- **Vehicle Attributes Recognition**

1. To download GV-AI Guard Plugin, select **Primary Applications** from the dropdown list and click **Download** of *GV-AI Guard Plugin* on the GeoVision Website.

2. Follow the onscreen instructions to complete the installation. When the feature selection interface appears, **choose your desired function(s).**



1.2.2 Running GV-AI Guard

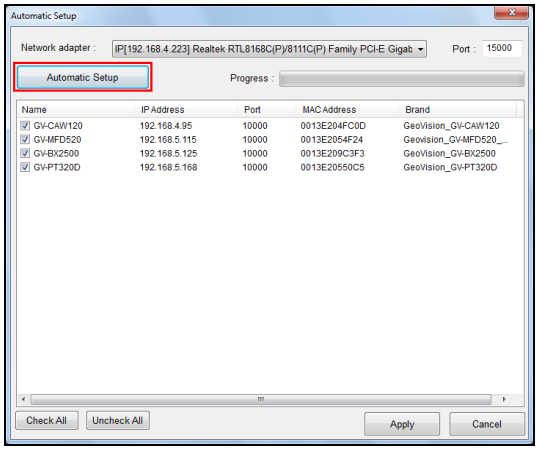
When you run GV-AI Guard for the first time, the system will prompt you for a Supervisor ID and Password.

1. Type the desired **ID**, **Password** and a **Hint** to remind you of the password.
2. Optionally configure the following functions:
   - **E-Mail List:** Type e-mail addresses used to receive the password when forgotten.
   - **Auto Login:** Allows automatic login as the current user each time when the system is launched.
   - **Allow removing password system:** Recommended option that allows removal of the password database if passwords are forgotten. For details, see the same option (Allow removing password system) in *Configuring Account Settings* later in this chapter.
   - : Click to open the onscreen keyboard for entering login information.
3. Click **OK**. The GV-AI Guard main screen appears, along with a dialog box.
4. Choose how to save your system database: **Microsoft Office Access Database** or **Microsoft SQL Server** and fill out the required fields.
5. Upon first-time starting of the GV-AI Guard, you are prompted with the **Automatic Setup** dialog box to assist you in quickly adding IP devices to GV-AI Guard.

1.2.3 Automatically Adding IP Cameras

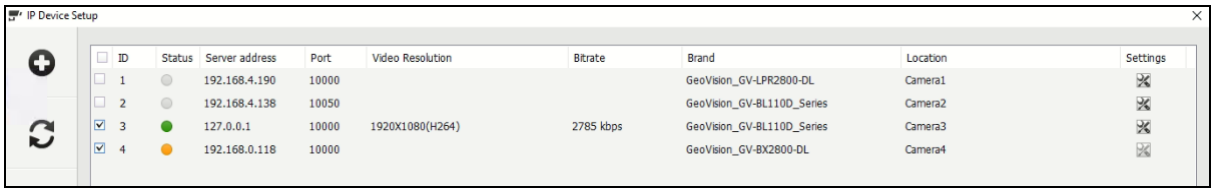
When logging in for the first time after installing GV-AI Guard, the **Automatic Setup** dialog box appears. Follow the steps below to add IP cameras.

1. Click **Automatic Setup** to search for IP cameras on the LAN. Select or deselect the desired cameras, and click **Apply**.



2. Double-click a camera in the list to specify its login credentials.

3. Cameras added are now listed in the IP Device Setup list.



Status icons illustrated:

	Connected	The camera is connected.
	Connecting	The system is attempting to connect to the camera.
	Connection Failed	Unable to connect. Move the cursor over the red icon to view the error message.
	Inactive Camera	The camera is inactive. Click the checkbox to connect.
	Started Monitoring	The camera is under monitoring.
	Pre-Rec Enabled	Pre-recording is enabled.

4. To adjust camera settings, click **Settings** for the connected camera. For details, see *Configuring Individual IP Cameras* in Chapter 2.
5. Close the dialog box by clicking **X** in the top-right corner. When adding cameras for the first time, they will be automatically assigned to the live view grid.

Note:

1. You can also access the IP Device Setup dialog box by clicking **Home** > **Toolbar** > **Configure** > **Camera Install**.
2. If your camera was not detected during the Automatic Setup scan, you can click the **Add Camera** button on the IP Device Setup dialog box and specify connection settings manually.

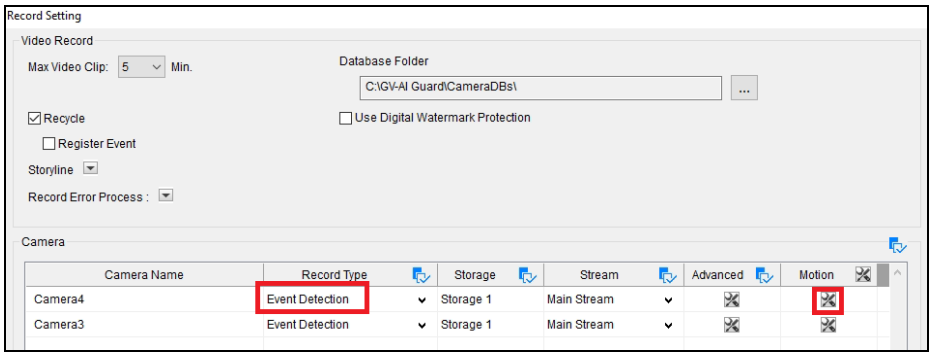
To manually add cameras, see *Adding IP Cameras* in Chapter 2.

1.3 Basic AI Video Analytics

1.3.1 Starting Basic AI Video Analytics

Prerequisites

1. To record AI video analytics events, first configure the following two camera settings in the Recording Setting dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting**).



A. **Verify the recording type is set to Event Detection.**

Ensure **Event Detection** is enabled under Record Type.

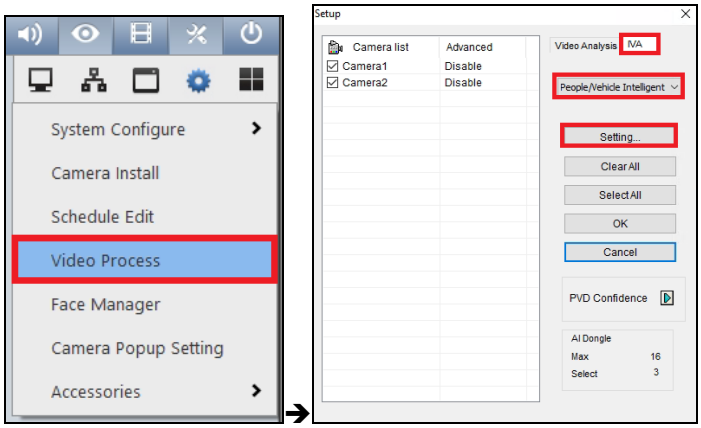
B. **Enable Registered Motion Event.**

Click the **Tool** icon for the camera. In the Advanced Motion Detection Setup dialog box, enable **Registered Motion Event**.

Accessing the Settings

2. To access basic AI analytics settings, click **Home** > **Toolbar** > **Configure** > **Video Process** > the **IVA** tab.

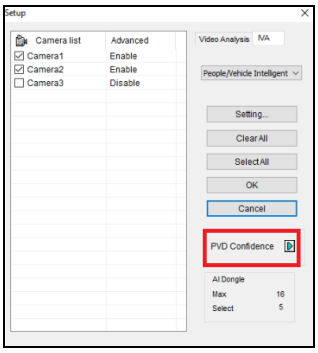
3. Select at least one camera and the desired AI video analytics function from the dropdown list, then click **Setting** to start the configuration.

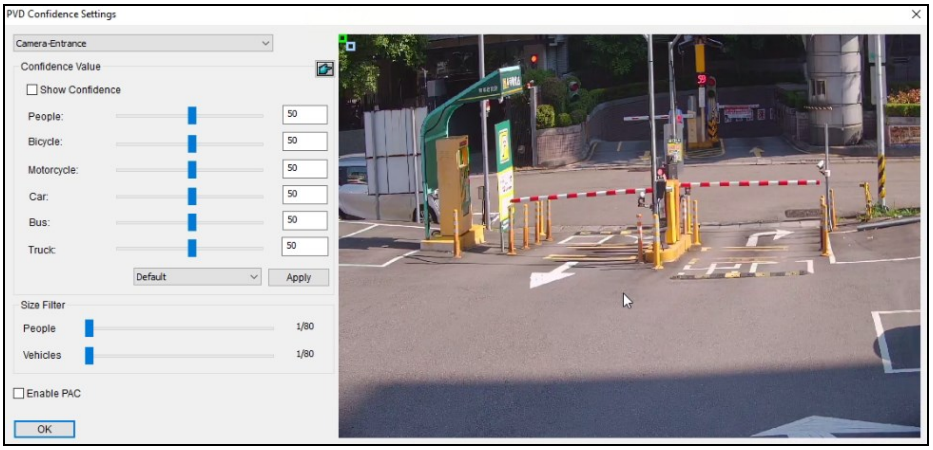


Optional Setup for PAC and PVD

4. You can enable the system to collect people attributes (PAC) and fine-tune the people and vehicle detection (PVD) confidence parameters to optimize performance based on your camera and application scenario. For real-world examples, see *Confidence Threshold Setting* in this technical notice.

   Click the  icon next to **PVD Confidence**, then configure the following options:

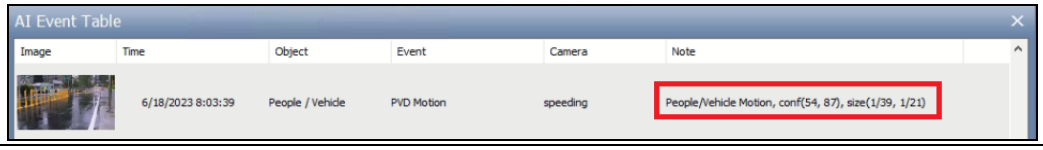




- **Camera Channel:** Select the desired camera from the dropdown list in the upper left corner, to apply your configurations.
- **Confidence Value:** Set the detection confidence value for different objects on a scale from 1 to 95. The higher the confidence value, the more definitive and stricter the system is in detecting events. Optionally, select **Default** or **High Precision** and click **Apply** to load preset confidence values. You can enable **Show Confidence** to display detecting confidence values in the AI Event Table.
- **Size Filter:** Define the minimum detection size for people or vehicles. Object smaller than the configured size will not be detected, helping prevent false alarms. The configured size will be displayed on the image to the right.
- **Enable PAC:** People Attribute Classification. Enable the system to collect people attributes, such as gender, age group, clothing, and accessories. These attributes can later be used in AI Query to filter and search for specific targets.

Note:

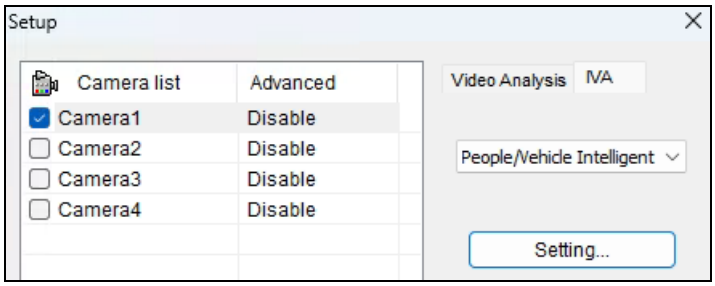
1. The minimum object size ratio relative to the video image is 1/80 for both people and vehicle detection. For example, for the video image that is set to 1920 x 1080, the minimum PVD object size should be 24 x 24 pixels.
2. PVD triggers motion events only when people or vehicles are detected. The system uses a detection threshold to identify objects, with higher confidence levels resulting in fewer events – each more likely to include a valid person or vehicle detection. The detected PVD motion type, confidence value, and size ratio are displayed in the AI Event Table (see *1.5.3 AI Event Logs)*. To optimize detection accuracy for your camera and environment, adjust the PVD settings, (Confidence, Size Filter), and evaluate the results.



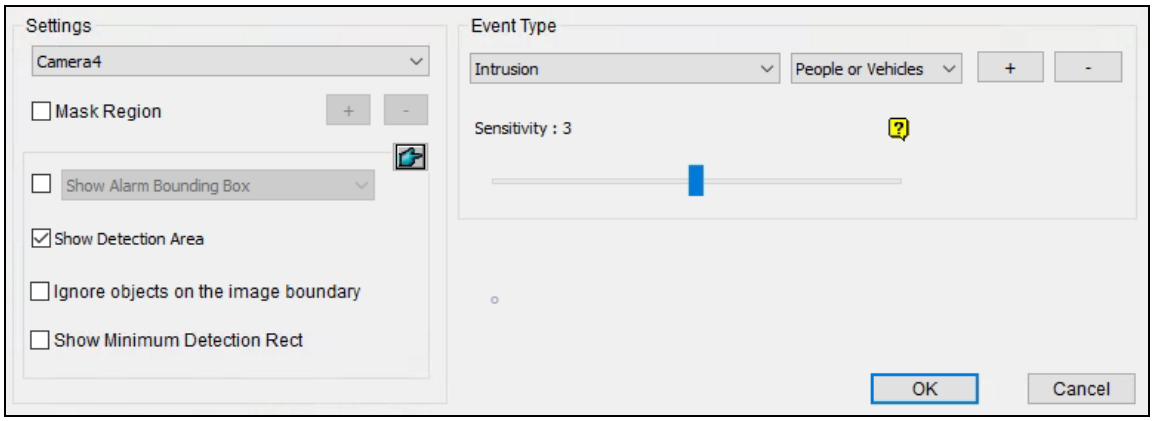
1.3.2 Intrusion

The Intrusion is to detect and capture any person or vehicle entering predefined areas.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select at least one camera > **People/Vehicle Intelligent Analysis**, and click **Setting**.



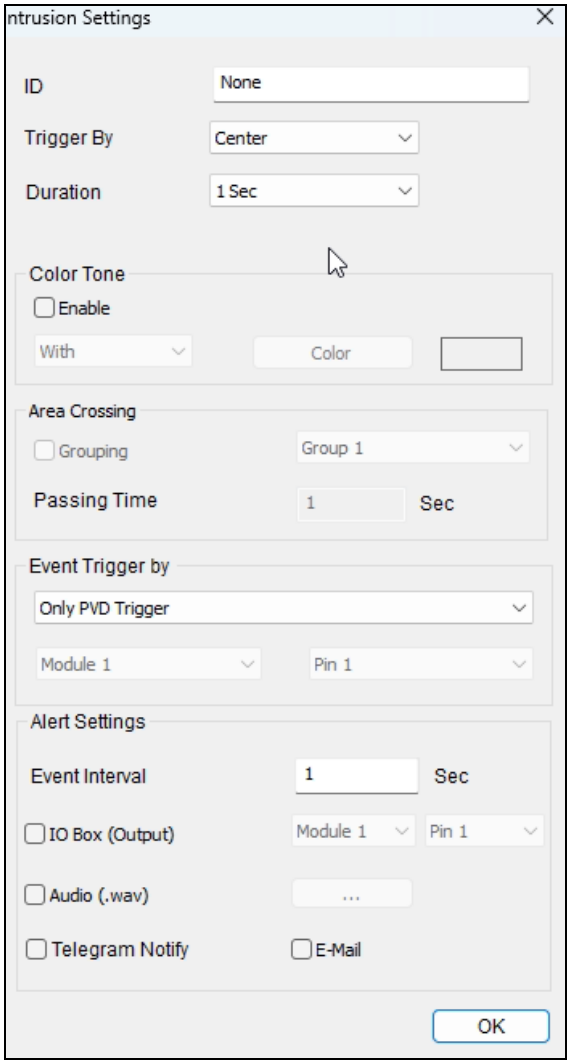
3. On the People/Vehicle Intelligent Video Analysis Settings window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.
- **Sensitivity:** The higher the value, the more sensitive the detection is. The default value is 3.

4. Select **Intrusion** from the **Event Type** dropdown list, and select the type of objects, **People** and/or **Vehicles**, you want the Intrusion to be detected.
5. Select **Add** +, and drag to draw an intrusion area on the image. Any person or vehicle entering the area will be detected as an intrusion. To shape a polygon area, double-click on the sides of the lines and drag the joints.

6. Right-click on the drawn intrusion area and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger By:** Define the detection sensitivity.
  - **Center:** Intrusion is triggered only when the center of a person or vehicle crosses the set area.
  - **Touch:** Intrusion is triggered when any part of a person or vehicle touches the set area.
- **Duration:** Intrusion is triggered only when any person or vehicle remains in the set area exceeding the specified duration (1-5 seconds).
- **Color Tone:** Intrusion is triggered when a specified color, included or excluded, is detected. Click the **Color** button, and click and draw on the image with the color you want to be detected.
- **Area Crossing:** Only for *People Intrusion*. Intrusion is triggered when a person passes through two defined areas of *the same group*. For this, you need to draw two intrusion areas on the image and then specify the two as the same group.

- **Passing Time:** Specify the maximum time required to travel from the start of entering one detection area to the other detection area.

Note:

1. Grouping Detection Areas:

   A group is used to associate two detection areas. Only two areas can be included in a single group, and area crossing detection is only triggered when both areas belong to the same group. Area crossings between different groups will not be detected.

2. Limitation in Basic Version:

   In the Basic version of GV-AI Guard, area crossing detection does not support individual tracking. An alert will be triggered if a person appears in one detection area but fails to enter the corresponding paired area, regardless of whether it is the same person.

- **Event Trigger by:** Intrusion is triggered upon a PVD trigger (People/Vehicle Detection event) and/or a sensor activated.

7. Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon intrusion events. To prevent frequent alerts, specify **Event Interval** (1-9999 sec) between events, and any events that occur during that time are ignored. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.
8. Click **OK**.
9. Start monitoring.

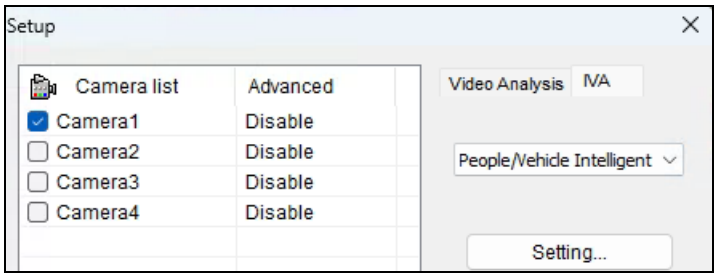
Once set up, intruding people or vehicles will be highlighted by red rectangles on the live view.



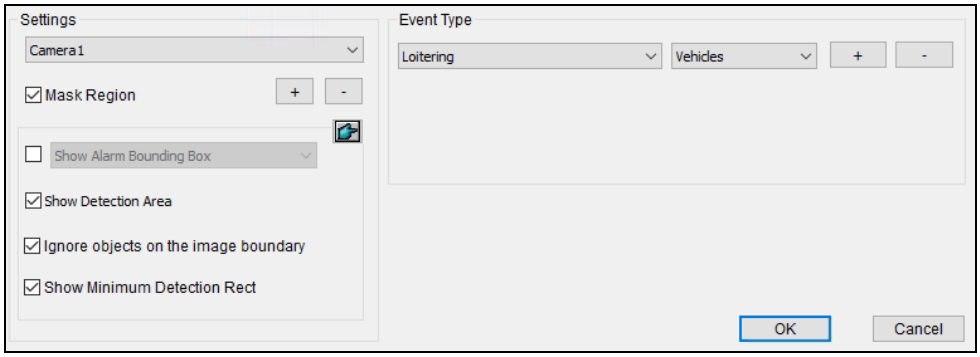
1.3.3 Loitering

The Loitering detects and notifies the user of people or vehicles caught staying/parking in no standing areas.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics.*
2. On the Setup window, select at least one camera > **People/Vehicle Intelligent Analytics** and click **Setting**.



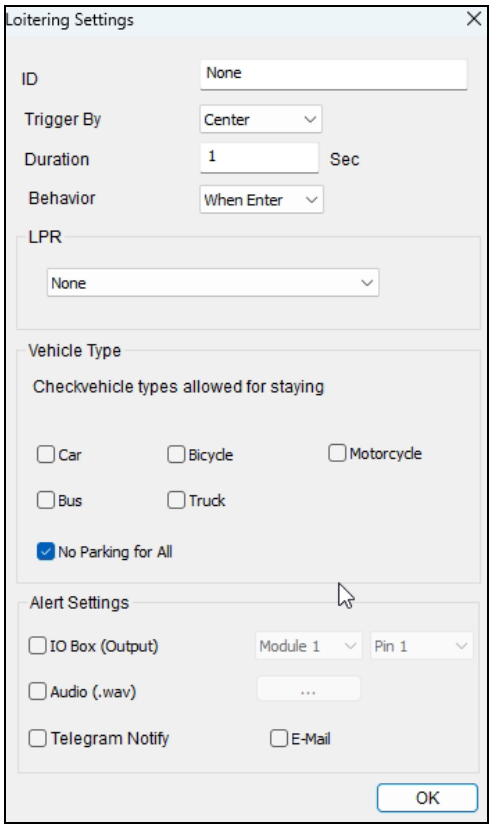
3. On the People/Vehicle Intelligent Video Analysis Settings window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.

- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

4. Select **Loitering** from the Event Type dropdown list, and select the type of objects, **People** or **Vehicles**, you want the loitering to be detected.
5. Select **Add** , and drag to draw an area on the image. Any person or vehicle remaining in the area will be detected as a loitering event. To shape a polygon area, double-click on the sides of the lines and drag the joints.
6. Right-click on the drawn area and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger by:** Define the detection sensitivity.
  - **Center:** Loitering is triggered only when the center of a person or vehicle crosses the set area.
  - **Touch:** Loitering is triggered when any part of a person or vehicle touches the set area.
- **Duration:** Loitering is triggered only when any person or vehicle remains in the set area exceeding the specified duration (1-9999 seconds).
- **Behavior**: Define the object's behavior in the set area to trigger the loitering event, which include **When Stopped** or **When Enter.**

- **LPR:** For *Vehicle Loitering* only. The selected camera will detect and recognize license plate numbers. For this function, you must set up the camera for LPR recognition in advance. For details, see *1.3.8 LPR Setting*.
- **Vehicle Type:** For *Vehicle Loitering* only. Select the types of vehicles that are permitted to remain in the defined area, e.g. buses only at bus stops.
- Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon loitering events. To prevent frequent alerts, specify **Event Interval** (1-9999 sec) between events, and any events that occur during that time are ignored. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

7. Click **OK**.
8. Start monitoring.

Once set up, people or vehicles detected loitering will be highlighted by red rectangles on the live view, with the duration in seconds counting.



1.3.4 Personal Protective Equipment Detection

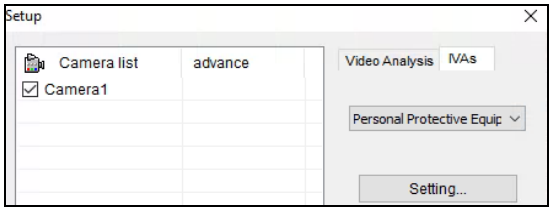
The Person Protective Equipment Detection is used to trigger alerts when a person without a hard hat and/or safety vest is detected.

Examples of Hard Hats and Vests:

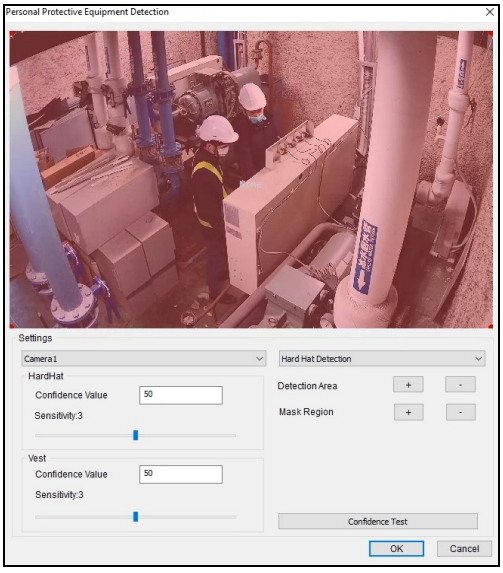
The following examples illustrate common types of hard hats and safety vests used for PPE detection. Note that variations in color, design, or reflectivity may affect detection accuracy and could result in false alarms or missed detections.



1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select at least one camera > **Personal Protective Equipment (PPE) Detection** and click **Setting**.



3. On the Personal Protective Equipment Detection window, select the detection object, **Hard Hat Detection** and/or **Vest Detection** from the right dropdown list.



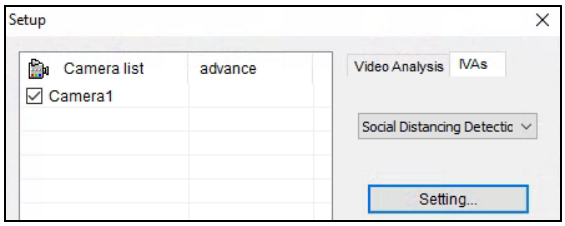
4. On the same window, configure the following settings:
   - **Confidence Value:** The higher the value, the more definitive and stricter the system is in distinguishing those who do not wear a hard hat or vest. The default value is 50. You can click **Confidence Test** to see the detection results based on the set value.
   - **Sensitivity:** The higher the value, the more sensitive the detection is. The default value is 3.
   - **Detection Area:** By default, the whole image is set to be the detection area. Optionally, click **Delete** , and click and drag on the image to remove the detection area. And click **Add** to draw new detection areas.
   - **Mask Region:** Click **Add** to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
5. Right-click on the detection area drawn and select **Edit** to have further settings:
   - **ID:** Name the set area.
   - **Event Interval:** Specify the time interval between events to prevent frequent alerts. Any events that occur during that time are ignored.
   - **Recognition:** Select to trigger recognition by **Motion Detection** or **I/O Detection** (input trigger), and set the recognition time.
   - **Alert Settings:**
     - **Alarm mode**: Select **No PEE Detected** for alerting when people without hard hats / vests are detected; select **PPE Detected for Access** for I/O devices to be activated and grant access to people detected with hard hats / vests.
     - **Notification type**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon hot hat detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.
6. Click **OK**.
7. Start monitoring.

Once set up, people not wearing hard hats or vests will be highlighted by red rectangles on the live view.

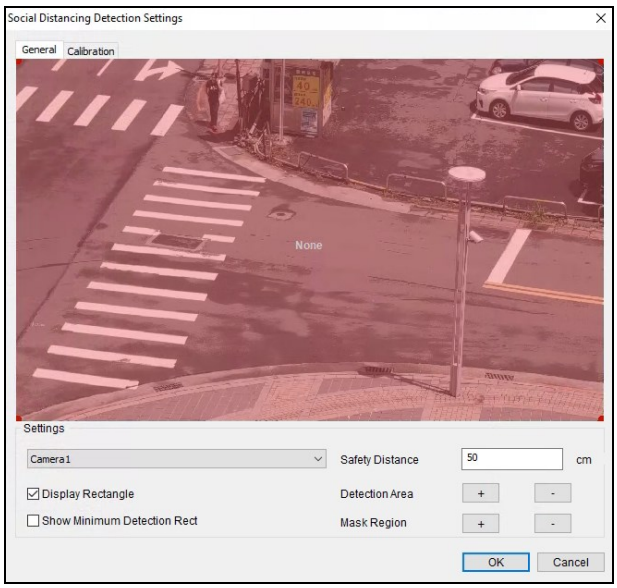
1.3.5 Social Distancing Detection

The Social Distancing Detection is used to activate alerts when people are not maintaining a safe distance from each other.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics.*
2. On the Setup window, select at least one camera > **Social Distancing Detection** and click **Setting**.



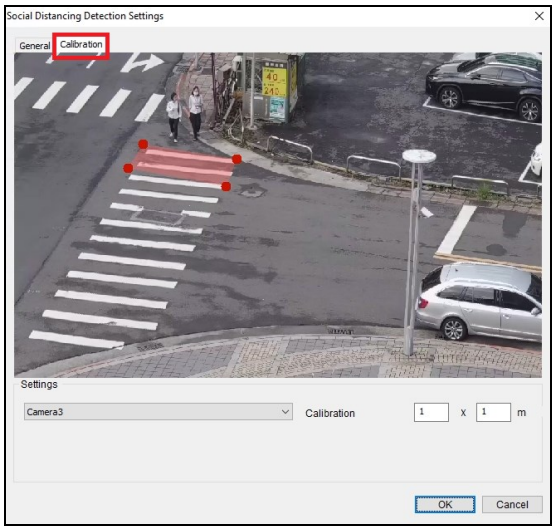
3. On the Social Distancing Detection Settings window, configure the following settings:



- **Display Rectangle:** Display red rectangles on the live view, highlighting people detected violating the social distancing.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect on the top left corner of the setting image as a reference.
- **Safety Distance:** Specify a safe distance in centimeter. When the distance between people is shorter than the specified value, the alerts will be triggered.

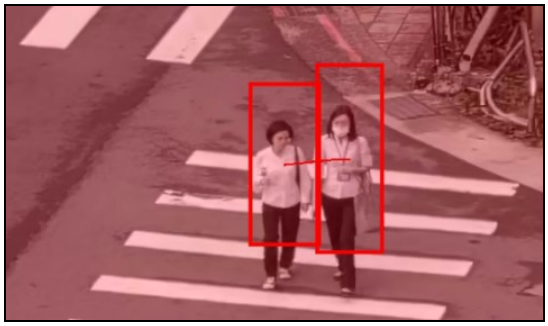
- **Detection Area:** By default, the whole image is set to be the detection area. Optionally click **Delete** -, and click and drag on the image to remove the detection area. And click **Add** + to draw new detection areas.
- **Mask Region:** Click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.

4. Right-click on the drawn detection area and select **Edit** to have further settings:
   - **ID:** Name the set area.
   - **Event Interval:** Specify the time interval (1-9999 sec) between events to prevent frequent alerts. Any events that occur during that time are ignored.
   - **Trigger by:** Define the detection sensitivity.
     - **Center:** The detection is triggered only when the center of a person crosses the set area.
     - **Touch:** The detection is triggered when any part of a person touches the set area.
   - **Alert Settings:** Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon social distancing detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.
5. Click the **Calibration** tab on the settings window. This function serves as a reference for the system to rate the proportion of an area in a video image compared to that in the real world, thereby increasing detection accuracy. Draw an area and estimate its length and width in meter, e.g., the area size of two standing persons.



6. Click **OK**.
7. Start monitoring.

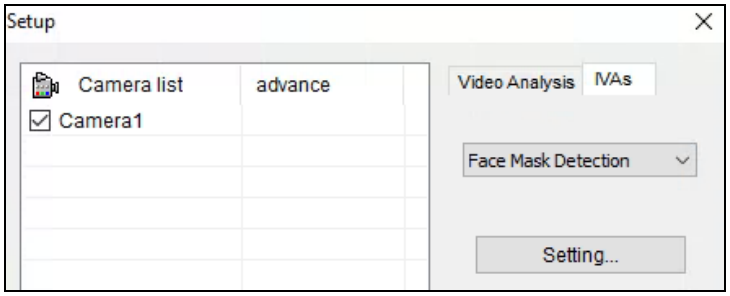
Once set up, those whose distances are less than the specified safe distance will be highlighted by red rectangles, with a line drawn between them to emphasize this measure.



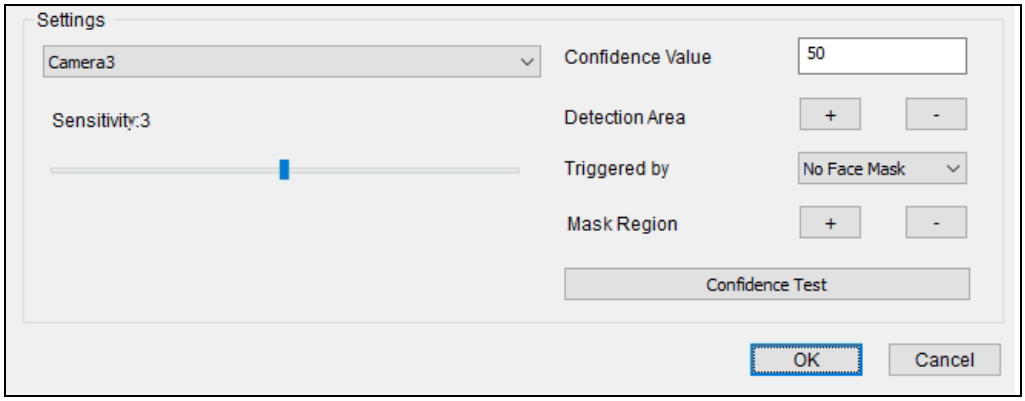
1.3.6 Face Mask Detection

The Face Mask Detection is used to trigger alerts when a person wearing or not wearing a face mask is detected.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select at least one camera > **Face Mask Detection** and click **Setting**.



3. On the Face Mask Detection Settings window, configure the following settings:



- **Sensitivity:** The higher the value, the more sensitive the detection is. The default value is 3.
- **Confidence Value:** The higher the value, the more definitive and stricter the system is in distinguishing whether or not a person is wearing a mask. The default value is 50. You can click **Confidence Test** to see the detection results based on the set value.
- **Detection Area:** By default, the whole image is set to be the detection area. Optionally, click **Delete** -, and click and drag on the image to remove the detection area. Click **Add** + to draw new detection areas.
- **Triggered by:** Select whether to trigger an alert when any person wearing or not wearing a face mask is detected.
- **Mask Region**: Click **Add** + and draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.

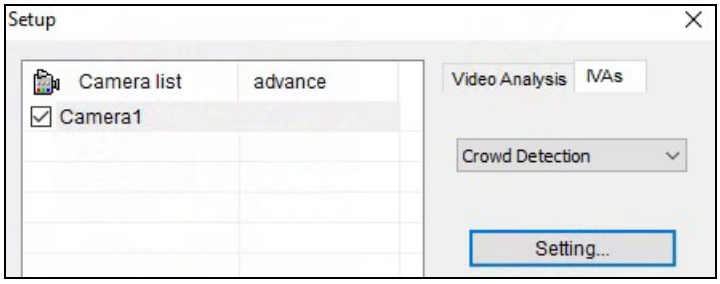
4. Right-click on the detection area drawn and select **Edit** to have further settings:
   - **ID:** Name the set area.
   - **Event Interval:** Specify the time interval between events to prevent frequent alerts. Any events that occur during that time are ignored.
   - **Alert Settings:** Select **E-mail**, **Telegram Notify**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon face mask detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.
5. Click **OK**.
6. Start monitoring.

Once set up, people detected, wearing or not wearing face masks according to your settings, will be highlighted by red rectangles on the live view.

1.3.7 Crowd Detection

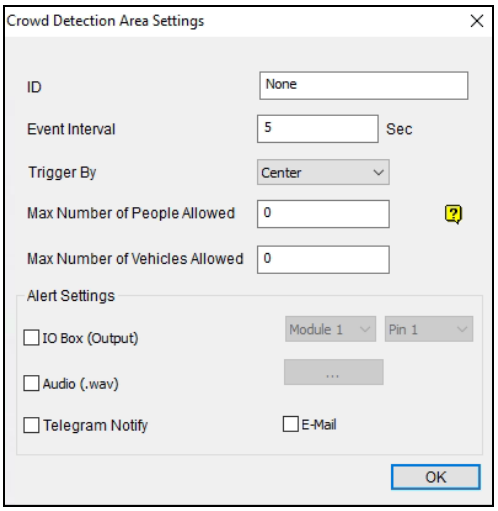
The Crowd Detection is used to trigger alerts when a group of people or vehicles gathering together is detected.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select at least one camera > **Crowd Detection** and click **Setting**.



3. On the Crowd Detection Settings window, configure the following settings:
   - **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
   - **Detection Area:** By default, the whole image is set to be the detection area. Optionally, click **Delete** -, and click and drag on the image to remove the detection area. Click **Add** + to draw new detection areas.
   - **Detection Type:** Select to detect **Human Heads**, or **People or Vehicles.**
   - **Confidence Value:** Available only when *Human Heads* is selected as detection type. The higher the value, the more definitive and stricter the system is in distinguishing whether people are gathering. The default value is 50. You can click **Confidence Test** to see the detection results based on the set value.
   - **Sensitivity:** Available only when *Human Heads* is selected as detection type. The higher the value, the more sensitive the detection is. The default value is 3.
   - **Mask Regio**n: Click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.

4. Right-click on the detection area drawn and select **Edit** to have further settings:



- **ID:** Name the set area.
- **Event Interval:** Specify the time interval between events to prevent frequent alerts. Any events that occur during that time are ignored.
- **Triggered by:** Define the detection sensitivity.
  - **Center:** Crowd Detection is triggered only when the center of a person or vehicle crosses the set area.
  - **Touch:** Crowd Detection is triggered when any part of a person or vehicle touches the set area.
- **Max Number of People Allowed:** Crowd Detection is triggered when a specified number of people is reached.
- **Max Number of Vehicle Allowed**: Crowd Detection is triggered when a specified number of vehicles is reached.
- **Max Number of Heads Allowed:** Available only when *Human Heads* is selected as detection type. Crowd Detection is triggered when a specified number of heads is reached.
- **Alert Settings:** Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon crowd detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

5. Click **OK**.
6. Start monitoring.

Once set up, when the capacity of people or vehicles is detected over the threshold, they will be highlighted by red rectangles on the live view.

1.3.8 LPR Setting

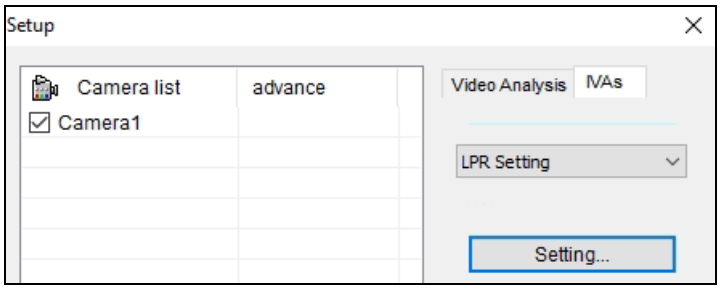
The LPR Setting is used to define an LPR recognition engine for a camera to detect and recognize license plate numbers. The LPR settings work with the following functions to allow the camera to recognize license plates:

- Vehicle Loitering (see *1.3.3 Loitering*)
- Average Speed Detection (see *1.3.9 Average Speed Detection*)
- Vehicle Attributes Recognition (see *1.4.9 Vehicle Attributes Recognition*)

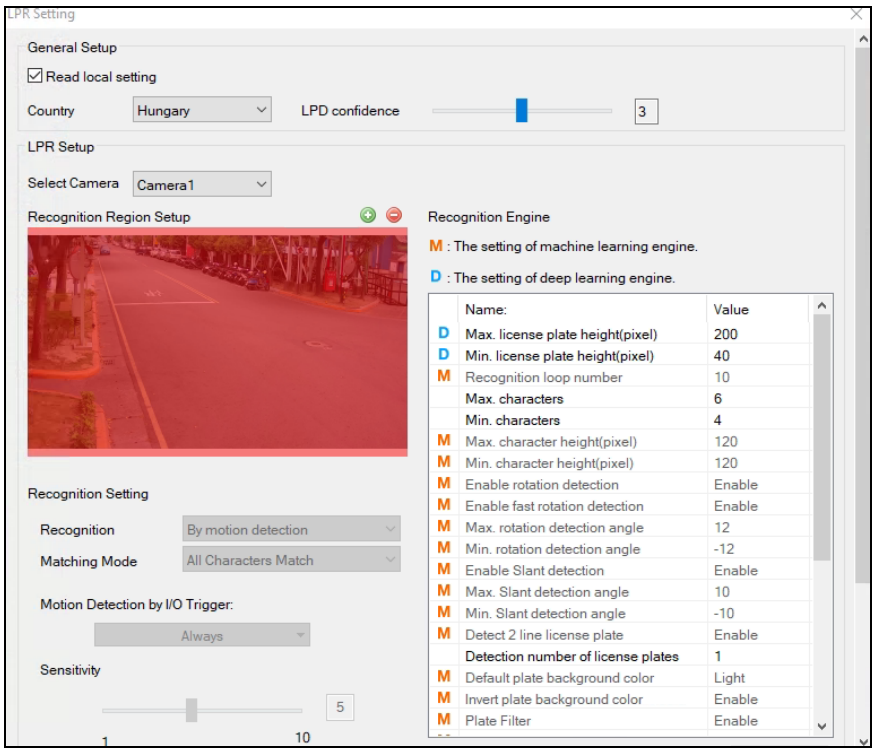
Note:

1. The **LPR-Related Event** license is required to enable this function. See the *License* section in the datasheet.
2. The LPR engines for license plate recognition include the following 14 countries/areas: Europe, France, Germany, Hungary, Israel, Italy, Myanmar, Netherlands, Slovakia, Taiwan, UK, USA (California, Georgia), and Vietnam.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Analytics*.
2. On the Setup window, select at least one camera > **LPR Setting** and click **Setting**.



3. On this dialog box, define the settings for the LPR application.



[General Setup] Enable **Read Local Setting** and select a **Country** for the LPR application.

[LPR Setup] Select the camera to be applied to.

[Recognition Region Setup] By default, the whole image is set to be the detection area. Optionally, click **Delete**, and click and drag on the image to remove the detection area. Click **Add** to draw new detection areas.

[Recognition Region Setup] The system automatically sets the recognition mode and license plate matching mode, and turns on motion detection by I/O trigger.

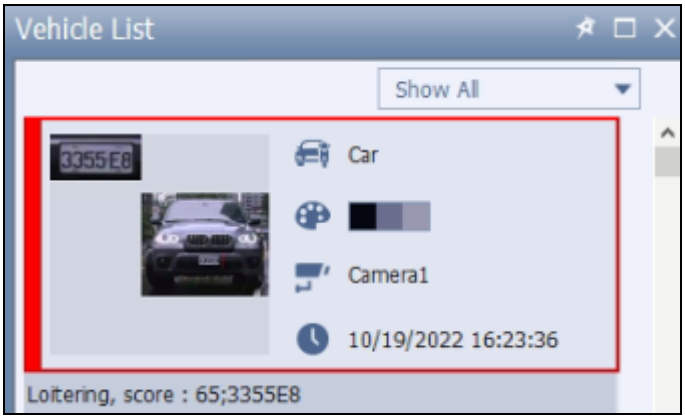
[Recognition Engine] Define the recognition engine. Currently, only the following options are available:

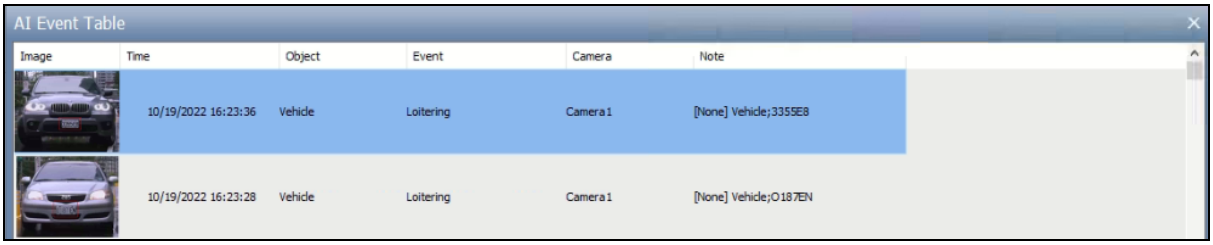
- **Max. / Min. license plate height (pixels):** Set the maximum, from 12 ~ 999 (default = 200), or minimum, from 1 ~ 999 (default = 40), heights of the license plates to activate the recognition process. If the height of the license plate exceeds the maximum or is under the minimum, the system will not start the recognition.
- **Recognition loop number:** Repeat recognition for the number of times specified, from 1 ~ 20 (default = 10).

- **Max. / Min. characters:** Set the maximum, from 3 ~ 16, or minimum, from 2 ~ 16, number of characters on the license plate to activate the recognition process. If the number of characters exceeds the maximum or is under the minimum, the system will not start the recognition. The default values of max. and min. are dependent on the country of recognition engine.
- **Detection number of license plates:** Set the maximum number of plates to be recognized simultaneously, from 1 ~ 8 (default = 1).

4. Click **OK.**
5. Set up vehicle loitering. For details, see *1.3.3 Loitering*.

Once set up, you can see the detected license plate numbers in the two places: Vehicle/Others List and AI Event Table.





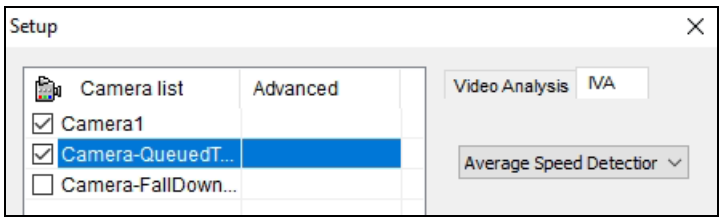
1.3.9 Average Speed Detection

The Average Speed Detection is used to trigger alerts when vehicles overspeed in a predefined area.

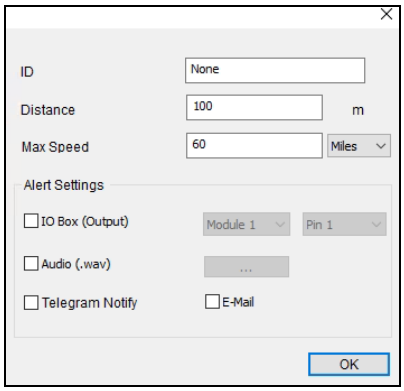
Note:

1. Average Speed Detection requires a minimum of 2 **LPR-Related Event** license channels to operate, with a maximum of 16 sets of Average Speed Detection functions enabled. See the *License* section in the datasheet.
2. Before the configurations, make sure **Read local setting** is enabled. See *1.3.8 LPR Setting* for details.

1. Ensure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select **two** cameras > **Average Speed Detection** and click **Setting**.



3. On the Speed Dlg window, select the detection cameras under **Camera In / Out.**
4. Click **Add** at the left lower corner on the window to establish the detection rule.
5. Click and drag to draw the detection areas on the images of *camera in / out* to identify over speeding events.
6. Click the **Settings** button . The dialog box appears:

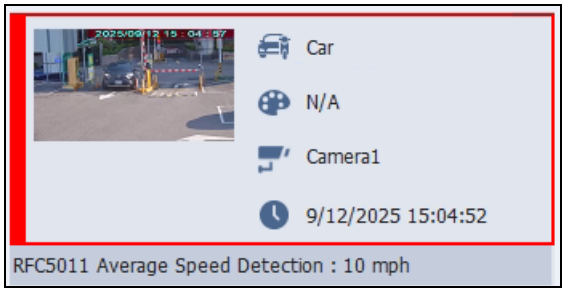


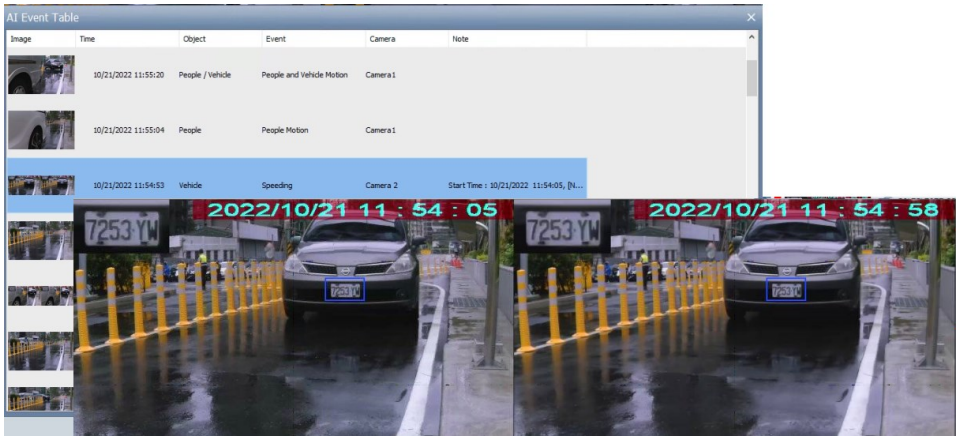
- **ID:** Name the set area.
- **Distance:** Specify the distance between the 2 detection cameras (unit: meters).
- **Max Speed:** Specify the maximum speed of the vehicle in miles or kilometers.

- **Alert Settings**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon over speed events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

7. Click **OK**.
8. Start monitoring.

Once set up, you can see the detected license plate numbers and speed (miles per hour) in the Vehicle/Others List and AI Event Table.



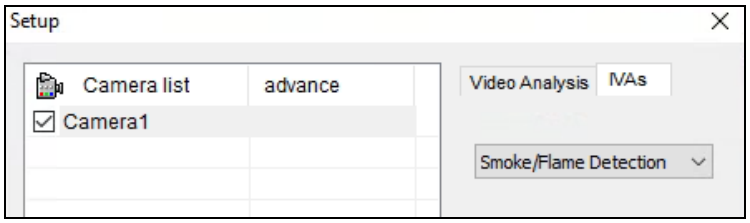


Using the AI Query filter, you can search for vehicles with specific license plates and speeds. See *1.6.1. AI Query* for details.

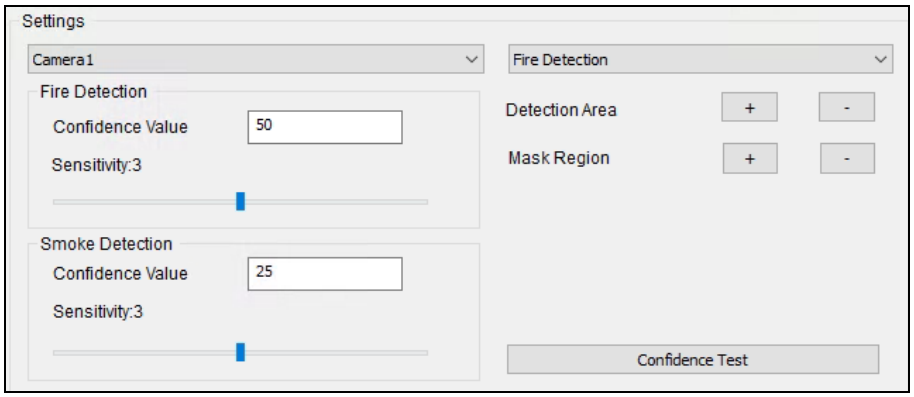
1.3.10 Smoke/Flame Detection

The Smoke/Flame Detection is used to trigger alerts when smoke or flames are detected in a predefined area.

1. Ensure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics*.
2. On the Setup window, select at least one camera > **Smoke/Flame Detection** and click **Setting**.

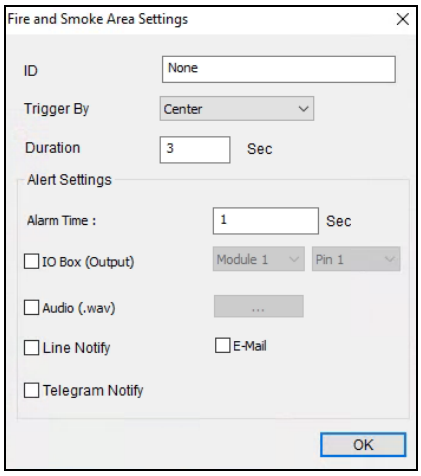


3. On the Fire and Smoke Settings window, select the detection object, **Fire Detection, Smoke Detection,** or **Fire or Smoke Detection** from the right dropdown list.



- **Confidence Value:** The higher the value, the more definitive and stricter the system is in distinguishing whether there is smoke or fire. You can click **Confidence Test** to see the detection results based on the set value.
- **Sensitivity:** The higher the value, the more sensitive the detection is. The default value is 3.
- **Detection Area:** By default, the whole image is set to be the detection area. Optionally click **Delete** -, and click and drag on the image to remove the detection area. And click **Add** + to draw new detection areas.
- **Mask Region:** Click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.

4. Right-click on the detection area drawn and select **Edit** to have further settings:



- **ID:** Name the set area.
- **Sensitivity:** Define the detection sensitivity.
  - **Center:** Smoke/Flame Detection is triggered only when the center of the smoke or fire crosses the set area.
  - **Touch:** Smoke/Flame Detection is triggered when any part of the smoke or fire touches the set area.
- **Duration:** The detection is triggered only when the smoke or fire is detected in the predefined area exceeding the specified duration (1-9999 seconds).
- **Alert Settings:** Specify the **Alarm Time** in seconds for IO Box / Audio. Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon smoke/flame detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

5. Click **OK**.
6. Start monitoring.

Once set up, any detected fired or flame will be displayed in the Vehicle/Others List and highlighted in red rectangles on the live view.

Disclaimer: Geovision stands by the principle that traditional fire alarm systems should not be replaced by video-based fire alarm systems; instead, video-based fire alarm systems should complement traditional setups. Users should understand that a properly installed and well-maintained fire indication system will reduce the possibility of fire or accident, but it is not an insurance policy or an absolute guarantee against such incidents. Its presence doesn't ensure immunity from personal injury or property damage.

1.3.11 Fall Down Detection

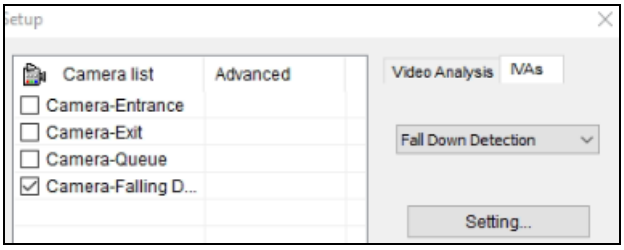
The Fall Down Detection is designed to detect falls experienced by the elderly or individuals.

Note: The Fall Down Detection is designed for healthcare settings. When the feature is used in an outside situation, detection may fail or misrecognize.

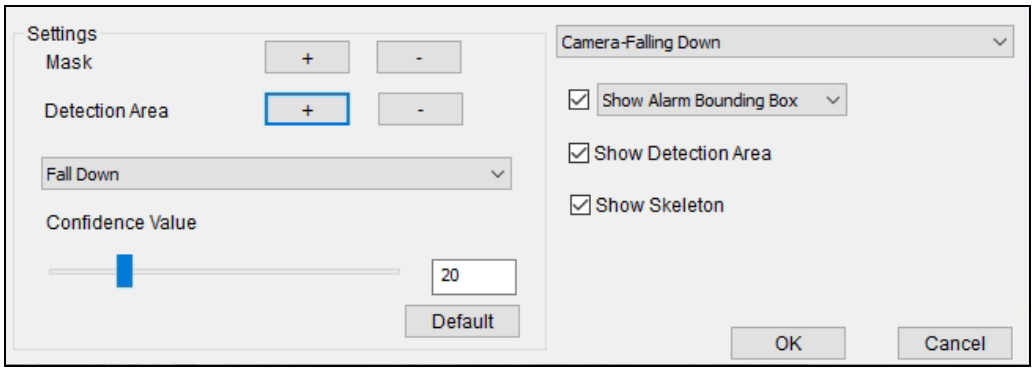
Activation Requirements

To enable **Fall Down Detection**, the corresponding **GV-AI Guard Plugin** must be installed. You can download the plugin from GeoVision Website.

1. Make sure you have started AI video analytics settings described in *1.3.1 Starting Basic AI Video Analytics.*,
2. On the Setup window, select at least one camera > **Fall Down Detection** and click **Setting**.



3. On the Fall Down Detection Settings window, configure the following settings.



- **Mask:** Click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Detection Area:** Select **Add** +, and drag to draw a detection area on the image. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Confidence Value:** The higher the value, the more definitive and stricter the system is to detect objects.

- **Show Alarm Bounding Box:** Display red bounding boxes around people detected as having fallen. Select **Show All** to display not only red bounding boxes for fall events and green bounding boxes around detected people.
- **Show Detection Area:** Display the defined detection area on live view and recordings.

4. Click **OK**.
5. Start monitoring.

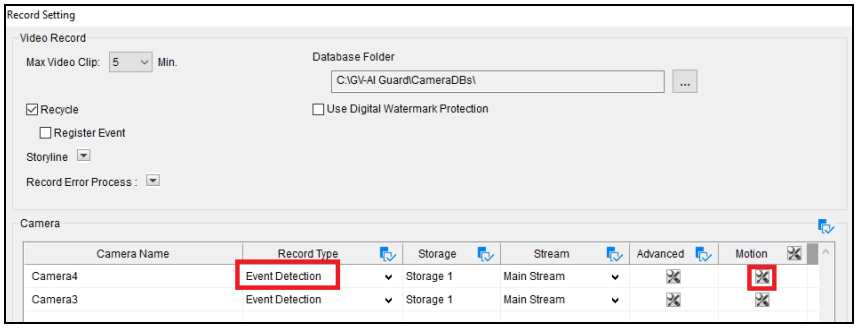
Once set up, persons who fall will be displayed in the Human Detection list and highlighted in red rectangles on the live view.

1.4 Advanced AI Video Analytics

1.4.1 Starting Advanced AI Video Analytics

Prerequisites

1. To record AI video analytics events, first configure the following two camera settings in the Recording Setting dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting**).



A. **Verify the recording type is set to Event Detection.**

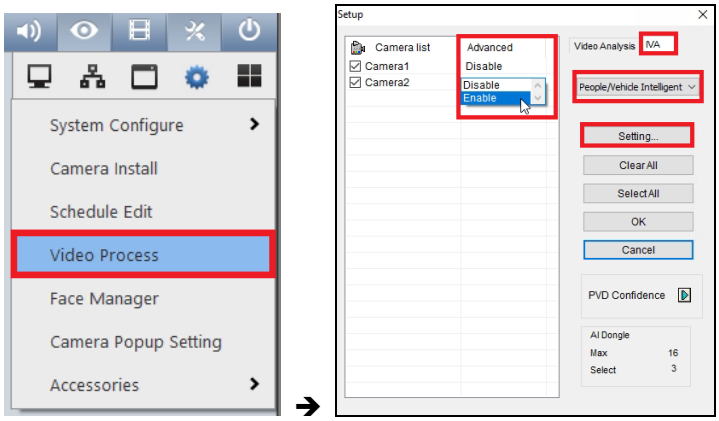
Ensure **Event Detection** is enabled under Record Type.

B. **Enable Registered Motion Event.**

Click the **Tool** icon for the camera. In the Advanced Motion Detection Setup dialog box, enable **Registered Motion Event**.

Accessing the Settings

2. To access advanced AI analytics settings, click **Home** > **Toolbar** > **Configure** > **Video Process** > the **IVA** tab.
3. Select at least one camera, and select **People/Vehicle Intelligent Analysis**.
4. In the Advanced field, select **Enabled** to enable advanced AI analytics, then click **Setting** to start the configuration.



Optional Setup for PAC and PVD

5. You can enable the system to collect people attributes (PAC), and fine-tune the people and vehicle detection (PVD) confidence parameters to optimize performance based on your camera and application scenario. For real-world examples, see *Confidence Threshold Setting* in this technical notice.

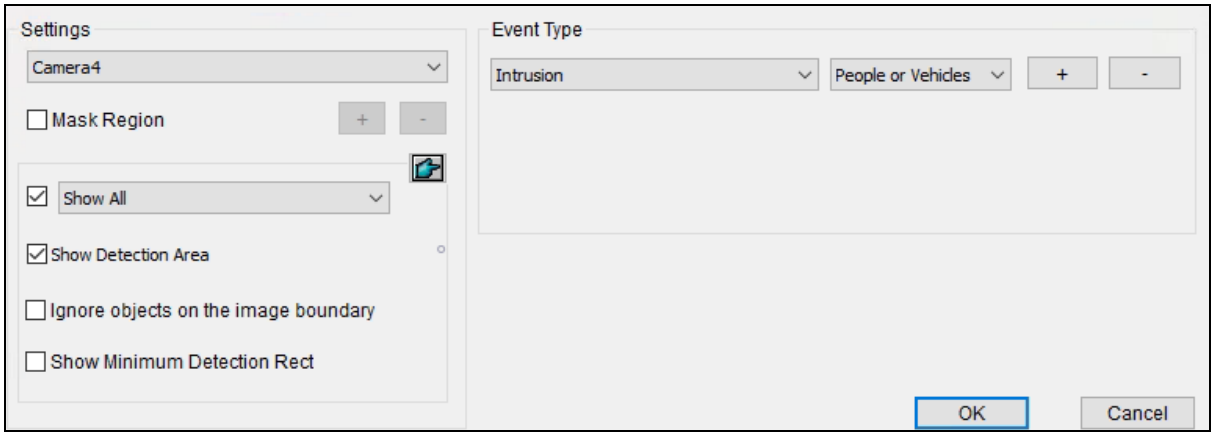
   - Click the  icon next to **PVD Confidence** in the Setup dialog box. See Step 4, *1.3.1 Starting Basic AI Video Analytics* for details.

Note: Each enabled **Advanced AI Video Analytics** requires 2 channels of the AI Analytics licenses. See the *Licenses* section in the datasheet.

1.4.2 Intrusion (Advanced)

The Intrusion (advanced) function is to detect and capture any person or vehicle entering predefined areas of the same group at the set direction.

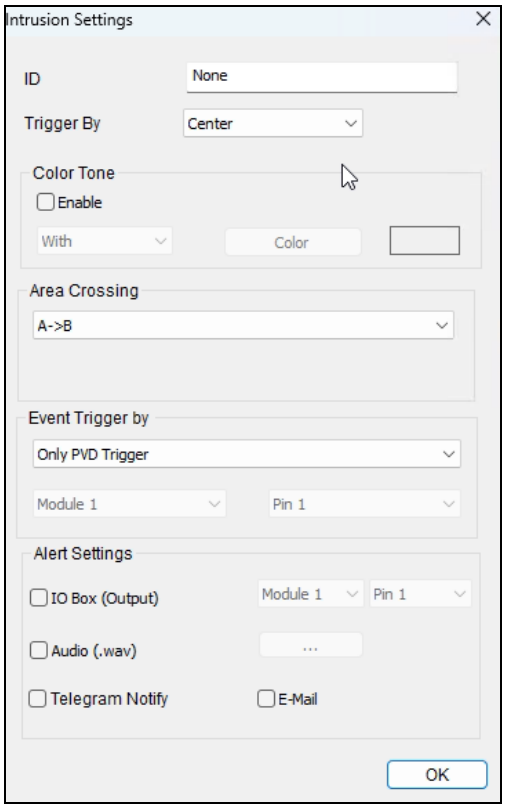
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics*.
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Bounding Box Display:**
  - **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
  - **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles, or green bounding boxes around detected people.
  - **Show All:** Display bounding boxes around all objects, including people and vehicles, that trigger event alerts.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Intrusion** from the Event Type dropdown list, and select the type of objects, **People** and/or **Vehicles**, you want the Intrusion to be detected.

4. Select **Add** +, and click and drag to draw pairs of intrusion areas on the image, where each pair is categorized as the same detection group.
5. Right-click on the drawn intrusion areas and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger By:** Define the detection sensitivity.
  - **Center:** Intrusion is triggered only when the center of a person or vehicle crosses the set area.
  - **Touch:** Intrusion is triggered when any part of a person or vehicle touches the set area.
- **Color Tone:** Intrusion is triggered when a specified color, included or excluded, is detected. Click the **Color** button, and click and draw on the image with the color you want to be detected.
- **Area Crossing**: Intrusion is triggered when any person / vehicle passes through two defined areas of *the same group*.

Note: Grouping Detection Areas:
A group is used to associate two detection areas. Only two areas can be included in a single group, and area crossing detection is only triggered when both areas belong to the same group. Area crossings between different groups will not be detected.

- **Event Trigger by:** Intrusion is triggered upon a PVA trigger (People/Vehicle Detection event) and/or a sensor activated.

6. Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon intrusion events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.
7. Click **OK**.
8. Start monitoring.

Once set up, people or vehicles detected intruding will be highlighted by red rectangles on the live view.

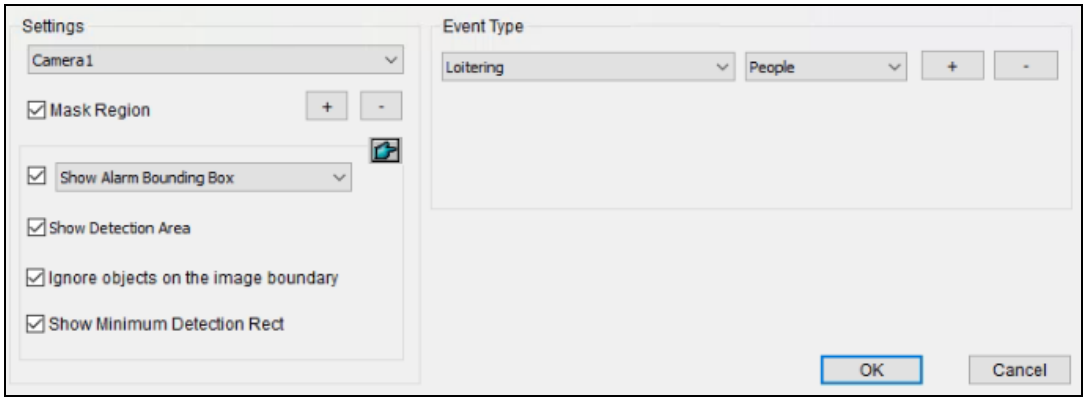
1.4.3 Loitering (Advanced)

With the advanced detection mechanism, the Loitering (advanced) function detects and notifies the user of people or vehicles caught staying/parking in the prohibited area more accurately.

Note:

1. The **LPR-Related Event** license is required to enable the Loitering LPR function. See the *License* section in the datasheet.
2. Before the configurations of Loitering LPR, ensure **Read local setting** is enabled. See *1.3.8 LPR Setting* for details.

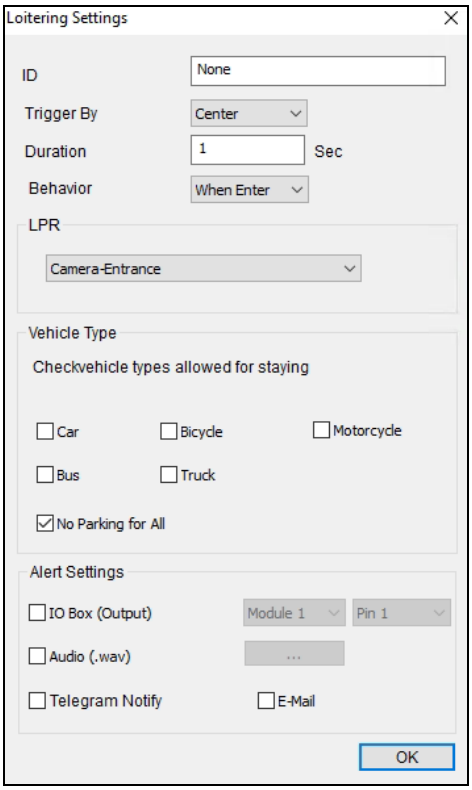
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics.*
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Bounding Box Display:**
  - **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
  - **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles, or green bounding boxes around detected people.
  - **Show All:** Display bounding boxes around all objects, including detected people and vehicles, that trigger event alerts.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.

- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Loitering** from the Event Type dropdown list, and select the type of objects, **People** or **Vehicles**, you want the Loitering to be detected.
4. Select **Add** , and drag to draw an area on the image. Any person or vehicle remaining in the area will be detected as a loitering event. To shape a polygon area, double-click on the sides of the lines and drag the joints.
5. Right-click on the drawn loitering areas and select **Edit** to define which conditions the alert will be triggered.

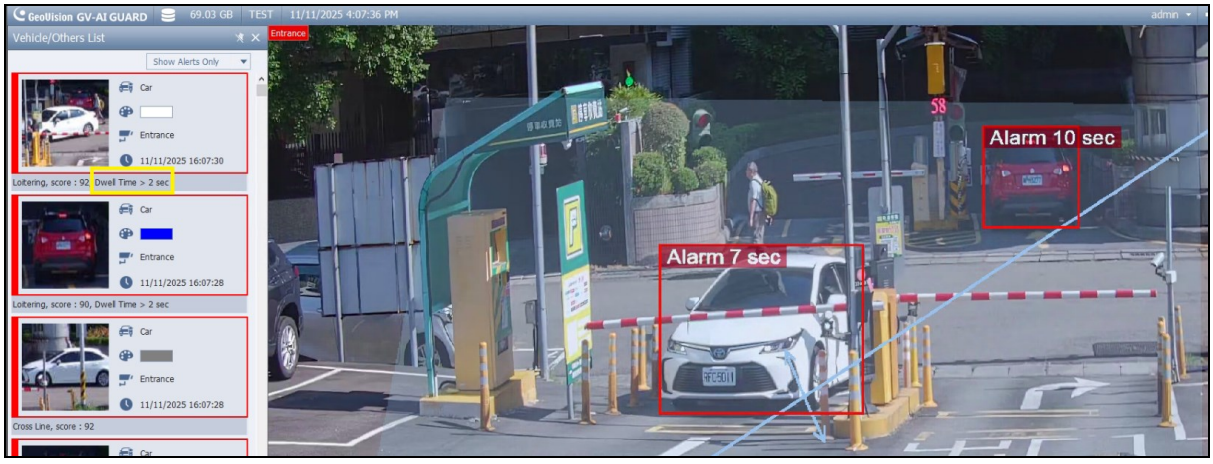


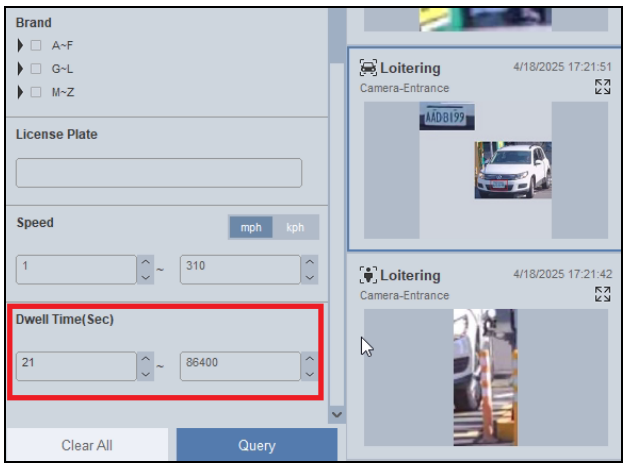
- **ID:** Name the set area.
- **Trigger by:** Define the detection sensitivity.
  - **Center:** Loitering is triggered only when the center of a person or vehicle crosses the set area.
  - **Touch:** Loitering is triggered when any part of a person or vehicle touches the set area.
- **Duration:** Loitering is triggered only when a person or vehicle remains in the set area exceeding the specified duration (1-9999 seconds).

- **Behavior**: Define the object's behavior in the set area to trigger the loitering event, which include **When Stopped** or **When Enter.**
- **LPR:** For *Vehicle Loitering* only. The selected camera will detect and recognize license plate numbers. For this function, you need to set up the camera for LPR recognition in advance. For details, see *1.3.8 LPR Setting*.
- **Vehicle Type:** For *Vehicle Loitering* only. Select the types of vehicles that are permitted to remain in the defined area, e.g. buses only at bus stops.
- **Alert Settings:** Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon loitering events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

6. Click **OK**.
7. Start monitoring.

Once set up, **people or vehicles detected as loitering** will be highlighted with red rectangles on the live view. And In the Vehicle/Others List, loitering events are also displayed along with the corresponding **Dwell Time**.



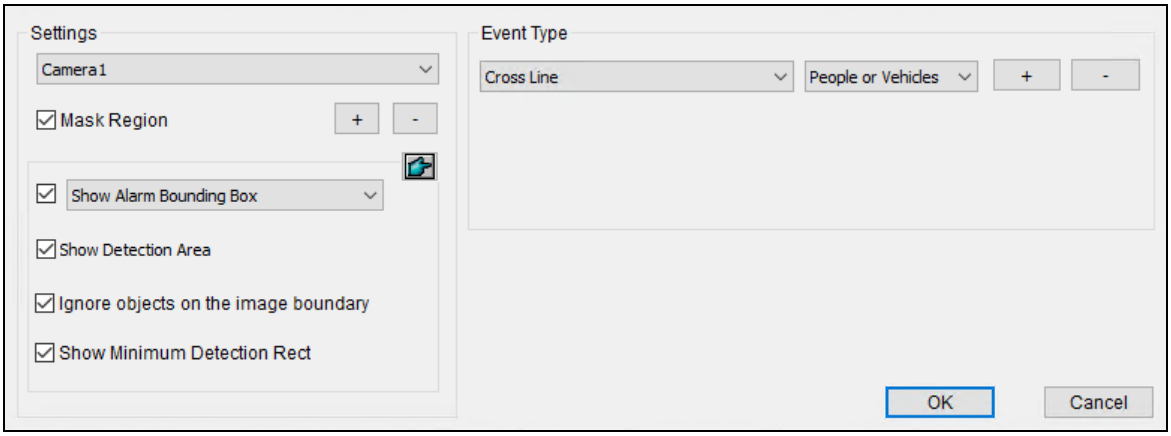


Tip: To search for loitering events, use the AI Query filter and specify the **Dwell Time (sec)** under **Person** or **Vehicle** attributes based on the loitering Dwell Time. See*1.6.1 AI Query*.

1.4.4 Cross Line

The Cross Line function detects and notifies the user of people or vehicles crossing the predefined detection line in the set direction.

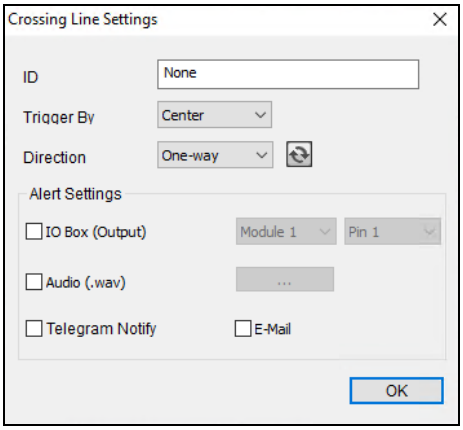
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics*.
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles, or green bounding boxes around detected people.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Cross Line** from the Event Type dropdown list, and select the type of objects, **People** or **Vehicles**, you want the Cross Line to be detected.
4. Select **Add** + under Event Type, and click and drag to draw a detection line on the image. When any person or vehicle crosses the detection line at the set direction, it will be detected as a crossline event.

5. Right-click on the drawn line and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set line.
- **Sensitivity:** Define the detection sensitivity.
  - **Center:** The detection is triggered only when the center of a person crosses the set line.
  - **Touch:** The detection is triggered when any part of a person touches the set line.
- **Direction:** Select the detection direction. Click to reverse the direction when one-way detection is selected.
- **Alert Settings**: Select **IO Box (Output)**, **Audio (.wav)**, **Telegram Notify**, or **E-mail** to activate output modules, computer audio alarms, or notifications upon loitering events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this chapter.

6. Click **OK**.
7. Start monitoring.

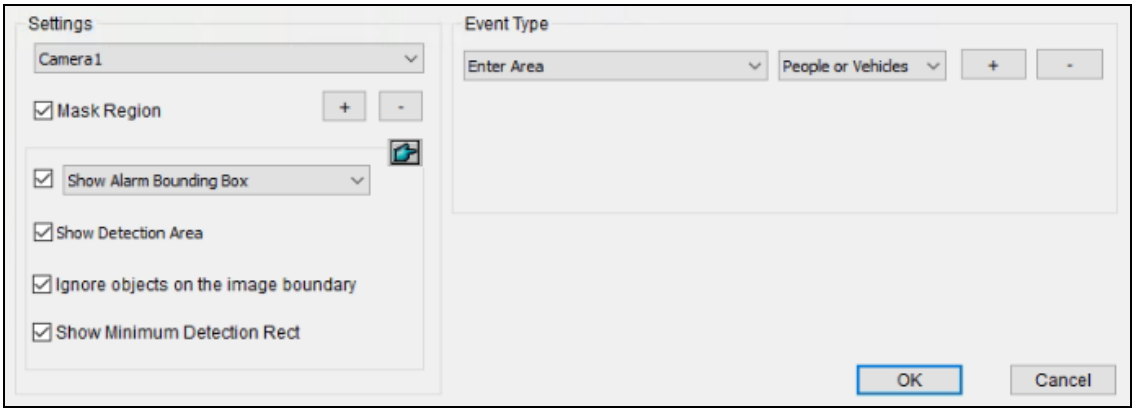
Once set up, people or vehicles detected crossing lines will be highlighted by red rectangles on the live view.



1.4.5 Enter / Leave Area

The Enter / Leave Area function detects and notifies the user of people or vehicles entering / leaving the predefined area.

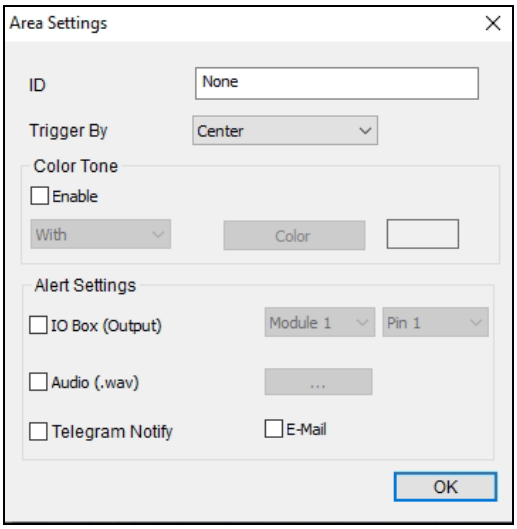
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics.*
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles, or green bounding boxes around detected people.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Enter Area** or **Leave Area** from the Event Type dropdown list, and select the type of objects, **People** or **Vehicles**, you want the Enter / Leave Area to be detected.
4. Select **Add** +, and drag to draw an enter / leave area on the image. Any person or vehicle entering / leaving the area will be detected as an enter / leave area event. To shape a polygon area, double-click on the sides of the lines and drag the joints.

5. Right-click on the drawn enter / leave areas and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger By:** Define the detection sensitivity.
  - **Center:** The detection is triggered only when the center of a person / vehicle crosses the set area.
  - **Touch:** The detection is triggered when any part of a person / vehicle touches the set area.
- **Color Tone:** Enter / Leave Area is triggered when a specified color, included or excluded, is detected. Click the **Color** button, and click and draw on the image with the color you want to be detected.
- **Alert Settings**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon loitering events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

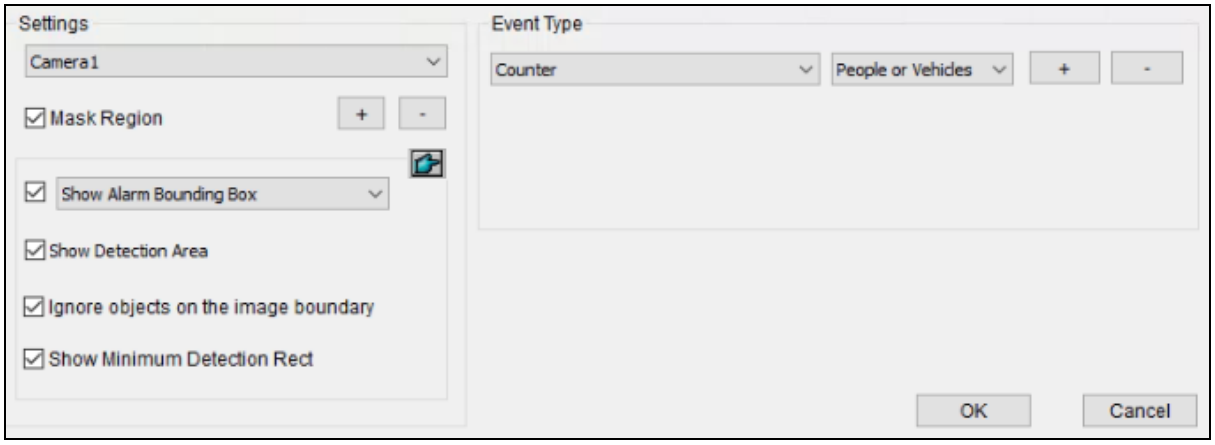
6. Click **OK**.
7. Start monitoring.

Once set up, people or vehicles detected entering / leaving areas will be highlighted by red rectangles on the live view.

1.4.6 Counter

The Counter function counts people or vehicles crossing the predefined detection lines at the set direction.

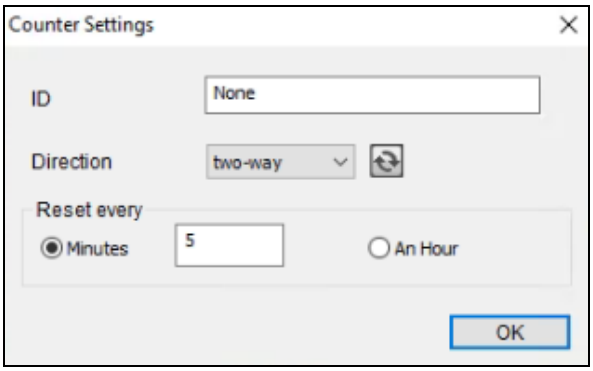
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics.*
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles, or green bounding boxes around detected people.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any people and vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Counter** from the Event Type dropdown list, and select the type of objects, **People** or **Vehicles**, you want the Counter to be detected.
4. Select **Add** +, and click and drag to draw a counting line on the image. Any person or vehicle crossing the line will be counted as going in / out.

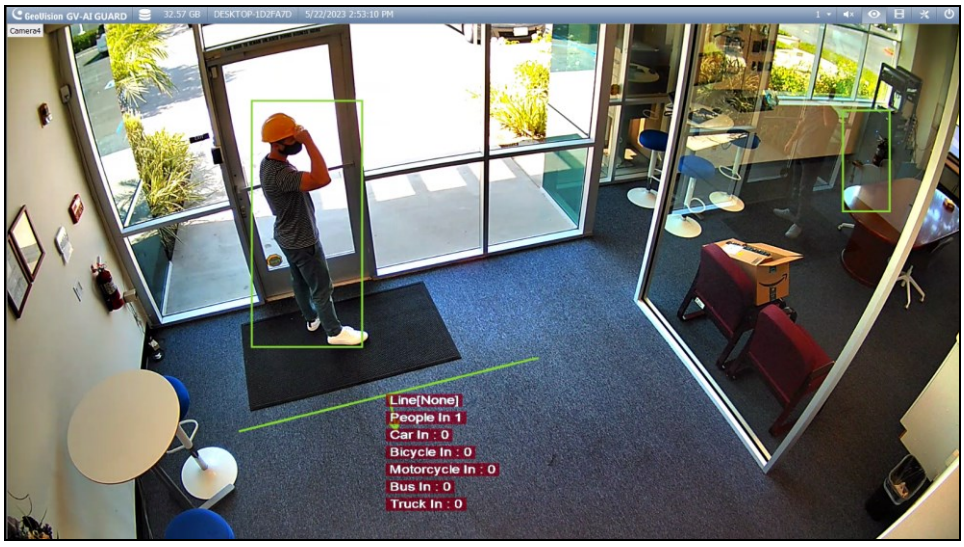
5. Right-click on the drawn line and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Direction:** Select the counting direction. Click  to reverse the in / out direction.
- **Reset Every:** Specify the time after which the counting data will be cleared; optionally, select **An Hour** to reset the data hourly.

6. Click **OK**.
7. Start monitoring.

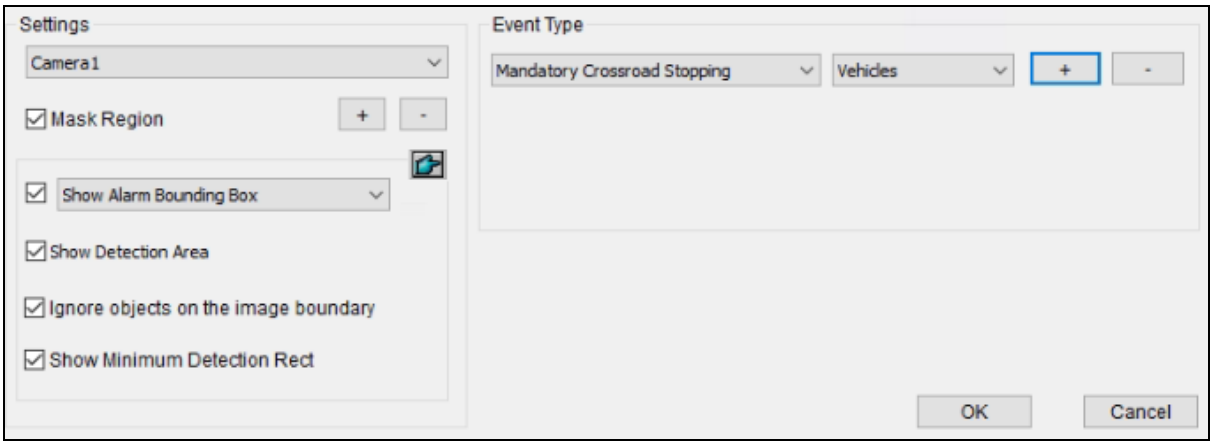
Once set up, the number of people or vehicles detected crossing the detection lines will be displayed on the live view.



1.4.7 Mandatory Crossroad Stopping

The Mandatory Crossroad Stopping function is used to monitor crossroad scenarios where certain types of vehicles, such as trucks, are required to stop and be aware of current traffic conditions before proceeding. Mandatory Crossroad Stopping detects and captures vehicles that are required to stop but fail to do so, thereby violating safety regulations.

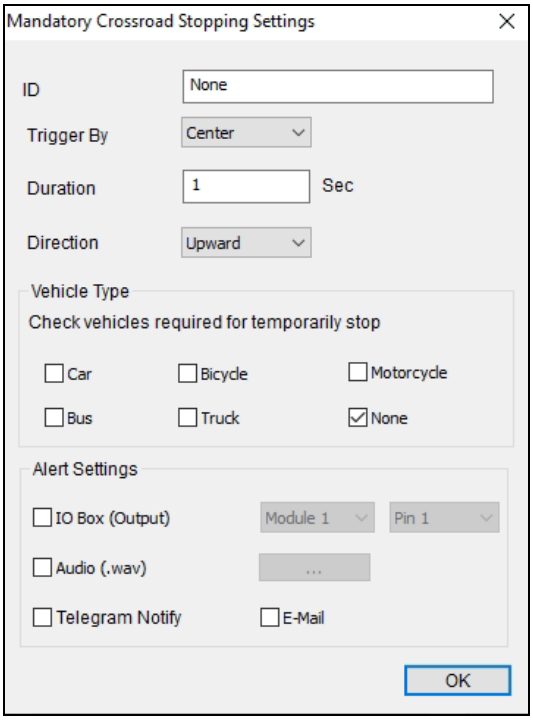
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics*.
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. **Vehicles** is selected by default from the Event Type dropdown list.

4. Select **Add** +, and drag to draw a detection area on the image. Any vehicle passing the area below the specified duration will trigger the alert. To shape a polygon area, double-click on the sides of the lines and drag the joints.
5. Right-click on the drawn line and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Sensitivity**: Define the detection sensitivity.
  - **Center:** The detection is trigger ed only when the center of vehicles crosses the set area.
  - **Touch:** The detection is triggered when any part of vehicles touches the set area.
- **Duration:** The alert is triggered when the time length of a vehicle passing the set area is shorter than the specified duration (1-9999 seconds).
- **Direction:** Select the passing direction of the vehicle. When the vehicle passes the set area in the designated direction under the specified duration, the alert will be triggered.
- **Vehicle Type:** Select the types of vehicles that should temporarily stop at the set area.
- **Alarm Settings**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon loitering events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

6. Click **OK**.
7. Start monitoring.

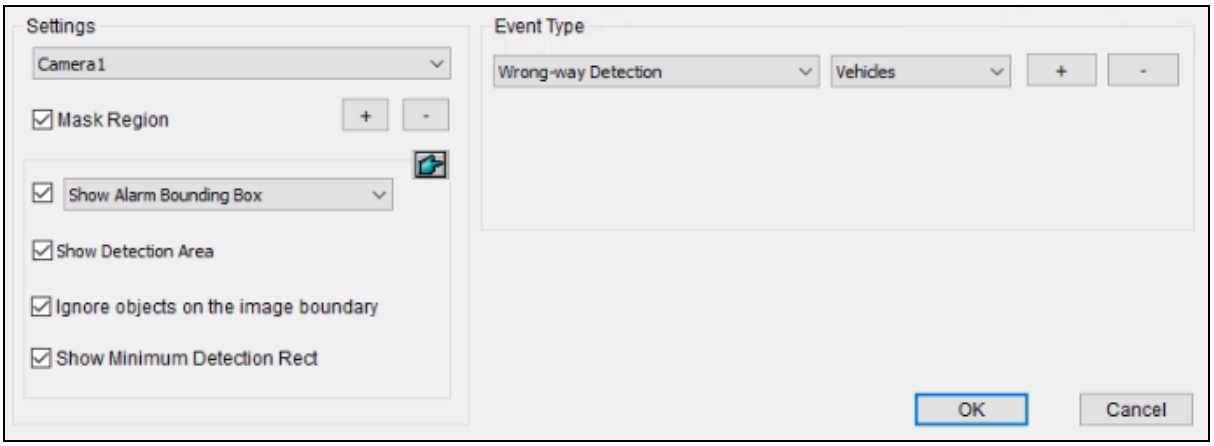
Once set up, vehicles detected passing through Mandatory Crossroad Stopping Areas without stopping will be highlighted by red rectangles on the live view.



1.4.8 Wrong-way Detection

The Wrong-way Detection function detects and notifies the user of vehicles detected passing the detection line in the wrong direction.

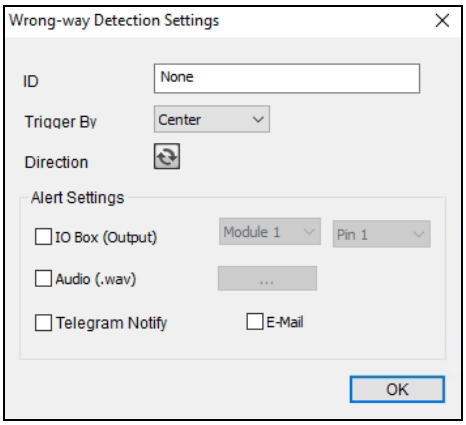
1. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics.*
2. On the People/Vehicle Intelligent Video Analysis window, configure the following settings:



- **Mask Region:** Select and click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Show Alarm Bounding Box:** Display red bounding boxes around objects that trigger event alerts.
- **Show Object Bounding Box:** Display light blue bounding boxes around detected vehicles.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Ignore Objects on the Image Boundary:** Ignore any vehicles detected and captured at the edges of the video.
- **Show Minimum Detection Rect:** Display the min size of objects that the system can detect in the top left corner of the setting image as a reference.
- **Apply All** : Optionally, click the button to apply above settings, except Mask Region, to all channels.

3. Select **Wrong-way Detection** from the Event Type dropdown list. Only *Vehicles* is applicable for the function.
4. Select **Add** +, and click and drag to draw a detection line on the image. Any vehicle passing the line in the wrong direction will trigger the alert.

5. Right-click on the drawn line and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set line.
- **Sensitivity**: Define the detection sensitivity.
  - **Center:** The detection is triggered only when the center of vehicles crosses the set line.
  - **Touch:** The detection is triggered when any part of vehicles touches the set line.
- **Direction:** Click to reverse the detection direction.
- **Alert Settings**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon loitering events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

6. Click **OK**.
7. Start monitoring.

Once set up, vehicles detected passing the detection line in the wrong direction will be highlighted by red rectangles on the live view.



1.4.9 Vehicle Attributes Recognition

The Vehicle Attributes Recognition functions provide comprehensive vehicle information, including license plate numbers, eTag details, and key attributes such as vehicle type, brand, and color. This feature is ideal for applications such as vehicle entrance/exit management and queued traffic control, enhancing operational efficiency.

When integrated with the GV-RU9003 RFID reader, the **Zone Monitor** function expands functionality by detecting eTags carried by employees within a monitoring area, enabling seamless employee tracking and access management.

Supported Applications

The Vehicle Attributes Recognition cover the following applications and sections:

- *1.4.9.1 Vehicle and Employee Registration*
- *1.4.9.2 Entrance*
- *1.4.9.3 Zone Monitor*
- *1.4.9.4 Exit*
- *1.4.9.5 Queued Traffic*
- *1.4.9.6 Vehicle Attribute Event Search*

Limitations

- Motorcycles, bicycles, and buses are not supported for vehicle type recognition.
- For details on supported object types and vehicle brands, see the document.

License Requirements

- **Queued Traffic** and **Zone Monitor** each require 2 AI license channels.
- **Entrance** requires 2 AI license channels and 1 LPR-Related Event license to operate.
- **Exit** must be paired with Entrance, with each requiring 2 AI Analytics channels and 1 LPR-Related Event license. A paired Entrance + Exit setup requires a total of 4 AI Analytics channels and 2 LPR-Related Event licenses.

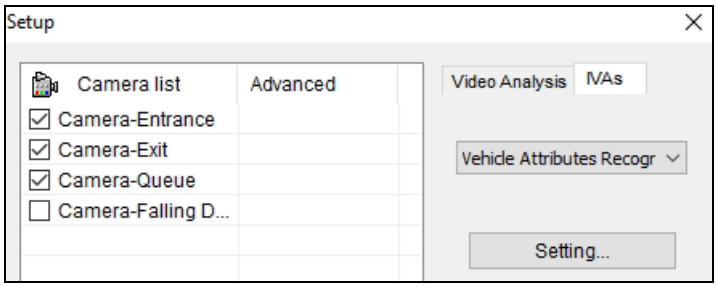
See the *License* section in the datasheet.

Activation Requirements

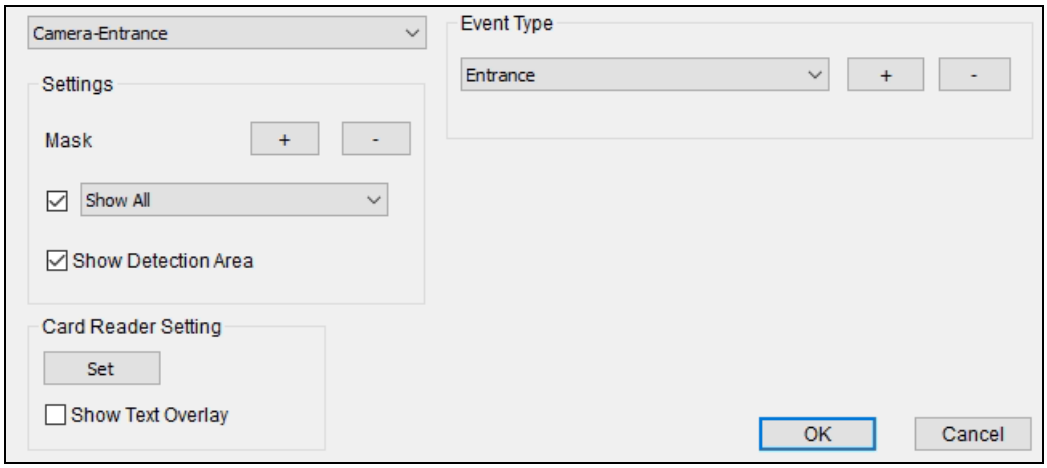
The Vehicle Attributes Recognition requires the corresponding **GV-AI Guard Plugin** to be installed. You can download the plugin from GeoVision Website.

To configure vehicle attributes recognition, follow the steps below:

1. Ensure that you have enabled **Read local setting** described in *1.3.8 LPR Setting.*
2. Ensure you have started AI video analytics settings described in *1.4.1 Starting Advanced AI Video Analytics.*
3. On the Setup window, select at least one camera > **Vehicle Attributes Recognition** and click **Setting**.



4. On the Vehicle Attributes Recognition Settings window, configure the following settings:



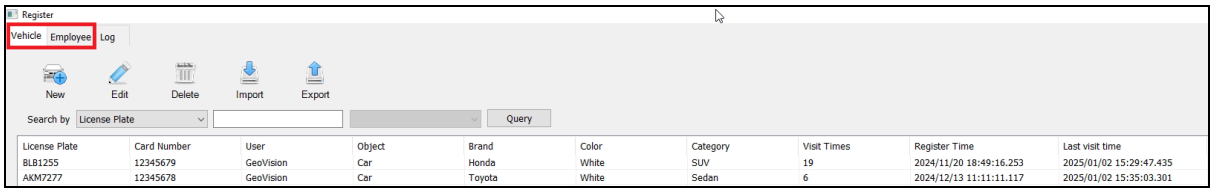
- **Camera:** Select a camera to configure.
- **Mask:** Click **Add** + to draw areas on the image that the detection will ignore. To shape a polygon area, double-click on the sides of the lines and drag the joints.
- **Bounding Box Display:**
  - **Show Alarm Bounding Box:** Display red bounding boxes around detected vehicles.
  - **Show All:** Display bounding boxes around all objects, including detected people and vehicles, that trigger event alerts.
- **Show Detection Area:** Display the defined detection area on live view and recordings.
- **Card Reader Setting:** Only available when **Entrance** or **Zone Monitor** is selected from the Event Type dropdown list for using the GV-RU9003 RFID reader to detect eTag.

- **Event Type:** Refer to sections 1.4.9.2 through 1.4.9.5 for configuration details on the following settings:
  - **Entrance** (Section 1.4.9.2)
  - **Zone Monitor** (Section 1.4.9.3)
  - **Exit** (Section 1.4.9.4)
  - **Queued Traffic** (Section 1.4.9.5)

1.4.9.1 Vehicle and Employee Registration

Creating a **vehicle database** allows the system to classify vehicle recognition events as either "Authorized" or "Unauthorized", based on the registered data.

Creating an **employee database** enables the **Zone Monitor** function to work with the GV-RU9003 RFID reader, allowing detection of eTag for employee identification.



1. Click **Home** > **Toolbar** > **Configure** > **Vehicle Management**.
2. To create vehicle data, click the **Vehicle** tab > **New**.
   - For card detection, ensure to enter **Card Number** under the Vehicle tab.
3. To create employee data, click the **Employee** tab > **New**.

Note: A maximum of 10,000 vehicle profiles and 10,000 employee profiles can be created separately.

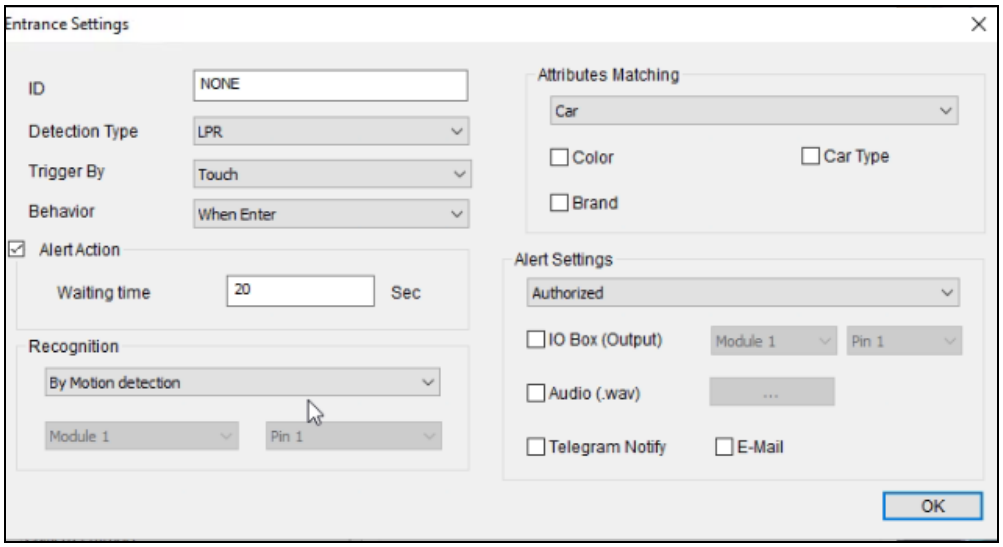
1.4.9.2 Entrance

The Entrance function detects license plate numbers, eTag data, and key vehicle attributes, including color, type and brand, when vehicles enter a perimeter. This functionality is ideal for applications such as parking lots or car wash stations. By comparing detected information with entries in the vehicle database, the system can trigger authorized or unauthorized events. Additionally, vehicle waiting time data can be utilized to optimize operations and improve service satisfaction.

Follow the steps below:

1. Create a vehicle database by following the steps in *1.4.9.1 Vehicle and Employee Registration*.
2. To start Vehicle Attributes Recognition settings, follow Steps 1 ~ 3 in *1.4.9 Vehicle Attributes Recognition.*

3. On the Vehicle Attributes Recognition Settings window, select **Entrance** from the Event Type dropdown list.
4. Select **Add** +, and drag to draw the entrance area on the image. To shape a polygon area, double-click on the sides of the lines and drag the joints.
5. Right-click on the drawn area and select **Edit** to define which conditions the alert will be triggered.

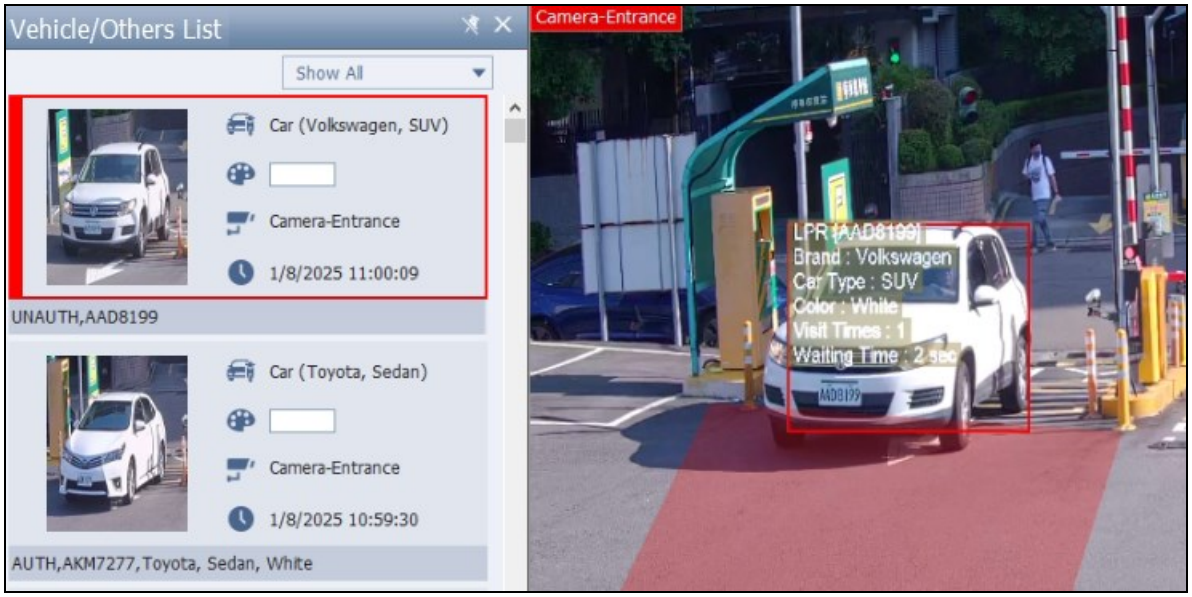


- **ID:** Name the set area.
- **Detection Type:** Select a detection and recognition object: **LPR** for license plates only, **Card** for eTag only, or **LPR or Card** for both.
- **Trigger By:** Define the detection sensitivity.
  - **Center:** Events are triggered only when the center of a vehicle crosses the set area.
  - **Touch:** Events are triggered when any part of a vehicle touches the set area.
- **Behavior**: Define the vehicle's action in the set area to trigger events, which include **When Stopped** or **When Enter**.
- **Alert Action - Waiting Time:** Set the time in seconds that a vehicle remains in the set area. After the time, a Time Waiting Event will be marked in the Vehicle/Others List and the system log, and alerts can be activated.
- **Recognition:** Select to trigger recognition by **Motion Detection** or **I/O Detection** (input trigger). Specify the input device's module and pin number if I/O detection is selected.
- **Attributes Matching**: Select **Car** or **Truck** and the attributes (Color, Car Type, and Brand) for vehicle database comparison. When the specified attributes are met, the event will be marked as "Authorized" in the Vehicle/Others List and the system log. When no attributes are specified, but the license plate numbers or card match, the event will also be marked as "Authorized".

- **Alert Settings:** Select **Authorized** for alerting when authorized events occur, **Unauthorized** for alerting when unauthorized events occur, and **Time Waiting Event** for alerting when the specified Waiting Time is exceeded.
  - Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules and/or computer audio alarms upon entrance detection events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

6. Click **OK**.
7. Start monitoring.

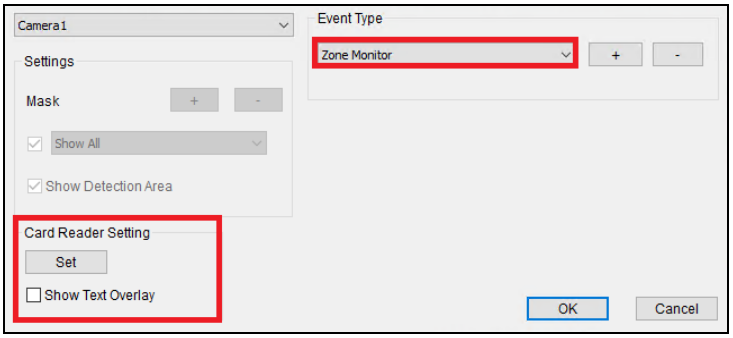
Once set up, both the live view and the Vehicle/Others List will display the detected vehicle attributes (brand, type, and color), as well as the waiting time during which the vehicle remains in the detection area.



1.4.9.3 Zone Monitor

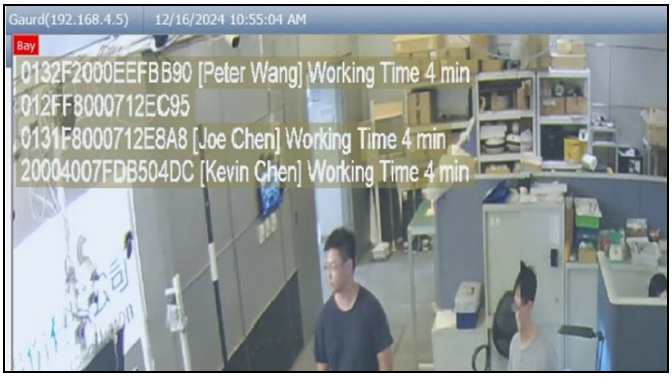
The Zone Monitor function uses the GV-RU9003 RFID reader to detect eTag carried by employees within the designated monitoring area. It captures data such as card numbers, cardholder information, and the duration of each employee's stay. For details on the reader, see the datasheet.

1. Create an employee database by following the steps in *1.4.9.1 Vehicle and Employee Registration*.
2. To start Vehicle Attributes Recognition settings, follow Steps 1 ~ 3 in *1.4.9 Vehicle Attributes Recognition.*
3. On the Vehicle Attributes Recognition Settings window, configure the following settings:
   - **Event Type:** Select **Zone Monitor**.
   - **Card Reader Setting:** Click **Set** to select the COM port on the GV-AI Guard system connecting to the GV-RU9003 RFID reader. To display eTag data on the video, select **Show Text Overlay**.



4. Click **OK**.
5. Start monitoring.

Once set up, the live view will display eTag data, such as the card number, card holder, and time duration of the eTag detected in the monitoring area.



Note: The detected eTag data is not recorded in the system log.

1.4.9.4 Exit

When paired with the Entrance function, the Exit function allows the system to estimate a vehicle's duration of stay within the monitored perimeter upon departure. This supports efficient vehicle tracking and management.

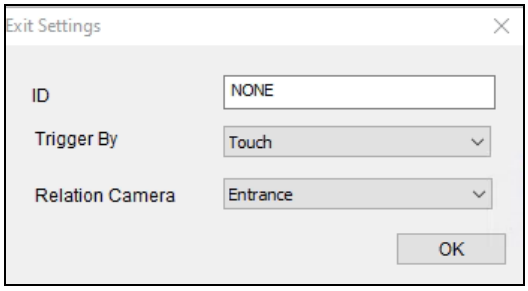
Note: Exit must be paired with Entrance, with each requiring 2 AI Analytics channels and 1 LPR-Related Event license. A paired Entrance + Exit setup requires a total of 4 AI Analytics channels and 2 LPR-Related Event licenses. See the License section in the datasheet.

---

1. To set up the Entrance function, see *1.4.9.2 Entrance*.
2. On the Vehicle Attributes Recognition Settings window, select **Exit** from the Event Type dropdown list.

8. Select **Add** +, and drag to draw the exit area on the image. To shape a polygon area, double-click on the sides of the lines and drag the joints.

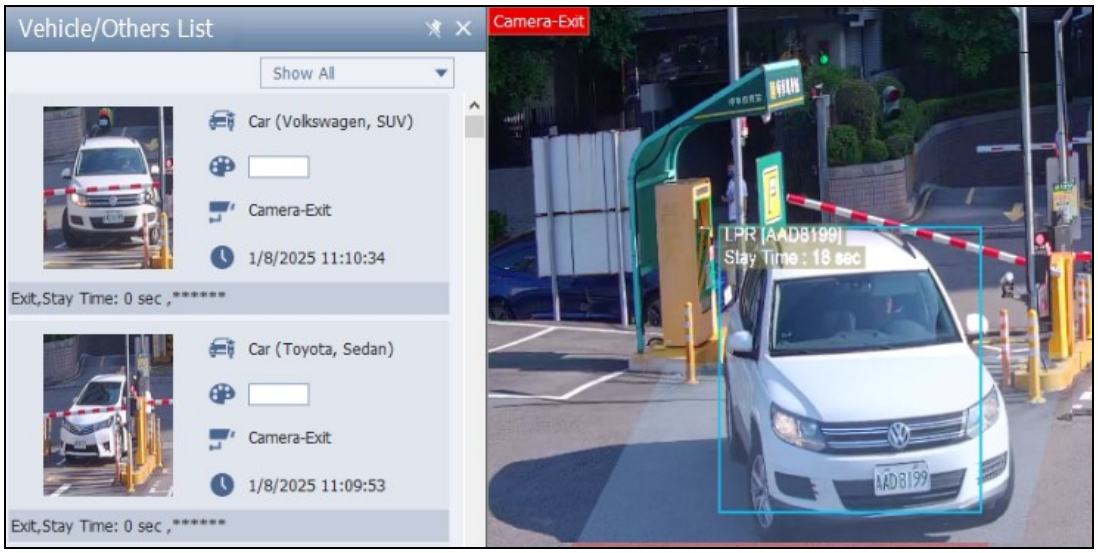
3. Right-click on the drawn area and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger By:** Define the detection sensitivity.
  - ⊙ **Center:** Events are triggered only when the center of a vehicle crosses the set area.
  - ⊙ **Touch:** Events are triggered when any part of a vehicle touches the set area.
- **Relation Camera:** Select an entry camera that pairs to the exit camera to estimate stay duration.

4. Click **OK**.
5. Start monitoring of both exit and entry cameras.

After the entry and exit cameras are triggered, the live view and the Vehicle/Others List will display the stay time.

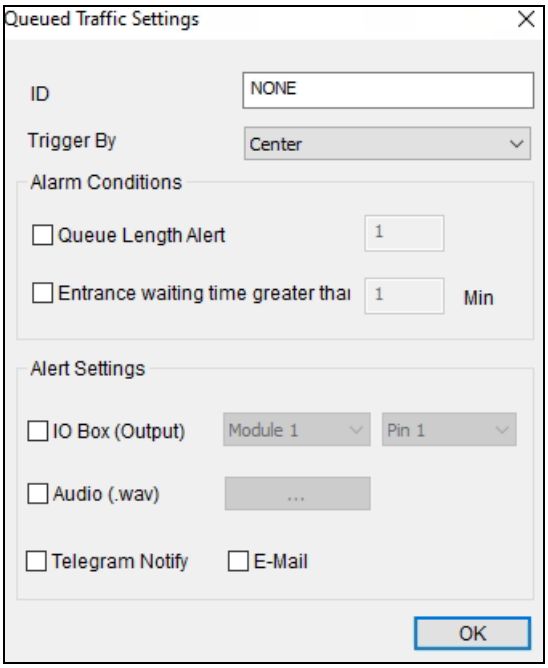


1.4.9.5 Queued Traffic

The Queued Traffic function detects and alerts on traffic congestion by reporting the number of queued vehicles, entrance waiting time, average entrance wait time, and maximum queue duration.

Note: The camera used for the Queued Traffic application should be mounted higher to get a better view of all vehicles.

1. To start Vehicle Attributes Recognition settings, follow Steps 1 ~ 3 in *1.4.9 Vehicle Attributes Recognition.*
2. On the Vehicle Attributes Recognition Settings window, select **Queued Traffic** from the Event Type dropdown list.
3. Select **Add** + and two drawing boxes display. One box is for drawing the start space (entrance) for a queue area while the other is for drawing a queue area. To shape a polygon area, double-click on the sides of the lines and drag the joints.
4. Right-click on the drawn queue area and select **Edit** to define which conditions the alert will be triggered.



- **ID:** Name the set area.
- **Trigger By:** Define the detection sensitivity.
  - ⊙ **Center:** Events are triggered only when the center of a vehicle crosses the set area.
  - ⊙ **Touch:** Events are triggered when any part of a vehicle touches the set area.

- **Queue length alert:** Set the maximum number of queued vehicles to trigger alerts when this limit is exceeded.
- **Entrance waiting time greater than x min:** Set the maximum waiting time in the entrance area to trigger alerts when it exceeds the specified minutes.
- **Alert Settings**: Select **E-mail**, **Telegram**, **IO Box**, or **Audio (.wav)** to activate notifications, output modules or computer audio alarms upon queued traffic events. Also see *Telegram Notify* and *Setting up E-Mail Notifications* later in this Chapter.

6. Click **OK**.
7. Start monitoring.

Once set up, the live view will display the number of queued vehicles (including vehicles in both the entrance area and queue area), the entrance waiting time, the average waiting time at entrance, and the maximum queue duration. When the specified queue length or entrance waiting time are exceeded, the event will be highlighted in the Vehicle/Others List.

In the following example, alerts are triggered in the Vehicle/Others List becasue the **Queue length alert** is set to 3 vehicles and the **current queue length** is 4 vehicles.



1.4.9.6 Vehicle Attribute Event Search

You can filter the following **vehicle events** by camera, detection time, license plate, card number, vehicle type (Car / Truck), vehicle color, and vehicle brand:

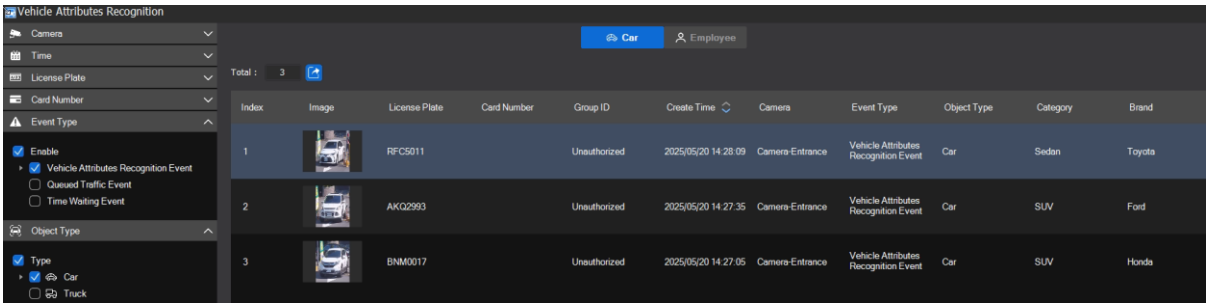
- **Vehicle Attributes Recognition Event** (Authorized or Unauthorized)
- **Queued Traffic Event**
- **Time Waiting Event**

Also, **Zone Monitor events** can be filtered by camera, detection time, user name, gender, card number, employee ID, and attendance time.

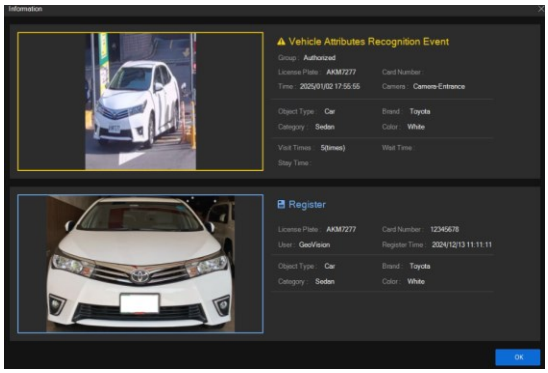
Follow the steps below:

1. Click **ViewLog** > **Toolbar** > **Tools** > **Vehicle Attributes Recognition**. The filter window appears.
2. Select **Car** or **Employee** 

from the top to filter vehicle events or Zone Monitor events:

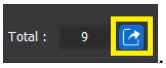


3. Use the left criterion options to narrow down your search. Click **Query**.
4. Click a found event. You can view the event or registration information.



Note: The Vehicle Attributes Recognition functions have the following limitations:

- Motorcycles, bicycles, and buses are not supported for vehicle type recognition.
- For details on supported object types and vehicle brands, see the document.

Tip: To export query results, click the export icon beside the event count at the top of the interface 

.

- CSV: Saves as an Excel file and an image folder.
- PDF: Saves as a PDF file.

1.5 Live AI Events

1.5.1 Live Event Lists

To view real-time AI events recorded by GV-AI Guard, click **Home** > **Toolbar** >**Tools** > **Vehicle/Others List** or **Human Detection**.

Note: This function only works when at least one camera with AI analytics settings is recording.



Vehicle/Others List Human Detection List

1. **AI Event:** Each event is displayed with a snapshot, gender, clothing color, vehicle type / color, camera channel, and detection time if available or supported.
2. **Event Type:** Display the type of detection, such as Motion, Intrusion, Loitering, Hard Hat Missing, etc.
3. **List Content:** Select to display either alert events only or all AI events in the list.

Double-clicking on a snapshot plays back the recording of the corresponding event in ViewLog.

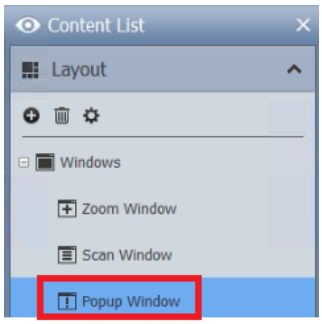
1.5.2 Popup AI Events

The live view can be popped up to alert the operator upon AI events in either of the following ways:

1. In a separate popup window
2. In full-screen mode

To pop up on a separate window:

1. In the Content List, click **Layout** > **Windows** > **Add** > **Add camera popup window** to select the desired AI events and cameras to be popped up once triggered.
2. Drag the Popup Window from the Content List to a live view grid.



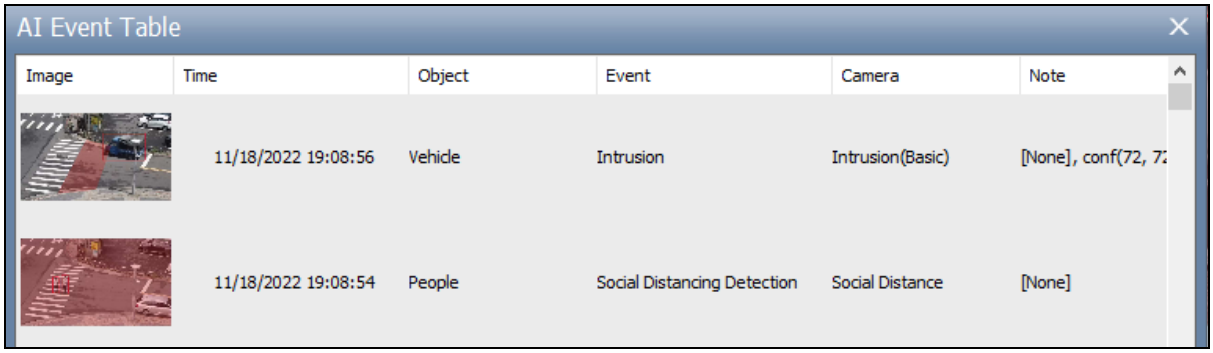
To pop up in full-screen mode:

Click **Home** > **Toolbar** > **Configure** > **Camera Popup Setting** and select the desired AI events and cameras to be triggered.

For details, see *Setting up Popup Live View* later in this Chapter.

1.5.3 AI Event Logs

To view the system log of AI events for the current day, click **Home** > **Toolbar** > **Tools** > **System Log** > **AI Event Table**. The AI Event Table appears. Double-clicking an event entry allows playback of the recorded video in ViewLog.

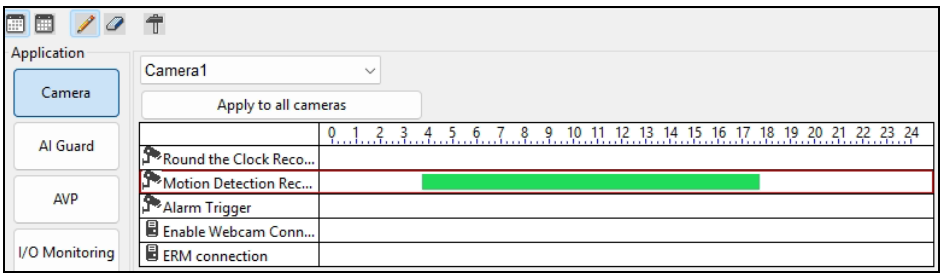


To search for AI events based on certain criteria, see *1.6 AI Event Playback and Search*.

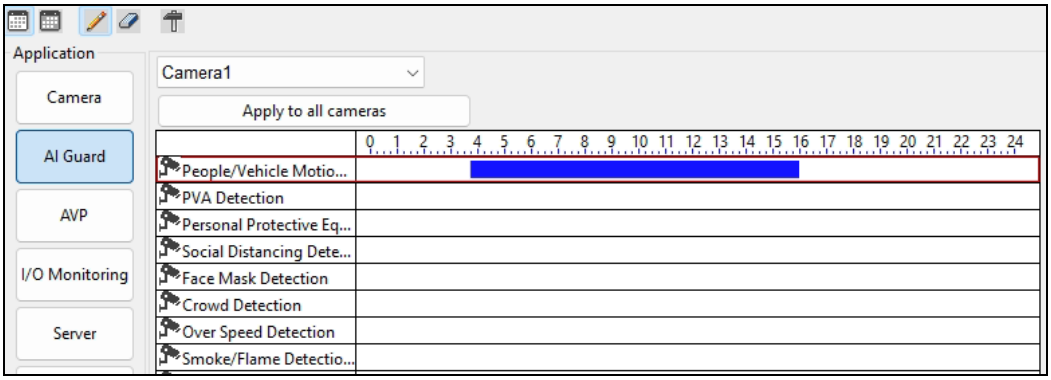
1.5.4 AI Event Detection Schedule

You can create schedules to enable AI event detection at certain times during the day, week, or month.

1. Click **Home** > **Toolbar** > **Configure** > **Schedule Edit**, and select **Plan** to add a schedule.
2. Double-click the added **Plan** on the left pane.
3. To enable **Motion Detection Recording** at a specific time, select a camera from the dropdown list and drag the timeline.



4. To enable any AI event detection at a specific time, click **AI Guard**, select the camera from the dropdown list, and drag the timeline.



5. To schedule a network connection to the central monitoring station **Center V2 AI** for AI event monitoring, click **Server** and define the desired time.
6. Click **OK**.
7. Drag the created plan on the left pane of the Schedule window to the desired dates on the calendar to apply it.
8. On the main screen, enable **Start Schedule Monitoring**.

For details, see *Schedule* later in this chapter.

1.6 AI Event Playback and Search

There are three methods to access and play back AI event recordings:

- **Live Event List:** Double-clicking on a snapshot in the live event lists (Vehicle/Others List and Human Detection) to play back the corresponding event. For details, see *1.5.1 Live Event Lists*.
- **AI Query:** Use AI Query to search for AI events or filter by specific people and vehicle attributes. For details, see *1.6.1 AI Query*.
- **Advanced Log Browser:** Search for general system events or people/vehicle counting data. For details, see *1.6.2 Advanced Log Browser*.

1.6.1 AI Query

The AI Query function enables post-event review and filtering of AI events, including face, people and vehicle attributes, using detailed criteria such as camera, time range, event type, and specific attributes.

Prerequisites

Before AI events can be filtered using the AI Query, ensure the corresponding settings are configured beforehand.

1. **Vehicle Attribute Search:** *Type* and *Brand* filters are only supported by GV-IP cameras that provide video metadata.
2. **People Attribute Search:** Requires enabling **PAC (People Attribute Classification)** before recording. To enable PAC, Home > Toolbar > Configure > Video Process > IVA > PVD Confidence Settings. See Step 4, *1.3.1 Starting Basic AI Video Analytics* for details.
3. **Face Search:** Only supports face recognition results from GV-Face Recognition Cameras or GV-AI FR software. See *3.1 Face Recognition* for details.

IMPORTANT: The AI Query (Vehicle Attribute Search) cannot be used to search for **Vehicle Attributes Recognition** events. Instead, use the designated Vehicle Attributes Recognition Event Search. For details, see *1.4.9.6 Vehicle Attribute Event Search.*

Follow the steps below:

1. Click **ViewLog** > **Toolbar** > **Tools** > **AI Query**. The AI Query window appears.
2. To filter by camera model, click the icon at the right of the All Cameras field. In the Camera List dialog box, select one or more cameras to include in the search.
3. Define a time range in the **Time Filter**.
4. You must select at least one of the four categories to filter events: *Face*, *Event*, *Person*, and *Vehicle*. Use the Filter dropdown list to refine the results for these categories, or configure the corresponding filter options in the lower section of the left panel as described below.

Searching by facial recognition

5. Enable the **Face** filter and select the desired face attributes. The search returns results that match all selected attributes simultaneously. For example, selecting **Male** for Gender and **Adult** for Age will return only adult male faces.
6. You can also enter a person's **name** if they are enrolled in the face database, or select a predefined **face group** for search.
7. Click **Query**. The matching face events are displayed.

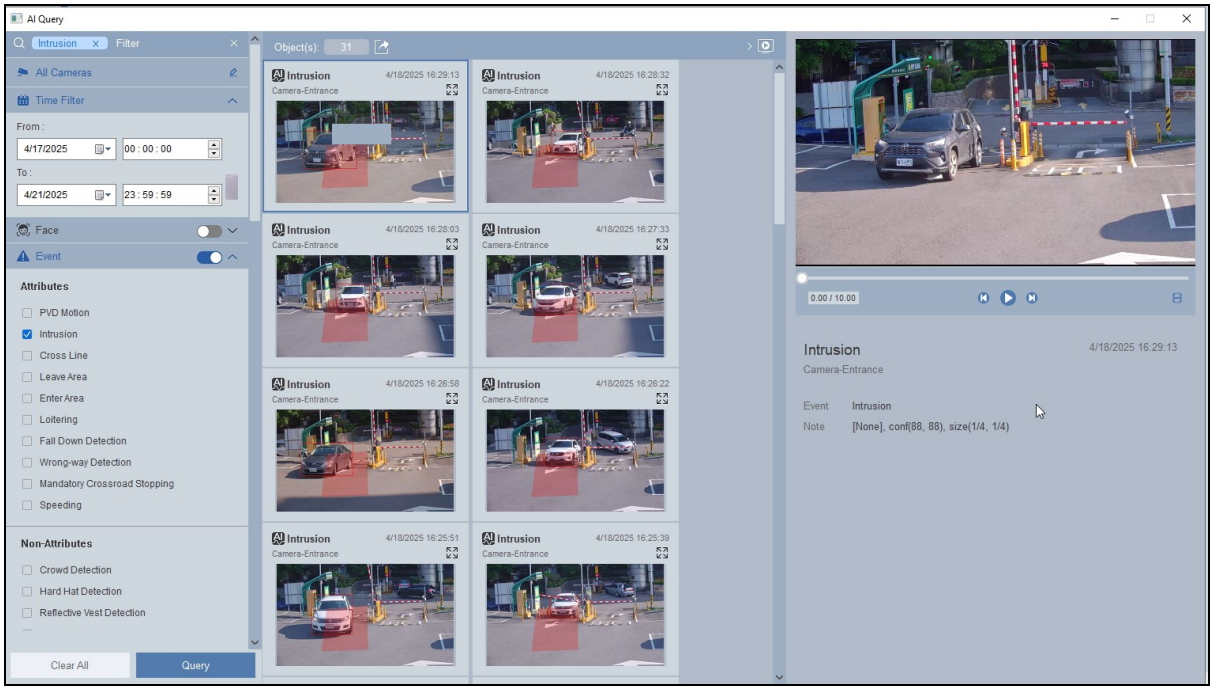
Searching by event types, person attributes, or vehicle attributes

8. Enable the **Event** filter and select the desired AI event types. The search returns results that match any of the selected event types. For example, selecting **Intrusion** and **Cross Line** will return both Intrusion and Cross Line events.

   Alternatively, enable **Person** or **Vehicle** and filter by their respective attributes. The search returns results that match all selected attributes simultaneously. Available attributes include:

   - **Person:** *Age*, *Gender*, *Upper/Lower Wear*, *Accessories, and Dwell Time (Dwell Time of Advanced Loitering)*.
   - **Vehicle:** *Type*, *Color*, *Brand*, *License Plate*, *Speed*, and *Dwell Time (Dwell Time of Advanced Loitering)*.
9. Click **Query**. The matching events are displayed.

You can view the playback and event details by clicking on any found event. The event playback window will open on the right side of the AI Query.



In the event playback window, click **View by ViewLog** beside the playback controls to view the playback in ViewLog. To return to AI Query, click **Maximize** in the minimized AI Query window at the bottom left of the ViewLog window .

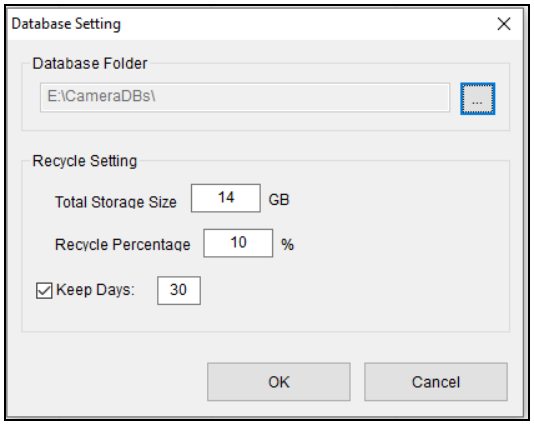


Tip: To export query results, click the export icon beside the object count at the top of the winodw .

- **CSV:** Saves as an Excel file and an image folder.
- **PDF:** Saves as a PDF file.

Note:

1. The maximum number of query results is 10000.
2. To configure AI event log storage path and recycle rules, click **Home** > **Toolbar** > **Configure** > **Face Manager**. Click the **Configure** icon at the bottom left corner, and select **DB Setting**. This dialog box appears.

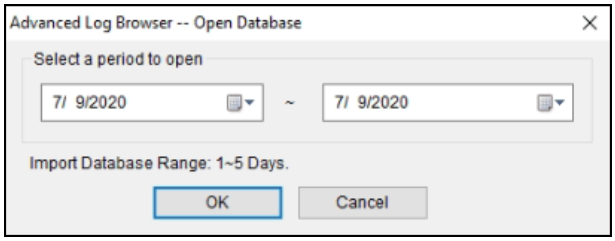


3. For timely processing of abundant AI events, it is suggested to set the database storage path at an independent disk drive.

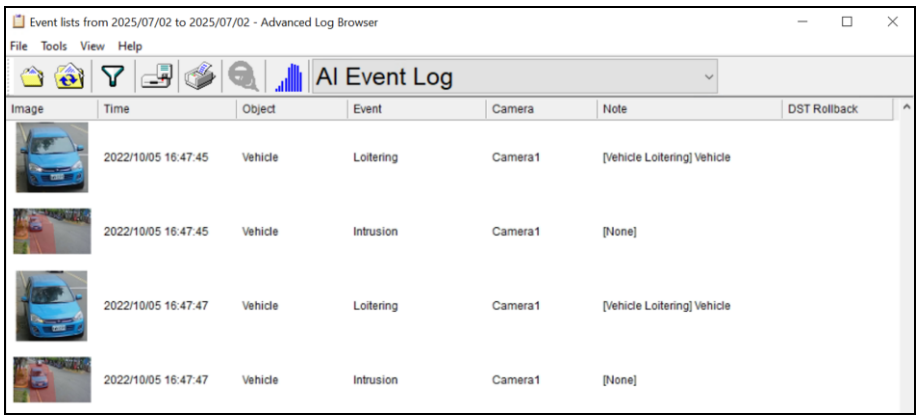
1.6.2 Advanced Log Browser

Using the Advanced Log Browser, you can access a more detailed search of various AI events.

1. Click **ViewLog** > **Toolbar** > **Tools** > **Advanced System Log**. This dialog box appears.



2. Define a date range you want to search for, from 1 to 5 days.
3. Select **AI Event Log** to display all AI events within the date range set.



4. To search for specific events, there are two ways:
   A. Click **Filter** > **Default Filter**
   B. Click the **Counter Table** icon .
5. Define the following search criteria: camera channel, event type, date and time, Note, or DST rollback.
   - **Note:** Specify the information for search: the ID of a detection area, object type (Human or Vehicle), or license plate numbers.
   - **DST Rollback:** Select to include the events within daylight saving time.
6. Click **OK**. Your filter results are displayed.
7. Double-click on the desired event to play back its recording.

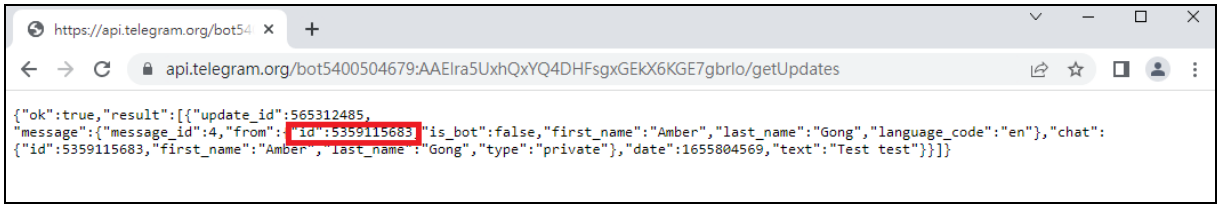
For details, see *Advanced Log Browser* in Chapter 4.

1.7 Telegram Notify

You can configure the system to send Telegram notifications when AI events occur.

To obtain Bot Token and Chat ID on Telegram

1. Search for @BotFather on Telegram and start the chat by clicking **Start**.
2. In the chat, type "/newbot" to build a new bot.
3. Create the username for the bot. Note that the username must end with "_bot." For example, "AI-Guard_bot."
4. The bot should generate the bot token.
5. To acquire the chat ID, type random content in the chat room with the new bot to create the chat history.
6. On the browser, type: **https://api.telegram.org/botTOKEN/getUpdates.** The token is as acquired in *step 4.*
7. Access the chat ID on the webpage as follows:



To apply the Token on GV-AI Guard:

1. Click **Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**. The Alert Approach dialog box appears.
2. Enable Telegram and select **Setup**.
3. Fill in the **Telegram Token** column.
4. Right-click on the **Chat ID** column and click **Add**.
5. Click **Test** to make sure the connection is properly established.

Video Surveillance

1.8 Getting Started on Video Surveillance

1.8.1 Main Screen



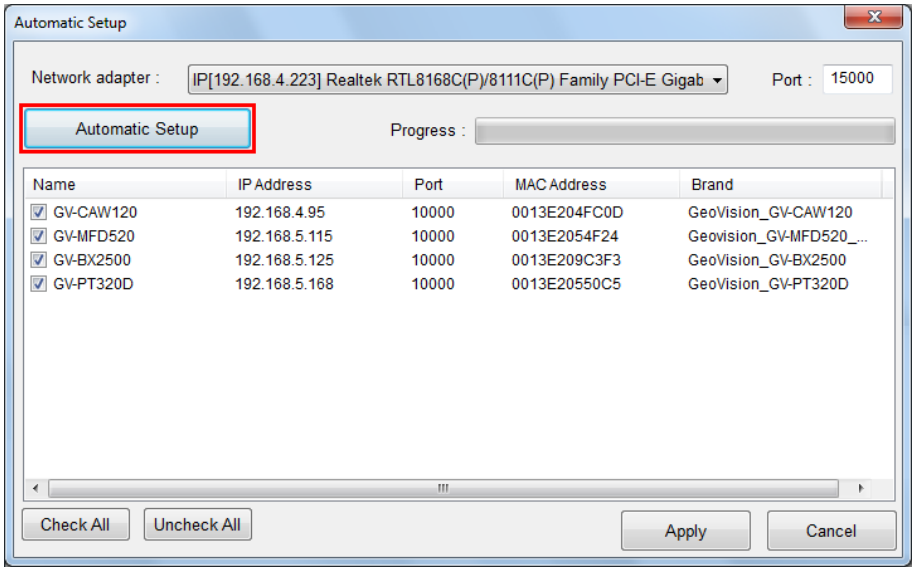
Name	Description
Version Info	Click to display the version of the system installed.
Storage Space	Displays the remaining storage space. When an HDD error occurs, an exclamation mark is displayed on the storage icon .
Login ID	Click to manage accounts and passwords for accessing the system.
Audio	Click to control the volume of your PC.
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: • **Monitor:** Start / Stop monitoring, I/O monitoring and schedule monitoring • **Network:** Enable Webcam Server and connection to other GeoVision software. • **Tools:** Show / hide volume indicator and set up Object Index. • **Configure:** Set up camera, recording, system, schedule, video processing and I/O devices.

	• **Content List:** Access live view layout, camera and I/O device lists and panorama view.
Exit	Click to minimize or exit the system.

1.8.2 Adding Cameras

To add cameras to the system, click **Home** > **Toolbar** > **Configure** > **Camera Install**. When the camera list is empty, the Automatic Setup dialog box automatically pops up.

Click **Automatic Setup** to search for IP cameras on the LAN. Then select / deselect the desired cameras listed and click **Apply**.



Note:

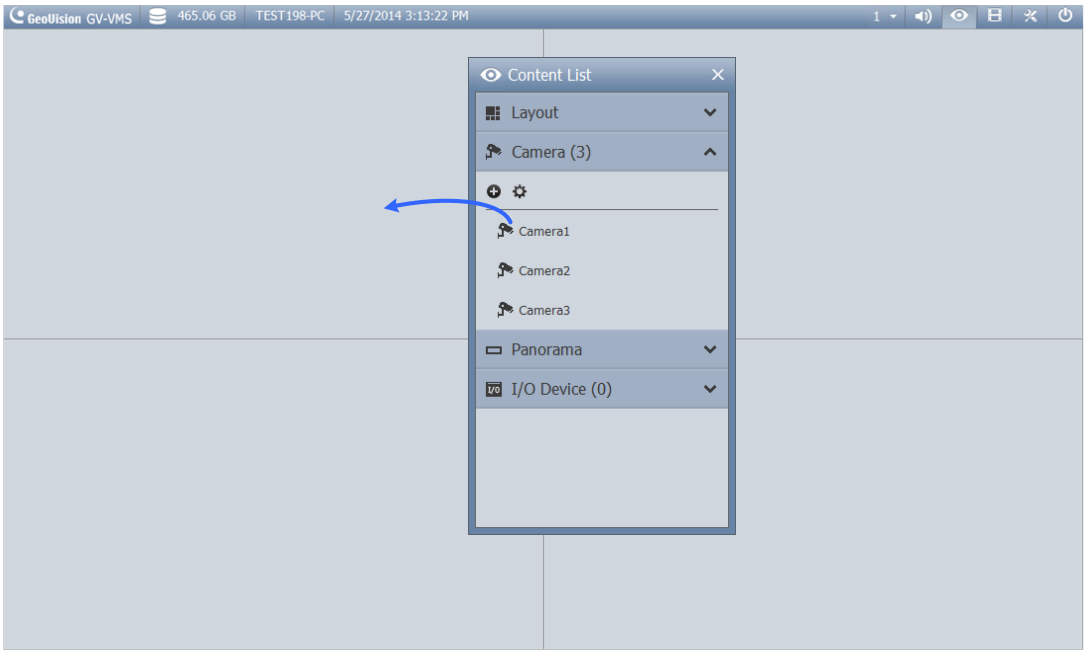
1. Double-click the camera to specify its login credentials. If you select **Apply All**, the login info will be applied to all selected cameras.
2. When cameras are added for the first time, they are automatically assigned to the live view grid.

To manually add cameras, see *Adding IP Cameras* in Chapter 2.

1.8.3 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.

Click **Home** > **Toolbar** > **Content List**. Then click **Camera** in the content list to see the list of cameras added, and drag the desired cameras to the live view grid.



See *Live View and Layouts* later in this chapter for details.

1.8.4 Enabling Recording

To start recording, click **Home** > **Toolbar** > **Monitor** > **Start All Monitoring**. Alternatively, select the cameras you want to start monitoring.

By default, every camera records with the following settings:

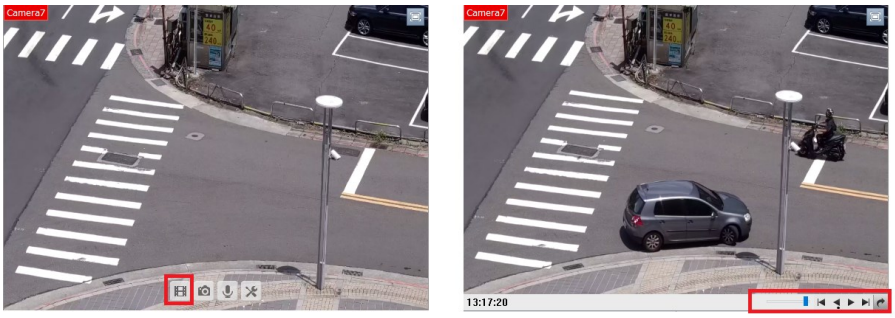
Default Recording Settings	
Recording Mode	Motion Detection
Resolution / Codec	The camera's current resolution / codec will be used.

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

1.8.5 Playing Back Video

Instant Playback

You can instantly play back the recorded video of a single camera from the camera live view by clicking the **Instant Playback** button.



ViewLog

For comprehensive playback functions, click **ViewLog**  on the top-right corner. For details, see *Video Playback* in Chapter 4.

1.9 Recording Settings

To configure the recording setting of the cameras, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting**. The Recording Setting dialog allows you to configure the following settings:

1.9.1 Setting up Global Recording Settings for All Cameras

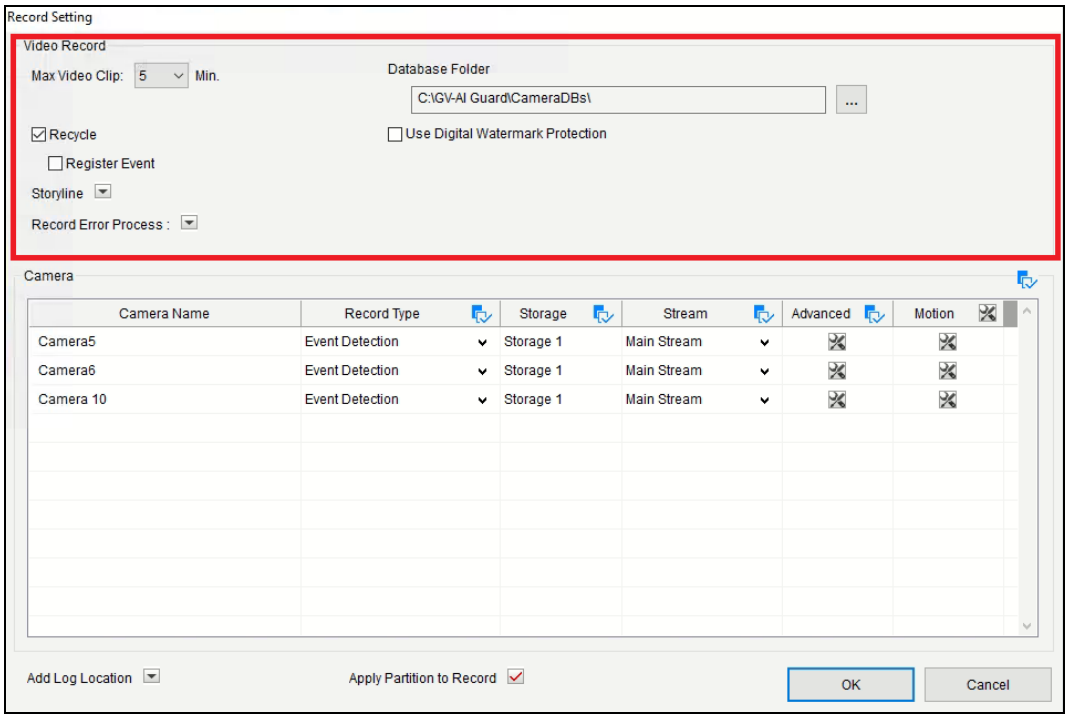
1.9.2 Setting up Recording Settings for Individual Cameras

1.9.3 Setting up Video Storage Locations

1.9.4 Setting up Motion Detection

1.9.1 Setting up Global Recording Settings for All Cameras

You can configure global recording settings to be applied to all cameras, such as maximum length of each video clip, recycling function and the actions to take upon recording errors.



[Video Record]

- **Max Video Clip:** Specifies the maximum time length of each recorded file (from 1 to 5 minutes), i.e. if you select **5 Min**, a 30-minute event will be chopped into six 5-minute event files.

- **Recycle:** When selected, the oldest recordings will be deleted when the system requires storage space for new files. If not selected, the system will stop recording when disk space is full. Select **Register Event** if you want to recycle registered events from the system log.

[Storyline]

- **Keep Image Ratio:** Keeps the image ratio of the recorded storyline videos.
- **Resolution:** Specifies the resolution of the recorded storyline videos.
- **Path:** The default storage path for Storyline is at C:\ProgramData\Geovision\. Click ... to specify a new storage path.
- **Add Copyright Text:** Select to stamp user-defined copyright texts to the storyline video.
  - ⊙ **Position:** Click to set the position of the copyright text on the storyline video.

Note: To record a storyline, see *Storyline* later in this chapter.

[Record Error Process] Define which actions to take when a recording error occurs.

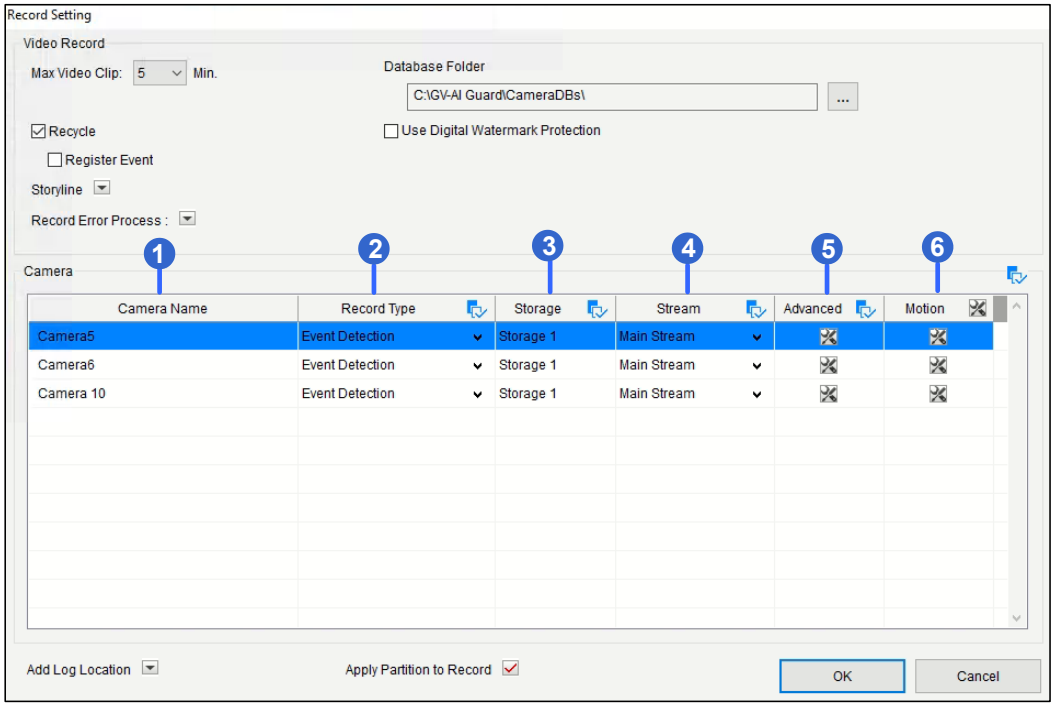
- **Invoke Alarm:** Activates computer alarm by playing the selected sound file.
- **Invoke to Send Alerts:** Sends e-mail notifications. For details, see *Setting up E-mail Notifications* later in this chapter.
- **Register Event:** Records errors to the system log.
- **Output Module:** Triggers the selected output device. To configure output devices, see *Chapter 6 I/O Applications*.

[Database Folder] The default storage path for Event Database (**.db** files) is at C:\GV-AI Guard\CameraDBs\. Click ... to specify a new storage path. Note that the storage path of recorded videos is specified in the **Add Log Location** option. For details, see *Setting up Video Storage Locations* later in this chapter.

[Use Digital Watermark Protection] Watermarks all recordings. For details, see *Watermark Viewer* in Chapter 9.

1.9.2 Setting up Recording Settings for Individual Cameras

You can configure the recording mode and video storage location for the selected cameras only.



The Recording Setting dialog box

1. Select the camera you want to configure. Hold the Shift key to select multiple cameras if needed.
2. Under Record Type, select **Disable**, **Event Detection** or **Round-the-Clock**.
3. If there are more than one storage locations, select **Storage** to specify where to store the recordings. For details, see *Setting up Video Storage Locations* later in this section.
4. Select the **Stream** you want to record. By default, **Main Stream** is set to record high-resolution videos. Select **Sub Stream** to record lower-resolution videos. Select **Main Stream and Sub Stream** to record both streams simultaneously.

5. Under **Advanced**:

   [Sync recording from camera SD card when reconnected] Retrieves and restores recordings from the SD cards of cameras selected when reconnecting after a temporary disconnection. Recordings that are synced from the SD cards are displayed in yellow within the Timeline of ViewLog.

Note: This function is only supported by ONVIF cameras (Profile G conformant)

   [Pre-Record] Configures post-recording and pr-recording.

   - **Post-Rec:** Keeps on recording for a set period of time after an event stops.
   - **Pre-Rec:** Records video for a set period of time before an event starts. 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 recording, 3 files of 5 seconds each, before each motion or input event are recorded.
   - **Urgent** / **General Event:** Select **Urgent Event** to record full frame rates or select **General Event** to record key frames only.

6. Under **Motion**, set up the advanced motion detection settings. For details, see *Setting up Motion Detection* later in this chapter.

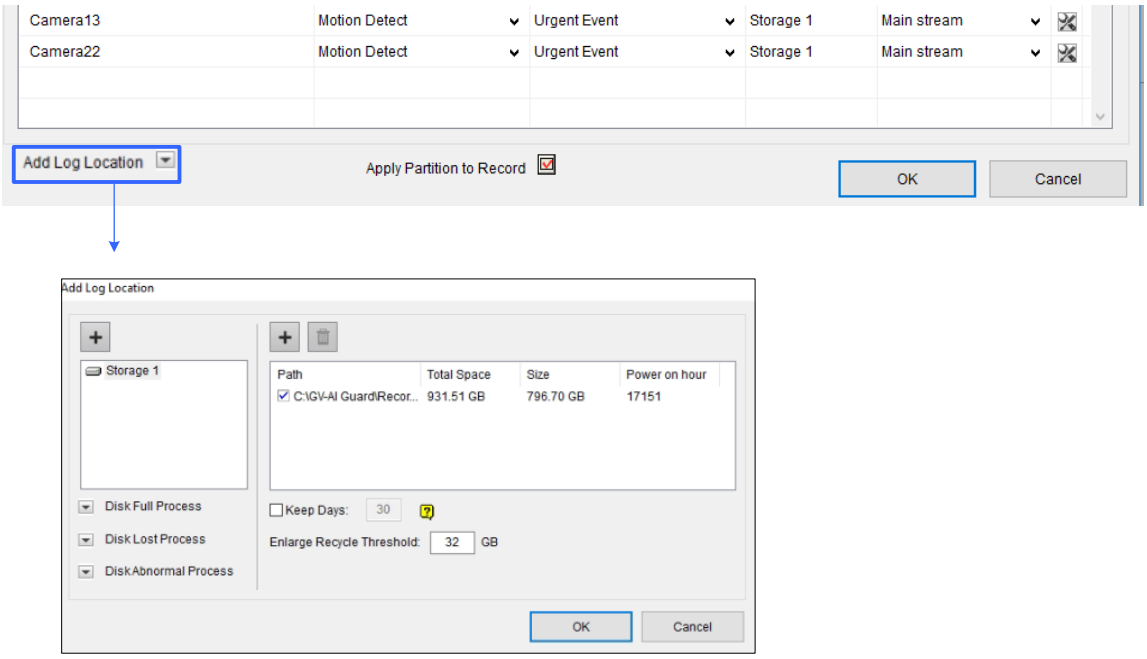
Note: You can define the frame rate of Urgent Event and General Event. For details, see the **Record Frame Rate Contro**l option, *Configuring General Settings* in Chapter 2.

1.9.3 Setting up Video Storage Locations

Add Log Location

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

1. On the Recording Setting dialog box (see *1.9.2 Setting up Recording Settings for Individual Cameras*), select a camera and click ▼ next to **Add Recording Location**. This dialog box appears.



2. To add a new folder in the first storage group, click + 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 + 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 (minimum 5 GB; maximum 999 GB) if needed. Recycle threshold is the file size at which the recycling begins.
6. To specify the actions to take under different disk conditions, click ▼ next to **Disk Full Process / Disk Lost Process / Disk Abnormal Process**.
   - **Invoke Alarm:** Activates computer alarm by playing the selected sound file.
   - **Invoke to Send Alerts:** Sends e-mail notifications. See *Setting up E-mail Notifications* later in this chapter.
   - **Register Event:** Records errors to the system log. (Not available for **Disk Abnormal Process**.)
   - **Output Module:** Triggers the selected output device. For how to set up I/O devices, see *Chapter 6 I/O Applications*. (Not available for **Disk Abnormal Process**.)
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.

Automatically Assign Partition to Camera

The system can automate the configuration of recording paths for multiple camera channels. Each of your cameras will be equally distributed to the assigned recording paths after you have set up the storage locations.

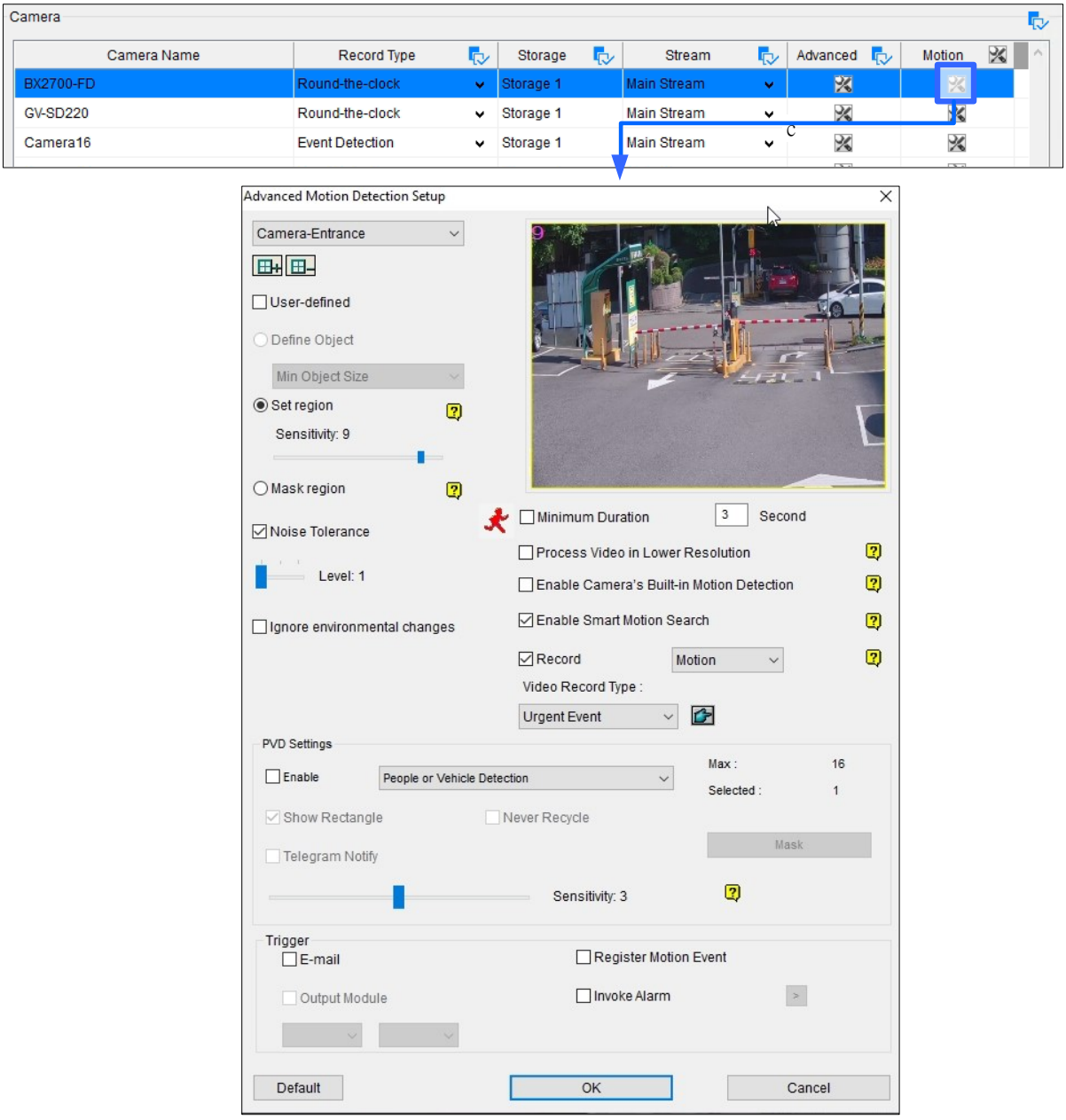
1. In the Recording Setting dialog box, click **Automatically Assign Partition to Camera**.
2. Select the desired recording paths (at least one) to store camera recordings and click **OK**.

1.9.4 Setting up Motion Detection

The motion detection settings will be applied to motion events in both recording types of Round-the-Clock and Event Detection. 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.
- **Minimum Duration:** Set the minimum duration for which motions must persist for the system to trigger a motion alarm.
- **PVD:** Only detect human or vehicle movement (up to 16 CH is supported; a maximum of 32 CH is supported with a GV-AI Accelerator Module).

1. On the Recording Setting dialog box (see *1.9.2 Setting up Recording Settings for Individual Cameras*), select a camera and click  button under the **Motion**. The Advanced Motion Detection Setup dialog box appears.



2. The camera's built-in motion detection is enabled by default. To use the system's software motion detection instead of camera's, deselect **Enable Camera's Built-in Motion Detection**.

Note: The camera's built-in motion detection is enabled by default in all GeoVision cameras when connected.

The following steps 3 ~ 6 are for defining the **software motion detection** of the system:

3. You can refine motion detection by setting either Object Size or Region Sensitivity.
   - **Define Object:** Limits motion detection to objects within a size range. Select **User-defined** and set the **Min. Object Size** and **Max. Object Size** in the respective dropdown lists.
   - **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 drag an area on the image. You can create several areas with different sensitivity levels. You can use the **Add/Cut Mask**  buttons to create irregular shapes. By default, the entire image is set to sensitivity level 9.
4. To ignore motion in specific areas of the image, click **Mask Region**, and drag areas on the image.
5. 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.
   - **Ignore environmental changes:** Ignore 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:** Set the minimum duration for which motion must persist for the system to issue a motion alarm. Set the minimum duration in seconds (up to 60).
6. To reduce CPU loading, optionally select **Process Video in Lower Resolution**. When enabled, the system compresses live view into a lower resolution before detecting if there is motion, which reduces CPU loading but may affect accuracy.
7. To mark motion and search for events based on defined regions of interest, select **Enable Smart Motion Search**. For Smart Motion Search, see *4.2 Object Search*.

The following features of steps 8 ~ 9 are applied to both **software motion detection** and **camera's built-in motion detection**:

8. To set the recording type and frame rate, enable **Record.**
   - **Record**: Select **Motion** to record motion, or **PVD Motion** to only record people and/or vehicle movement.
   - **Video Record Type:** Select **Urgent Event** for full-frame recording, or **General Event** for key-frame recoridng.
9. To set PVD Motion recording, select **People Detection**, **Vehicle Detection**, or both to only detect specific motion. The function only supports up to 16 camera channels for free.
   - **Show Rectangle:** Display rectangles, highlighting people and/or vehicles detected, on the live view.

- **Never Recycle:** When selected, the recorded events are not recycled when the recycle threshold is reached.
- **Telegram Notify:** Send Telegram notifications when PVD events occur. To configure, see *1.7 Telegram Notify*.
- **Mask:** Click **Add** to draw areas on the image that the detection will ignore. Double-click on the sides of the masks and drag the joints to shape the polygon masks.
- **Sensitivity:** The higher the value, the more sensitive the detection is. The default value is 3.

10. Under Event Trigger, select the actions to take when motion is detected.

    All trigger actions listed below are based on the detection method selected in the upper section of the Advanced Motion Detection Setup dialog box.

    - If **Camera's Built-in Motion Detection** is enabled, the selected actions are triggered by motion events using the camera's built-in motion detection.
    - If **the system's software motion detection** is used (when Camera's Built-in Motion Detection is disabled), the actions are triggered by motion events using the system's software motion detection.
    - If **PVD (People and Vehicle Detection)** is enabled, the actions are triggered only by PVD motion events.

    Available trigger actions:

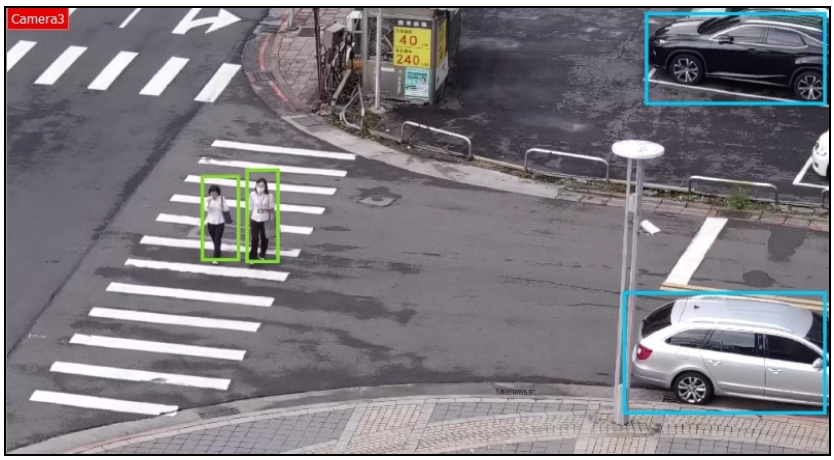
    - **E-mail:** Send e-mail notifications. See *Setting up E-mail Notifications* later in this chapter.
    - **Output Module:** Trigger an output device. See *Chapter 6 I/O Applications* to set up I/O devices.
    - **Register Motion Event:** Register motion events to the system log.
    - **Invoke Alarm:** Activate computer alarm by playing the selected sound file.

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

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** functions enabled.
3. You can define the frame rate of Urgent Event and General Event. For details, see the **Record Frame Rate Contro**l option, *Configuring General Settings* in Chapter 2.
4. A maximum of 16 independent channels of PVD is supported besides Basic / Advanced AI Analytics functions. With GV-AI Accelerator Module, a maximum of 32 channels of PVD is supported.

Once the PVD Motion is set up, the people or vehicles detected are highlighted by different color rectangles (people=green rectangles, vehicles=blue rectangles) on the live view.



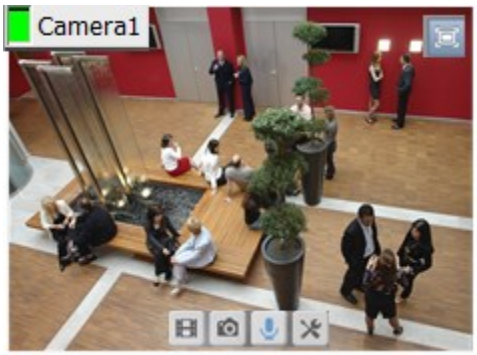
1.10 Live View and Layouts

This section describes the functions on the camera live view and how to create new live view layouts.

1.10.1 Utilizing Live View Functions

Live View Icons

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



Icons	Functions
Instant Play	Plays back the video recorded.
Snapshot	Captures a snapshot of the current live view.
Wave Out	Enables live view audio. See *Configuring Audio Setting* in Chapter 2.
Talk Back Toggle / Push-to-Talk	Talk to the surveillance site. For details, see *[The behavior of the talk back button]*, *Configuring General Setting*s later in this chapter.
Tools	Includes the following options: ■ **Monitor:** Starts monitoring the camera. ■ **Properties:** ⊙ **Show Caption:** Shows camera name on the live view. ⊙ **Keep Image Ratio:** Locks aspect ratio of the camera image. ■ **Close:** Removes the camera from the layout grid. The following options are available when related function is enabled or supported: ■ **Storyline:** Records a sequence of short video clips of a specific incident. (See *Storyline* later in this chapter)

	■ **Add to bookmark:** Bookmarks a scene to watch later in ViewLog player. The function is only available when the channel is recording. ■ **PTZ Control:** Enables PTZ functions. (See *PTZ Camera* later in this chapter) ■ **Measure Temperature:** For GV-TMEB5800 only. After the thermography rules are set up on the camera Web interface, select this option to trigger the alarms when the detected temperature exceeds the pre-defined threshold.
Zoom 	Switches the live view to full screen. If there is a designated Zoom window, clicking the **Zoom** button will display the live view in the zoom window instead.
Volume Indicator 	Display an audio volume indicator on the top-left corner of the camera live view. Click **Home**  > **Toolbar**  > **Tools**  > **Audio** > **Show Volume Indicator**. When the channel is actively recording, the volume indicator is displayed in orange.
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.	

Functions on Live View and Content List

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

Actions	Functions
Double-click	Toggles full-screen mode for the live view.
Mouse scroll	Zooms in or out on the live view.

In the Content List (**Home**  > **Toolbar**  > **Content List**), right-click a camera to access the following options, when enabled or supported:

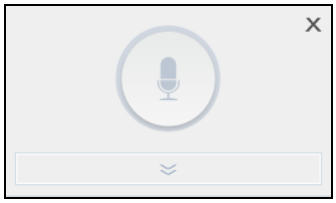
- **Monitor:** Starts monitoring the camera. See *Start Monitoring* later in this section.
- **Wave Out:** Enables live view audio. See *Configuring Audio Setting* in Chapter 2.
- **Talk Back Toggle:** Talks to the surveillance site from the PC. See *Configuring Audio Setting* in Chapter 2.
- **Video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

Audio Broadcasting

When necessary, the system operator can broadcast audio to multiple cameras simultaneously with the speaker function.

Note: This function is not supported by cameras connected through RTSP protocol.

1. Click **Home** > **Toolbar** > **Tools** > **Audio Broadcast**. This window appears.

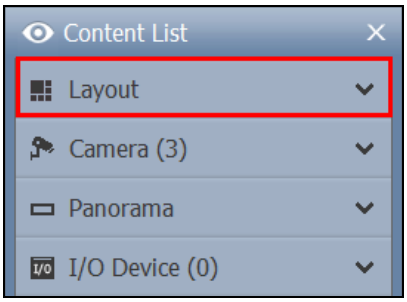


2. Click the **Down** arrow button to select the cameras you wish to broadcast audio to.

3. To start audio broadcasting, press and hold the **Push to Broadcast** button while talking to the microphone connected to the computer of the system.

1.10.2 Arranging Live View Layouts

1. In the Content List, click **Layout**.



2. To add a layout, click **Add** and click **Add Layout**. The Add New Layout dialog box appears.
3. Name the new layout and select one of the three available methods under Layout Setup to define a layout and click **OK**.
4. If you select **Customize** in the step above, the Customize Layout dialog box will appear.
   a. Click **Reset** to specify a dimension for the grid if needed.
   b. Select multiple squares and click **Merge** to create a larger square.

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

5. A message appears. Click **Yes** if you want to automatically assign the cameras to the new layout.

Tip: You can right-click a layout in the Content List to access other functions to arrange the layout.

1.10.3 Setting up 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.

Note:

1. Up to two Zoom Windows can be created on each live view layout.
2. When there are two Zoom Windows, the system will alternate between the first Zoom Window and the second Zoom Window each time you click the Zoom button of a camera.

---

1. In the Content List, select **Layout**, click **Windows** and drag **Zoom Window** to a live view grid.
2. Move the mouse cursor to a camera live view and click **Zoom**  in the top-right corner. The camera live view is displayed in the Zoom Window.
3. To remove the camera from the Zoom window, place the cursor on the live view, click **Tools**  and select **Close**. To change the live view grid back to a normal window, repeat this step again to close the Zoom Window.

1.10.4 Setting up Scan Window

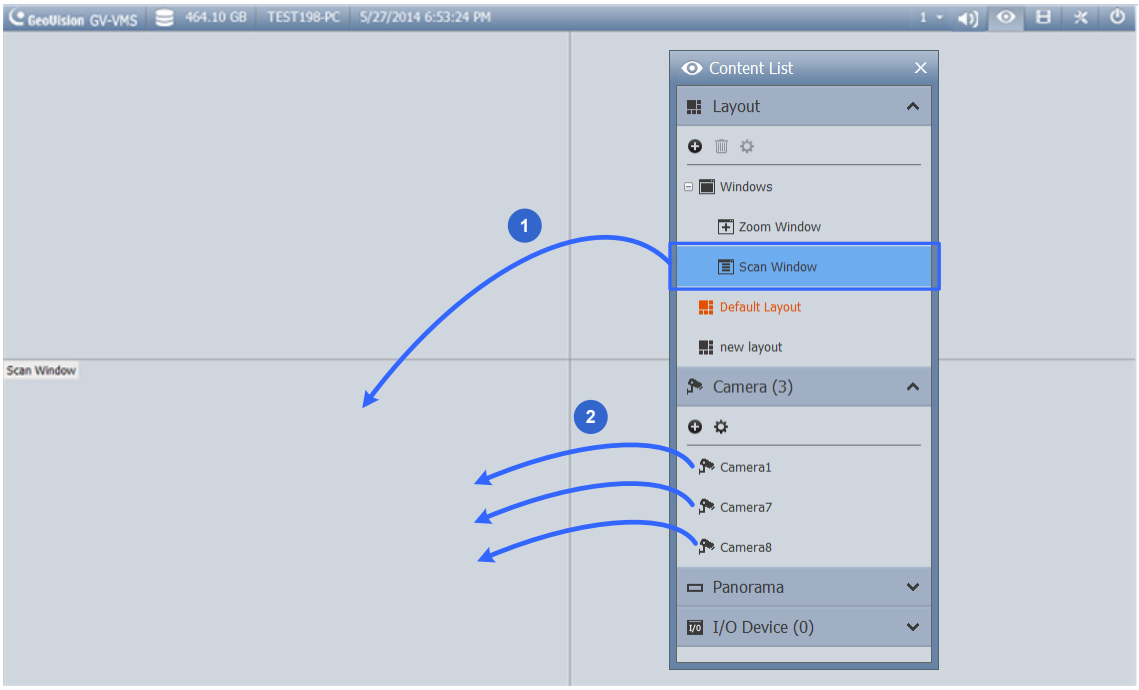
You can assign multiple cameras to a Scan Window, and each camera will be shown in sequence for the Scan Interval specified.

Note: Up to four Scan Windows can be created on each live view layout.

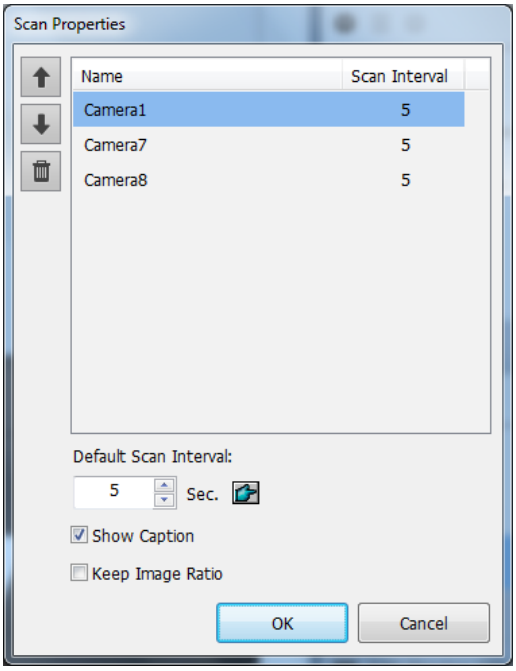
---

1. In the Content List, click **Layout**, double-click **Windows**, and drag **Scan Window** to a live view grid.

2. Drag multiple cameras into the Scan Window.



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



4. To adjust the order of a camera, select a camera and click the Up and Down arrows.

5. To specify how many seconds each camera is shown in the live view, select a camera and adjust its **Scan Interval**. Optionally click **Apply All** to apply this Scan Interval to all cameras.
6. To show the camera name on the live view, select **Show Caption**. Optionally adjust the font size.
7. To lock the original aspect ratio of the camera image, select **Keep Image Ratio**.
8. Click **OK**.

1.10.4.1 Creating a Camera Group

You can also add multiple cameras to a group and the created group can be dragged into a live view grid directly or Scan Window for display. At least 8 cameras are required in the camera list for this function to work.

1. Click **Camera** in the Content List, click **Add**, and click **Add Group**. Rename the group if necessary.
2. Drag the desired cameras from the camera list to the group created.
3. Drag the created group either into a live grid or Scan Window. For details on setting up a Scan Window, see *Setting up Scan Window* earlier in this chapter.

1.10.5 Setting up Popup Window

You can designate a Popup Window to display live images of cameras, upon events, in a separate monitor. For this function to work, you must first create a live view layout on another monitor.

1. In the Content List, click **Layout** > **Add** > **Add Layout** to create a new layout.
2. After clicking **OK**, select a desired monitor from the **Apply to…** list to activate the layout on the designated monitor.
3. In the Content List, click **Layout**, right-click **Windows**, and click **Add camera popup window** to select the cameras and events to be displayed in the Popup Window. For details, see *Setting up Popup Live View* later in this chapter.
4. Drag the Popup Window from the Content List to the layout created.

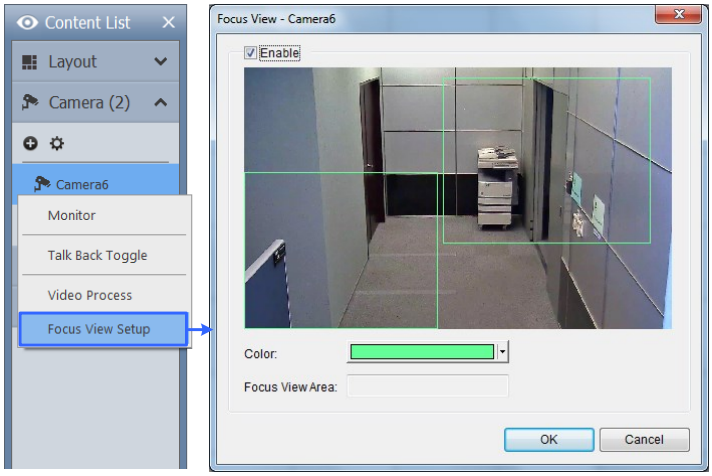
Tip:

1. To modify the camera popup settings for the Popup Window you just set up, right-click the Popup Window in the Content List, and select **Camera Popup Settings**.
2. To set up a popup live view that overlays the entire main screen, see *Popping Up Live View* later in this chapter.

1.10.6 Setting up Focus View

You can create up to 7 close-up views per camera and place these created close-up views inside the live view grid.

1. In the Content List, right-click a camera and select **Focus View Setup**. This dialog box appears.



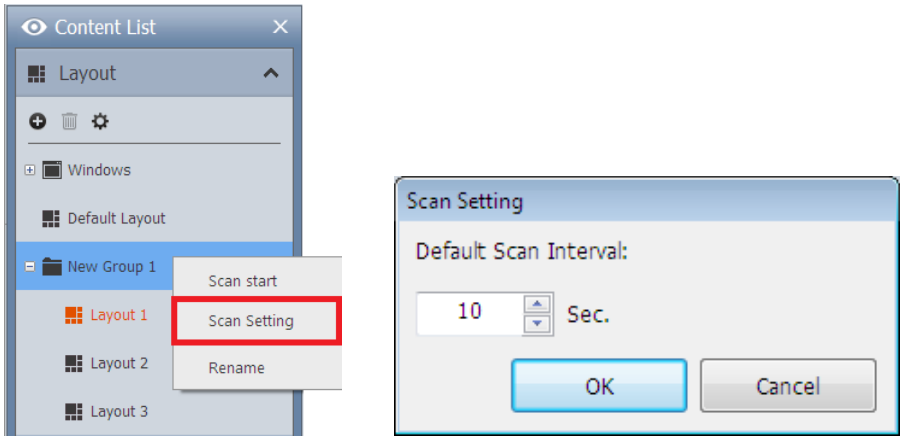
2. Click **Enable** and draw a box on the camera view to create a focus view. You can create multiple focus views if needed.
3. Optionally click the **Color** dropdown list to change the color of the box.
4. Click **OK**. The created focus views are listed under the camera.
5. You can now drag the focus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

Note: This function is not supported for Fisheye Cameras and PTZ Cameras.

1.10.7 Automatic Switch among Different Live View Layouts

You can have different layouts automatically alternated at a specified interval.

1. Create and group several layout templates under the Content List.
2. Right-click the group to configure its **Scan Setting** to specify the scan interval.



To start the automatic switch, right-click the group and select **Scan Start**. In the example above, Layout 1, Layout 2, and Layout 3 are automatically switched among each other every 10 seconds, with the currently displayed layout highlighted in orange.

1.10.8 Adding GV-IP Decoder Box for Remote Monitor Display

Users can add a GV-IP Decoder Box to the system to be assigned the desired camera channels for remote monitor display. For details, see *Chapter 6 Integration to GV-Software* in the *GV-IP Decoder Box Series and Display User's Manual*.

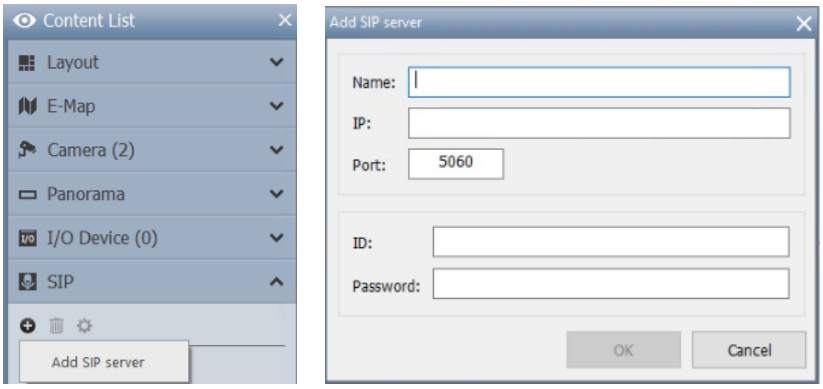
1.10.9 Adding GV-IP Speaker for Broadcasting

Users can add a GV-IP Speaker to GV-AI Guard for broadcasting or active deterrence. For details, see *Chapter 3 Adding to GV-VMS / GV-AI Guard* in the *GV-IP Speaker User's Guide*.

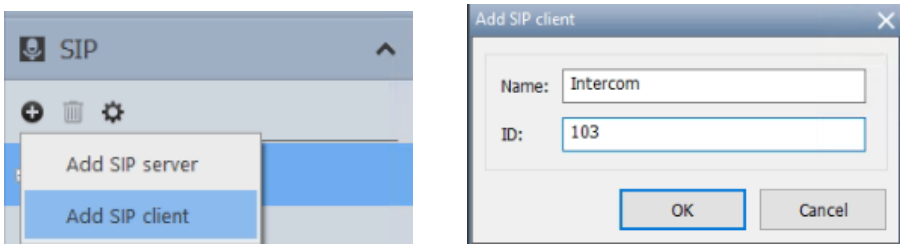
1.10.10 Setting up SIP Audio Communication for Dial-out

Users can connect the system to a SIP server for dialing out to and communicate with devices connected to the same SIP server.

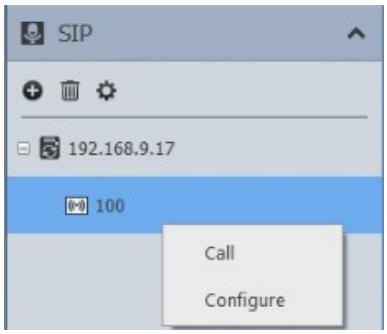
1. From the Content List, select **SIP** > **Add** > **Add SIP Server**.



2. Type a desired name and the IP address of the SIP server, optionally modify the port if necessary.
3. Within **ID** and **Password**, type a desired ID number for the system to be recognized as on the server and a desired password for protection. Click **OK**.
4. Select **SIP** > **Add** > **Add SIP Client**.



5. Type a desired name for the client device and its ID number, as assigned on the SIP server. Click **OK**.
6. To add multiple client devices, repeat Step 5.
7. Once all the desired client devices have been added, users can right-click on any of the clients and select **Call** to dial out to that client device for 2-way audio communication.

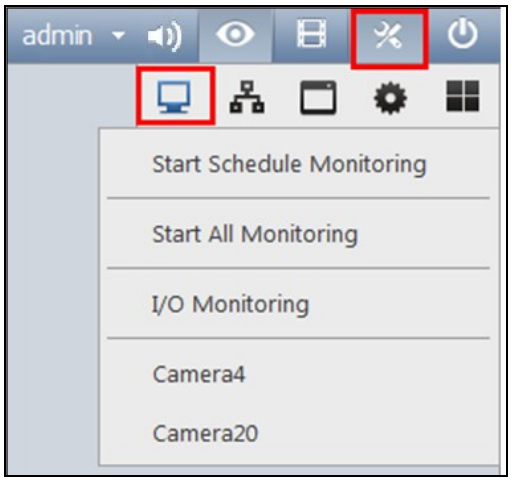


8. To modify the name and/or the ID number of a client device, right-click on it and select **Configure**.

1.11 Start Monitoring

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

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



- **Start Schedule Monitoring:** Start monitoring based on a previously set schedule. The schedule takes precedence over the current settings, and the following functions will start and stop according to the schedule: Recording, Motion Event Trigger, AI Event Monitoring, Video Analysis, I/O Monitoring, Network Connections with GV-WebCam Server / Edge Recording Manager / Center V2 / Vital Sign Monitor / Mobile Service, and PTZ Object Tracking. For details, see *Schedule* later in this chapter.
- **Start All Monitoring:** Start monitoring on all cameras to begin recording and related 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. For details, see *Setting up I/O Devices* in Chapter 6.
- **Camera#:** Start monitoring of selected cameras. You can also start monitoring individual cameras by right-clicking the camera in the Content List and select **Monitor**.

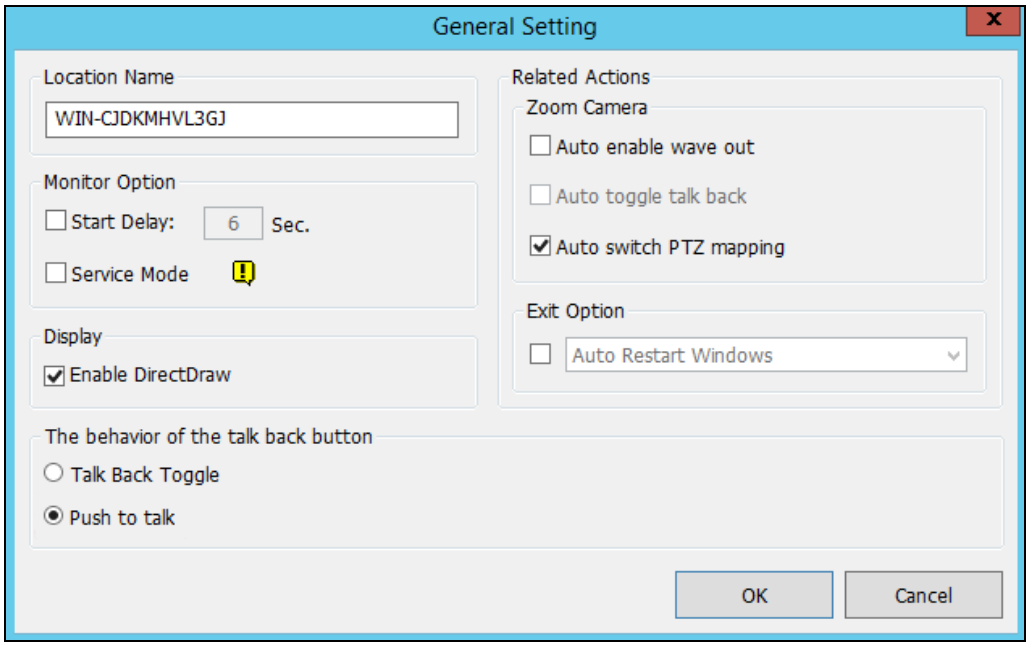
Note: Motion detection and input trigger will only be registered in the System Log if monitoring is started. You will also need to enable **Register Motion Event** in the Advanced Motion Detection Setup (see *1.9.4 Setting up Motion Detection*) and **Register Input Event** in the I/O Application Setting (see *6.2.1 Setting up Actions upon I/O Trigger*).

1.12 System Configuration

This section introduces system configurations.

1.12.1 Configuring General Settings

Start configuring **General Setting** by clicking **Home** > **Toolbar** > **Configure** > **System Configure** > **General Setting**. This dialog box appears.



[Location Name] The given name (maximum 14 characters) is displayed in the 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, the system starts automatically upon PC startup and runs in the background without logging into Windows.

[Display]

- **Enable DirectDraw:** Enabled by default to enhance image quality. For some graphics cards, DirectDraw can result in blurred images. To avoid the issue and maintain DirectDraw, change the image quality to **Standard** in Video Setting (see *2.2.1 Configuring Video Settings*).

[The behavior of the talk back button]

- **Talk Back Toggle:** Click the  button on the live view to talk to the surveillance site and click the button again to stop talking.
- **Push to Talk:** Click and *hold* the  button on the live view to talk to the surveillance site and *release* the button to stop talking.

[Zoom Camera]

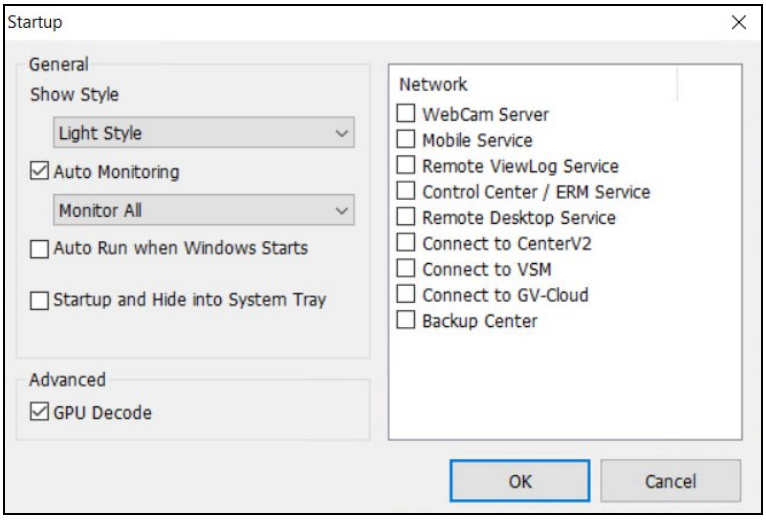
- **Auto enable wave out:** Automatically enables Wave Out function of the camera in Zoom Window or in full screen. Note that the Wave Out function needs to be enabled in the Audio Setting page of the camera first.
- **Auto toggle talk back:** Automatically enables Toggle Talk Back function of the camera. 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-Keyboard connected to the system. When selected, PTZ control by GV-Keyboard will be applied to the mapped PTZ camera. When not selected, GV-Keyboard can only control the first available PTZ camera.

[Exit Option]

- **Auto Restart Windows:** Restarts Windows OS after exiting the system.
- **Auto Shut Down Windows:** Shuts down Windows OS after exiting the system.

1.12.2 Customizing Startup Settings

To configure the system to enable certain features upon startup, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Startup**. This dialog box appears.



[General]

- **Show Style:** Change the color scheme of the system.
- **Auto Monitoring:** Select one of the following monitoring modes upon system startup:
  - **Monitor All:** Starts monitoring of all cameras and I/O (if available).
  - **Schedule Monitor:** Starts monitoring of cameras by schedule. See *Schedule* later in this chapter.
  - **I/O Monitoring:** Starts monitoring of all I/O devices.
  - **Camera Monitoring:** Enables all cameras for monitoring.
- **Auto Run when Windows Starts:** Automatically runs the system after Windows starts.
- **Startup and Hide into System Tray:** Hides the system in Windows system tray after Windows starts.



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, see *Setting up a Startup Auto Login User* later in this chapter.

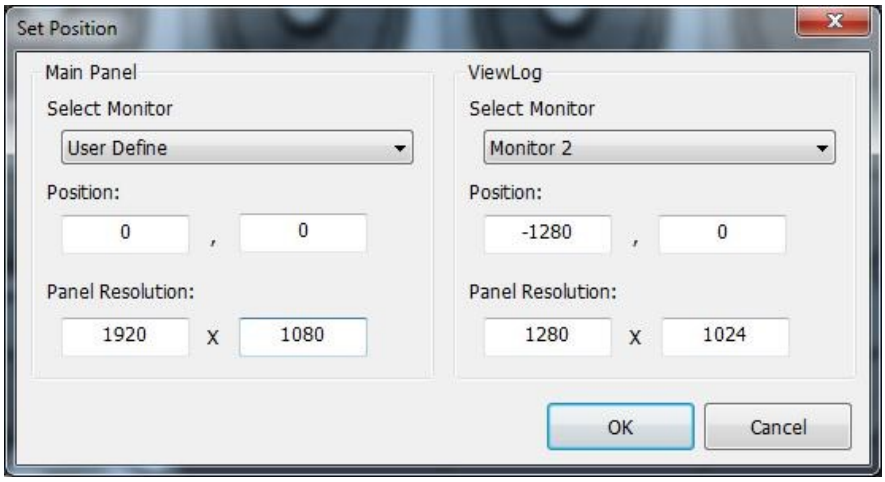
[Advanced]

- **GPU Decode:** Enabled by default, GPU (Graphics Processing Unit) decoding lowers the CPU loading and increases the total frame rate supported by the system. But if your PC does not meet the system requirements as listed in *GPU Decoding* at the beginning of the manual, you can disable this function to optimize system operations. It is required to restart the system for the change to take effect.

[Network] Automatically enables connection to the following applications upon startup: **WebCam Server**, **Mobile Service**, **Remote ViewLog Service**, **Control Center / ERM Service**, **Remote Desktop Service**, **Center V2**, **VSM**, **GV-Cloud**, **Backup Center**

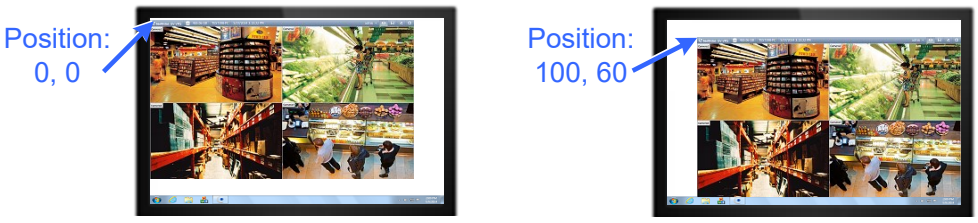
1.12.3 Customizing Display Position and Panel Resolution

You can customize the display settings of the system by clicking **Home** > **Toolbar** > **Configure** > **System Configure** > **Set Position**. This dialog box appears. The ViewLog section is only available when multiple monitors are installed.



- **Select Monitor:** Select the monitor you want to configure from the dropdown list.

- **Position:** Offsets the position of the main window (panel) relative to the upper-left corner of the screen. The default position is 0, 0. A position of 100, 60 will place the main window 100 pixels to the right and 60 pixels below the upper-left corner. This function is only supported when the main window does not take up the entire screen.

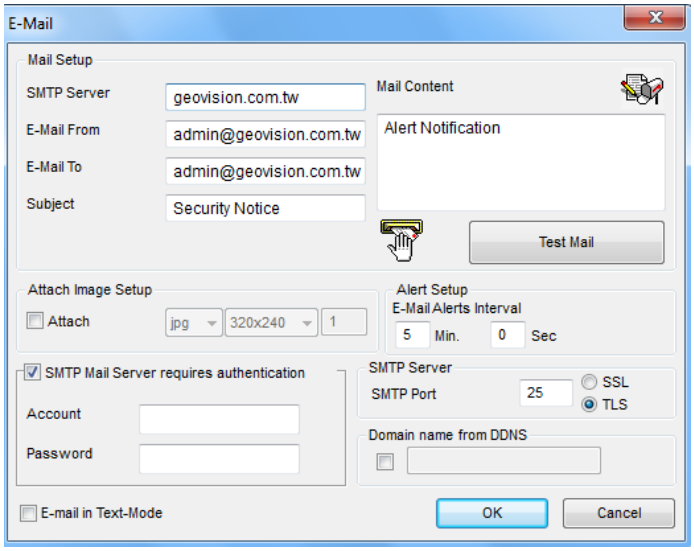


- **Panel Resolution:** Sets the Panel Resolution of the system.

1.12.4 Setting up E-mail Notifications

E-mail notifications can be triggered by the following events: Video Loss, Recording Error, Disk Full, Motion Detection, I/O Trigger, Intruder Event, Crowd Detection, Advanced Unattended Object, Advanced Scene Change Detection, Advanced Missing Object, Basic and Advanced AI Video Analytics events.

1. To receive e-mail notifications when an event occurs, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**. The Alert Approach dialog box appears.
2. To enable the e-mail server, select **Send Email**. This dialog box appears.



3. Under Mail Setup, type the host name of your outgoing mail server (SMTP), the sender's e-mail address, the recipient's e-mail address, and a subject for e-mail notifications. For multiple recipients, add a semicolon between each e-mail address.

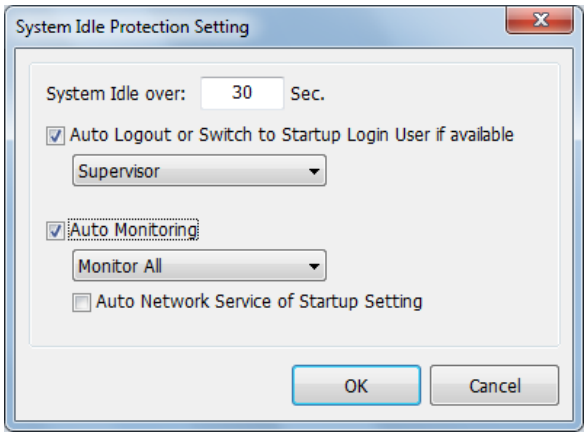
4. Click the **Test Mail** button to send a test e-mail and see whether the setup is correct. If the e-mail fails to send, you may need to check the following settings:
   - **SMTP Mail Server requires authentication:** If the SMTP mail server needs authentication for login, select this option and type 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** or **TLS** if your e-mail server requires the SSL/TLS 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 notificaitons.
   - **Attach Image Setup:** Select **Attach** to include up to 6 snapshots in the e-mail. The image format and size are selectable. Note the actual size can be either the main stream or the sub stream depending on the On Demand setting. See *On Demand Display* later in this chapter.
   - **Email-Alerts Interval:** Specify the time interval (0-60 seconds) between e-mail notifications to prevent e-mails from being sent too frequently. The default interval is 5 minutes.
   - **Domain Name from DDNS:** This option generates URL links in sent e-mails for remote video playback. For this function to work, type the system's fixed IP address or domain name and enable **WebCam Server**.
   - **E-mail in Text Mode:** When **WebCam Server** is enabled, e-mail notifications are sent in HTML format. Select this option if you want to send the e-mail in plain text.

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

1.12.5 System Idle Protection

The System Idle Protection automatically logs off or starts monitoring after the system is idle for a set period of time.

1. Click **Home** > **Toolbar** > **Configure** > **System Configure** > **System Idle Protection Setting**. This dialog box appears.



The System Idle Protection Setting dialog box

2. Type a value between 10 and 14400 seconds for **System Idle Over**.
3. To automatically log out or switch to Startup Auto Login User, select **Auto Logout or Switch to Startup Login User if available** and select an account type to log out.

   If you have set up a Startup Auto Login User, the system will switch to the Startup Login User instead of logging out. See *Setting up a Startup Auto Login User* later in this chapter.
4. To automatically start monitoring, select **Auto Monitoring**, and choose **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.

   ■ To enable network connections to specified applications, select **Auto Network Service of Startup Setting**. See *Customizing Startup Settings* earlier in this chapter.
5. In the **System Idle Over** field, type an idle time between 10 and 14400 seconds.
6. Click **OK**.

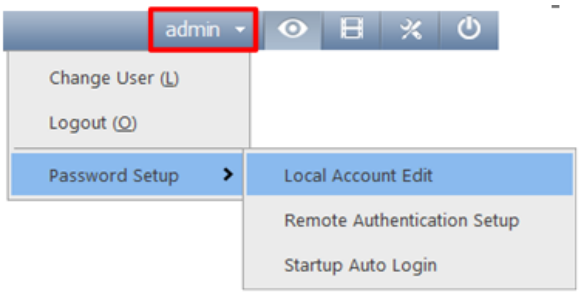
Note: The feature can monitor keystrokes, mouse clicks and actions from IR Remote Control and GV-Keyboard.

1.12.6 Configuring Fast Key Locks

1. To enable/disable certain fast keys, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Fast Key Lock Setup**. The Fast Key Lock Setup dialog box appears.
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**.

1.13 Account and Password

The password setup allows you to assign permission and rights to accounts. You can create up to **1,000** passwords. Only Supervisor-level accounts are pre-set with access to password settings. Click the account ID on the top right of the main window, click **Password Setup** > **Local Account Edit** to start.



1.13.1 Creating an Account

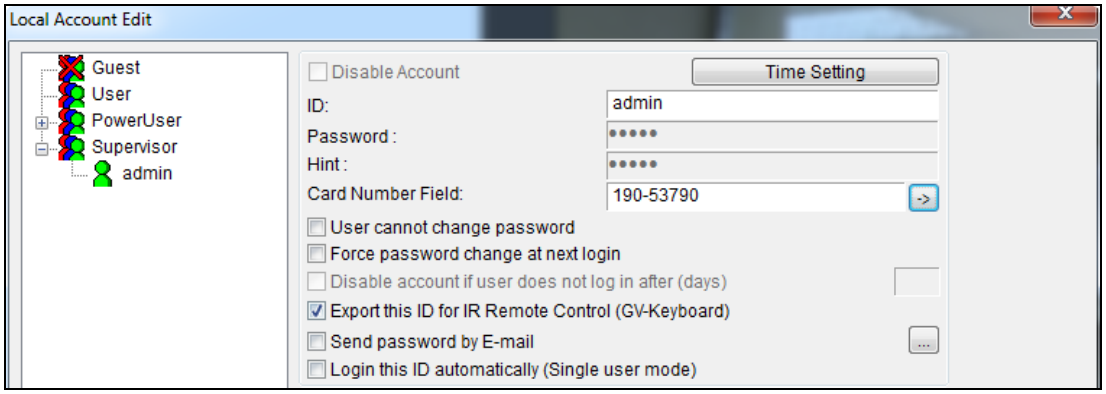
To create a new account, click the **New** button on the lower left of the Local Account Edit dialog box. You can create three types of accounts **Supervisor**, **Power User** and **User**.

- Supervisors have permissions over all system settings.
- Power Users have the same permissions as Supervisors, except that they cannot edit user accounts and delete the password system (described later).
- Users are restricted from all system settings and have limited access to certain functions.

If you want to enable the guest account, click **Guest** and deselect the **Disable Account** option. Guests will only be allowed to watch live view.

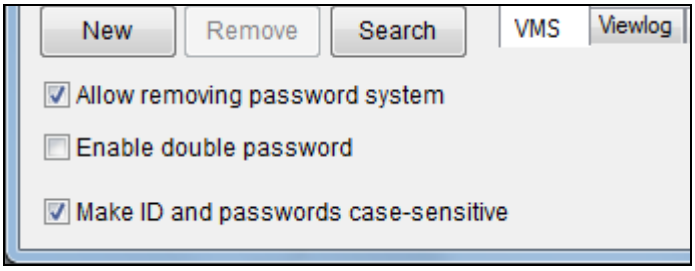
1.13.2 Configuring Account Settings

In the Local Account Edit dialog box, you may find these options to the right of the account list depending on the authorization level.



- **Disable Account:** Select if you want to disable this account.
- **Time Setting:** The account will expire and be disabled automatically after a set number of days. Click **Time Setting**, and select **Expire in (days)**. Specify the number between 1 and 9999.The number you set will count down automatically.
- **Card Number Field:** Users are allowed to automatically log into their accounts by inserting the card in GV-PCR310 Enrollment Reader. Manually type your card number in the field, or insert your card in GV-PCR310 Enrollment Reader and the card number will be shown in the field automatically. Click -> to attach the card number to the user account.
- **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 using GV-Keyboard instead of using the general keyboard and mouse. 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. See *Changing or Retrieving Password at Login* later in this chapter.
- **Login this ID automatically (Single User Mode):** Automatically logs into this account after you click **Login** at startup.

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



- **Allow removing password System:** Enables the password removal utility. The option is critical if you forget or are unable to retrieve any Supervisor password. With this option selected, you can run the password removal utility ***PassUNINStall*** 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 starting ViewLog, you will need to type the passwords of any two supervisors to continue. At least 2 supervisor accounts are required.
- **Make ID and passwords case-sensitive:** Select to make all ID and passwords case-sensitive.

Note:

1. Before running the ***PassUNINStall*** utility, you must disable Service Mode on the system (see *1.12.1 Configuring General Settings*) and then close the system. After running the utility, restart the system.
2. The loss of passwords can be solved in the following two ways:
   - Retrieving password through e-mails.
   - Removing password database by using *PassUNINStall* 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 lose the passwords.

1.13.3 Changing or Retrieving Password at Login

You can change or retrieve passwords of the system through e-mail upon login.

Changing Password

1. In the Login dialog box, click **Change Password**. The Change Password dialog box appears.
2. Type a new password, and click **OK**.

Note: Only Supervisors can change the password.

Retrieving Password through E-mail

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

- If you are a supervisor 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 remember your ID but forgot your password, enter your ID and click **Send Password**. The password will be sent to your e-mail account.

1.13.4 Preventing Unauthorized System Termination

1. To restrict a non-supervisor account from exiting or restarting the system, click the account ID on the top right of the main window, click **Password Setup** > **Local Account Edit**. The Password Setup dialog box appears.
2. Select a user from the user list to display its properties.
3. Select the **AI Guard** tab at the bottom, and deselect the **Exit System** option to restrict the user from quitting or restarting the system.



1.13.5 Setting up a Startup Auto Login User

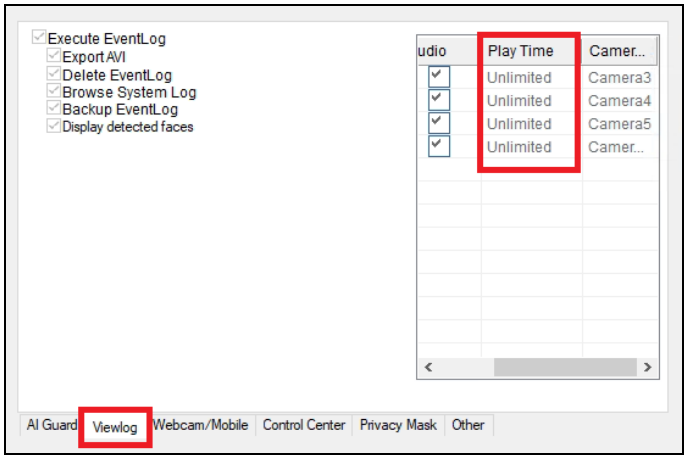
The function is to automatically log in a user account with limited access rights after system startup.

1. Click the account ID on the top right of the main window, click **Password Setup** > **Startup Auto Login** and enable **Startup Auto Login Setup**.
2. Type the ID and Password of an existing account you want to use for the auto login.
3. Click **OK**.

If you have selected **Auto Logout or Switch to Startup Login User if available** in the System Idle Protection Setting dialog box (see *1.12.5 System Idle Protection*), the system will switch to the Startup Auto Login account after it is idle for the set period of time.

1.13.6 Setting up Limits on Playback Time

1. To restrict playback time of camera channels, on the Local Account Edit dialog box, select a account, click the **ViewLog** tab, and click the **Play Time** column you wish to configure.



2. Select **Limited Playback Time** and specify a time limit. If you click , the time limit will be applied to other cameras.

Note: The Setting Limits on Playback Time is based on the time when the user logged into the account. To reset, please log out and log in again.

1.14 Schedule

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

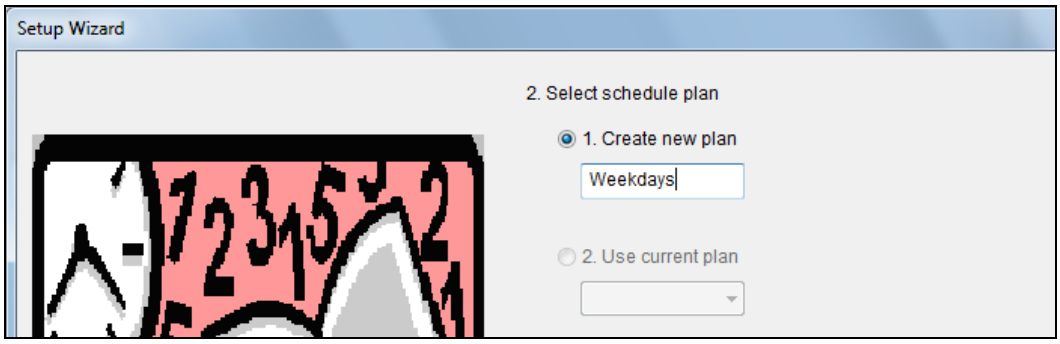
- Recording
- Alert upon motion detection
- AI event monitoring
- Video analysis processing
- I/O monitoring
- Network connection to GV-WebCam Server, GV-Edge Recording Manager, GV-Center V2, GV-Vital Sign Monitor, and Mobile Service.
- PTZ object tracking

Click **Home** > **Toolbar** > **Configure** > **Schedule Edit**. This Schedule window appears.

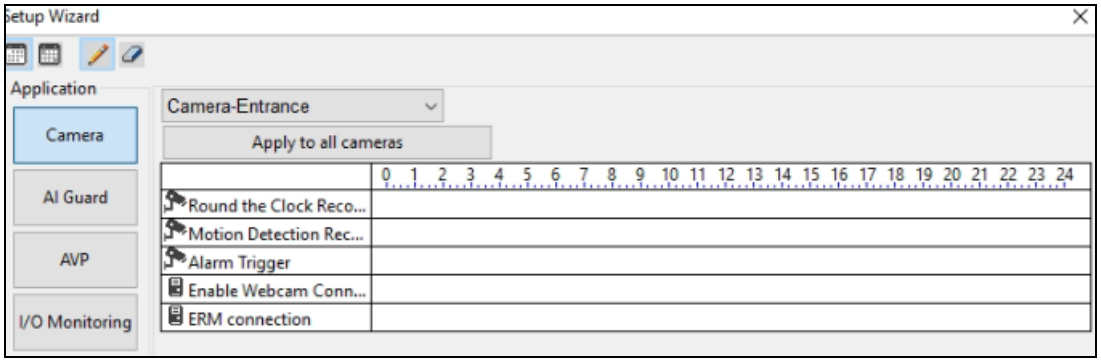
1.14.1 Creating a Schedule with Setup Wizard

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

1. On the Schedule window, click **Schedule** > **Setup Wizard**.
2. Specify when to apply the schedule plan and click **Next**.
   - **Weekly:** Applies the schedule plan to the selected days each week.
   - **Special Day:** Applies the schedule plan to a specific date.
   - **Monthly:** Applies the schedule plan to a specific day each month.
3. Name the schedule plan.



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



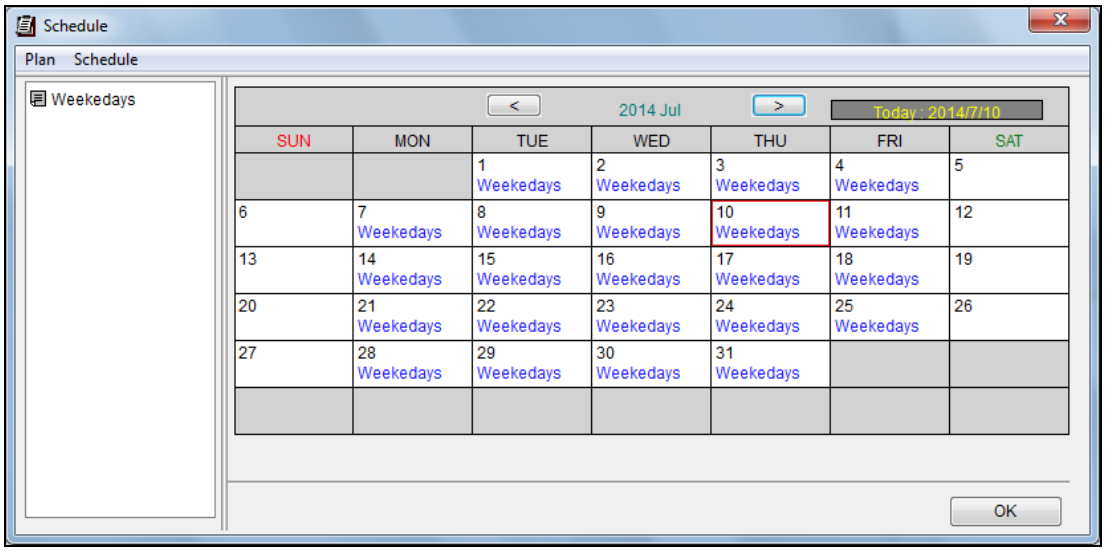
5. When the **Include** button is selected, you will start with an empty timeline. Click the **Add** button and drag across the timeline to enable the function during the specified time. Use the **Erase** button when you want to disable the function.
6. You can also click the **Exclude** button and start 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.

IMPORTANT: When using Schedule and GV-Cloud simultaneously, highlight the entire 24-hour timeline for **Enable Webcam Connection** under Camera and **Start Mobile Server** under Server in the Schedule Plan settings to ensure a proper connection to GV-Cloud.

7. On the left, you'll find the available categories for scheduling.
   - **Camera:** Mainly enables recording-related functions, including continuous and event-triggered recording, within the highlighted time periods.
     - **Round-the-Clock Recording:** Specify times for round-the-clock recording. When highlighting the timeline, you can choose the frame rate settings of **General Event** or **Urgent Event** to apply once the schedule monitoring starts.
     - **Motion Detection Recording:** Specify times for motion detection recording. When highlighting the timeline, you can apply different motion sensitivity levels. If you select **User Defined**, the sensitivity level set in Advanced Motion Detection Setup (see *1.9.4 Setting up Motion Detection*) will be applied.
     - **Alarm Trigger:** Specify times for the Event Trigger actions selected in Advanced Motion Detection Setup (see *1.9.4 Setting up Motion Detection*) to activate upon motion detection.
     - **Enable Webcam Connection:** Specify access times for WebCam Server.
     - **Enable ERM Server:** Specify access times for GV-Edge Recording Manager.
   - **AI Guard:** Specify times for enabling AI event detection.
   - **AVP:** Enables the video processing functions according to the defined monitoring schedule.
     - **Privacy Mask:** Enables Privacy Masking within the highlighted time periods. For details, see *Setting up a Privacy Mask* in Chapter 3.
     - **Advanced Scene Change Detection:** Enable Advanced Scene Change Detection within the highlighted time periods. For details, see *Advanced Scene Change Detection* in Chapter 3.
   - **I/O Monitoring:** Specify times for enabling I/O monitoring.
   - **Server:** Enables network connection to other GeoVision applications within the highlighted time periods.
     - **Connect to CenterV2:** Enables network connection to GV-Center V2 within the highlighted time periods.
     - **Connect to VSM:** Enables network connection to GV-Vital Sign Monitor (VSM) within the highlighted time periods.
     - **Start Mobile Server:** Enables network connection to Mobile Service within the highlighted time periods.

- **PTZ Object Tracking:** Specify times for PTZ related tracking.

8. To apply the Camera / AI Guard / AVP / PTZ Object Tracking schedules to specific cameras, use the camera dropdown list above the timeline or click the **Advanced Setting** button .
9. Click **OK**. The schedule plan appears on the days specified.



10. Click **Home** > **Toolbar** > **Monitor** > **Start Schedule Monitoring**.

Tip:

1. You can add multiple plans to the calendar.
2. You can also apply a plan to a date by dragging it from the left panel and dropping it onto the calendar on the right.
3. To edit a schedule, double-click the plan in the calendar.

1.14.2 Creating a Schedule Manually

1. In the Schedule window, select **Plan** > **Add** from the menu at the top.
2. Name the plan and click **OK**.
3. Click **Schedule** and select an option below:
   - **Edit Special Day:** Applies the plan to a specific date each year. Select a **Date** and a **Plan** and click the **Add** button.
   - **Edit Weekly:** Applies the plan to the selected days each week.
   - **Edit Monthly:** Applies the plan to a specific date each month. Select a **Day** of the month and a **Plan**, and click the **Add** button.

4. Double-click the plan to edit the schedule timeline. For details, see *Creating a Schedule with Setup Wizard* earlier in this section.

1.14.3 Exporting and Importing Schedule Settings

Schedule settings can be exported into an .xml file, and imported back later or to another system.

1. In the Schedule window, select **Schedule** > **Export** or **Import** from the menu at the top. A dialog box appears.
2. Specify a path to save the .xml file. Or, specify where the exported .xml file has been stored.
3. Click **OK.**

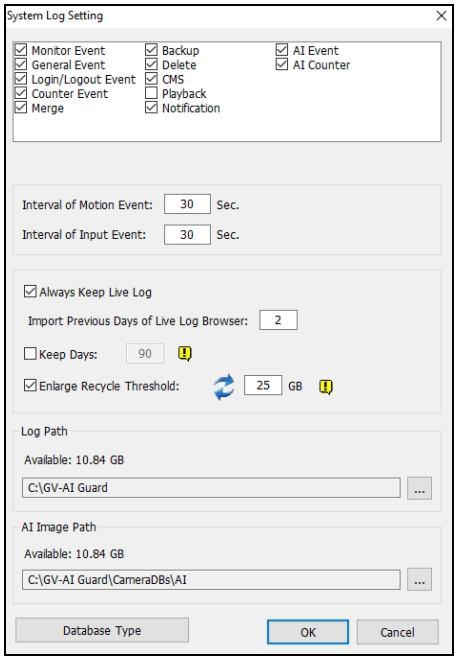
1.15 System Log

The System Log provides a text-based record of general events, system activities, and people / vehicle counting events, offering fast access to recent event data for tracking and reviewing past system behavior.

For more comprehensive and detailed log data, including the ability to apply advanced filters such as device, time range, and event subtype to general, system, or counting events, see *Advanced Log Browser* in Chapter 4.

1.15.1 Setting up System Log

In the System Log Setting, you can specify which events to record, the interval time to write events into the log, the number of days to keep the log for, and the system log path. Click **ViewLog**  > **Toolbar**  > **Configure**  > **System Log Setting**. This dialog box appears.



Select the event type register in the system log:

- **Monitor Event:** Registers motion-triggered and input-triggered events. For this function to work, you need to enable **Register Motion Event** in the Advanced Motion Detection Setup (see *1.9.4 Setting up Motion Detection*) and **Register Input Event** in the I/O Application Setting (see *6.2.1 Setting up Actions upon I/O Trigger*).
- **General Event:** Registers system startup/exit, network server start/stop, and monitoring start/stop.
- **Login/Logout Event:** Registers login/logout activities of local users to the system and remote servers.
- **Counter Event:** Registers counting results.
- **Merge:** Registers the merging of recorded videos.
- **Backup:** Registers the backup of recorded videos.
- **Delete:** Registers the deletion of recorded videos through remote connection.
- **CMS:** Registers the events of central monitoring services.
- **Playback:** Registers playback of recorded videos.
- **Notification:** Registers e-mail notifications.
- **AI Event:** Registers AI events.
- **AI Counter:** Registers the count data from GV-3D People Counter V2 and AI-capable GV-IP cameras for People Count.

The following settings are also available:

- **Interval of Motion Event:** Specify the log interval between motion-triggered events, which prevents the system to record events too frequently when motion triggers are intensive.

- **Interval of Input Event:** Specify the log interval between input-triggered events, which prevents the system to record events too frequently when input triggers are intensive.
- **Always Keep Live Log:** Display the latest logs in the system log tables (see *Viewing System Log* later in this chapter). When not selected, the logs of the time selected in the ViewLog timeline will be displayed if available.
- **Import Previous Days of Live Log Browser:** Specify how many days of data to be loaded into the system log.
- **Keep Days:** Set the number of days to keep the logs.
- **Enlarge Recycle Threshold:** Set the recycle threshold for the system to delete old AI images and logs to make space for new data when the free space of the **AI Image Path** is below the threshold. The default threshold is set to 25 GB.
- **Log Path:** Specify a storage path for the logs. The default path is at :\GV-AI Guard\Logs. The free space in the storage path will be displayed.
- **AI Image Path:** Specify a storage path for AI event images. The default path is at:\GV-AI Guard\AI. The free space in the storage path will be displayed.
- **Database Type:** Select **Microsoft Office Access Database** or **Microsoft SQL Server** as a database, and fill out the required connection information.

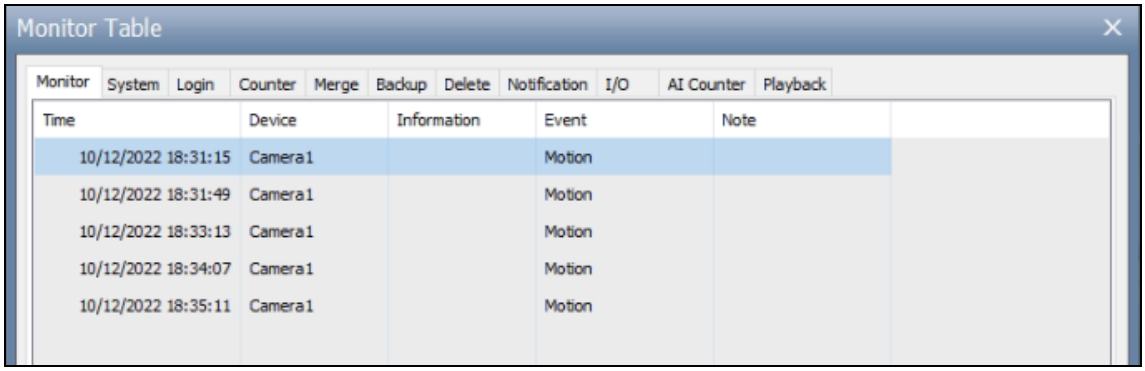
Note: If the designated storage space is not big enough to keep all video files for the defined days, the **Enlarge Recycle Threshold** setting will override the **Keep Days** setting.

1.15.2 Viewing System Log

To view the system log, click **Home** > **Toolbar** > **Tools** > **System Log**. The following options are available: Monitor Table, POS Table, CMS Table, and AI Event Table.

Monitor Table

This table displays local events in the system.



[Monitor] Shows events related to camera connection and motion. Double-clicking an event entry allows playback of the recorded video in ViewLog if available.

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

[Login] Shows whom and when has logged in and out of the system and WebCam server.

[Counter] Shows the information and results of the Counter functions.

[Merge] Shows the merging events of recorded videos.

[Backup] Shows the backup events of recorded videos.

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

[Notification] Shows e-mail notifications.

[I/O] Shows the events of I/O trigger.

[AI Counter] Shows AI counter data.

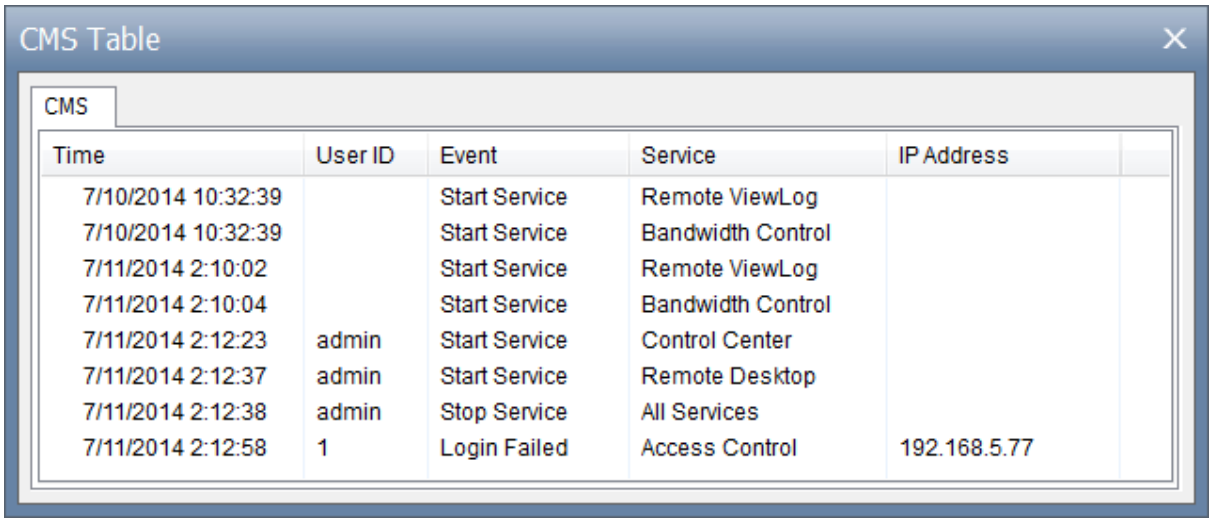
[Playback] Shows the playback events of recorded videos.

POS Table

See *Chapter 10 Point-Of-Sale (POS) Application*.

CMS Table

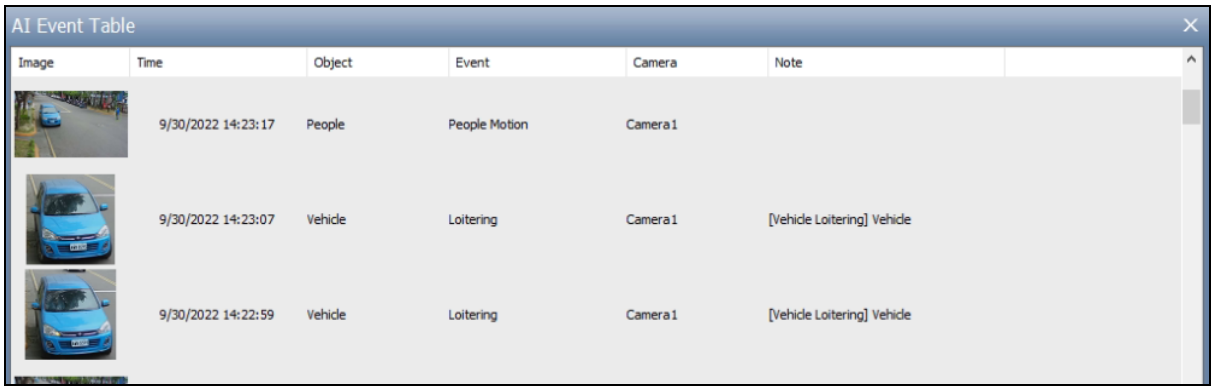
This table displays the connection status, login activities and service started/stopped of central monitoring service (CMS).



AI Event Table

This table displays the captured image, time, event type, and camera name of AI events.

Double-clicking an event entry allows playback of the recorded video in ViewLog.

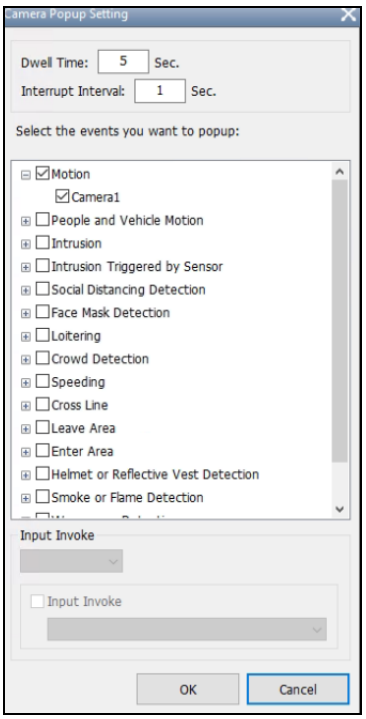


To search for AI events based on certain criteria, see *1.6 AI Event Playback and Search*.

1.16 Other Functions

1.16.1 Setting up Popup Live View

To set up a popup live view that overlays the entire main screen when an event occurs, click **Home** > **Toolbar** > **Configure** > **Camera Popup Setting**. The Camera Popup Setting dialog box appears.



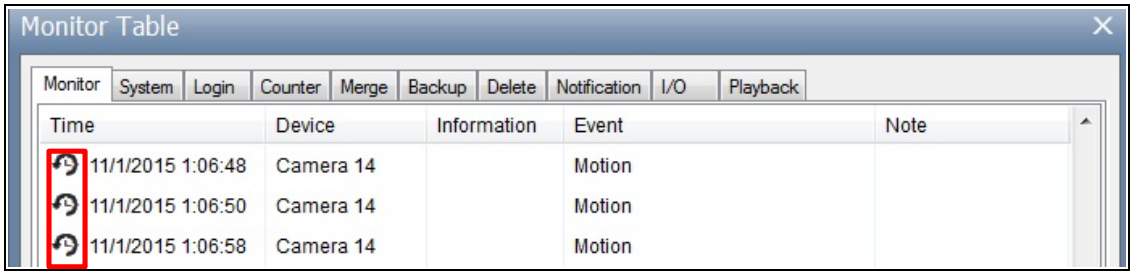
- **Dwell Time:** Specify the duration of a popup view to remain in the foreground.
- **Interrupt Interval:** Specify the interval between popup views, which prevents frequent popup alerts when several cameras are activated at the same time.
- **Events:** Select the camera channel to pop up upon motion and event detection.
- **Input Invoke:** Select **Input Invoke** and assign a camera to the defined input device. Whenever the input is triggered, the live view of the assigned camera pops up. For this function to work, it is required to enable I/O monitoring along with camera monitoring.

Tip: You can use the **Mask Region** function in the Advanced Motion Detection Setup (see *1.9.4 Setting up Motion Detection*) to mask off certain areas of the camera image from motion detection.

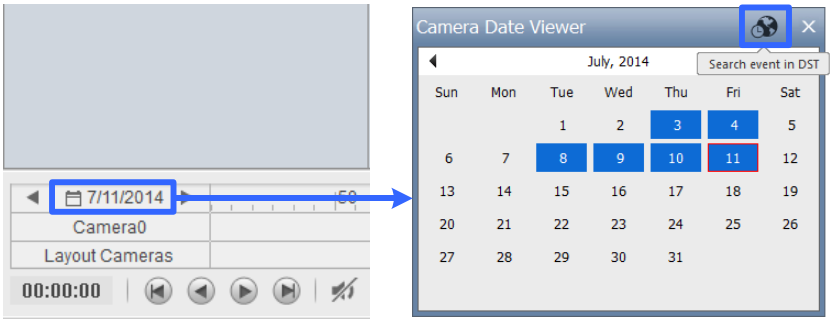
1.16.2 Adjusting to Daylight Saving Time

The system can automatically adjust for Daylight Saving Time (DST). If you live 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.

In the system log, DST events are labeled with the clock icon in the **Time** column.



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

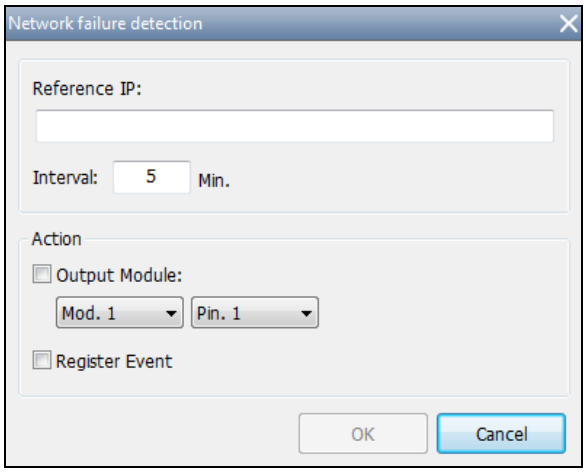


Note: Videos recorded during DST periods start with “GvDST”, e.g. GvDST20140722.avi, to differentiate from regular video files that start with “Event”, e.g. Event20081022.avi.

1.16.3 Setting up Network Failure Detection

The Network Failure Detection triggers an output device when the network connection between the system and the specified network host has failed.

1. Click **Home** > **Toolbar** > **Network** > **Network Failure Detection**. This dialog box appears.



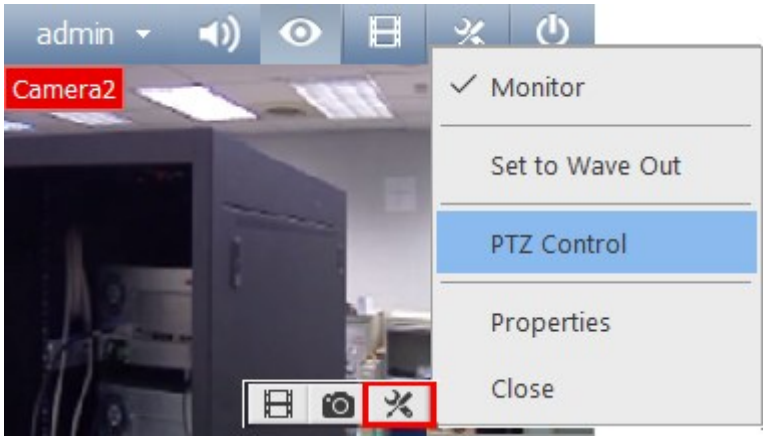
2. Under **IP Address**, type the IP address or domain name of the remote host.
3. Next to **Interval**, type the time interval between each ping in minutes ranging from 1 to 999. If the interval is 5 minutes, the system will ping the network host every 5 minutes to check if the connection is still active.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

The selected output device will be triggered when the network host does not respond to the system’s ping message.

1.17 PTZ Camera

With the PTZ control panel, you can control PTZ functions, e.g., pan, tilt, zoom, focus and preset points.

1. Move the cursor to the camera live view of a connected PTZ camera and click **Tools** .



2. Click **PTZ Control** to enable PTZ function.
3. You can control GV-IP Speed Domes 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.

1.17.1 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.

Note: ONVIF PTZ cameras do not support Iris Open / Close function on the PTZ control panel.



In the PTZ control panel, click **Home** 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.
- **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.
- **Add Preset:** 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.
- **Remove Preset:** Allows you to remove existing preset points.

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 Tracking**.

Cruise

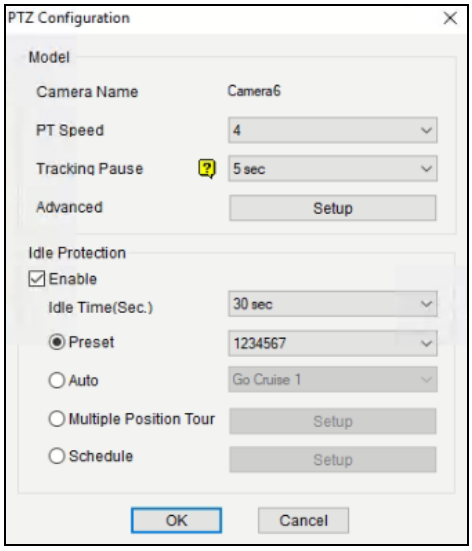
You can set up a route consisting of different directions, angles, and zooms for the PTZ camera to follow. Up to 4 Cruises can be created.

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 Tracking**.

1.17.2 Setting up PTZ Idle Protection and Advanced Functions

In the Content List, right-click the PTZ camera and select **PTZ Setup**. This dialog box appears.



[Model]

- **PT Speed:** Adjusts the speed of pan and tilt movements.
- **Tracking Pause Interval:** Define the pause time, from **5 sec** to **60 sec**, for the PTZ that stops tracking.
- **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]

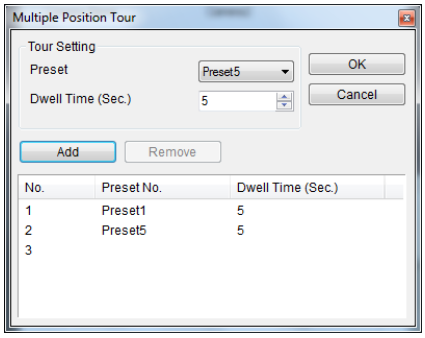
When the PTZ camera remains stationary for a certain period of time, the PTZ can automatically move to a Preset Point, enable an Auto function, begin a Multi Position Tour, or start a PTZ schedule.

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

Setting Multiple Position Tour

You can create a PTZ tour with up to 64 preset points. The number of preset points supported depends on the camera's capacity.

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

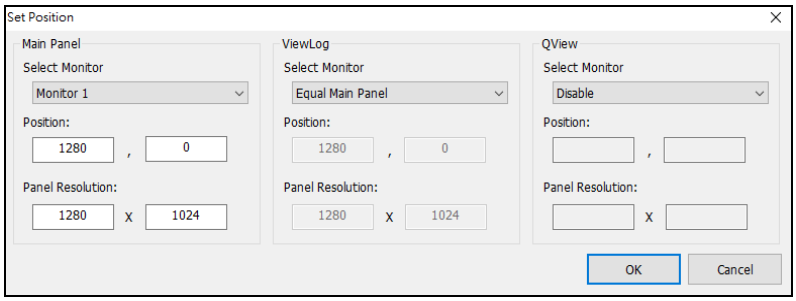


2. Select a **Preset** as a start point.
3. Set the **Dwell Time** that the camera remains at each preset point, from **15 sec** to **60 sec**.
4. Click **Add** and repeat Steps 2 to 3 to create more points in the tour.

1.18 QView

If there are multiple monitors connected, you can use the QView feature to display full-screen live view of a camera on a separate monitor.

1. Click **Home** > **Toolbar** > **Configure** > **System Configure** > **Set Position**. This dialog box appears.



2. In the QView section, select a monitor from the **Select Monitor** dropdown list for a full-monitor display and click **OK**.
3. Double-click a camera view on the main window. The camera view is displayed in full screen on the designated monitor.

4. To switch another live view to a full-monitor display, simply double-click another camera view.

To record short video clips on a full-monitor display, see *Creating a Storyline in QView* later in this chapter.

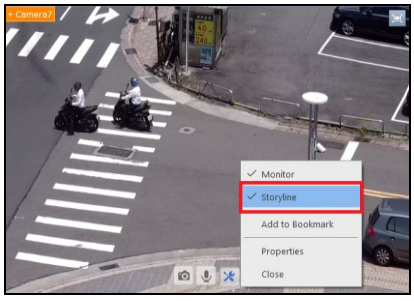
1.19 Storyline

With the Storyline feature, you can combine camera images from multiple channels into a sequence of short video clips of a specific incident, such as gambling fraud, shoplifting and other fraudulent activities. The recorded videos can be saved and played back later using a media player. This feature is available in live view, video playback and QView display.

1.19.1 Creating a Storyline in Live View

To create a storyline in live view, follow the steps below.

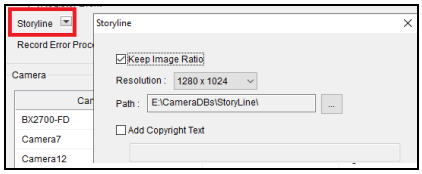
1. Select **Home** and set up the screen division.
2. In the Content List, click **Layout**, double-click **Windows**, and drag **Zoom Window** to a live view grid. Any camera views on the Zoom Window will be recorded as a storyline.
3. To display cameras in the Zoom Window for recording, either drag the desired cameras into the Zoom Window or click the **Zoom** button at the top right of a camera view already in the layout.
4. On the Zoom Window, click the **Tools** icon > **Storyline** to start recording. The orange label indicates that the recording is in progress.



5. To record from another camera view, click the **Zoom** button of that camera view.
6. When you finish, deselect **Storyline** to stop recording. The Edit Description dialog box appears.
7. Type a name or description for the video clip and click **OK**.

Note:

1. The recording duration is limited to 30 minutes per storyline.
2. The storyline resolution can be set to 1280 x 1024 (default) or 1920 x 1080. To change the resolution, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting** and click the down button next to *Storyline*.



1.19.2 Creating a Storyline in Video Playback

The procedures of creating a storyline with playback videos are similar to those for the live view.

1. Click **ViewLog** > **Toolbar** > **Content List**, and drag **Zoom Window** onto a playback grid.
2. To display a video on the Zoom Window, click the **Zoom** button on the top right of a playback video.
3. On the Zoom Window, click the **Tools** icon > **Storyline** to start recording.
4. To record another video, click the **Zoom** button of that playback video.

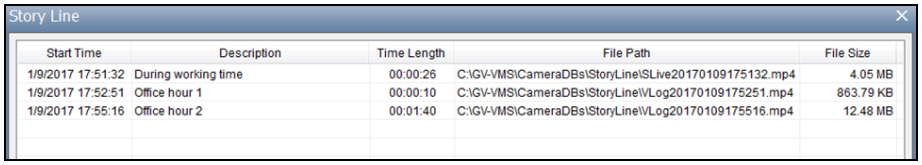
1.19.3 Creating a Storyline in QView

To create a storyline in QView, follow the steps below.

1. Follow the instructions in *QView* earlier in this chapter to set up a full-monitor display.
2. On the designated monitor, click **Tools** > **Storyline** to start recording.
3. To record the live view from another camera, simply double-click another camera view.

1.19.4 Accessing a Storyline

After creating the storyline, select **ViewLog** > **Toolbar** > **Tools** > **Storyline**. Your storyline will be listed in the window below.



Right-click a storyline in the list to access more features, such as playback, changing the file path and editing the description. You can also use the **Filter** button to search for the desired storylines.

Chapter 2

IP Camera Setup 140

2.1 Adding IP Cameras 140

2.1.1 Adding Cameras Manually 142

2.1.2 Scanning for Cameras 144

2.1.3 Mapping GV-IP Cameras using GV-IP Device Utility 144

2.2 Configuring Individual IP Cameras 145

2.2.1 Configuring Video Settings 145

2.2.2 Configuring Audio Settings 147

2.2.3 Configuring Abnormality Settings 149

2.3 Connection through RTSP, ONVIF & PSIA 151

2.4 On Demand Display 153

2.5 Wide Angle Lens Dewarping 155

2.6 Fisheye View 157

2.6.1 Setting up Fisheye View 157

2.6.2 Setting up a Third-Party Fisheye Camera 160

2.6.3 Object Tracking 162

2.6.4 Virtual PTZ Tour 164

2.7 PTZ Object Tracking 166

2.7.1 Dual-Camera Tracking 166

2.7.2 Single Camera Tracking 168

2.8 Panoramic PTZ Object Tracking 170

2.8.1 Accessing the Live View 171

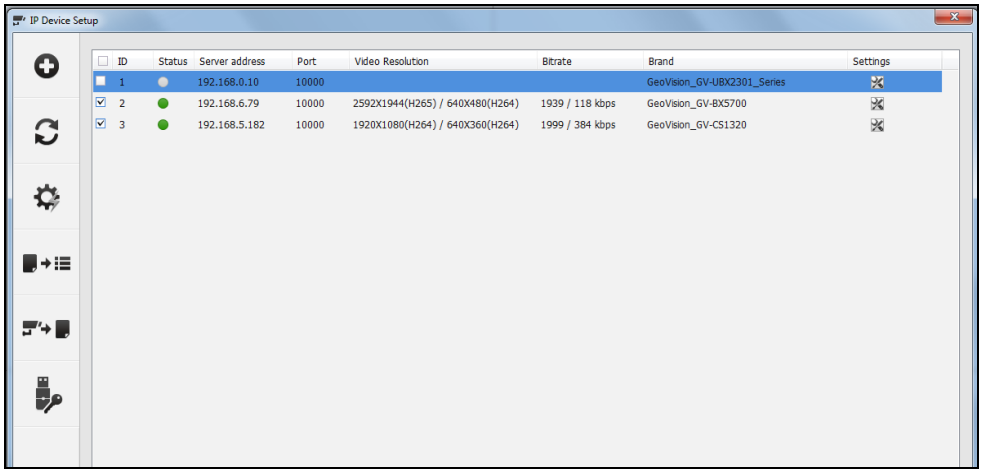
2.8.2 Automatic Object Tracking 172

CHAPTER 2

IP Camera Setup

2.1 Adding IP Cameras

There are several ways to connect IP devices to the system, and the procedures may vary depending on the device. To access the IP Device Setup, click **Home** > **Toolbar** > **Configure** > **Camera Install**.



IP Device Setup

- To manually set up an IP device, click **Add Camera** .
- To detect IP devices on the LAN, click **Scan Camera** .
- To detect and automatically add multiple IP devices on the LAN, click **Automatic Setup** .
- To import IP devices from GV-IP Device Utility, click **Import Camera** .
- To map IP devices through GV-IP Device Utility, click **IP Device Utility** .
- To license the system and third-party cameras using a software license or GV-USB dongle, click **GeoVision License Activation Tool** . For software licensing instructions, see the technical notice.

Note: *GeoVision License Activation Tool* is not supported by **GV-AI Guard**.

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

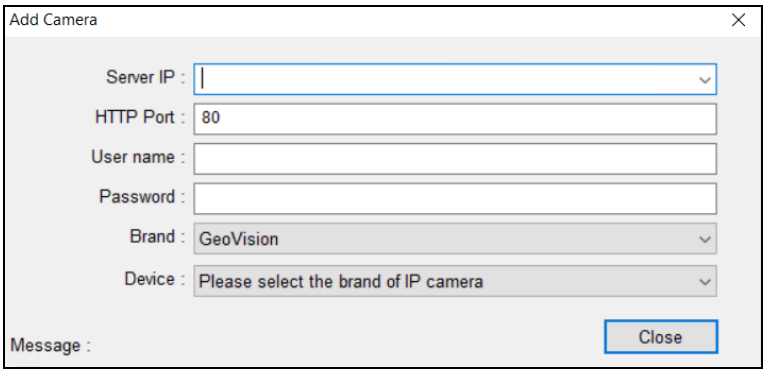
Third-Party IP Devices

The system supports not only GV-IP devices but also 3rd-party IP devices through ONVIF, RTSP, and/or PSIA protocols.

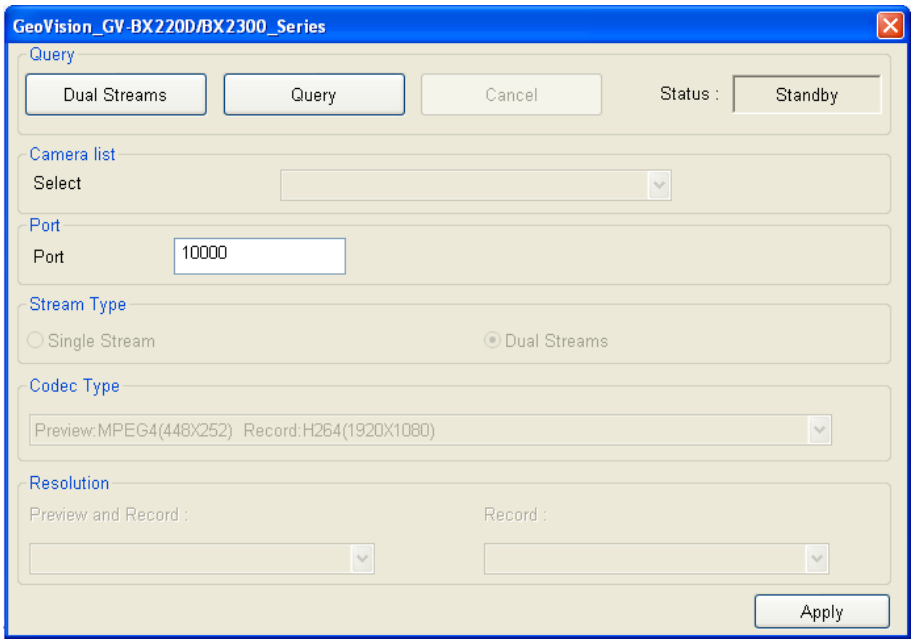
If a 3rd-party device cannot be detected using *Scan Camera* or *Automatic Setup*, you can add it manually using the **Add Camera** function. For details, see *Connection Through RTSP, ONVIF & PSIA* later in this chapter.

2.1.1 Adding Cameras Manually

1. To manually add IP devices, click **Add Camera** in the IP Device Setup (see *2.1 Adding IP Cameras*).
2. Type the IP address, username and password of the IP device. Modify the default HTTP port if necessary.



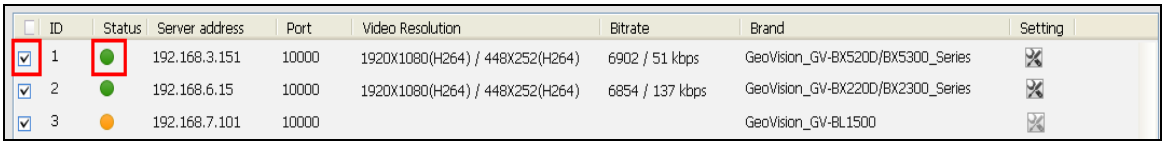
3. Select a camera brand and model name from the **Brand** and **Device** dropdown lists, respectively. This dialog box appears.



4. Configure the options listed below, which may vary between 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 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 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, select the checkbox beside the **ID** column in the IP Device Setup dialog box. The **Status** icon turns green upon successful connection, with the video resolution and bit rate being displayed in the corresponding columns.



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

Note: The indication of status icons is as below.

	Connected	The camera is connected.
	Connecting	The system 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 camera's own configuration interface by right-clicking the camera in the IP Device Setup dialog box and selecting **Remote Camera Setting**.

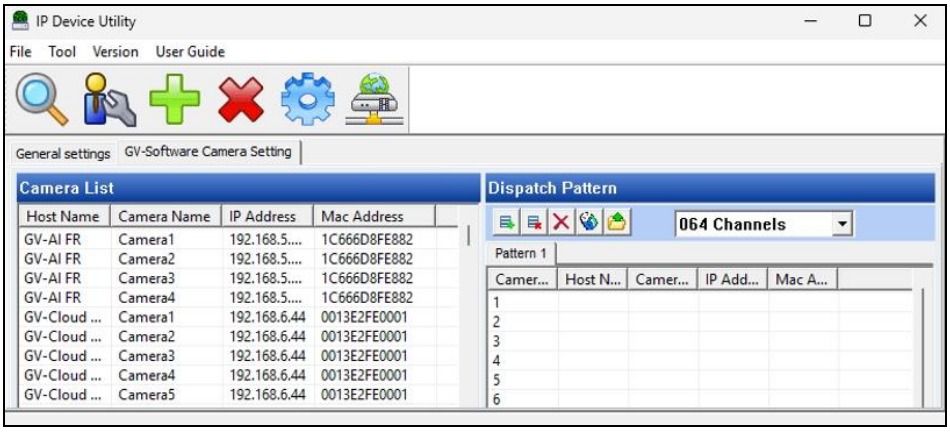
2.1.2 Scanning for Cameras

1. To detect IP devices on the LAN, click **Scan Camera** in the IP Device Setup (see *2.1 Adding IP Cameras*). The Scan Camera dialog box appears.
2. Click **Start Scan**. The IP devices detected are displayed.
3. Double-click the IP device you wish to connect to, type its username and password, and click **OK**. The Camera Streaming Settings dialog box appears.
4. Click **Apply**. The IP camera is added to the IP Device List and automatically enabled for connection.

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

GV-IP Device Utility detects all available IP devices within the LAN and allows users to map detected cameras to the specified channels. Users can then export the device list and import it into the system. In addition, GV-IP Device Utility also lets users quickly set IP addresses, upgrade firmware, export/import device settings, and reboot IP devices.

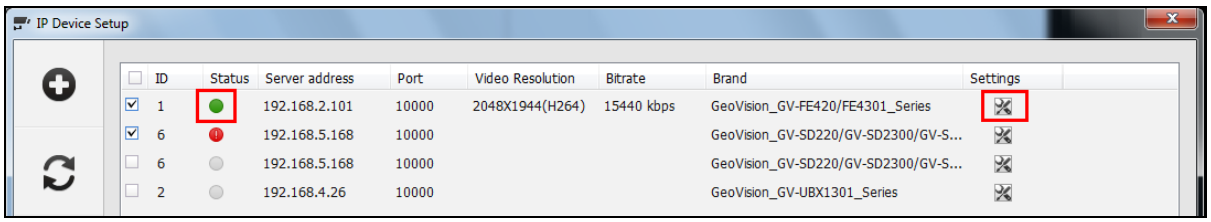
Click **IP Device Utility** in the IP Device Setup (see *2.1 Adding IP Cameras*). All the available IP cameras on the LAN are detected and listed in the window.



To map IP cameras to the channels of the system, see *7. Assigning Camera Channels for GV-DVR / NVR / VMS* in the *GV-IP Device Utility Guide*.

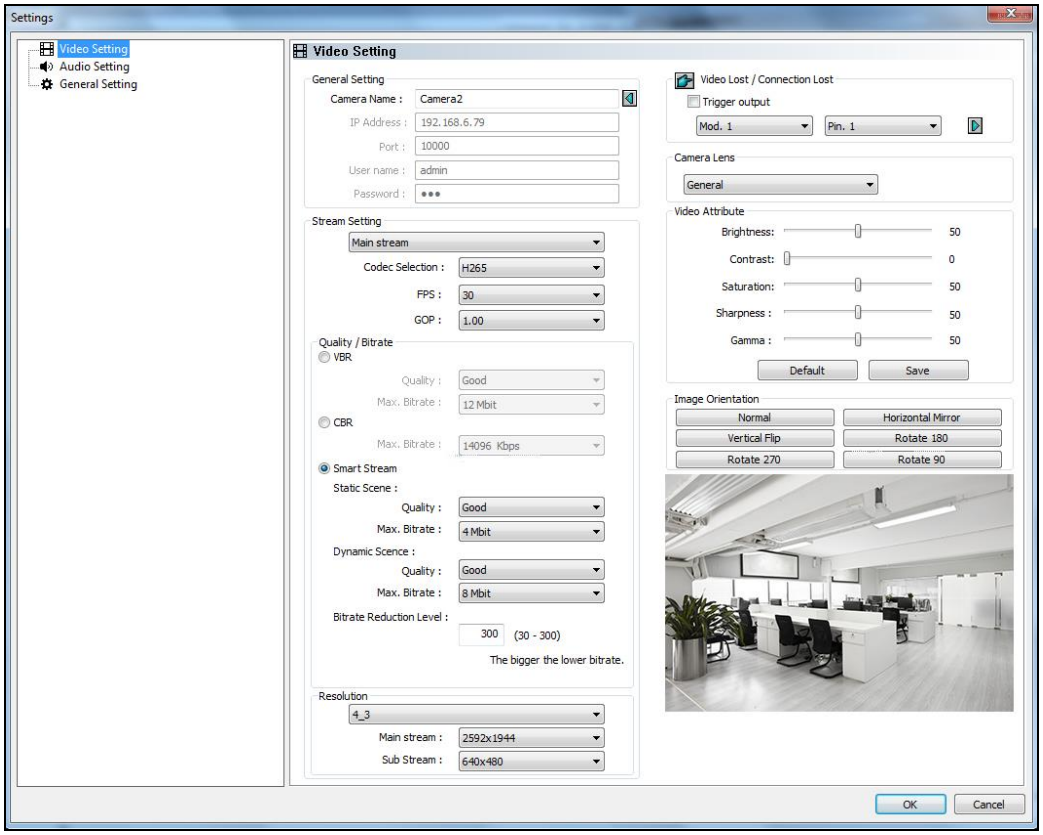
2.2 Configuring Individual IP Cameras

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



2.2.1 Configuring Video Settings

In the Video Settings dialog box, you can configure video settings such as codec type, frame rate, and camera resolution.



[Stream Setting] Select a stream from the dropdown 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 *On Demand Display* later in this chapter.

- **Codec Selection:** Set the codec to **MJPEG**, **H.264**, or **H.265**.
- **FPS:** Set the number of frames per second.
- **GOP:** Set the number of frames between each key frame (I-frame), ranging from 5 to 255. For example, with an FPS of 15, a GOP of 30 means one key frame is inserted every 30 frames (i.e., every 2 seconds).
- **Quality and Bitrate:** When using the H.264 / H.265 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 / H.265 stream. Select one of the bitrates from the dropdown list.
- **Smart Streaming:**
  - **Static Scene**: Set the image quality to one of the 5 standards: **Standard**, **Fair**, **Good**, **Great** and **Excellent**. Set a **Max. Bitrate** if needed.
  - **Dynamic Scene**: Set the image quality to one of the 5 standards: **Standard**, **Fair**, **Good**, **Great** and **Excellent**. Set a **Max. Bitrate** if needed.
  - **Bitrate Reduction Level**: The bigger the value the more bitrates can be reduced in static scenes, thus saving the recording size.
- **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. 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. For details, see *Wide Angle Lens Dewarping* later in this chapter.

If you are using third-party fisheye cameras, select **IMV1 Panorama** for the camera installed with an ImmerVision IMV1 Panorama Lens, and select **Fisheye** for other third-party fisheye cameras. For details, see *Setting up a Third-Party Fisheye Camera* later in this chapter.

[Video Attribute] Adjust video characteristics, such as brightness, contrast, saturation, sharpness and gamma.

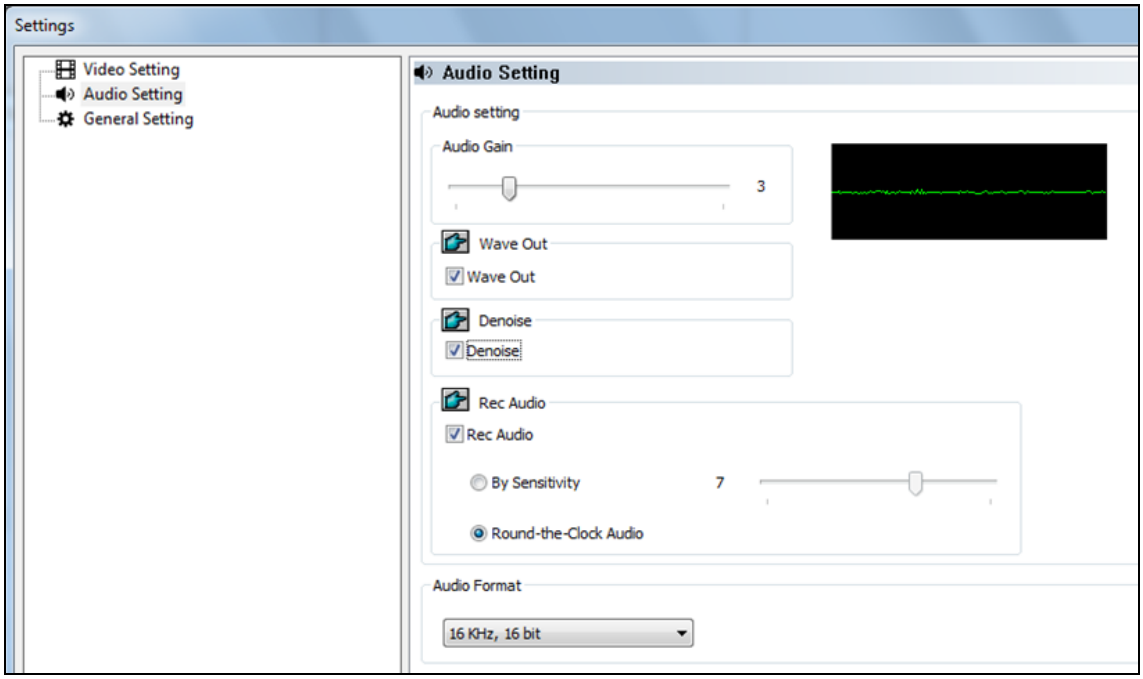
[Image Orientation] Adjust the image orientation by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip**, **Rotate 180**, **Rotate 90**, or **Rotate 270 (Corridor format)**. Select **Image Orientation by Software** for the system to perform the function; otherwise, it's performed by the IP camera.

Note:

1. Changes made to the Video Setting page will change the settings on the IP camera.
2. The Image Orientation options for **Rotate 90** and **Rotate 270 (Corridor format)** are only available for GV-IP Cameras that support the function.
3. When PVD Motion is enabled and the IP camera's GOP value exceeds its frame rate, the GOP value will be automatically adjusted to ensure the detection accuracy.

2.2.2 Configuring Audio Settings

In the Audio Settings dialog box, you can adjust audio devices and listen to live sound.

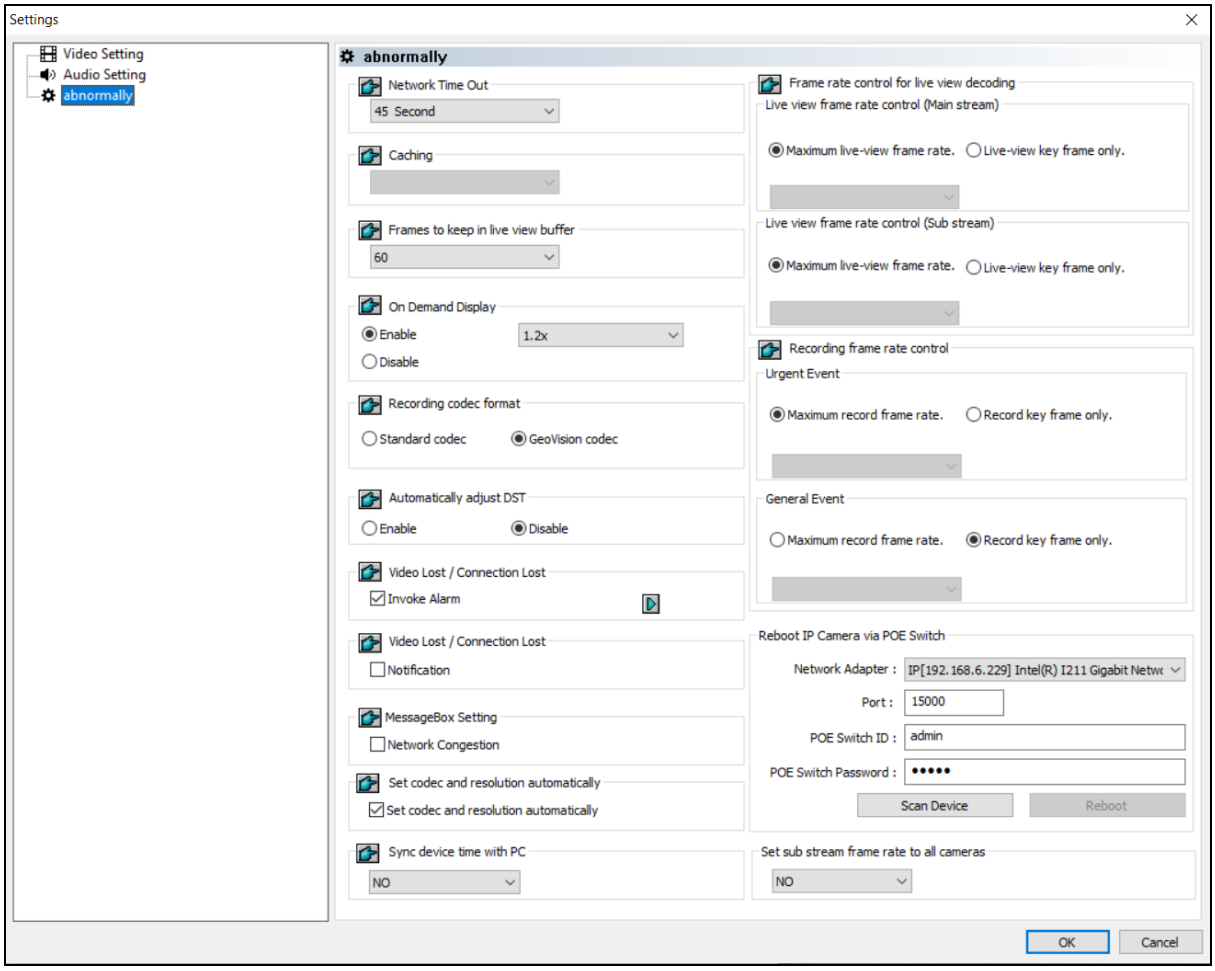


- **Audio Gain:** Increase or decrease the gain of the microphone.
- **Wave Out:** Select to listen to the audio around the camera.
- **Denoise:** Select to reduce audio noise.

- **Rec Audio:** Select **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 dropdown list. The default is **16 KHz, 16 bit**.

2.2.3 Configuring Abnormality Settings

In the Abnormality dialog box, you can configure settings such as network timeout behavior, video loss and connection loss responses, and message box alerts.



- **Network Time Out:** When network disconnection exceeds the specified time, the status icon on the IP Device Setup list (see *2.1 Adding IP Cameras*) becomes yellow.
- **Caching:** Specify the number of milliseconds to postpone live view decoding. When the network connection with the IP device is unstable or when the time length between frames is not evenly distributed, postponing the live view decoding will make the video smoother. Note that 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 *On Demand Display* later in this chapter.

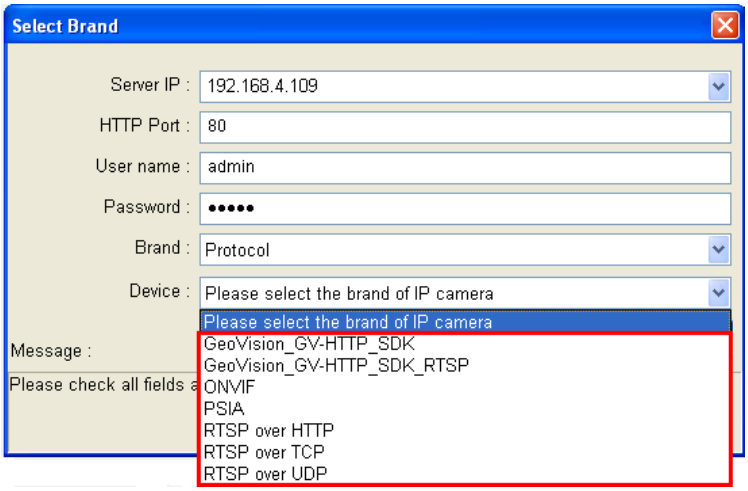
- **Recording Codec Format:** Specify whether to record in standard or GeoVision codec.
- **Automatically Adjust DST:** If enabled, the time on GV-IP Device's Web interface will be synchronized with that on the system when DST period starts or ends.
- **Video Lost / Connection Lost (Invoke Alarm):** 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 receive e-mail notifications upon connection lost. See *Setting up E-mail Notifications* in Chapter 1 to configure the e-mail server.
- **Message Box Setting (Network Congestion):** When enabled, the Network Congestion message will pop up under such a condition.
- **Set Codec and Resolution Automatically:** If enabled, the system will resume the configured codec and resolution when it detects the changes made by the camera.
- **Sync Device Time with PC:** This function is set to NO by default, meaning the camera time will not sync with the GV-AI Guard system time. When an interval of *1 – 24 hours* is selected, the camera time syncs with GV-AI Guard upon connection and re-syncs automatically at the specified interval.
- **Frame Rate Control for Live View Decoding (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 **Maximum live-view frame rate** and **Live-view key frame only** are grayed out.
  - When using **H.264 / H.265**, only one key frame is transmitted per the specified number of frames, so you can select **Live-view key frame only** to decode key frames only and omit all intermediate frames or **Maximum live-view frame rate** to include all 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. See *Setting up Recording Settings for Individual Cameras* in Chapter 1.
  - When using **MJPEG**, every frame is a key frame, so the options of **Maximum record frame rate** and **Record key frame only** are grayed out. You can specify the recording frame rate for **Urgent Event** and **General Event** respectively.
  - When using **H.264 / H.265**, only one key frame is transmitted per the specified number of frames. You can select **Maximum record frame rate** for **Urgent event** and select **Record key frame only** for **General event**.
- **Reboot IP Camera via POE Switch:** Restart a specified camera via its connected GV-POE Switch with the Web management functionality. Type the ID and Password of the switch to start rebooting.

- **Set Sub Stream Frame Rate to All Cameras:** When connected to over 32 channels, the system automatically adjusts the sub stream frame rate of all cameras to 15 fps. Select from the dropdown list to manually adjust the sub stream frame rate for all cameras at once.

2.3 Connection through RTSP, ONVIF & PSIA

To add IP devices compliant with RTSP, ONVIF or PSIA protocol to the system, follow the steps below.

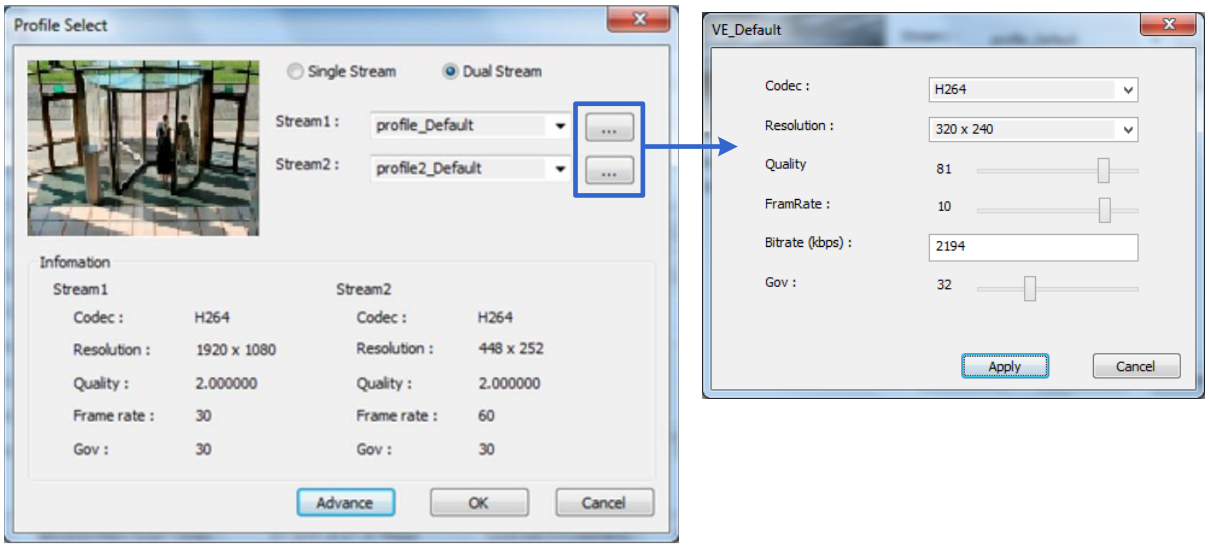
1. Click **Home** > **Toolbar** > **Configure** > **Camera Install**.
2. Click **Add Camera** to manually add an IP camera. This dialog box appears.
3. Type the IP address, username and password of the IP camera. Modify the default HTTP port if necessary.
4. Select **Protocol** from the **Brand** dropdown list.
5. Select the protocol that is supported by your IP camera from the **Device** dropdown list.



- **GV-HTTP_SDK:** For SDK users only. The RTSP protocol uses an HTTP port for data streaming from the IP camera.
- **GV-HTTP_SDK_RTSP:** For SDK users only. The RTSP protocol uses an 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 an 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 a 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 Stream 1 and Stream 2 to adjust the following information.



- **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**, a dialog box appears after the system confirms that the camera is PSIA compatible. Click **Apply**.
8. If you select **RTSP**, select **Dual Streams** to enable the Sub Stream if needed and type the RTSP link address.

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

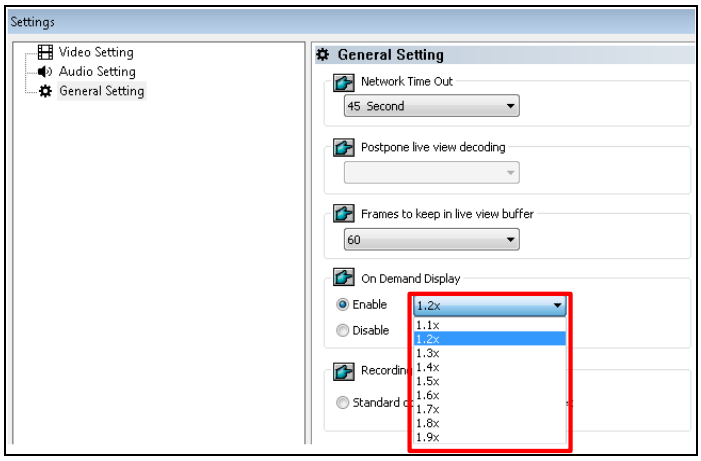
   - For an AXIS IP camera, type RTSP://<IP of the IP camera>/<codec>/media.amp
   - For a HIKVISION IP camera, type RTSP://username:password@<IP of the IP Camera>
9. Click **OK** to add the IP camera to the IP Device List.

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 a value of **X times the resolution of the sub stream** as the threshold. When the camera image on the screen is bigger than the threshold, the system will switch to the higher resolution streaming, usually the main stream. Such adjustment is enabled when using view modes that require higher image quality, such as Single View, PIP View, or Focus View. The system will switch to the lower resolution streaming to reduce CPU usage when watching live view in view modes where higher resolution does not make a difference, such as highly divided divisions.

1. Make sure the IP camera has been added to the system and you have selected **Dual Stream** during setup. For details, see *Adding IP Cameras* earlier in this chapter.
2. In the IP Device Setup (see *2.1 Adding IP Cameras*), click the **Setup** button of the desired connected camera within the IP Device List and select **Abnormality**.
3. In the On Demand Display field, click **Enable** and select a value. When the camera image on the screen is **X times** bigger than the resolution of sub stream, the system will switch to the higher resolution streaming.



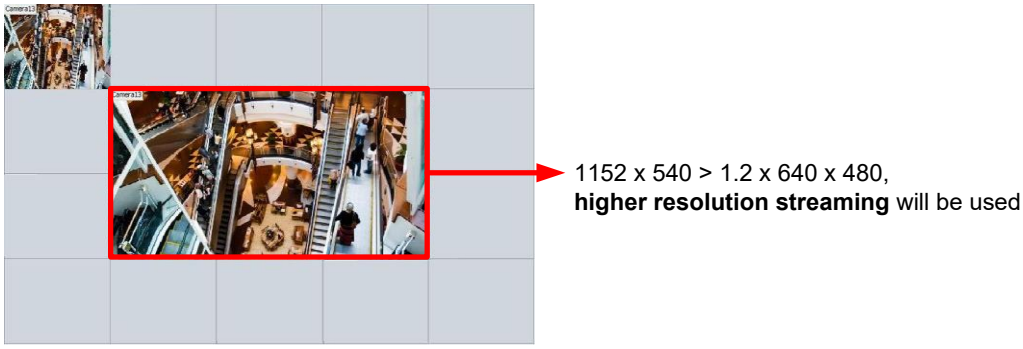
Note:

1. The **On Demand Display** function is not supported for the Privacy Mask function.
2. The **On Demand Display** function is not supported by GV-Fisheye cameras.

Application Example

The resolution of sub stream is 640 x 480, and a value of **1.2 times the resolution of the sub stream** has been selected for the On Demand Display function.

- **Higher Resolution Streaming**



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 1.2 x 640 x 480.

- **Lower Resolution Streaming**

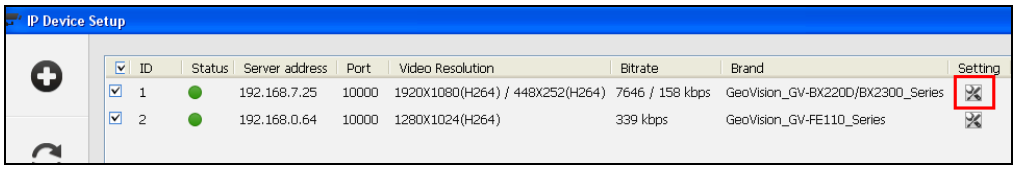


After switching to 9-channel screen division, the resolution for each channel is 640 x 360, which is smaller than 1.2 x 640 x 480, so the lower resolution streaming will be used.

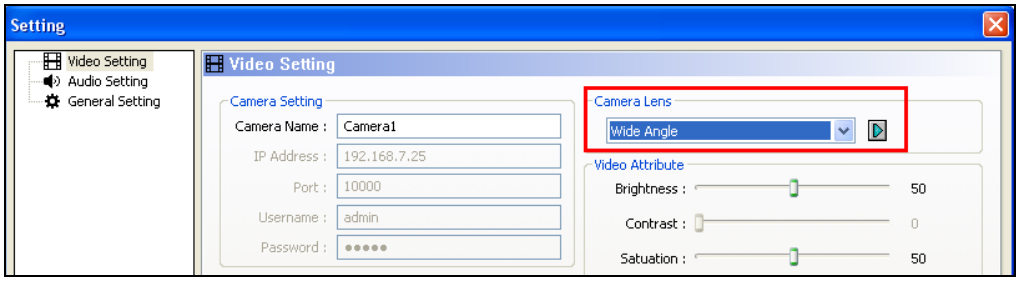
2.5 Wide Angle Lens Dewarping

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** > **Toolbar** > **Configure** > **Camera Install**. The IP Device Setup list appears.

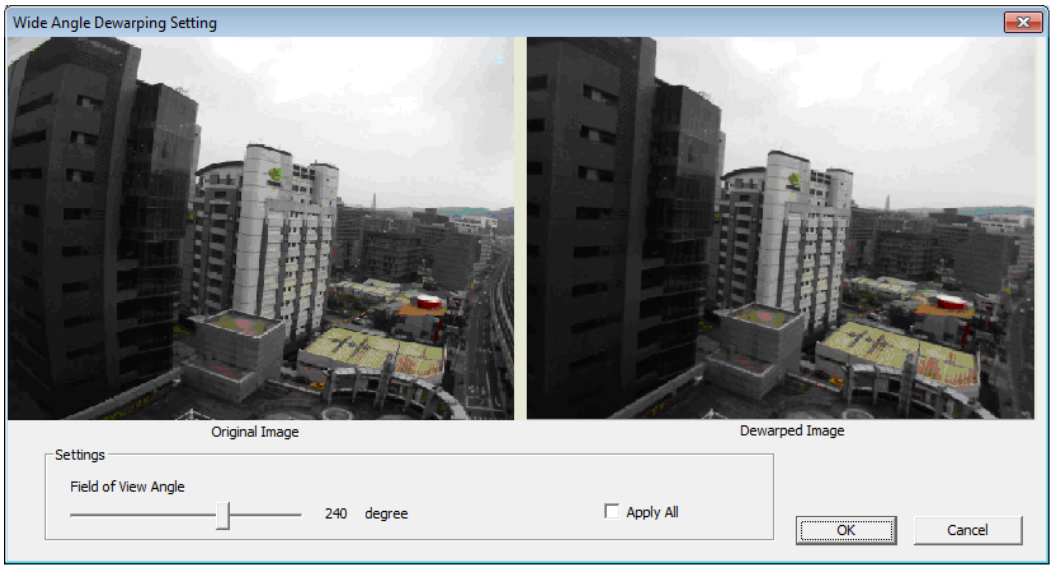


2. Click **Settings** . This dialog box appears.



3. Use the **Camera Lens** dropdown list to select **Wide Angle**

4. Click the button. This dialog box appears.



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 wide angle lens dewarping to recorded videos during playback, in **ViewLog**, right-click the desired image, and then select **Effects** > **Wide angle lens dewarping**. For details, see *Adjusting Distorted Views* in Chapter 4.
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 video resolution in single-channel division.

2.6 Fisheye View

A fisheye camera allows you to cover all angles of a location with just one camera. The circular fisheye view can be dewarped into the following four view modes, and you can drag PTZ views to different angles.

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



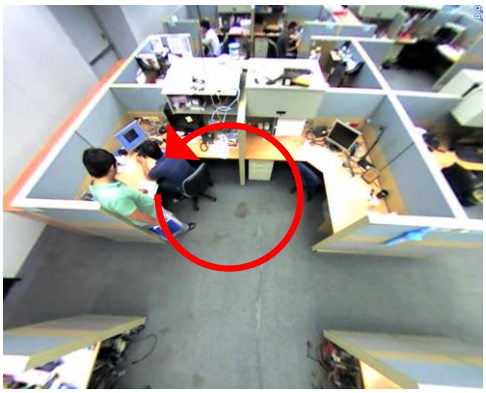
Quad view: 4 PTZ views



360 degree: 2 PTZ view & 1 360º view



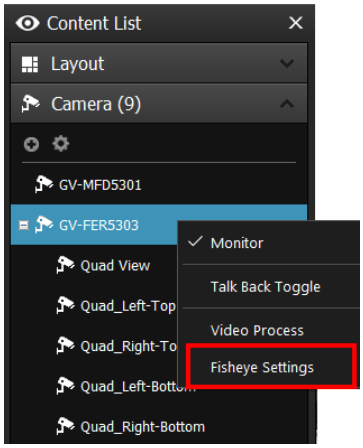
Dual 180 degree: 2 180º views



Single view: 1 PTZ view

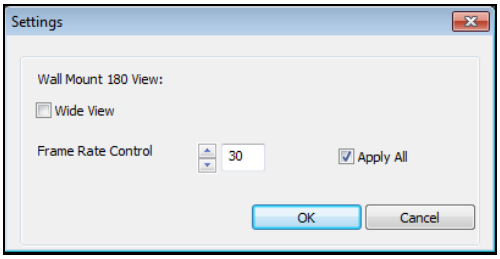
2.6.1 Setting up Fisheye View

1. To display the dewarped view, from the Content List, drag the fisheye camera (circular source image) or one of the dewarped views to the live view grid.
2. To change the dewarped settings, right-click the fisheye camera from the Content List > **Fisheye Settings**. The Fisheye Setting window appears.

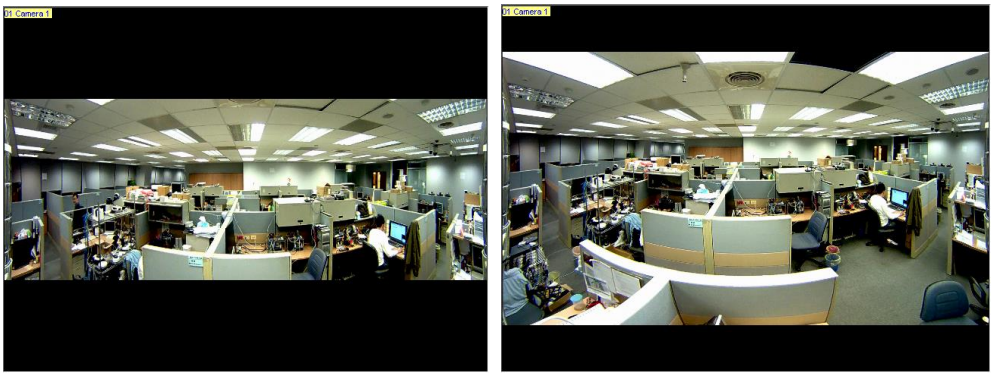


3. Right-click on the Fisheye Settings window > **Fisheye Option** to access the following settings:

   - **Camera Mode:** You can choose among four view modes.
     - **Quad view:** Composed of four PTZ views.
     - **360 degree:** Composed of two PTZ views and one 360º panoramic view.
     - **Dual 180 degree:** Composed of two 180º views.
     - **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 dewarped view without missing the entire view of surveillance site.
   - **Camera Position:** Select **Ceiling**, **Wall** or **Ground** according to installation scenarios.
   - **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 is only available in **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:** Only available in **360 degree** view. Track and highlight detected motion in live view. For details, see *Object Tracking* later in this chapter.
     - **Disable automatic zoom adjustment during 360 Object Tracking:** Enabled by default. When disabled, the zoom ratio will be kept at constant as configured.
   - **Disable PIP:** Disables the PIP function in Single View mode.
   - **Guard Tour Setting:** Only available in **Single View** mode. Enable to set up a virtual PTZ tour using the defined preset points on live view. For details, see *Virtual PTZ Tour* later in this chapter.
   - **Settings:**



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



Wide View Disabled ***Wide View Enabled***

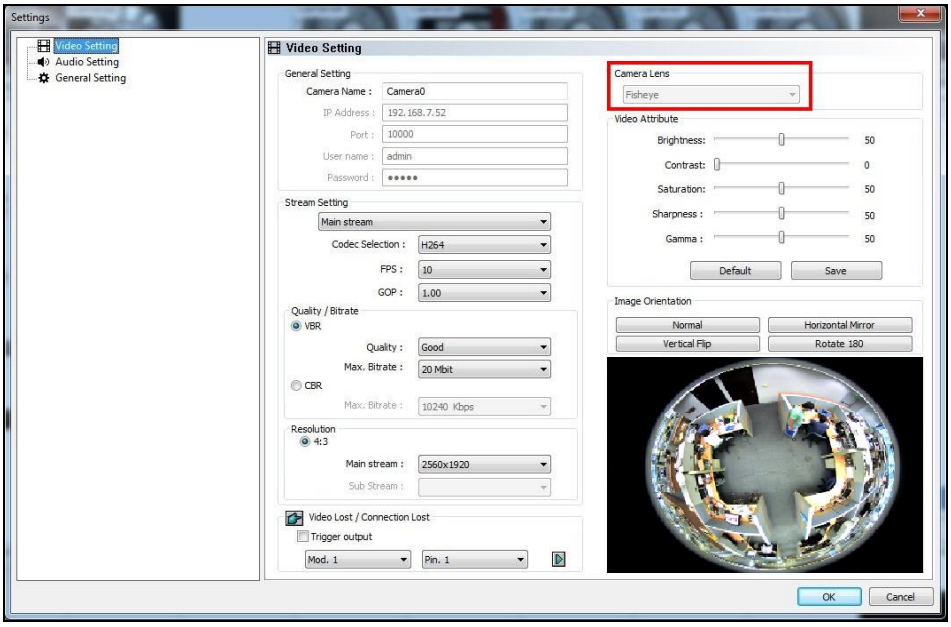
⊙ **Frame Rate Control:** Limits the frame rate of the fisheye view to the number specified here. Select **Apply All** to apply the frame rate control to other fisheye views.

4. Drag the dewarped fisheye views from the Content List to live view grids for display.You can drag and drop PTZ view or 180 degree view to adjust the viewing angle.

2.6.2 Setting up a Third-Party Fisheye Camera

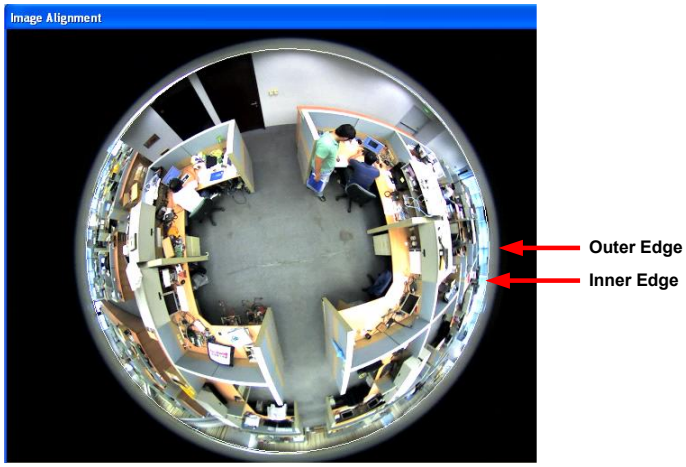
You can also enable dewarping for 3rd party fisheye cameras and access fisheye related functions.

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



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 Fisheye View* earlier in this chapter.

5. To adjust the image alignment for optimal results, follow Steps 2 and 3, *Setting up Fisheye View* earlier 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.

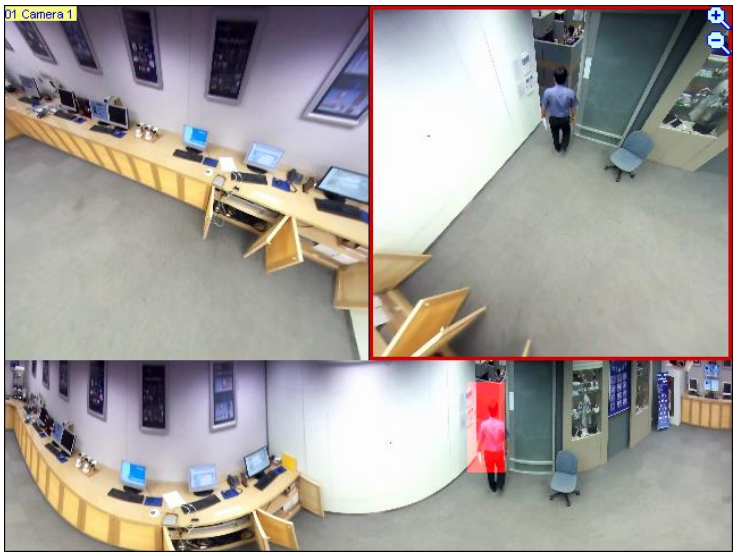


Note:

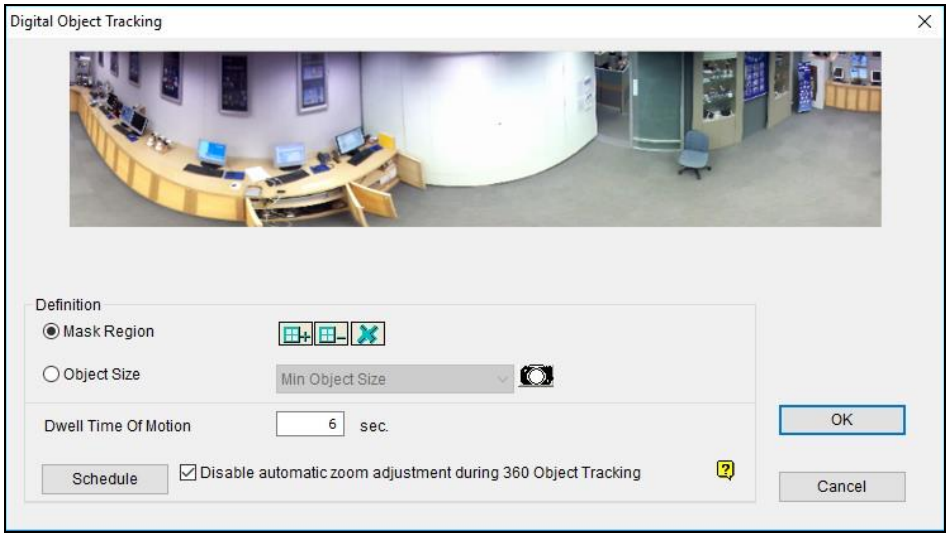
1. For GV-Fisheye Cameras, the image alignment function is only available on its Web interface.
2. Regardless of the view mode selected here, the hemispherical fisheye source image will be recorded. When playing back fisheye events in ViewLog, the system can convert the source image to different view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

2.6.3 Object Tracking

You can set up object tracking in fisheye view to track a moving object. The function is only available when the view mode is set to **360 degree**. When motion is detected in the fisheye view, the top-right channel will start tracking the moving object, which is highlighted in the 360-degree view at the bottom.



1. Set the fisheye view to **360 degree** by following Step 1 - 3 in *Setting up Fisheye View* earlier in this chapter, and selecting **Camera Mode** > **360 degree**.
2. On the Fisheye Settings window, right-click the fisheye view > **Fisheye Option** > **360 Object Tracking** > **Advanced Settings**. This dialog box appears.



- **Mask Region:** Use the mouse to outline a mask region where motion is ignored.

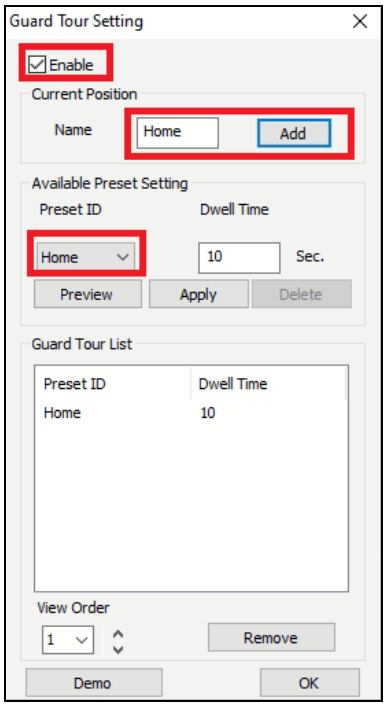
- **Object Size:** Click the  button to pause the live view and then use the mouse to outline the maximum and minimum size of the target object.
- **Dwell Time of Motion:** When the target object stops moving, the highlighted region and the top-right channel will remain fixed for the number of seconds specified. Any new motion detected during the dwell time is ignored to prevent the camera view from frequently jumping from one region to another.
- **Schedule:** Click **Schedule** to set up the times to start object tracking.

3. To enable object tracking, on the Fisheye Settings window, right-click the fisheye view > **Fisheye Option** > **360 Object Tracking** > **Tracking**.

2.6.4 Virtual PTZ Tour

You can set up a virtual PTZ tour to monitor important spots of your surveillance site. Before you start, make sure your fisheye camera has been set to Single View mode.

1. Set the fisheye view to **Single view** by following Steps 1 to 3 in *Setting up Fisheye View* earlier in this section and selecting **Camera Mode** > **Single view**.
2. Right-click the fisheye camera on the Content List > **Fisheye Settings**. The Fisheye Settings window appears.
3. Right-click the fisheye view on the window > **Fisheye Option** > **Guard Tour Setting**. The Guard Tour Setting dialog box appears along with the Fisheye Settings window.
4. On the Fisheye Settings window, move the live view to a desired starting point for the PTZ tour by clicking on the inset window at the bottom right.
5. Enable the settings, type a name for the current view and click **Add**. This view point (preset point) appears under Preset ID.



6. Specify the duration for the live view to stay on this preset point (dwell time). The default is **10** seconds.
7. Optionally click **Preview** to see a preview of the preset point.
8. Click **Apply**. This preset point is added to Guard Tour Setup.
9. To add more preset points, repeat the steps above.
10. To change the order of the preset points, use the **View Order** dropdown list to move a preset point up or down the list.
11. Optionally, click **Demo** to watch a preview of the PTZ tour.
12. Select **OK** to start the PTZ tour. To stop the PTZ tour, disable the function on the Guard Tour Setting.

2.7 PTZ Object Tracking

By combining a PTZ and a stationary camera, you can automatically track and zoom in on a single moving object on live view. You can also use only one PTZ camera for object tracking.

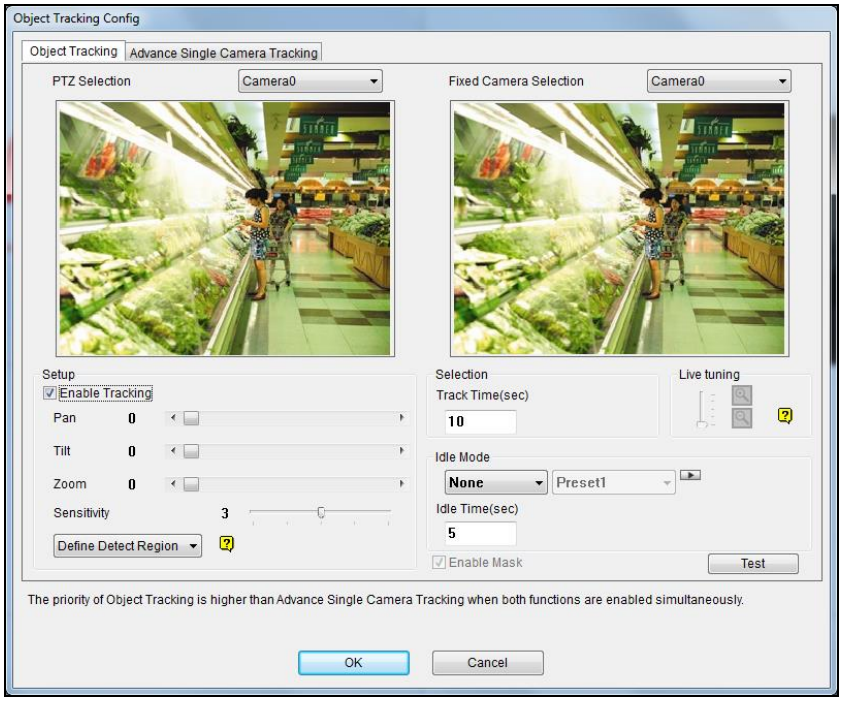
2.7.1 Dual-Camera Tracking

To automatically track an object, you need one PTZ camera set for tracking and one stationary camera set for a fixed view. Install the PTZ camera and the stationary camera in close proximity to each other so that the focus and the camera view of both resemble each other.

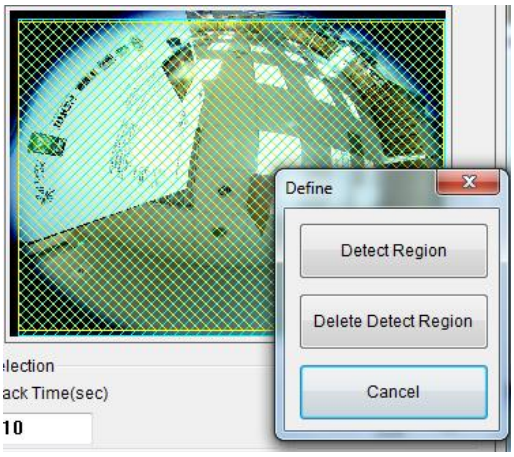
Note: The Dual-Camera Tracking function is only supported by GV-PTZ010D, GV-QSD5730-Indoor / QSD5730-Outdoor / QSD5731-IR, GV-SD220 Series, GV-SD2722-IR / SD2723-IR / SD2733-IR / SD2300 / SD2301 / SD2411 / SD4825-IR / SD4834-IR.

---

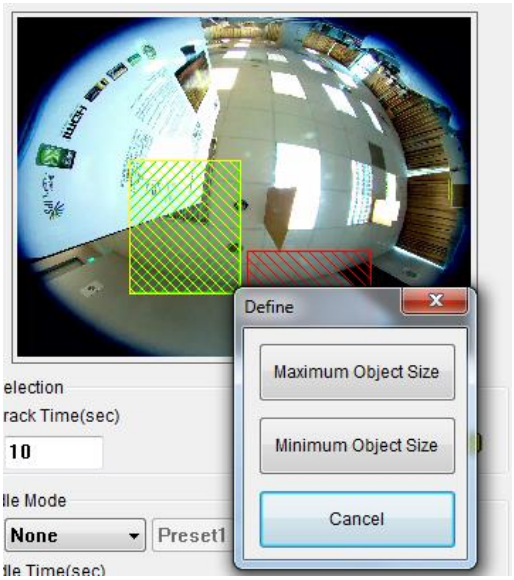
1. Click **Home** > **Toolbar** > **Configure** > **Object Tracking Setup**. The Object Tracking Config dialog box appears.
2. Select a **PTZ Camera** from the left dropdown list and a **Fixed Camera** from the right dropdown list.
3. Select **Enable Tracking** and start the settings.



4. Use the **Pan**, **Tilt**, and **Zoom** sliders to adjust the current PTZ camera view.
5. Specify **Tracking Duration** in seconds for every tracking movement.
6. Specify **Idle Mode** and **Idle Time**. When the PTZ camera remains stationary for a specified time, the camera can automatically move to a Home position, a Preset Point, or start an Auto setting.
7. Select **Define Detection Region** from the dropdown menu. Outline an area on the right (Fixed Camera) image. You are prompted to confirm **Detect Region**.



8. Select **Define Object Size** from the dropdown menu. Outline the max and min object sizes for tracking targets separately on the right (Fixed Camera) image. Every time when finishing the outlining, you will be prompted to confirm **Maximum Object Size** or **Minimum Object Size**.



9. Click **Test** and move an object through the camera view to see if its movement is tracked or not. There are two major settings you have to observe in the test.
   (1) **Tracking:** Observe if the target shown in the defined detection region is being tracked with a highlighted mask, and magnified automatically in the left (PTZ) image. If not, increase the sensitivity degree.
   (2) **Zooming:** Observe if the target is magnified in the left (PTZ) image clearly. If not, use the **Live Tuning** buttons to adjust the level of zooming.
10. Click **OK** to apply the settings.
11. To start object tracking, click **Toolbar** , select **Tools**  and select **Object Tracking Start**.

Tip: You can interrupt the PTZ camera tracking and take over the camera control by using PTZ Control Panel, PC's keyboard, and GV accessories such as GV-Keyboard, GV-IR Remote Control, and GV-Joystick. When the controlling device or panel is inactive for over 5 seconds, the PTZ camera will go back to tracking.

Note: When multiple objects are moving at the same time, the camera will track the object with the largest area.

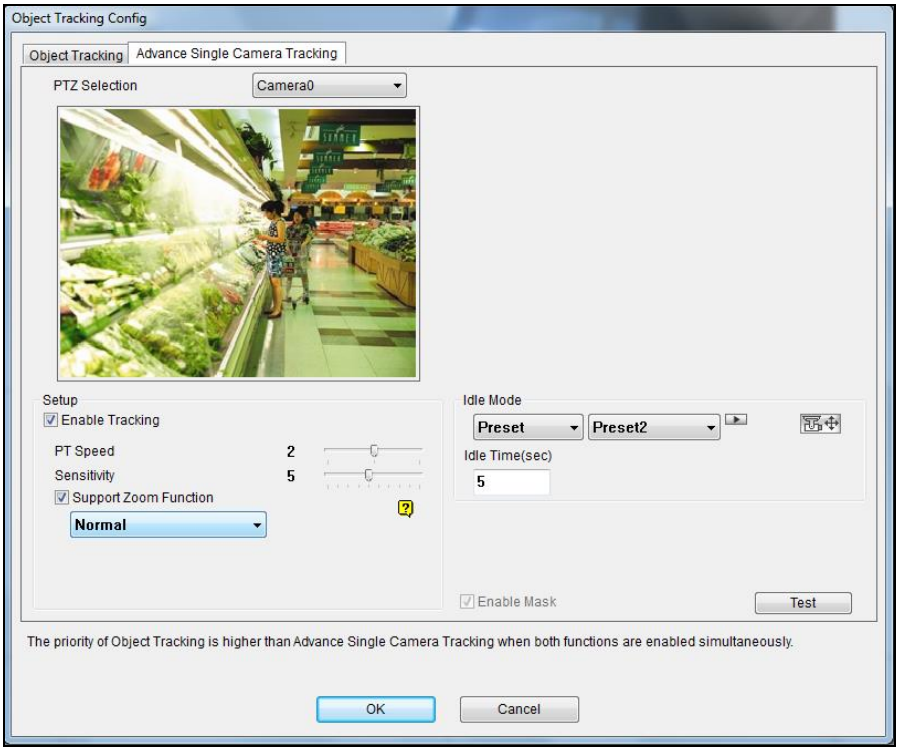
2.7.2 Single Camera Tracking

The Advanced Single Camera Tracking can track a moving object using only one PTZ camera. When an object moves within the view of the camera, the PTZ camera will follow its movement. When the object is out of view, the PTZ camera can be set to return to a designated position.

Note:

1. The Single Camera Tracking function is only supported by GV-PTZ010D, GV-SD200, GV-SD220 Series, GV-SD2723-IR / SD2733-IR / SD2300 / SD2301 / SD2411.
2. For GV-SD2722-IR / SD3732-IR, a similar tracking function can be accessed through the PTZ Control Panel. See *Accessing PTZ Control Panel and Auto Functions*, in Chapter 1.

1. Click **Home** > **Toolbar** > **Configure** > **Object Tracking Setup** > **Advanced Single Camera Tracking** tab. This dialog box appears.



2. Select the camera from the **PTZ Selection** dropdown list.
3. Select **Enable Tracking** to start the following settings.
4. Select **Support Zoom Function** to be able to zoom in and out. Select **Normal** and the camera will zoom in once on the moving object. Select **Deep Zooming** and the camera will zoom in three times on the moving object.
5. Click the button to adjust the direction and zoom level of the camera.
6. To set the camera to return to its home position or a preset position when no motion is detected for a certain time period, specify **Idle Mode** and **Idle Time** in seconds. Click the button to preview the designated position. Note that your camera will need to support home position and preset position.
7. To outline an area where motion will be ignored, draw an area on the camera view and select **Set Mask** on the dialog box that pops up. To remove the mask, draw an area bigger than the mask, and click **Remove Mask**.
8. Click **Test** and move an object through the camera view to see if its movement is tracked or not. If not, move the **Sensitivity** slider to increase the sensitivity of motion detection. If the tracking speed is not fast enough, move the **PTZ Speed** slider to adjust the speed of PTZ movement. If you have set up a mask, you can select **Enable Mask** to display the masked area during the test.

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

10. To start object tracking, click **Toolbar** > **Tools** > **Object Tracking Start**.

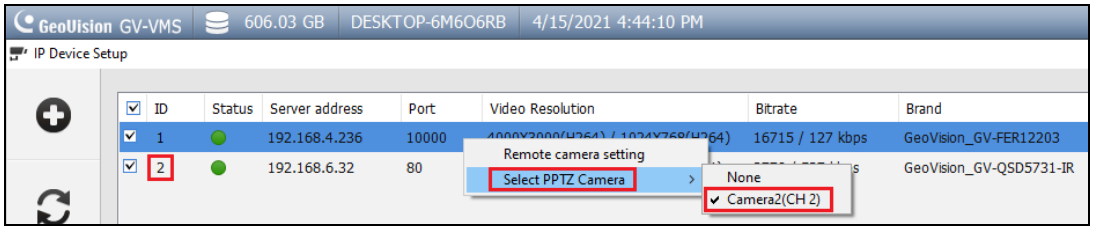
Tip: You can interrupt the PTZ camera tracking and take over the camera control by using PTZ Control Panel, PC's keyboard and GV accessories such as GV-Keyboard, GV-IR Remote Control, and GV-Joystick. When the controlling device or panel is inactive for over 5 seconds, the PTZ camera will go back for tracking.

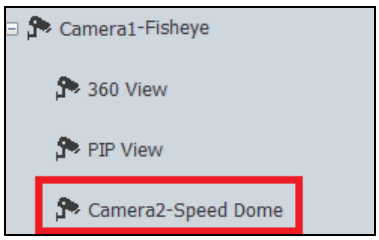
Note: When multiple objects are moving at the same time, the camera will track the object with the largest area.

2.8 Panoramic PTZ Object Tracking

With a single GV-Panoramic PTZ Camera (GV-PPTZ) or a pair of GV-Speed Dome Camera and GV-Fisheye Camera, you can track moving objects on live view. The fisheye camera allows you to monitor all angles of a location, while the speed dome can instantly point toward an area with just one click on the fisheye live view. In addition to that, you can also set up object tracking on fisheye live view to track a moving object automatically. When motion is detected in the fisheye, the speed dome will start tracking the moving object in the 360 degree view, and the moving object will be highlighted.

To use a pair of GV-Speed Dome Camera and GV-Fisheye Camera for object tracking, it is required to pair up the speed dome and fisheye camera first. Right-click on either camera in the IP Device Setup dialog box, click **Select PPTZ Camera**, and then click the camera you are pairing with. The speed dome will be grouped under the fisheye camera in the Content List.



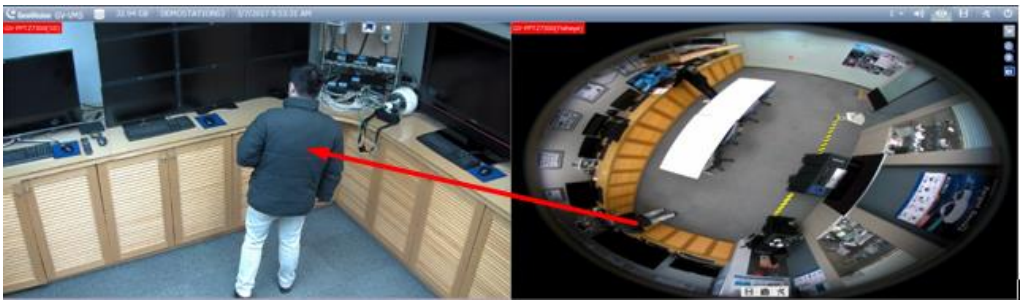


Note:

1. To use a pair of GV-Speed Dome Camera and GV-Fisheye Camera for object tracking, install the cameras in proximity to each other so that the focus and the camera view of both resemble each other.
2. The function is supported by GeoVision speed domes and fisheye cameras only. Refer to our website for supported models: speed domes and fisheye cameras.

2.8.1 Accessing the Live View

To access the live view of GV-Panoramic PTZ Cameras, drag both the fisheye camera channel and speed dome channel in the Content List to the live view grid. Click on the fisheye live view, and the camera will turn toward the selected location.

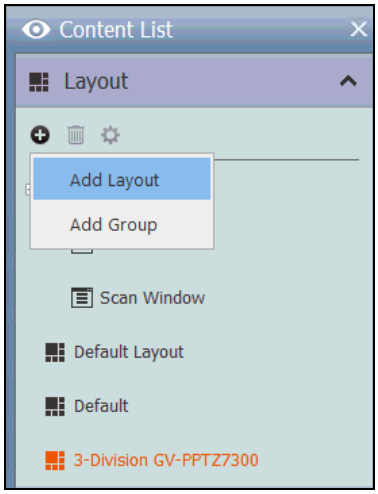


2.8.2 Automatic Object Tracking

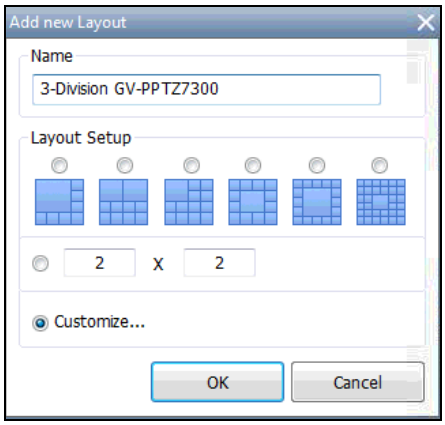
The PPTZ Automatic Object Tracking function only works in a 3-division live view. Follow the steps to create the 3-division live view and to enable the PPTZ Object Tracking in the 360 View.



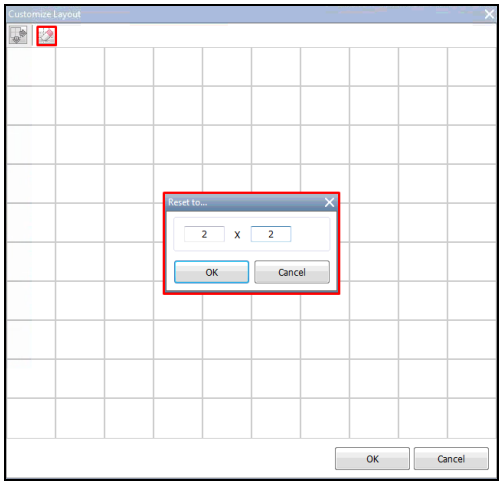
1. Click **Home** > **Toolbar** > **Content List**.
2. Under **Layout**, click **Add** > **Add Layout**.



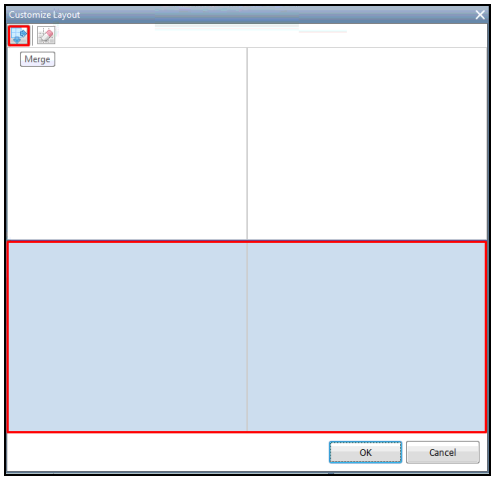
3. Type the name of the layout under **Name**, select **Customize**, and click **OK**.



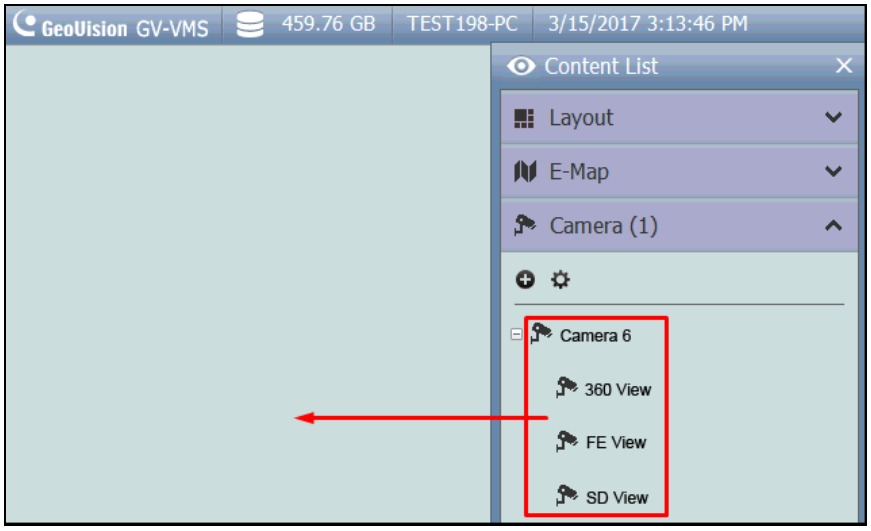
4. Click **Reset**  to create a 2 x 2 live view grid, and click **OK**.



5. Select the 2 grids at the bottom, click **Merge** , and click **OK** to merge the grids.

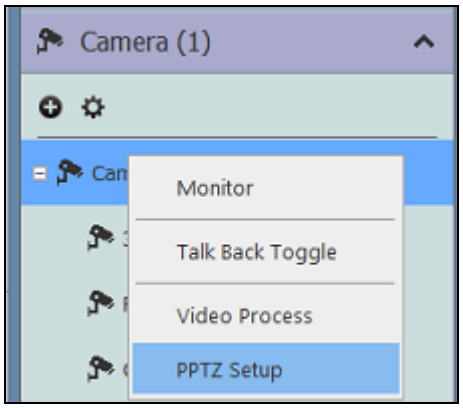


6. When the message “Do you want to assign the cameras to this layout automatically” appears, click **No** to assign the camera channels manually instead.
7. Drag **360 View**, **SD View**, **FE View** (for GV-PPTZ cameras), or **360 View, PIP View, Speed Dome camera** (for the paired fisheye and speed dome cameras) to the live view grid.

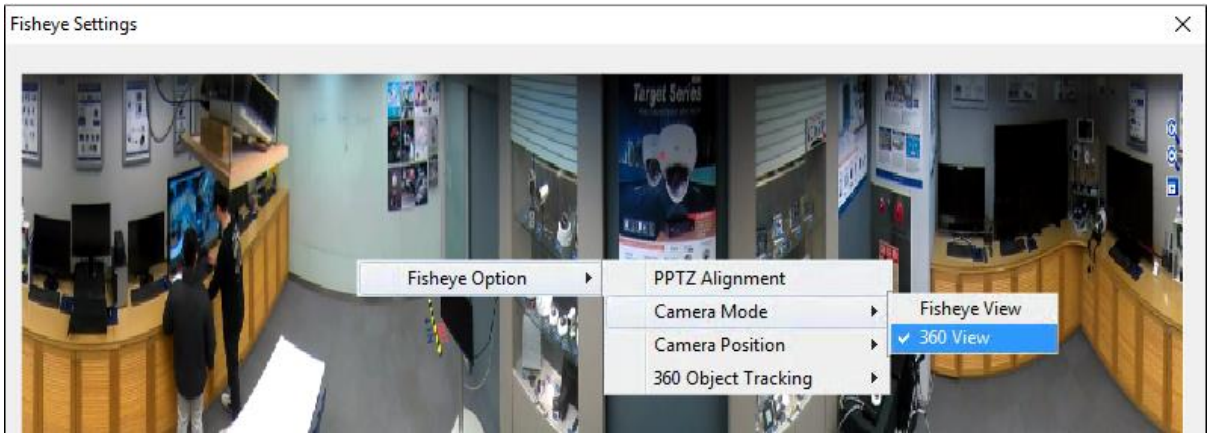


After creating the 3-division live view, go through the steps below to enable the object tracking.

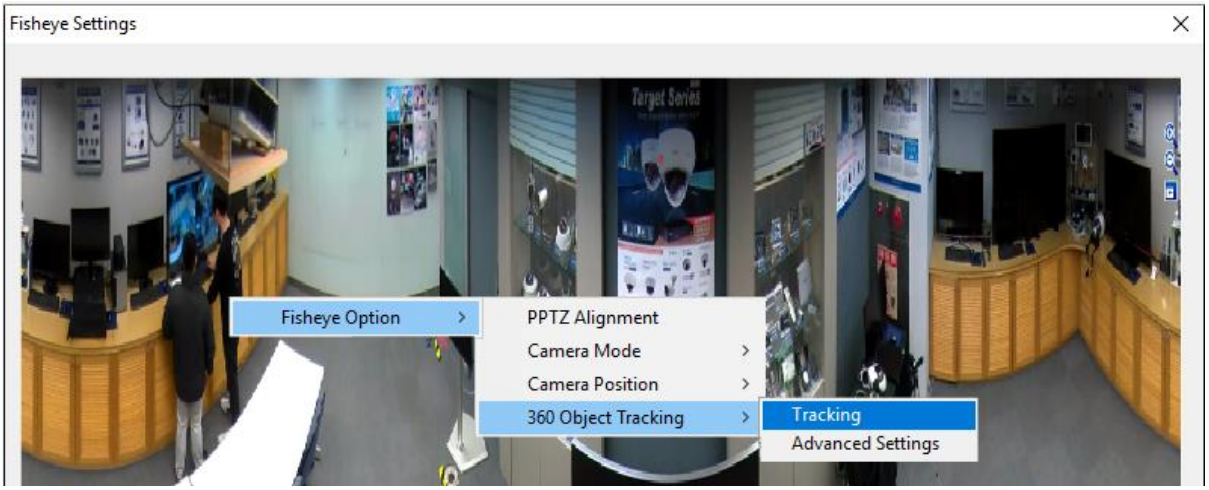
8. To track moving objects, click **Home** > **Toolbar** > **Content List**. The Content List appears.
9. Right-click the GV-PPTZ camera or the paired fisheye camera, and select **PPTZ Setup**. The Fisheye Settings window appears.



10. Right-click on the Fisheye Settings window, and select **Fisheye Option** > **Camera Mode** > **360 View**.



11. Select **360 Object Tracking** > **Advanced Settings** to customize the object tracking. For details, see Step 2 in *Object Tracking* earlier in this chapter.
12. Select **360 Object Tracking** > **Tracking** to enable the object tracking.



Chapter 3

Video Analysis 177

3.1 Face Recognition 177

3.1.1 Enrolling Face Data 178
3.1.2 Setting up Face Groups 181
3.1.3 Synchronizing Face Database 182
3.1.4 Defining Access Schedule 183
3.1.5 Setting up Recognition Alerts 186
3.1.6 Configuring Face Recognition Database 187
3.1.7 Backing up Face Database 188
3.1.8 Face ID — Live Recognition Profiles 188
3.1.9 Viewing and Searching for Face Recognition Events 189
3.1.10 Tracking Recognized Faces 190
3.1.11 Integrating Face Recognition to Access Control 193
3.1.12 Batch Enrolling Faces and Access Cards 196

3.2 Privacy Mask Protection 200

3.2.1 Setting up a Privacy Mask 200
3.2.2 Granting Access Privileges to Recoverable Areas 201

3.3 Advanced Scene Change Detection 202

3.4 Text Overlay 204

3.5 Video Analysis by Camera 205

CHAPTER 3

Video Analysis

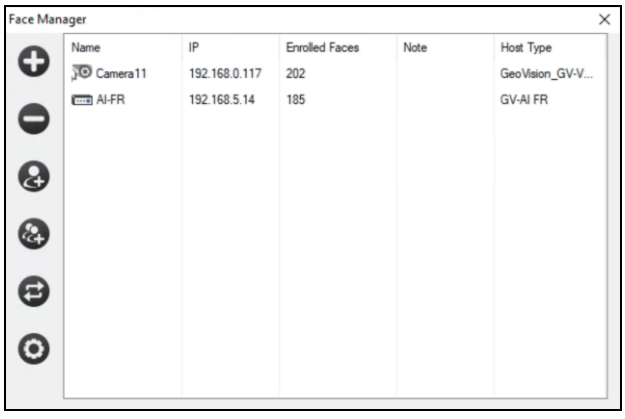
3.1 Face Recognition

Face Recognition integrates the facial recognition capabilities of the following cameras and software, enabling the system to identify detected human faces:

- **GV-Face Recognition Camera**: GV-VD8700 and GV-FD8700-FR
- **GV-AI FR software**

These recognition events can be configured to trigger actions such as sending email alerts, activating output devices, computer alarms, run the desired application, or send notifications to GV-Notify mobile app — based on recognition of designated face groups or unidentified individuals.

To manage the face databases of connected GV-Face Recognition Cameras or GV-AI FR, click **Home** > **Toolbar** > **Configure** > **Face Manager**.



- All GV-Face Recognition Cameras connected to the system are automatically added to the Face Manager.
- For GV-AI FR, users can manage their face databases only after adding them to the Face Manager by clicking **Add GV-AI FR**. See *Chapter 5 GV-VMS Integration* in the *GV-AI FR User's Manual*.

3.1.1 Enrolling Face Data

Before using Face Recognition, it is required to create the necessary recognition data via Face Enrollment — adding photos of the persons to be recognized into the face databases of the following:

1. **GV-Face Recognition Camera:** GV-VD8700 and GV-FD8700-FR
2. **GV-AI FR software**

There are two methods to enroll faces:

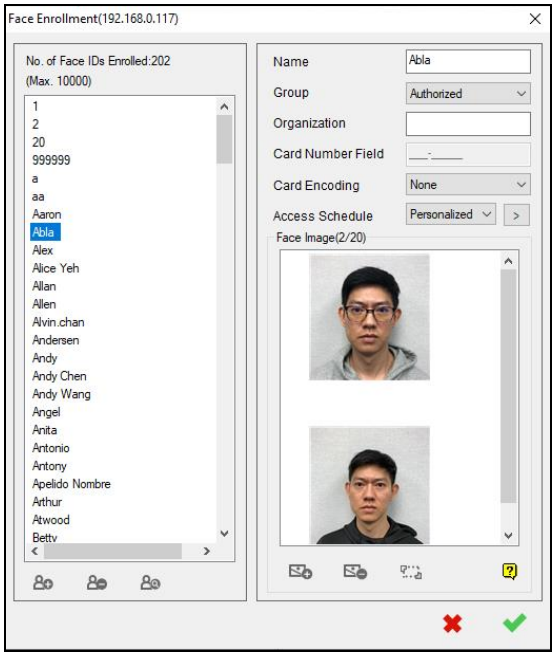
1. Enroll faces by adding portrait photos directly into the database of the connected cameras or GV-AI FR. See the steps below.
2. Synchronize face data from other connected cameras or GV-AI FR. See *Synchronizing Face Database* later in this chapter.

IMPORTANT:

1. GV-AI Guard directly accesses and manages the face database of GV-Face Recognition Camera and GV-AI FR, thus all changes made are done directly to their databases.
2. Photos used as recognition data can be pictures of the persons previously taken or snapshots of the persons captured by connected cameras.
3. All photos used for Face Enroll must meet the criteria as specified in *3.2.1 Photo Requirements* in the *GV-AI FR User's Manual*.

To enroll faces:

1. Select a host (GV-Face Recognition Camera / GV-AI FR) on **Face Manager** and click **Face Enrollment** .
2. Click **Add**  to define a new Face ID. Alternatively, select or search for an existing ID from the **Enrolled Face** list.



3. Click **Add** below Face Images to add photos and/or snapshots for the Face ID selected from your local PC. Optionally crop the image added by selecting it and click **Crop Image**.
4. You can also configure the following options for the Face ID selected:
   - **Name:** Type a desired name for the Face ID.
   - **Group:** Select a group to categorize the Face ID. This setting can be used to trigger alert response, such as an output alarm, when persons from a specified group are recognized. See *Setting up Face Groups* and *Configuring Face Setting* later in this chapter.
   - **Organization:** Name the organization associated with the Face ID.
   - **Card Number Field** and **Card Encoding:** Type an access card number and select the appropriate card encoding type from the dropdown list to pair the access card to the Face ID for face recognition-based access control. See *Integrating Face Recognition to Access Control* later in this chapter.
   - **Access Schedule:** Select a predefined schedule in which the Face ID is allowed access or select **Personalized** and click > to define an exclusive schedule for the person. To configure a schedule, see *Defining Access Schedule* later in this chapter.
5. Click **OK** to save.

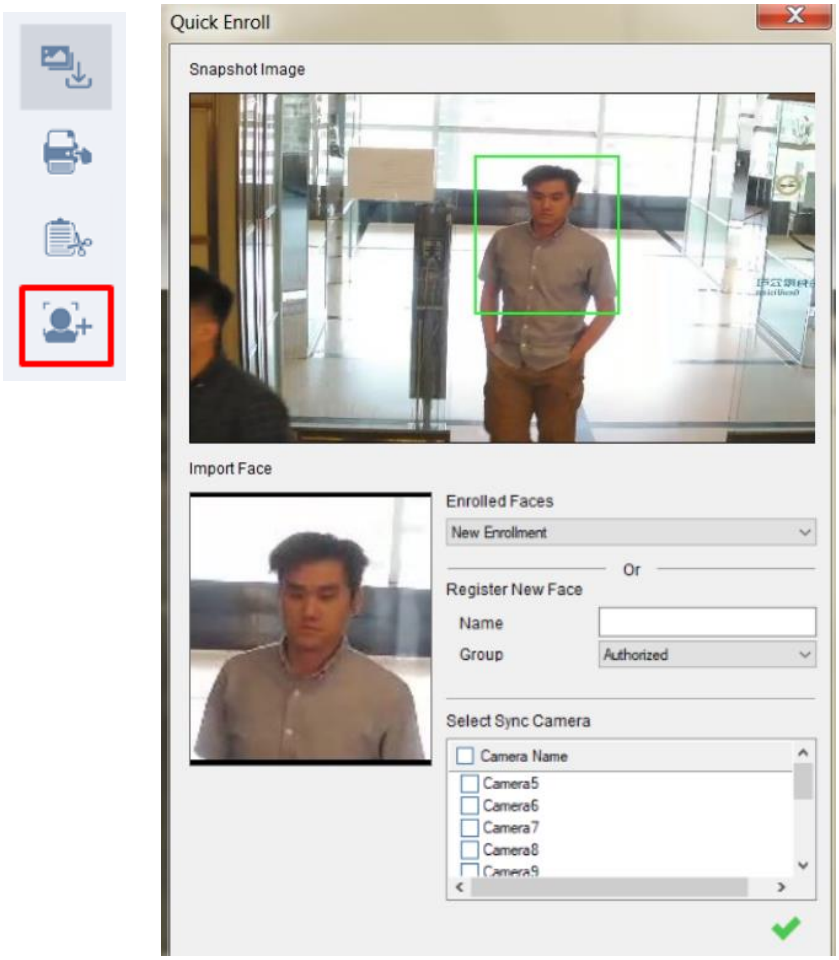
Note:

1. All changes made here take immediate effect on the face database of the selected GV-Face Recognition Camera or GV-AI FR.
2. To batch enroll multiple faces, see *Batch Enrolling Faces and Access Cards* later in this chapter.

3.1.1.1 Enrolling Faces from Live View / ViewLog

Alternative to enrolling face data with photos, you can also enroll with face images captured by any cameras connected to the system.

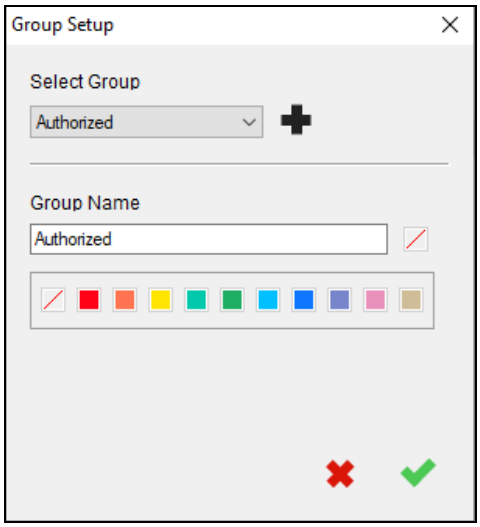
1. In Live View / ViewLog, click **Snapshot** at the bottom of a desired channel and select **Face Enroll** and click . The Quick Enroll window appears.



2. Click and drag on the image to highlight the face you want to enroll as a **snapshot**.
3. Select **New Enrollment**, type the desired name under **Register New Face** to create a new Face ID and select a **Face Group** to add it under. Otherwise select an existing one for the face image to be added to.
4. Select the desired GV-Face Recognition Camera / GV-FR Server for the face enrollment under **Select Sync Camera**.
5. Click to save.

3.1.2 Setting up Face Groups

To add and/or edit the Face Groups of a GV-Face Recognition Camera / GV-AI FR connected, select the desired camera / server on **Face Manager** and click **Group Setup** .



To add a face group, click **Add** .

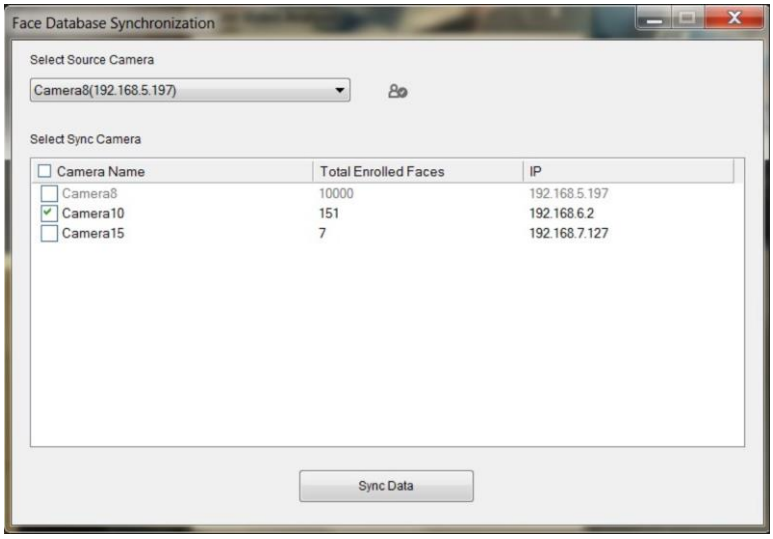
To edit the name of a face group, select the group from the **Select Group** dropdown list and edit its name under **Group Name**. Optionally select a color for highlighting the recognition events of the face group selected on the **Face ID** window. See *Face ID — Live Recognition Profiles* later in this chapter.

Once finished, click the to save.

3.1.3 Synchronizing Face Database

To synchronize the face databases among multiple GV-Face Recognition Cameras, or among multiple GV-AI FRs, click **Face Database Synchronization** on **Face Manager**. The following window appears.

Note: Face databases of GV-Face Recognition Cameras cannot be synchronized with those of GV-AI FRs.



- **Select Source Camera:** Select the camera you want to synchronize from.
- **Select Sync Faces** : Click to select the Face IDs that you want to synchronize with.
- **Select Sync Camera:** Select the cameras that you want to be synchronized.
- **Sync Data:** Click to start synchronizing.

3.1.4 Defining Access Schedule

Access Schedules are used to specify the time periods in which specific persons (Face ID) are allowed or denied access of from Monday to Sunday. Whenever a person is recognized outside of his/her allowed schedule, a schedule alert is recorded, which can be used to trigger e-mail alerts, outputs and computer alarms, run the desired applications and/or send notifications to GV-Notify mobile app.

The Access schedule can be set in three steps:

- **Step 1 Setting 24-hour Schedules**

  Define the minutes and hours a person is allowed / denied access of in a day.

- **Step 2 Setting Weekly Schedules**

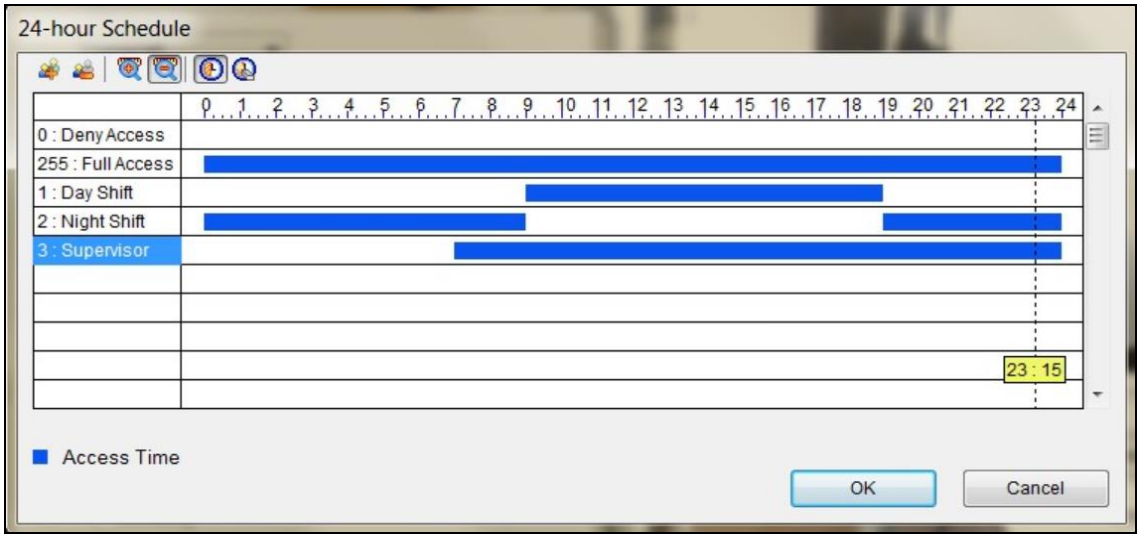
  Define the days a person is allowed / denied access of in a week.

- **Step 3 Assigning Access Schedules**

  Assign the defined schedules to the desired persons in Face Enrollment.

3.1.4.1 Step 1: Setting 24-hour Schedules

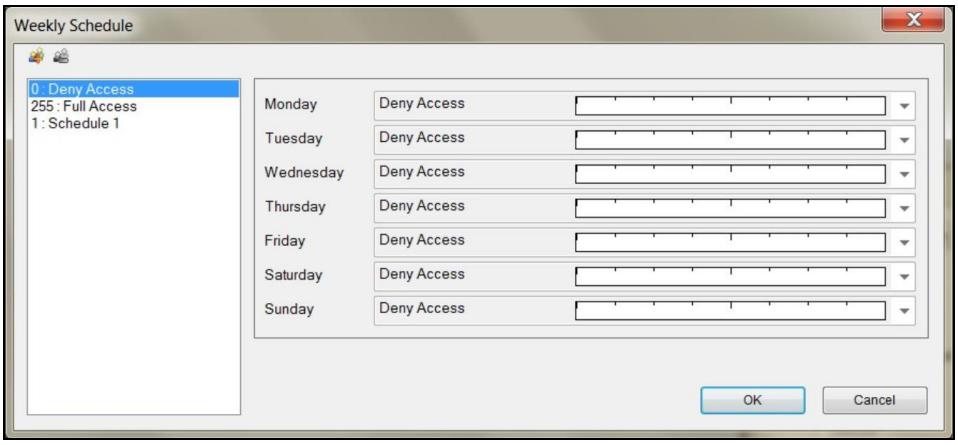
Before creating weekly schedules, you need to first define a number of desired 24-hour schedules that can be used to prepare the weekly schedules. On **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Configure** and select **24-hour Schedule**. In this window, up to 254 24-hour schedules can be defined, with two default schedules for “Full Access” and “Deny Access.”



1. Click the **Add** button . An ID number ascending from the lowest existing ID will be automatically generated. Type a desired name for the new schedule, e.g. **Day Shift** and click **OK**.
2. Click the **Add Access Time** button . Then drag the mouse on the timeline to specify the time periods of allowed access, e.g. **from 09:00 to 19:00**.
3. Repeat Steps 1 to 3 to create multiple schedules if needed, e.g. for **Night Shift from 00:00 to 09:00 and 19:00 to 24:00** and for **Supervisor from 07:00 to 24:00**.
4. To remove time periods of allowed access, click the **Delete Access Time** button . Then drag the mouse over the periods that you want to remove.
5. Click **OK** to save the changes.

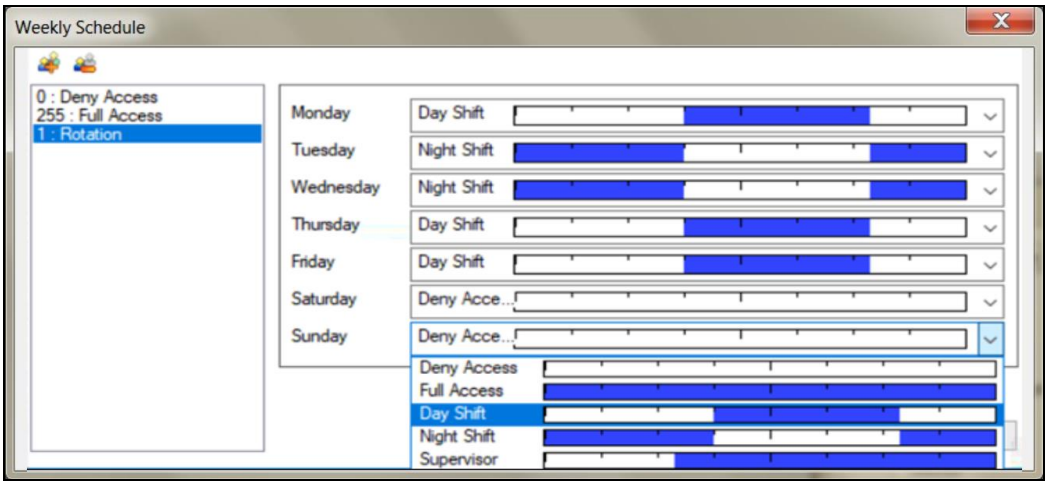
3.1.4.2 Step 2: Setting Weekly Schedules

Once the desired 24-hour schedules are set, click **Configure** on **Face Manager** and select **Weekly Schedule**. In this window, up to 254 weekly schedules can be defined, with two default schedules for “Full Access” and “Deny Access.”



1. Click the **Add** button . An ID number ascending from the lowest existing ID will be automatically generated. Type a desired name for the new schedule, e.g. **Rotation** and click **OK**.

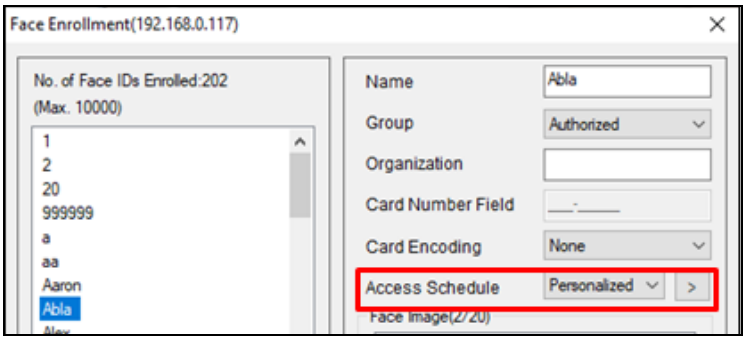
2. Select the desired schedules for **Monday** to **Sunday**, predefined from *Step 1* earlier in this section, in each of the respective dropdown lists, as exemplified below.



3. Repeat Steps 1 to 3 to create multiple schedules if needed, e.g. for **Daytime-only** and **Weekend-only** access.
4. To delete schedules, select the schedule to be deleted and click the **Remove** button .
5. Click **OK** to save the changes.

3.1.4.3 Step 3: Assigning Access Schedules

Once the weekly schedules are set, select the desired GV-Face Recognition Camera / GV-AI FR on **Face Manager** and click **Face Enrollment**. Select or search for a desired Face ID and select a schedule in the **Access Schedule** dropdown list.

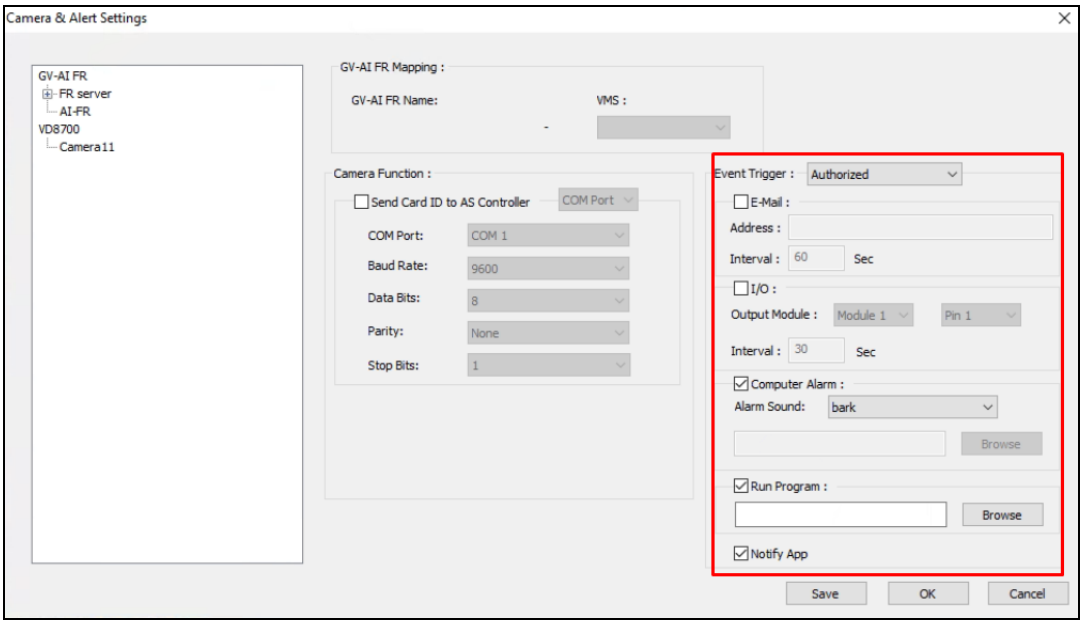


Once the Access Schedules are assigned, turn on monitoring of the camera channel to start access monitoring based on the schedules.

3.1.5 Setting up Recognition Alerts

In this section, you can use Schedule Alerts, Unknown Alerts or the Recognition Events of a specified group, such as Unauthorized, to send e-mail alerts, trigger outputs and computer alarms, run the desired applications, or send notifications to GV-Notify mobile app.

On **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Configure** and select **Camera and Alert Settings**. This window appears.



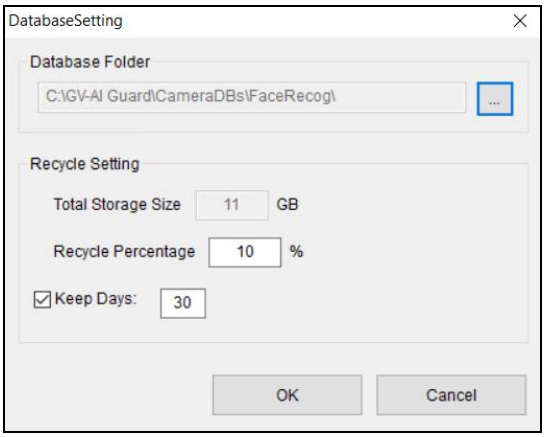
Select GV-Face Recognition Camera or GV-AI FR for which you want to set recognition alerts.

- **Event Trigger:** Select Schedule Alert, Unknown Alert or the Group of Face ID that the alerts set should be triggered for. For details on using Schedule Alerts, see *Defining Access Schedule* earlier in this chapter.
  - ⊙ **E-Mail:** Set the minimum time **Interval** from 0 to 3600 seconds between each e-mail notification upon face recognition.
  - ⊙ **I/O:** Select the desired **Output Module** and **Pin** number to be activated upon face recognition.
  - ⊙ **Computer Alarm:** Select a computer alarm, or click **Browse** to select an audio file from your PC, to be played upon face recognition.
  - ⊙ **Run Program:** Click **Browse** to select a program to be executed upon face recognition.
  - ⊙ **Notify App:** Enable the option to send face recognition events to GV-Control Center and GV-Cloud VMS.

Note: Make sure the e-mail and I/O functions are configured properly before use. For details, see *Setting up E-mail Notifications* and *Setting up I/O Devices* in Chapters 1 and 6, respectively.

3.1.6 Configuring Face Recognition Database

To configure the database of face recognition events, including storage path of the snapshots and log files of recognition events, click **Configure** on **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**) and select **DB Setting**. This window appears.



The following settings are available:

[Database Folder] Click the Browse button ... to modify the storage path for the snapshots and log files of recorded Recognition Events.

[Recycle Setting]

- **Total Storage Size:** Displays the maximum amount of disk space allocated for storing AI event images, PVD motion images, and face images. When the occupied space exceeds this limit, the system will start deleting the oldest files to free up space for new ones. The value is automatically calculated by multiplying the disk size by the Recycle Percentage.
- **Recycle Percentage:** Set the percentage of the disk space to allocate for the database. The default setting is 10%. Once the percentage is entered, the Total Storage Size is updated accordingly and displayed above.
- **Keep Days:** Set the number of days to keep the logs, from 1 to 999.

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

3.1.7 Backing up Face Database

To back up the face database of a GV-Face Recognition Camera / GV-AI FR, click **Configure** on **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), select **Backup Data From…** and select a desired host by its IP address. You can now save the database on your local PC as an **.fdb* file.

To import the face database into a GV-Face Recognition Camera / GV-AI FR, **Configure** on **Face Manager**, select **Import Backup Data To…** and select a desired host by its IP address.

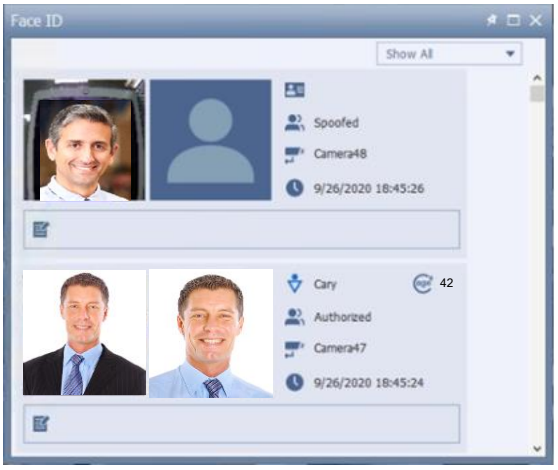
IMPORTANT: When a face database is imported into a host, it replaces all the original face data contained within.

3.1.8 Face ID — Live Recognition Profiles

The Face ID feature allows users to view the simplified info of real-time face recognition events, which can be pinned onto the main screen by clicking .

Note: This function only works when at least one GV-Face Recognition Camera / GV-AI FR is recording.

To access **Face ID**, click **Home** , **Toolbar** , select **Tools** and click **Face ID**. The following window appears.



Each real-time face recognition event is displayed with a snapshot, his/her enrolled face photo, the name and notes of the Face ID, the face group it is under, the camera channel, the time of recognition, and his/her gender and age (when applicable), and is highlighted by the color assigned to the face group.

Only applicable to events from GV-AI FR when Liveness Detection is enabled, faulty face recognition events identified as using inanimate objects, such as printed photos, are indicated as *Spoofed*.

For assigning the desired colors to face groups, see *Setting up Face Groups* earlier in this chapter.

3.1.9 Viewing and Searching for Face Recognition Events

During recording, all recognition events, along with recognition snapshots, recognition time, and schedule alerts, when applicable, are recorded in an event log during video recording. To view **Face Recognition** in recorded videos, click **ViewLog** > **Toolbar** > **Tools** > **Face Recognition**. This window appears.

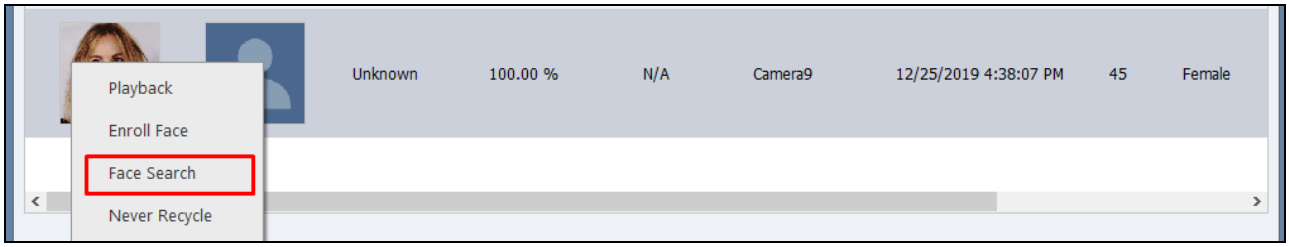


- **Show All:** Select **Show All**, **Show Identified Persons Only** or **Show Unknown Persons Only** to filter the recognition events displayed.
- **Event Image:** Display the captured Snapshot of the recognition event. Double-click the Snapshot to see the recording of the recognition event in ViewLog.
- **Recognition Result:** Display the photo of the Face ID the person is recognized as.
- **Name:** Display the Name of the individual recognized. Written as “Unknown” if unrecognizable.
- **Group:** Display the Group the recognized person is categorized under in the Face Database.
- **Camera Name:** Display the Channel in which the recognition event was recorded.
- **Time:** Display the Time of the recognition event.
- **Age:** Display the estimated age of the person recognized.
- **Gender:** Display the gender that the person is recognized as.
- **Alert:** Record Schedule Alerts when the recognition event recorded is outside of the person’s (Face ID) allowed access schedule.
- **Spoofed:** Display *Spoofed* if the event is identified as faulty and using inanimate objects, such as a printed photo for recognition, as determined by the Liveness Detection of GV-AI FR.
- **Note 1 / 2:** Display the Note 1 / 2 of the Face ID recognized.
- **Export as CSV:** Export the logs of the face detection/recognition events as an *.csv* file

Searching by Face Images

Click  to search for recognition events by using a face image from your PC. Optionally drag the **Confidence Score** to adjust the minimum level of the similarity of the search results as compared to the face image used.

Alternatively, right-click on the snapshot of a desired recognition event and click **Face Search** to use it to search for recognition events.



Searching by Query

Click **Query**  to filter and search for recognition events by time, camera channel, face group, age, gender, alert events and/or keyword search.

Note: The Name search in Query functions is a keyword search and is case-sensitive.

3.1.10 Tracking Recognized Faces

Tracking of recognized faces can be displayed on the E-Map when there are multiple cameras with synchronized Face Databases.

To display Face Tracking, refer to the following for the related settings:

- **Step 1 Synchronizing Face Database**

  To synchronize Face Databases, see *Synchronizing Face Database* earlier in this chapter.

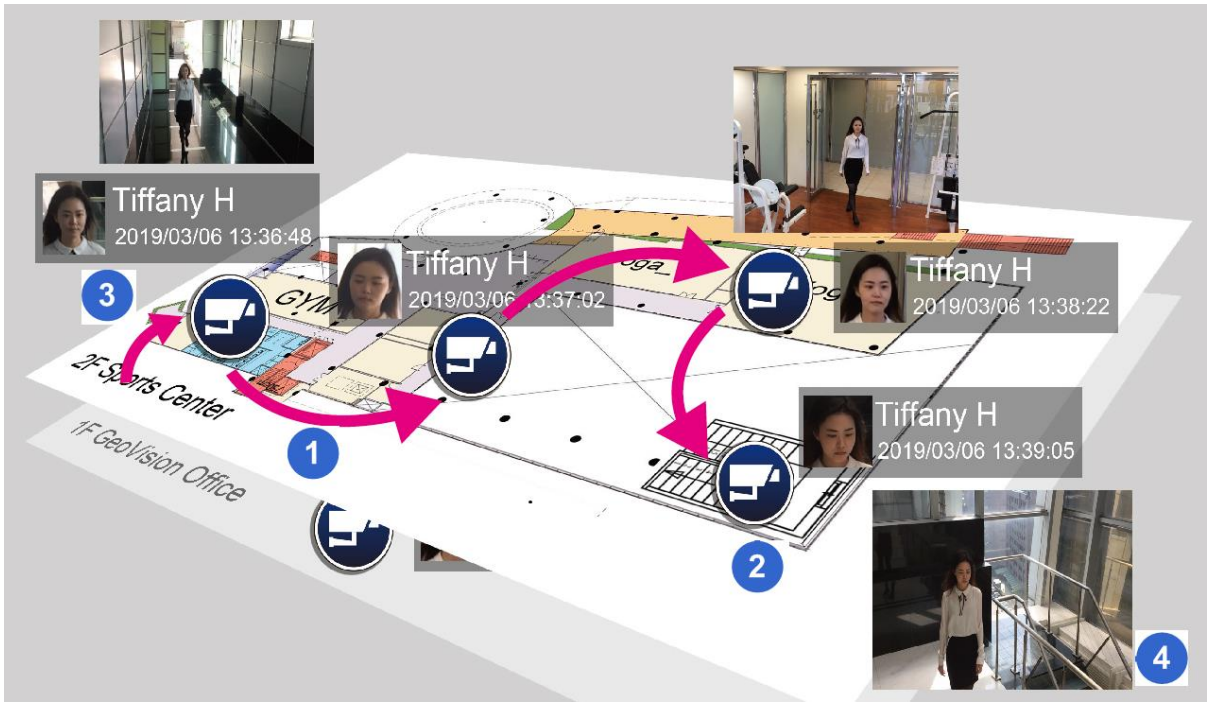
- **Step 2 Creating E-Map(s)**

  To create E-Map(s) and add the camera, see *Creating an E-Map* in Chapter 8.

- **Step 3 Turning on Monitoring and Viewing**

  Turn on monitoring for all the camera channels of GV-Face Recognition Cameras / GV-AI FRs where the face may be tracked and drag the E-map from the Content List to the live view screen.

Once all the related settings are set, you will see arrows indicating the movements of recognized persons on the E-Map.

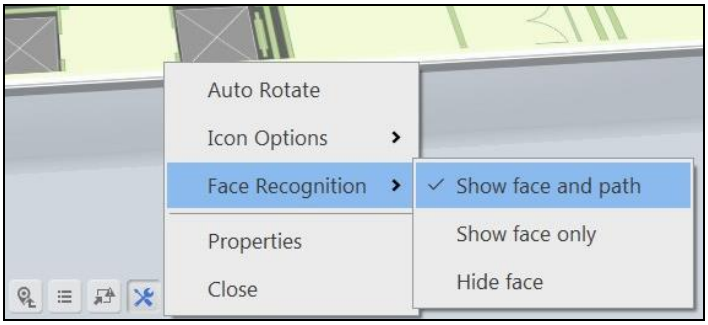


No.	Name	Description
1	Face Tracking	Display the direction of movement of the individual recognized.
2	Latest Recognition Site	The end point of the Face Tracking arrow indicates the surveillance site (camera channel) where the recognized individual was last seen.
3	Previous Recognition Site	The initial point of the Face Tracking arrow indicates the surveillance site (camera channel) where the recognized individual was previously seen.
4	Recognition Event	Display a live image of the Recognition Event.

Note: The Face Tracking feature is supported in live view on the E-Map, but not in playback.

Adjusting the Display Mode on E-Map

To adjust the display mode of the recognition events on E-Map(s), click **Tools** and select **Face Recognition** for the following options:

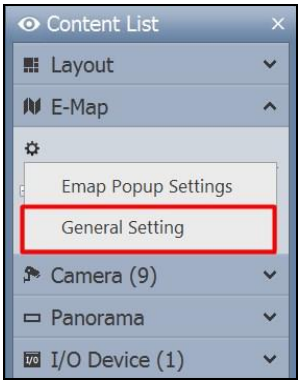


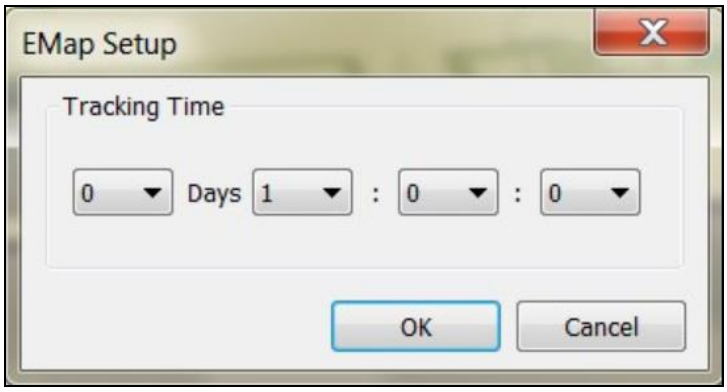
- **Show face and path:** Selected by default, display both Face Tracking and the Recognition Events on the E-Map.
- **Show face only:** Display only the Recognition Events on the E-Map.
- **Hide face:** Do not display any Recognition Events and Face Tracking on the E-Map.

Configuring Face Tracking

For an increased accuracy, you can modify the interval setting of **Face Tracking** based on your surveillance needs.

1. In Content List of Live view, click **Configure** > **General Setting**. This window appears.





2. Under **Tracking Time**, select the days (0~31), hours (0~23), minutes (0~59) and seconds (0~59) to define the time interval in which Face Tracking is effective for. Face Tracking will not be displayed for any subsequent Recognition Events occurring beyond the set Tracking Time.
3. Click **OK** to save the changes.

3.1.11 Integrating Face Recognition to Access Control

The system extends the face recognition feature of connected cameras by converting recognized faces into access card data for access control management. Prior to the integration, make sure the required controller(s) and access cards have both been properly configured on your access control system, e.g. GV-ASManager.

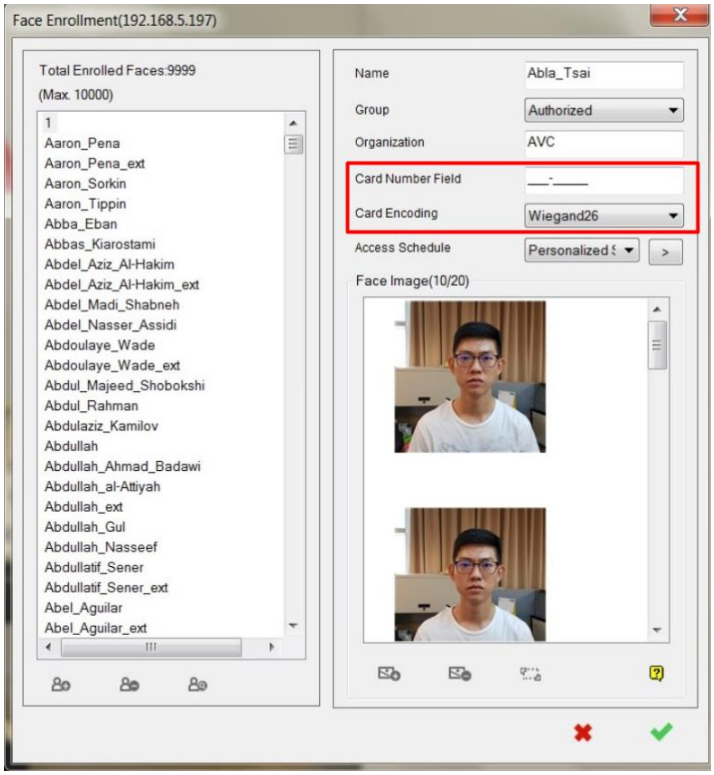
To configure the controller and access cards, to be paired with Face IDs, see *Adding Controllers* and *Setting Cards*, respectively, in Chapter 4 of the *GV-ASManager User's Manual*.

3.1.11.1 Pairing Face IDs with Access Cards

Face IDs of GV-Face Recognition Cameras / GV-AI FRs can be paired with GV-AS ID Cards / Key Fobs or 3rd-party smart cards to be used for access control regulated by GV-ASManager

To pair Face IDs with access cards, follow the steps below.

1. On **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Face Enrollment**.
2. Select a Face ID, type the **Card Number** to be paired with and select its encoding type from the **Card Encoding** dropdown list.



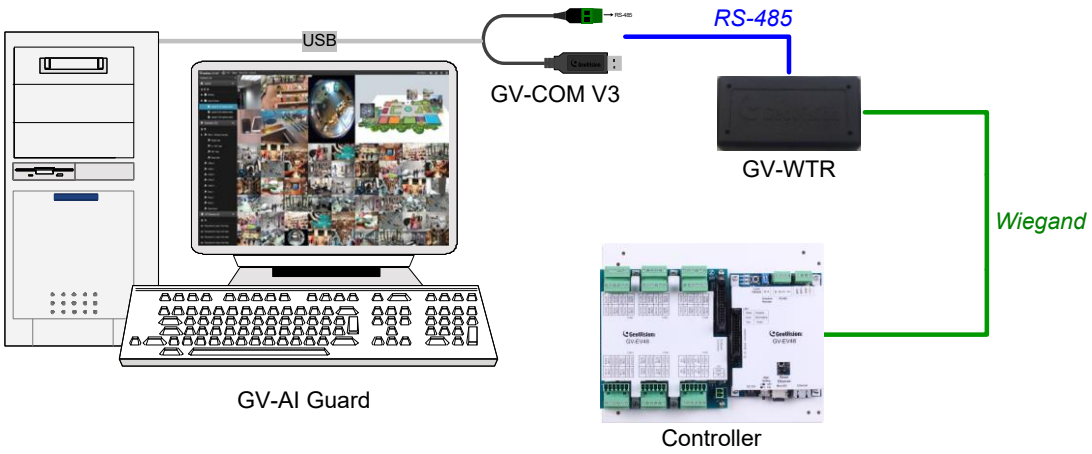
3. Click to save.

Note: To batch enroll multiple access cards and/or import from GV-ASManager, see *Batch Enrolling Faces and Access Cards* later in this chapter.

3.1.11.2 Connecting Controller

For the system send the paired card number to the connected controller upon face recognition, the controller must be properly connected, which can be done through one of the following two methods:

- **COM Port**



1. Connect GV-COM V3 to a USB port of the PC running the system.
2. Connect GV-WTR to GV-COM V3 using its RS-485 wires.
3. Connect GV-WTR to the controller using its Wiegand wires.

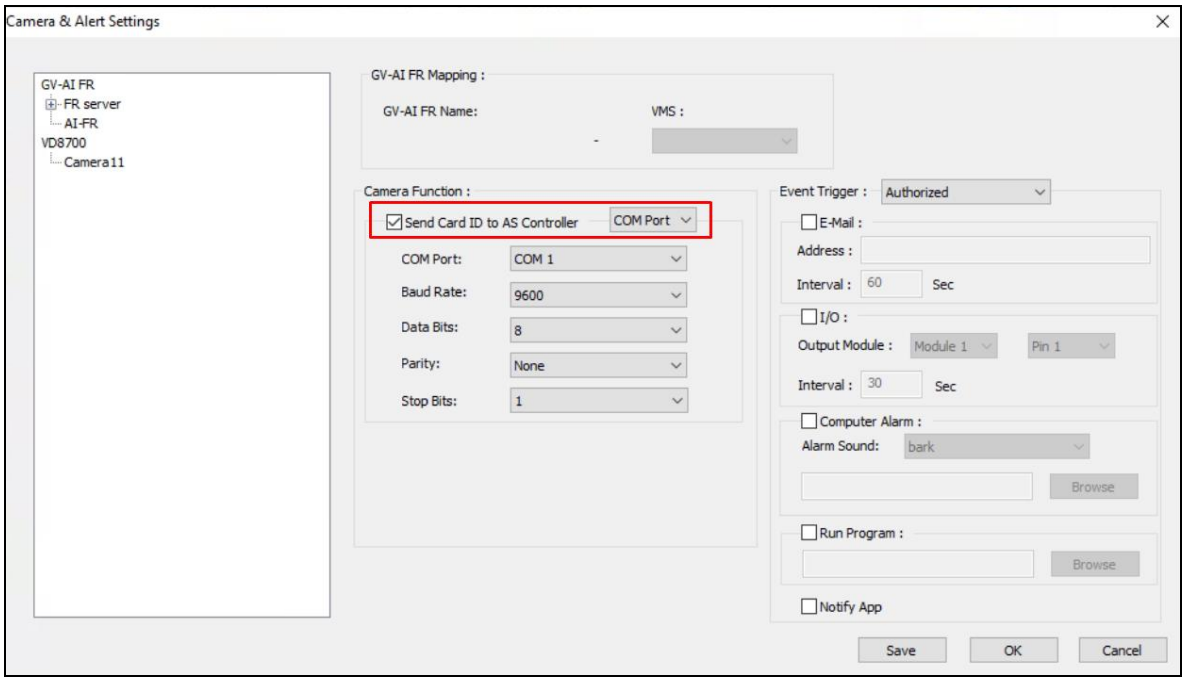
- **TCP/IP**

Connect the controller to the same network as the system.

Sending Card Number to Controller by Face ID

After the controller is successfully connected to the system, configure the necessary settings according to the type of connection established.

1. In **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Configure** and select **Camera and Alert Settings**.
2. Select the desired camera and enable **Send Card ID to AS Controller**. Then configure the necessary settings based on the type of connection used.



[COM Port]

- **COM Port:** Check the COM port number of GV-COM V3 connected to the system in **Device Manager** and select from the dropdown list accordingly. For details, see the *GV-COM V3 Installation Guide*.
- Keep the default values of **Baud Rate**, **Data Bits**, **Parity** and **Stop Bits** unless they've been changed manually.

[TCP/IP]

- **IP:** Type the IP address of the controller under the same LAN as the system.

3.1.12 Batch Enrolling Faces and Access Cards

The batch enrolling feature of Face Manager allows users to import a large quantity of face images and access card data to a connected GV-Face Recognition Camera / GV-AI FR at once.

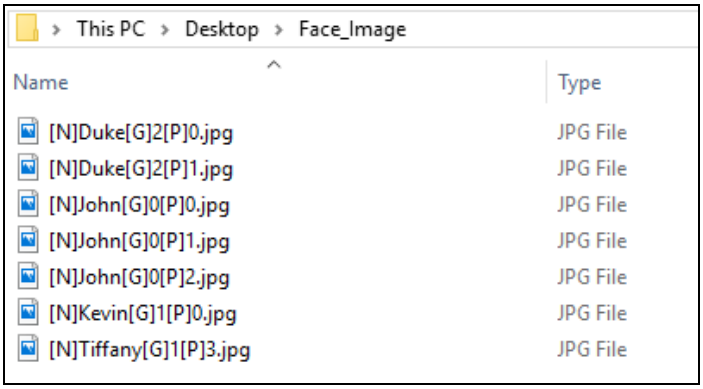
Batch Enrolling Faces Only

To enroll multiple face photos, save all of the face images to the same folder on your PC and rename them as exemplified below:

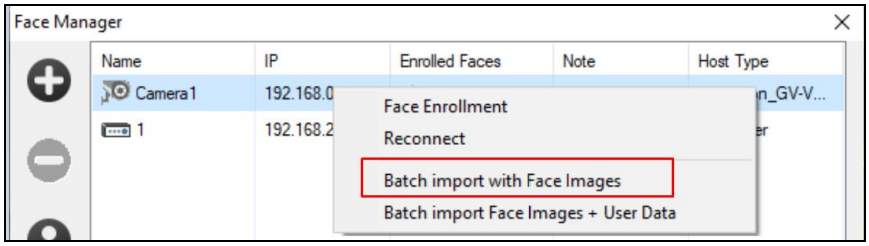
[N]<Face ID Name>[G]<Group No. – 1>[P]<Image No. – 1>.jpg

For example, [N]John[G]0[P]0.jpg, [N]John[G]0[P]1.jpg, [N]John[G]0[P]2.jpg

The above image files will be added to Face ID John, as the first, second and third images, with the ID being categorized under Group 1.



Once all the face images are named properly and saved under the same folder, right-click on the device you want them to be batch enrolled into on **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**) and click **Batch import from Face Images** to locate and select the folder.



Note:

1. <Group No. – 1> indicates the desired group number minus one.
2. <Image No. – 1> indicates the order of the images minus one.
3. All photos used for face enrollment must meet the criteria as specified in GV-Face Recognition Camera FAQ.

Batch Enrolling Faces + Cards

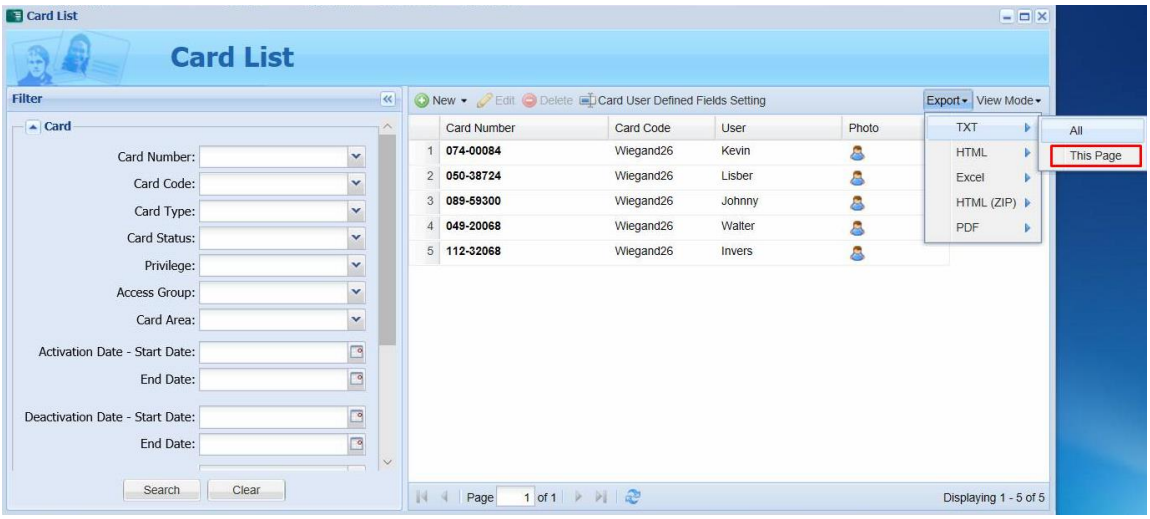
To enroll access card data along with multiple face photos from GV-ASManager to GV-Face Recognition Camera / GV-AI FR simultaneously, follow the steps below:

Note: Before batch enrolling user data and photos from GV-ASManager, make sure of the following:

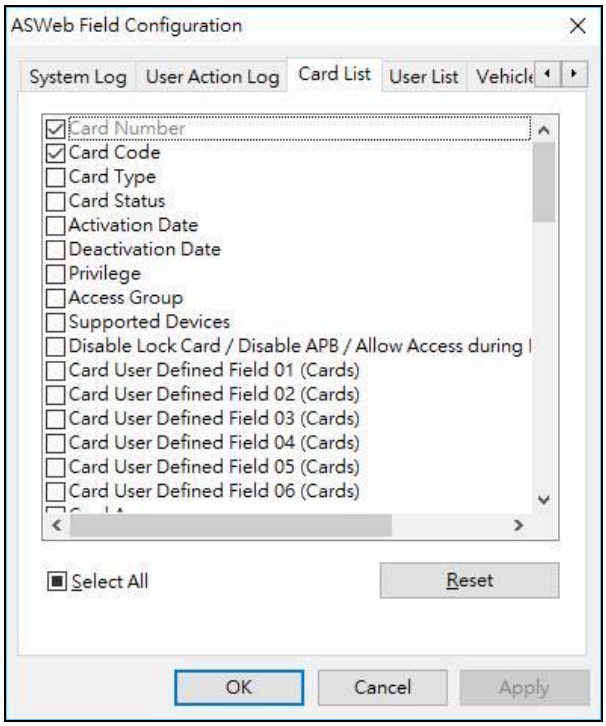
A. The Display Names of users on GV-ASManager, which will be used as Face ID names, must not contain any spaces.

B. Photos of users on GV-ASManager must meet the criteria as specified in GV-Face Recognition Camera FAQ.

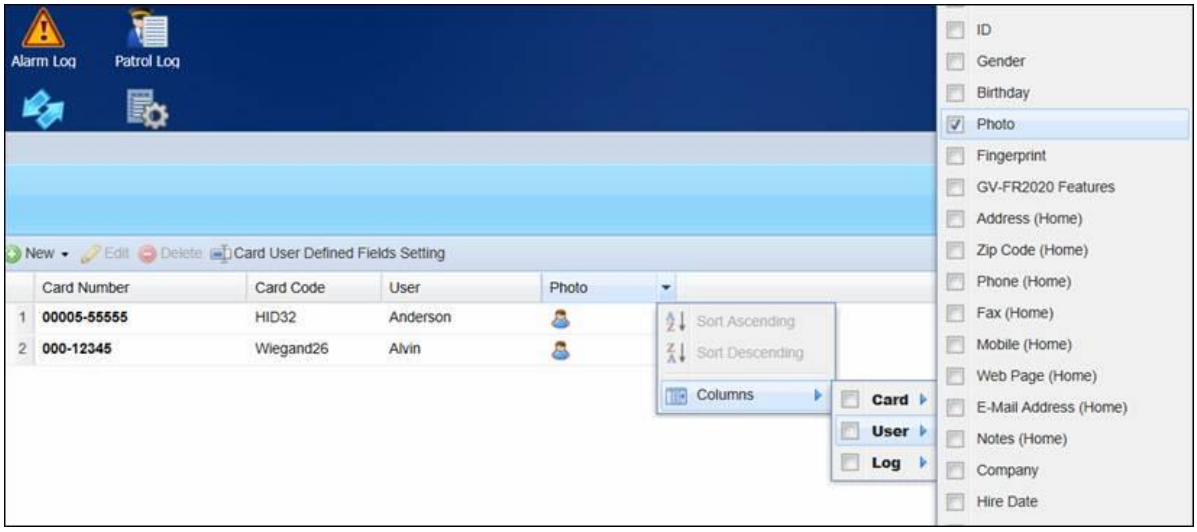
1. From the **Card List**  of GV-ASWeb, make sure the proper card data are contained within, namely *Card Number*, *Card Code*, *User* and *Photo*, then click **Export** and select **TXT** > **This Page**.



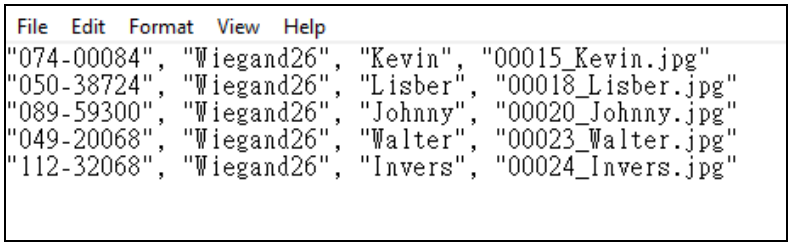
A. For the Card List to contain the proper data, open **ASWeb Field Configuration** (under **Tools** on GV-ASManager), click the **Card List** tab and select *Card Number*, *Card Code*, *User* and *Photo*.



B. In the **Card List**, select to display the fields of **Card Number**, **Card Code**, **User** and **Photo** by clicking one of the arrow buttons and deselect all other fields.

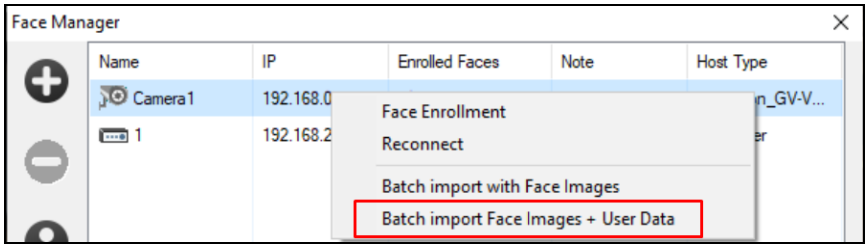


2. Save the exported TXT file, exemplified below, under a specific folder.



3. Copy the photos of the users to be enrolled from the GV-ASManager directory (default: C:\\ASManager\Photo) and save them under the same folder as the TXT file.

4. Once all the face images are saved within the same folder as the TXT file, right-click on the device you want them to be batch enrolled into on **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**) and click **Batch import Faces Images + User Data** to locate and select the folder.



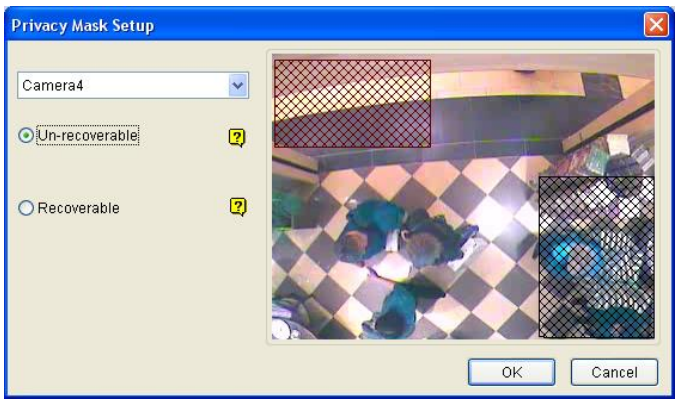
3.2 Privacy Mask Protection

The Privacy Mask blocks 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.

3.2.1 Setting up a Privacy Mask

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**.
2. In the Setup dialog box, select **Video Analysis** > **Privacy Mask Setup**, select the camera(s), and click **Setting**. This dialog box appears.



3. Select a camera from the dropdown list.
4. Select Un-recoverable and/or Recoverable.
   - **Un-recoverable:** The block-out area will not be retrievable in the recorded clips.
   - **Recoverable:** The block-out area will be retrievable with password protection.

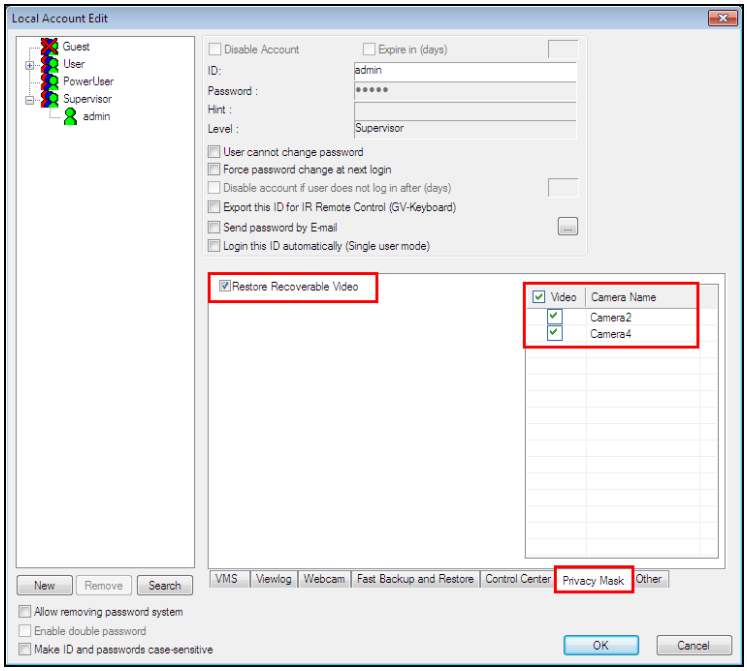
5. Drag the area where you want to hide on the image. You will be prompted to click **Add** to save the setting. The Un-recoverable area is marked in black, while the recoverable area is shown in red.
6. Click **OK** to apply the settings.

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

3.2.2 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 admin on the main screen, select **Password Setup** > **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.



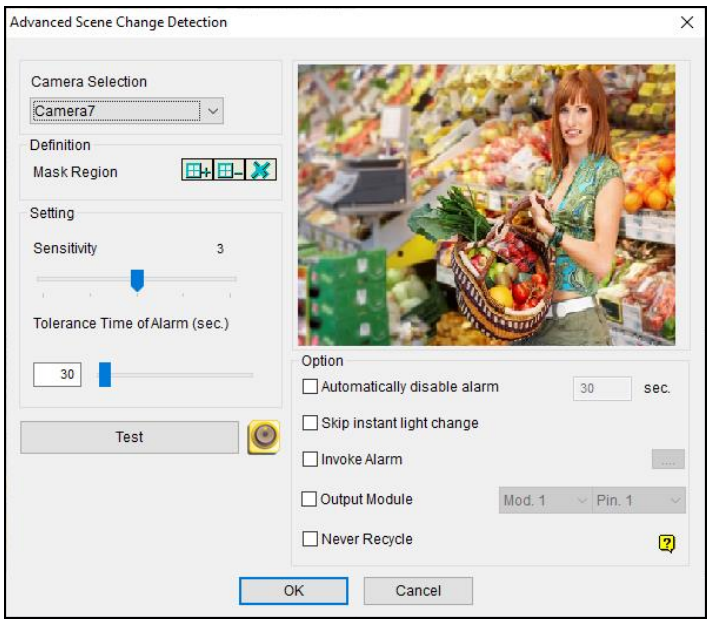
Note: If you open the event files (*.avi) directly from local disks, the valid ID and password are also required to access the block-out areas. For details on retrieving the block-out areas in the exported files, see *Merging and Exporting Video* in Chapter 4.

3.3 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** > **Toolbar** > **Configure** > **Video Process**.
2. In the Setup dialog box, select **Video Analysis** > **Advanced Scene Change Detection**, select the camera(s), and click **Setting**. This dialog box appears.



3. Select a camera from the Camera Selection dropdown 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 dropdown 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 view, the selected alarm or output will be activated, and the event will be recorded as **Advanced Scene Change** in the 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. To create schedules for Advanced Scene Change, see *Creating Schedules*, 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**.

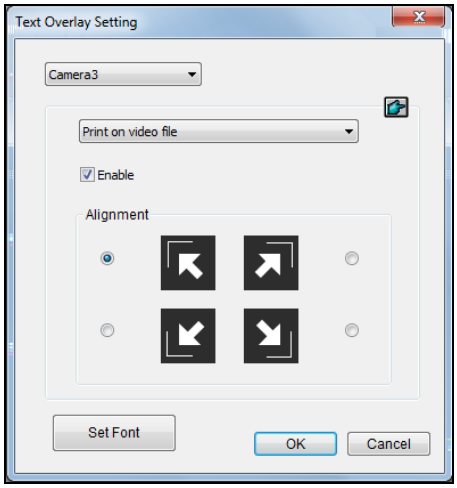
- **Reset Alert:** Disables and resets the triggered alert. After the alert is reset, if the scene change remains over the specified tolerance time, the system will still detect it as a scene change and keep generating alert.

3.4 Text Overlay

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

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

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**. The Setup dialog box appears.
2. Select **Video Analysis** > **Text Overlay Setting**, select the camera(s), and click **Setting**.



3. Select a camera from the dropdown list.
4. 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 the triggered input device on live view. This function requires mapping a camera to an input device, see *Other I/O Application Functions* in Chapter 6.
   - **Print ASManager Text on Screen:** Displays GV-ASManager data, such as the license plate number, on both live view and recorded videos. This function requires enabling the text overlay setting in GV-ASManager. See *Applying Text Overlay*, Chapter 5, in the *GV-ASManager User's Manual*.
   - **Alignment:** Enable alignment to customize where camera information appears on a camera view.
   - **Set Font:** Customize the font, font size, font style, and other settings.

3.5 Video Analysis by Camera

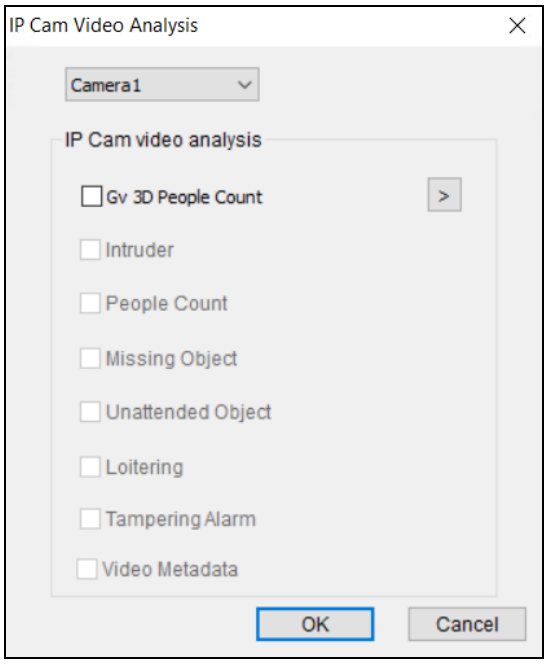
You can choose to process video analysis on the camera instead of on the system. To learn which camera's AI events are supported by the system, see *Camera's AI Events Supported by GV-VMS*.

Note:

1. You can only choose either the camera or the system to process video analysis.
2. To receive AI events from cameras, enable **Sync device time with PC** in advance; see *Configuring Abnormality Settings* in Chapter 2.

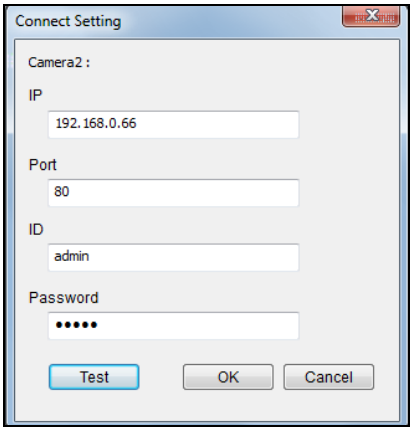
To access the feature, follow the steps:

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**.
2. In the Setup dialog box, select **Video Analysis > IPCVA (Video Analysis by Camera)**, select the cameras, and click **Setting**.
3. Select a camera, and select which video analysis to process on the camera.



4. For **GV-3D People Count:** Set up connection with GV-3D People Counter V2 to receive count data. Click the arrow button for setup.

   A. Type the IP address, ID, and Password of GV-3D People Counter V2. Select **Test** to see if GV-3D People Counter is properly connected. Select **OK** to establish connection.



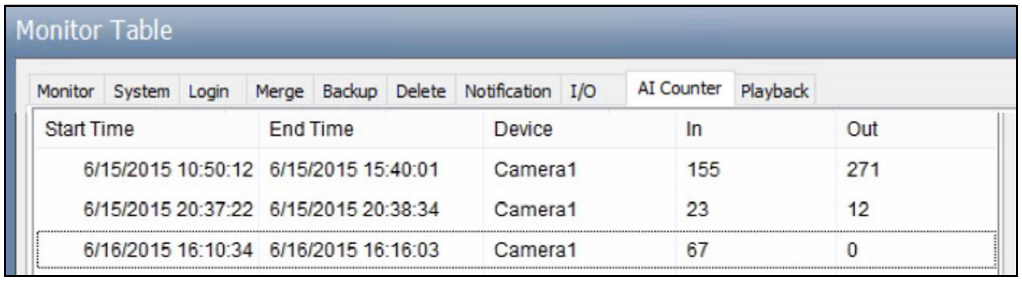
   B. On the live view of the camera, select **Tools** > **Monitor**. The number of people entering and exiting the detection area are displayed on the top left corner of the screen.



5. For **Video Metadata**: Receives camera metadata, allowing event searches based on person or vehicle attributes with the AI Query function. For the list of GV-IP cameras that support video metadata, see *Camera's Video Metadata Supported by GV-VMS* in *Camera Features Supported by GV-VMS V20*.

The people or object count data is recorded in the System Log. To view the logs, click **Home** > **Toolbar** > **Tools** > **System Log** > **Monitor Table**, and select **AI Counter**.

- **AI Counter:** Shows count results from the GV-3D People Count function in IPCVA (for GV-3D People Counter V2) and the People Count function in IPCVA (for AI-capable GV-IP cameras). For details, see *Viewing System Log* in Chapter 1.



Chapter 4

Video Playback..... 209

4.1 Playing back on ViewLog..... 210

4.1.1 ViewLog Window..... 211

4.1.2 ViewLog Control Panel..... 212

4.1.3 Adjusting the Camera View..... 216

4.1.4 Bookmarking Video Events in ViewLog..... 217

4.1.5 Merging and Exporting Video..... 218

4.1.6 Saving, Printing & Copying Images..... 223

4.1.7 Adjusting Distorted Views..... 224

4.2 Object Search..... 225

4.3 Advanced Log Browser..... 227

4.3.1 Controls on the Advanced Log Browser..... 227

4.3.2 Filter Settings..... 228

4.4 Remote ViewLog V2..... 230

4.5 Single Player..... 231

4.5.1 Single Player Window..... 231

4.6 Specifications..... 232

CHAPTER

4

Video Playback

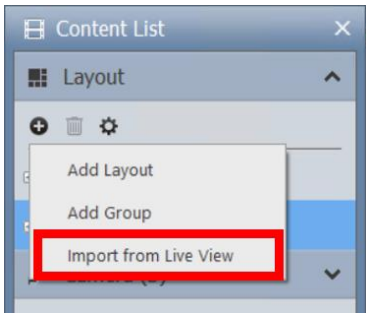
Recorded videos can be played back using the following various software applications. Below summarizes their main characteristic to help you decide which application to use under a given situation.

Application	Description
ViewLog	A full-function player to play back video, search for a video event, merge and export video and more. See *Playing Back on ViewLog* in this chapter.
Object Search	A more convenient tool to search video files recorded on motion or alarm. See *Object Search* in this chapter.
Remote ViewLog V2	A program to retrieve files from a remote GV-AI Guard and it supports most functions provided by the ViewLog player. See *Remote ViewLog V2* in this chapter.
WebCam Server	A server that remotely accesses live view and play back recordings on your Web browser without installing additional software. See *Remote Viewing* in Chapter 7.
Single Player	A player that plays back the backup recorded files with simple and easy playback functions. See *Single Player* in this chapter.

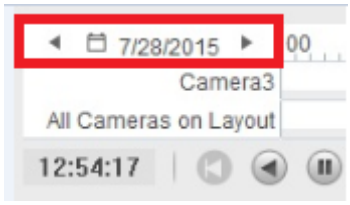
4.1 Playing back on ViewLog

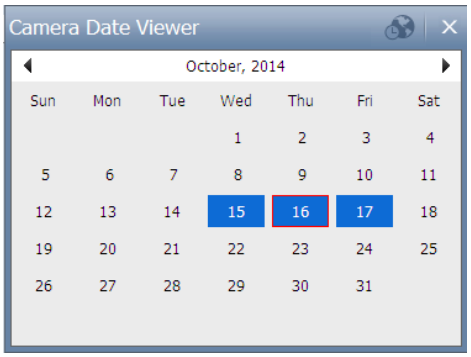
The ViewLog is a video player that plays back recorded videos without affecting the recording in process. To launch the ViewLog:

1. Select **ViewLog** > **Toolbar** > **Content List** . The Content List appears.
2. Select **Add** > **Import from Live View** to import current live views to the playback screen. For details on configuring the ViewLog layout, follow Steps 2 to 5 of *Arranging Live View Layouts* in Chapter 1.



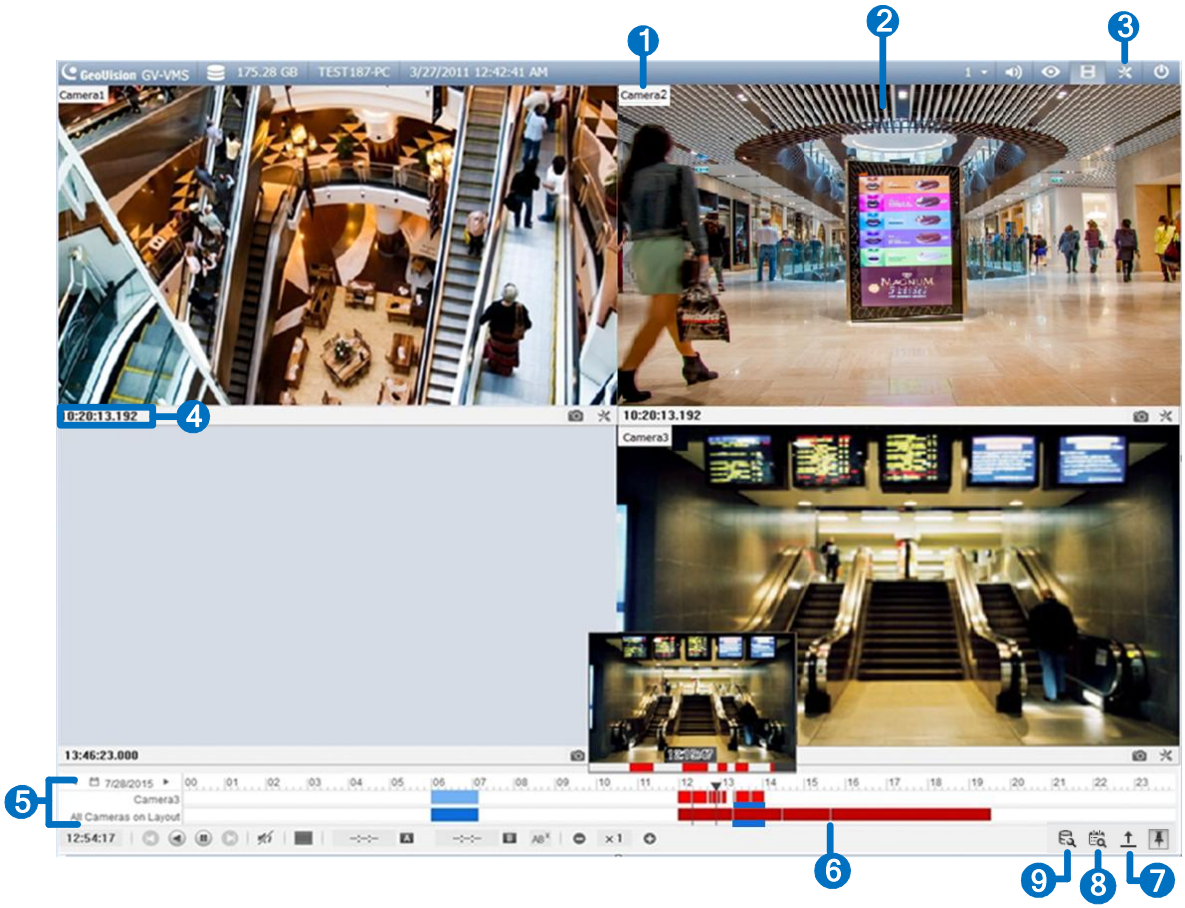
3. Optionally drag and drop more cameras from the Content List to the playback screen.
4. On the timeline, click the arrows or the date to select a date from a popup calendar.





5. Click **Play** to start play back. For details, see *ViewLog Control Panel* later in this chapter.

4.1.1 ViewLog Window



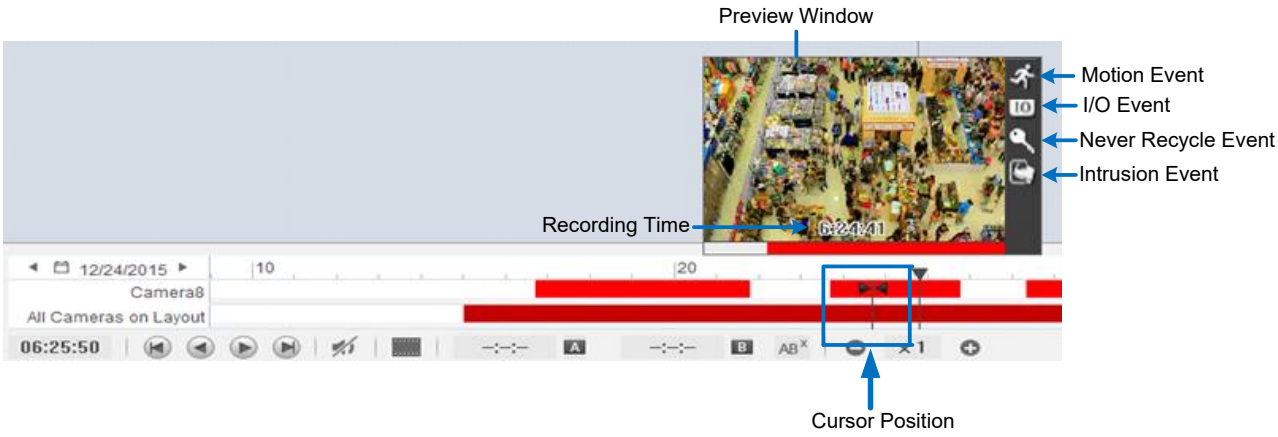
No.	Name	Description
1	Camera Name	Indicates the camera name.
2	Camera View	Displays the playback video.
3	Toolbar	Brings up these options when **ViewLog** is selected: • **Display Play Panel:** Display or hide the ViewLog timeline. This function is grayed out when the **Pinned** button is selected in 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.

		From **Setup** (Toolbar > Configure), you can enable/disable text overlay and object detection rectangles, set the timeline to the current time when ViewLog starts, prioritize sub stream display during playback (see *Multi-Channel Playback* at the beginning of this manual), and configure the size of the Preview window (see *ViewLog Control Panel* later in this chapter).
4	Recorded Time	Indicates the time of recording.
5	ViewLog Timeline	Indicates the recording date and reflects video recordings. See *ViewLog Control Panel* later in this chapter.
6	Playback Panel	Contains typical playback control buttons. See *ViewLog Control Panel* later in this chapter.
7	Display All Database	Displays the recording timelines of all camera channels.
8	Timeline Filter	Displays a popup window where you can select event types to show in different colors on the timeline.
9	Repair Database	Displays the background repair progress. See *Repairing Damaged File Paths* in Chapter 5.

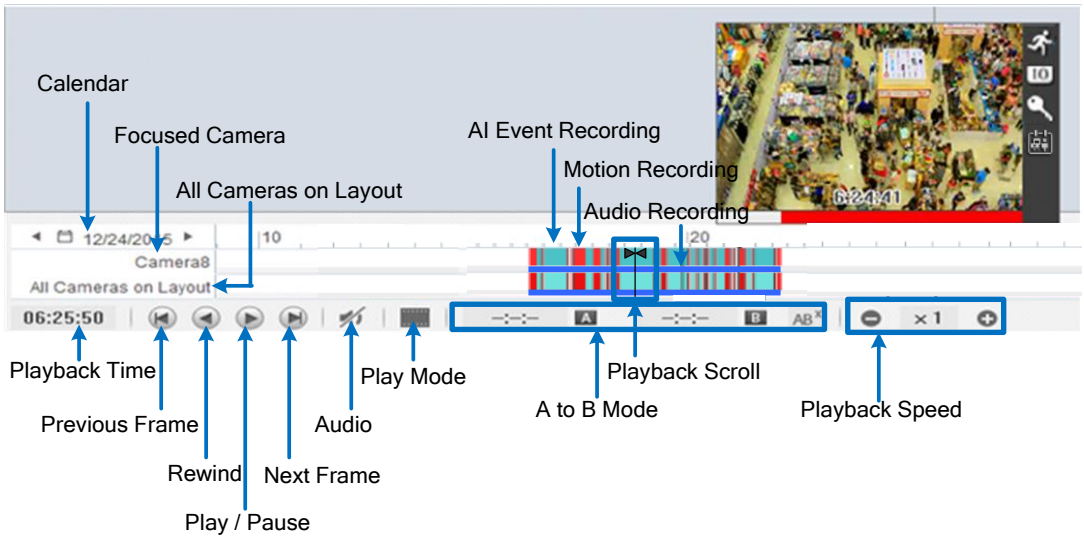
4.1.2 ViewLog Control Panel

Preview Window

Move the cursor on the timeline to see a preview of the recording. Click on the timeline to pause all channels at the selected time. To change the size of the preview, click **Toolbar** > **Configure** > **Setup**.



Timeline



Colors in the timeline:

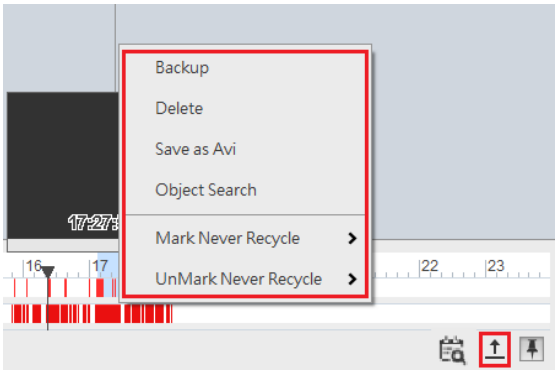
- **Blue:** Round-the-clock / Audio recordings
- **Red:** Motion / IO event recordings
- **Green:** Never Recycle recordings
- **Yellow:** Recordings retrieved from the SD cards of cameras when reconnecting after a temporary disconnection
- **Turquoise:** AI event / PVD Motion event recordings

Note: Round-the-Clock events are shown as blue, except the following conditions:

1. If **Register Motion Event** or **Intrusion** is enabled, the timeline interval of the triggered event becomes red.
2. If **Webcam Service** is enabled, the timeline interval becomes red when users log onto the system remotely (such as using mobile applications).
3. If **Control Center Service / ERM Service** is enabled, the timeline interval becomes red when the connected GV-Software receives events from the system.

Tip:

1. Right-click and drag on the timeline to have a quick access to various functions.
2. Click **Display All Database** to access the timelines of all camera channels.



3. Click **Display Timeline** to choose to display timelines of different event types of all camera channels.

Playback Mode Option

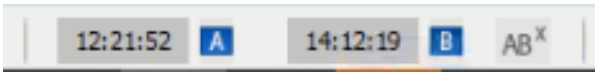
By default, ViewLog plays back video in Real Time mode. To switch playback modes, click or on the ViewLog Control Panel.

- **Real Time:** The icon indicates that the video is being played back in real time. This mode reduces rendering time but may drop frames. Click the icon to switch to Frame by Frame mode.
- **Frame by Frame (without audio):** The icon indicates that the video is being played back frame by frame without audio. Playback may be delayed depending on network bandwidth and computer performance. Click the icon to switch to Real Time mode.

A to B Playback Mode

When playing back videos, you can set a start frame and an end frame for auto-playing:

1. To set the start frame, click A and double-click a time on the timeline.
2. To set the end frame, click B and double-click a time on the timeline.
3. The start time and end time are displayed besides A and B as illustrated below.



4. Click to play back from frame A to B repeatedly.
5. To cancel this playback mode, click AB.

Changing the Displayed Date on the Recording Timeline

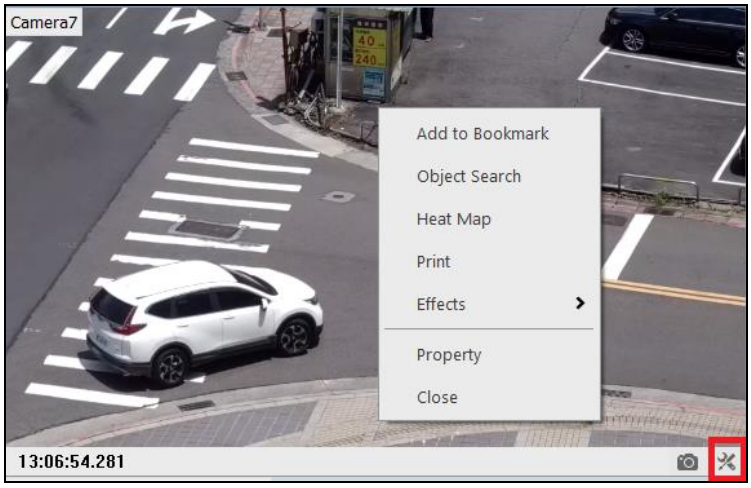
You can directly drag the timeline to search and view recordings of a previous or next day with recorded events.

1. Scroll the mouse wheel forth to enlarge the timeline. The default display of the timeline is 24 hours.
2. Click and drag the timeline back and forth. The timeline jumps between the recording days.



4.1.3 Adjusting the Camera View

To adjust the image quality for the recorded videos, right-click on the camera view or click **Tools** to access these settings:



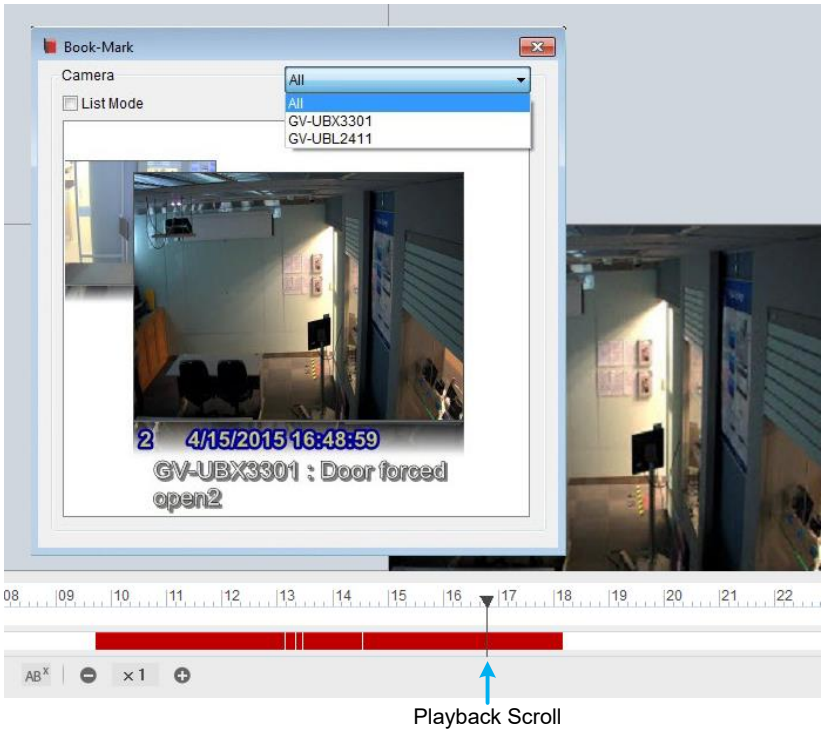
- **Add to Bookmark:** See the following subsection *Bookmarking Video Events in ViewLog*.
- **Object Search:** See *Object Search* later in this chapter.
- **Effects:** Click to apply image effects. After applying effects:
  - To take a snapshot of the current playback image, select **Copy** and then open a Word document or Paint 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**.
- **Property:**
  - **Show Caption:** Enabled by default. Shows the camera name.
  - **Keep Image Ratio:** Change the camera view to its original ratio.
- **Close:** Click to close the channel.

Note: To preview image effects on sample images, click **ViewLog** > **Toolbar** > **Configure** > **Effects – Sample**.

4.1.4 Bookmarking Video Events in ViewLog

The ViewLog player allows you to bookmark desired recordings.

1. To bookmark a recording image, right-click a camera view and select **Add to Bookmark**.
2. To access bookmarks, click **Toolbar** > **Tools** > **Bookmark**. Double-click any bookmark to advance the playback scroll to the relevant point on the timeline for further event investigation.



3. You can select **List Mode** to present all the bookmarks in a list.
4. To filter the bookmarks, you can select a camera from the dropdown list, or click **Filter** to narrow results by **Time Range** or **Search Description**. The Search Description option allows you to enter keywords or partial text from the bookmark descriptions to quickly locate relevant events.

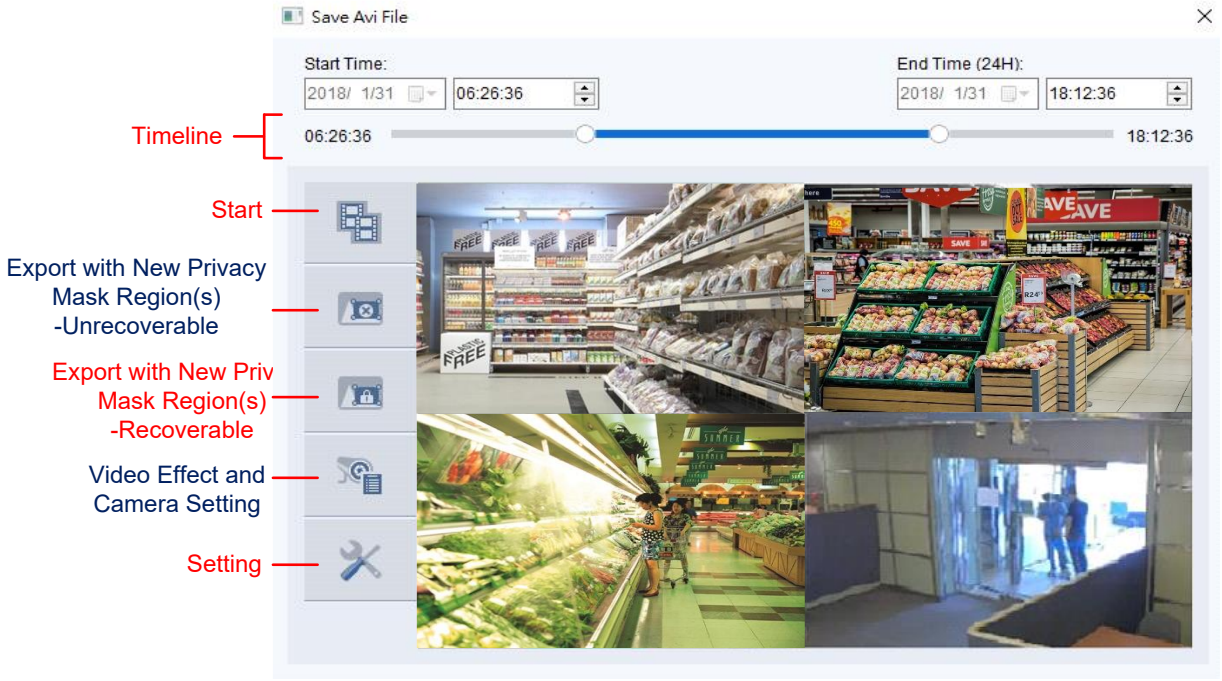
Note: The bookmarked video events will be marked as Never Recycle in the ViewLog.

4.1.5 Merging and Exporting Video

You can merge several videos into a single .avi or .exe file and export it to the local computer.

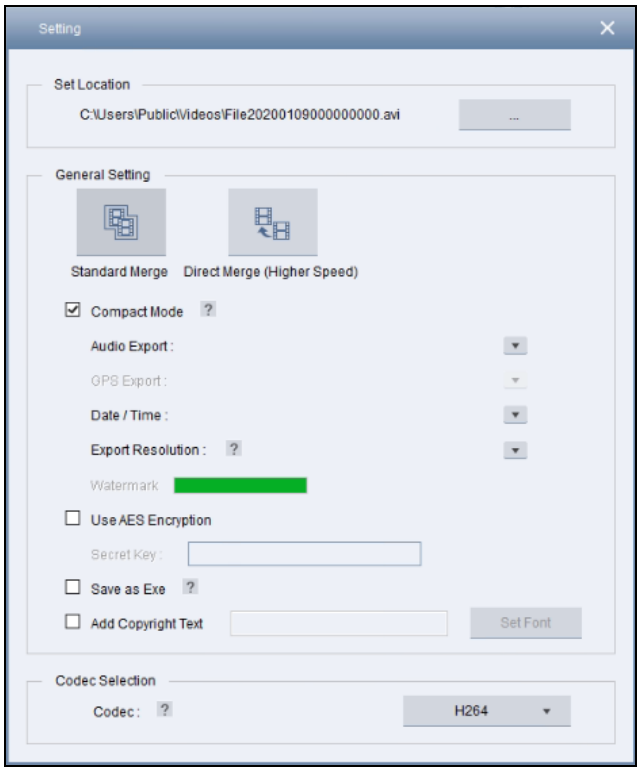
Note: The maximum size of the exported file is 2 GB. Any file exceeding 2 GB will be split into another file. A maximum of 16 channels are supported for merging and exporting multiple videos.

1. Click **ViewLog** > **Toolbar** > **Tools** > **Save as Avi**. This dialog box appears.



2. Click **Video Effect and Camera Setting** to select the camera channels you wish to export. Optionally enable additional camera settings.
3. Drag the timeline to set the start and end times for the videos to be exported.

4. To configure the saving path and format of the exported video, click **Setting** . This dialog box appears.



[Set Location] Click **[…]** to specify a save path.

[General Setting]

- **Standard Merge**: Save a full-length video, containing the images of a single camera or multiple cameras within ViewLog, with recorded and non-recorded periods. A blank blue screen will be displayed during the non-recorded periods. By default, **Compact Mode** is selected to merge only the periods with recorded images.
- **Direct Merge (Higher Speed)**: Only available when exporting the videos of one channel. It speeds up the video merging process and saves the video files in the codec in which it was originally recorded. By default, **Compact Mode** is selected to save compact video files by only exporting the key frames.

Note: When using **Direct Merge (Higher Speed)**, the conversion time is significantly reduced, but you will not be able to customize the following settings: codec selection, privacy mask recoverability, and digital watermark.

- **Audio Export:** Select **Denoise** to remove audio noises from the video, or select **Channel** for audio exporting.
- **Date / Time:** Select whether to show date and / or time stamps. You can also select the stamp position, font type and size and text color on the images.
- **Export Resolution:** Select a resolution for the exported video.
- **Watermark:** Only available when the watermark is applied to the recorded video. Select to include the watermark in the exported video.
- **Use AES Encryption:** Select and type a 16-digit **Secret Key**, containing only letters and numbers, to add additional security protection for the exported video.
- **Save as Exe:** Select to save files in EXE format to auto-play the files with any third-party player. Enable this feature to play back video at the computer without installing GeoVision codec.
- **Add Copyright Text:** Select to stamp user-defined copyright texts to the recording being exported.
  - ⊙ **Set Font:** Click to set the font type and size as well as the position of the copyright text on the recording image.

[Codec Selection]

- **Geo H264:** A codec created by GeoVision which provides better image quality, higher frame rates and smaller file size than other standard codecs. When selected, the GeoVision codec must be installed on the computer playing the exported video. Otherwise export the files in EXE format to play the video at any computer.
- **WMV9**, **H.264** or **MPEG4:** The standard codec allows users to play the video with Windows Media Player or other third-party video players without using GeoVision codec. When selected, the Privacy Mask you created in **Save as AVI** will be disabled.

5. Click the **Start** icon  to start exporting.

To check the merging or exporting status, click **ViewLog** > **Toolbar** > **Tools** > **Display Merging List**. The Merging List dialog box appears.

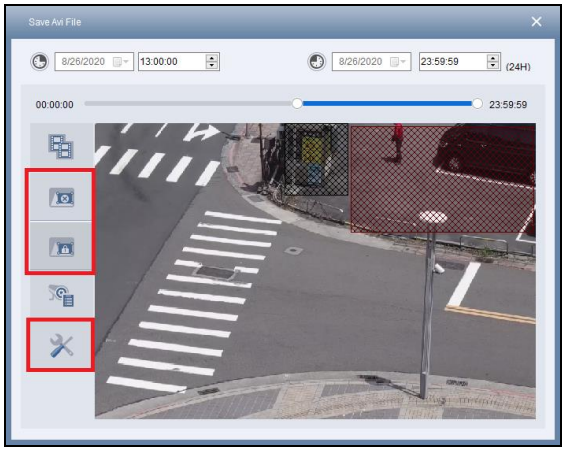


Note: Audio is not supported for videos exported in MPEG4 codec.

To optionally include other features in the exported video, refer to the following:

Configuring Privacy Mask

To configure the Privacy Mask settings for the exported files, click **Setting** and change the Codec to **Geo H264** first.

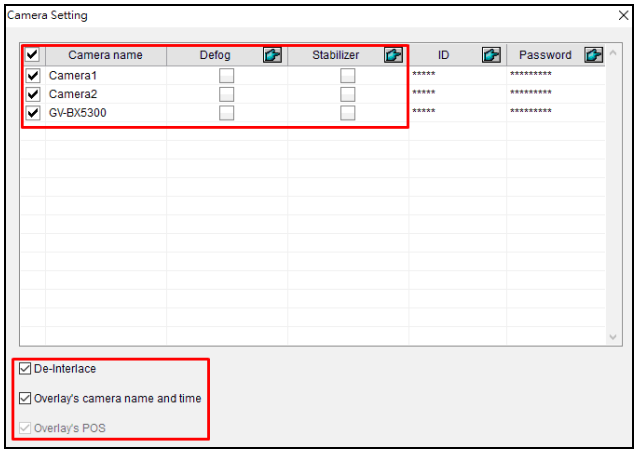


- **Unrecoverable privacy mask**: The block-out areas marked in black will not be retrievable in the exported files.
- **Recoverable privacy mask**: The block-out areas marked in red can be retrieved with the administrator's ID and password.

To set up the block-out area, click and drag on the image and select **Add** or **Delete**.

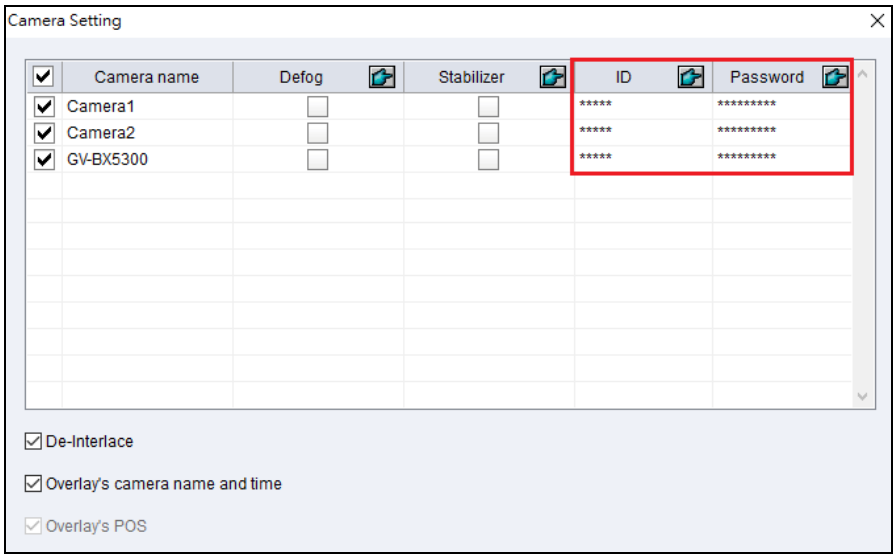
Combining Special Effects

To combine special effects to the exported video, click the **Video Effect + Camera Setting** icon and select the desired effects for each of the cameras selected.



Retaining Recoverable Block-out Areas

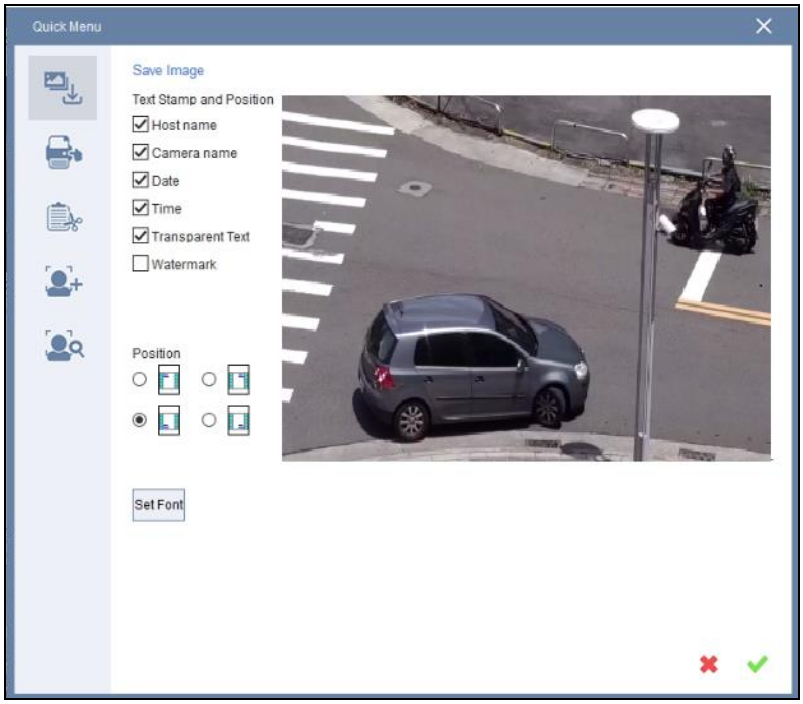
For recorded videos with Privacy Mask settings, by default, you can see the recoverable block-out area created in Main System when logging in with the administrator account. To retain the block-out area before exporting recorded videos, type a random ID and password in the fields or leave the fields blank. For details, see *Privacy Mask Protection* in Chapter 3.



Note: Only the administrator can set up the ID and password to retrieve or retain the recoverable block-out areas. To grant access rights to Power Users and Users, see *Granting Access Privileges to Recoverable Areas* in Chapter 3.

4.1.6 Saving, Printing & Copying Images

You can take a snapshot and save, print or copy the current camera view as an image while the recorded video is being played back.



1. Click from a camera channel on the ViewLog. The Snapshot Quick Menu appears.
2. Select the **Save Image**, **Print** or **Copy Image** tab, to respectively save, print or copy the snapshot captured.

   [Stamp Text on the Image] Select to add text(s) to the image. Selecting **Transparent Text** will create the stamps in transparent text.

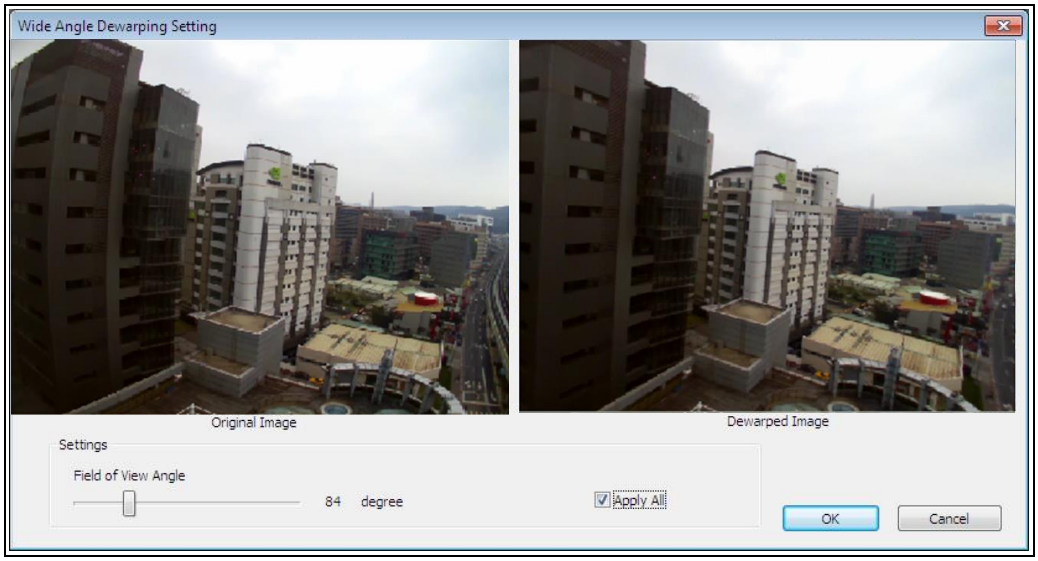
   [Position] Select a desired position, upper-left, upper-right, bottom-left or bottom-right, where the texts will be added to the image saved.

   [Set Font] Click to adjust the font style and/or size of the texts to be added.
3. Click .
   A. For saving an image, type a desired name, select a file format, assign the location to save the image file and click **Save**.
   B. For printing, optionally add a template or change the size of the image and its position on 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. In **ViewLog** , right-click the desired camera channel in the layout, and then select **Effects** > **Wide angle lens dewarping** > **On / Off**.
2. To adjust the degree of adjustment, right-click the desired camera channel in the layout, and then select **Effects** > **Wide angle lens dewarping** > **Modify**. This dialog box appears.



3. Move the slider to adjust the degree of warping. The adjusted view is shown on the right.
4. Optionally, select **Apply All** to apply the setting to all camera channels.
5. Click **OK**. The cameras are immediately dewarped.

4.2 Object Search

Object Search allows you to search for motion events by specifying regions of interest in recorded videos. Only one event type is supported: Smart Motion Search.

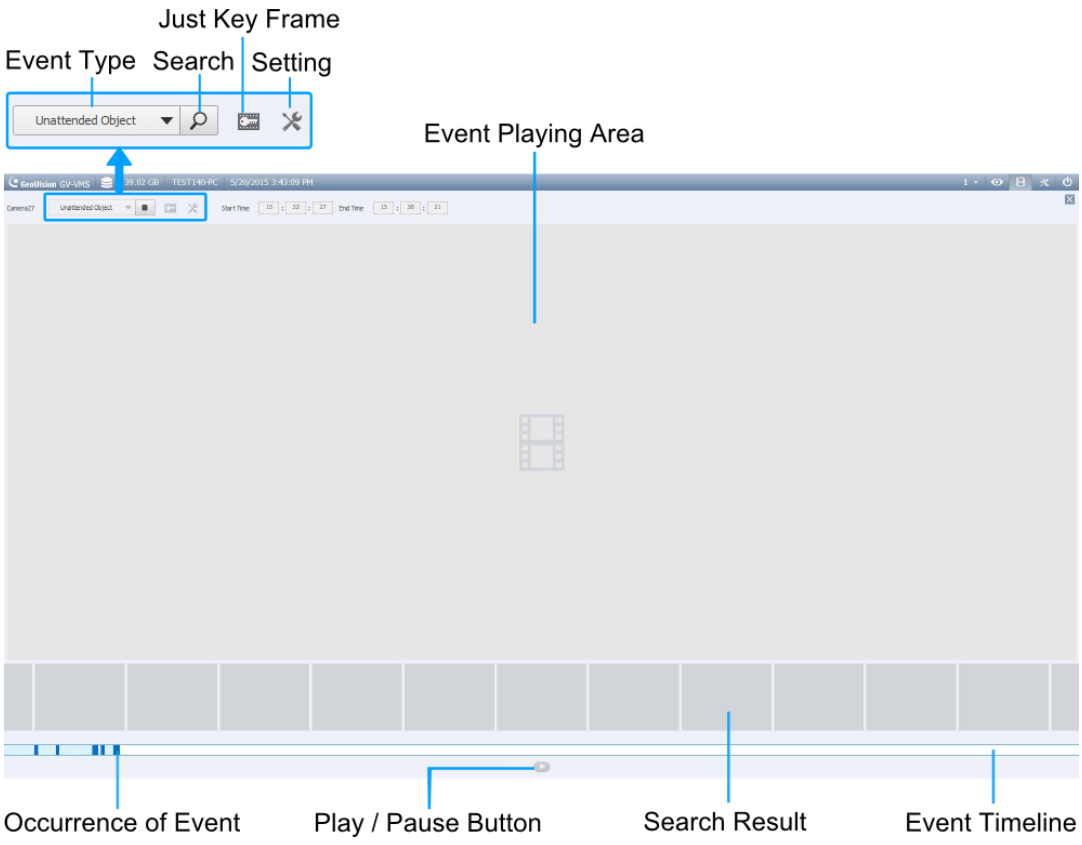
- **Smart Motion Search:** Marks motion while recording and allows you to search for motion in recordings by designating regions of interest.

This function is handy if you know something happened in a certain area of the camera's field of view, but do not know when it occurred. You can draw a box around the area of interest, and the system will search for video clips containing motion within that area.

Note: To use Smart Motion Search, it is required to enable this function on cameras before recording. For details on enabling the Smart Motion Search function, see *Setting up Motion Detection* in Chapter 1.

---

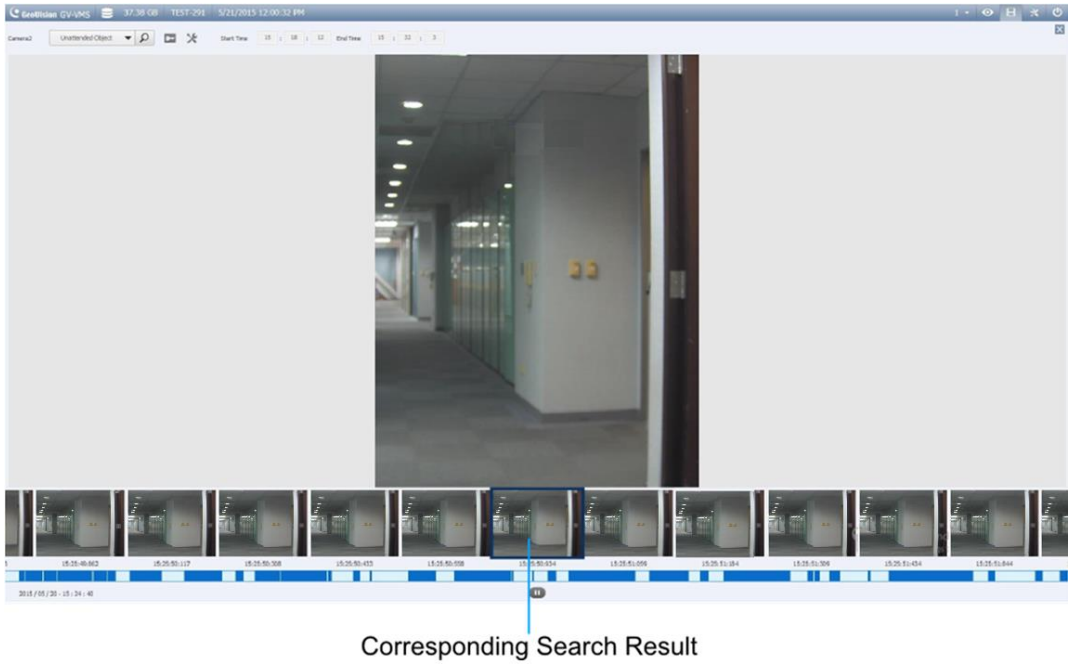
1. Select **ViewLog**, select a channel (the channel's recordings must be displayed on the timeline), and select **Toolbar** > **Tools** > **Object Search**. This window appears.



2. Specify **Start Time** and **End Time** for the search. Click the **Play** button to display images of the defined time range.
3. Select an event type from the dropdown list .
4. Click **Setting** .
5. Click on the image to add detection regions, or define an object size. You can also adjust the detection sensitivity for the added detection regions. For **Smart Motion Search**, draw detection regions on the image. The system will search for video clips containing motion within that area.



6. Click **Just Key Frame** to search only key frames, if necessary.
7. Click **Search** . The search results are shown in blue on the timeline.
8. Double-click an event or click the **Play** button to view the event.



4.3 Advanced Log Browser

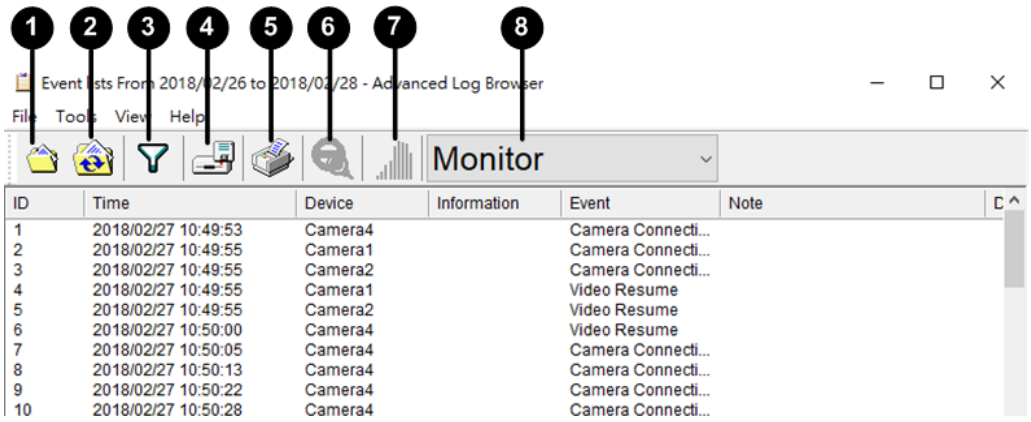
With the Advanced Log Browser, you can perform post-event review and filtering of general events, system activities, or people / vehicle counting events using advanced criteria such as device, time range, and event subtype. It provides more comprehensive and detailed log data than the System Log, making it ideal for in-depth analysis.

For fast access to recent event data from general, system, or counting events, see *System Log* in Chapter 1.

If you want to perform advanced filtering of AI and PVD events, including face, people, and vehicle attributes, see *AI Query* in Chapter 1.

1. Click **ViewLog** > **Toolbar** > **Tools** > **Advanced System Log**. The Advanced Log Browser Open Database dialog box appears.
2. Specify a time range and click **OK**. All events within the specified range are displayed on the Advanced Log Browser.

4.3.1 Controls on the Advanced Log Browser



Advanced Log Browser

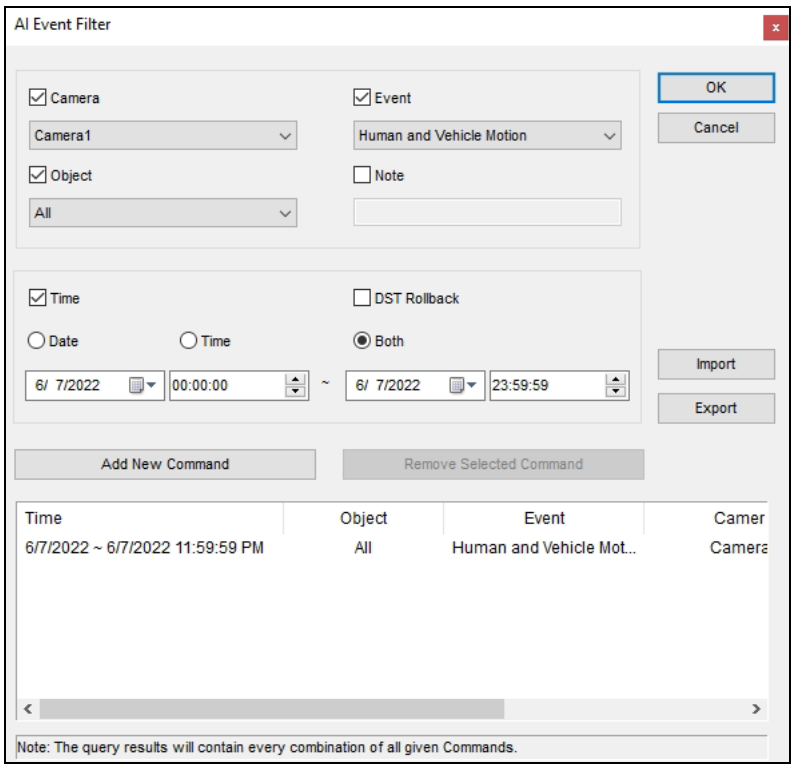
No.	Name	Description
1	Open	Opens an event log.
2	Reload	Select **Reload All Table** or **Reload Current Table** to refresh loaded data.
3	Filter	Defines the search criteria. See the following subsection *Filter Settings*.
4	Backup	Select **All Tables** to back up all logs, or select **Current Table** to back up the current log table opened. By default, audio and video are enabled for backup.
5	Print	Prints the current log table.

6	Filtering / Cancel Filtering	Only available when filtering starts. Click to cancel the filtering.
7	Counter Table	This function allows you to query and export the log data in .csv, .html, or .pdf format. When **AI Event Log** is selected as the log type, you can access the advanced AI event filter. When AI **Counter** is selected as the log type, you can access the counting results from the GV-3D People Count function in IPCVA (for GV-3D People Counter) and the People Count function in IPCVA (for AI-capable GV-IP cameras).
8	Log Type	Select to display logs of the following types: Monitor, Login, System, Merge, Delete, Backup, I/O, Notification, Playback, CMS, POS, AI Event Log, and AI Counter.

4.3.2 Filter Settings

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

1. On the toolbar, select the desired log type, click the **Filter** button (see No. 3 of the Advanced Log Browser, *4.3 Advanced Log Browser*) > **Default Filter**. This dialog box appears.



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

Tip: Next time you want to use the same exported settings, click the **Filter** button > **Favorites**, and select the exported file by name.

Note: The default Export path is **C:\GV-AI Guard\Syslog_Favorites**. If you change this path, the exported file will not appear under the **Favorites** option.

4.4 Remote ViewLog V2

You can retrieve the files from a remote system through the network using the Remote ViewLog V2.

Note: The integration of AI events from **GV-AI Guard** to GV-Remote ViewLog V2 is not supported.

GV-Remote ViewLog V2:

- Supports most of the functions provided by the ViewLog, such as Backup, Save as AVI, Object Search, Database Files Backup, as described earlier in the chapter.
- Capable of disabling camera connections under heavy network load.
- Can back up recordings from a remote GV-AI Guard.

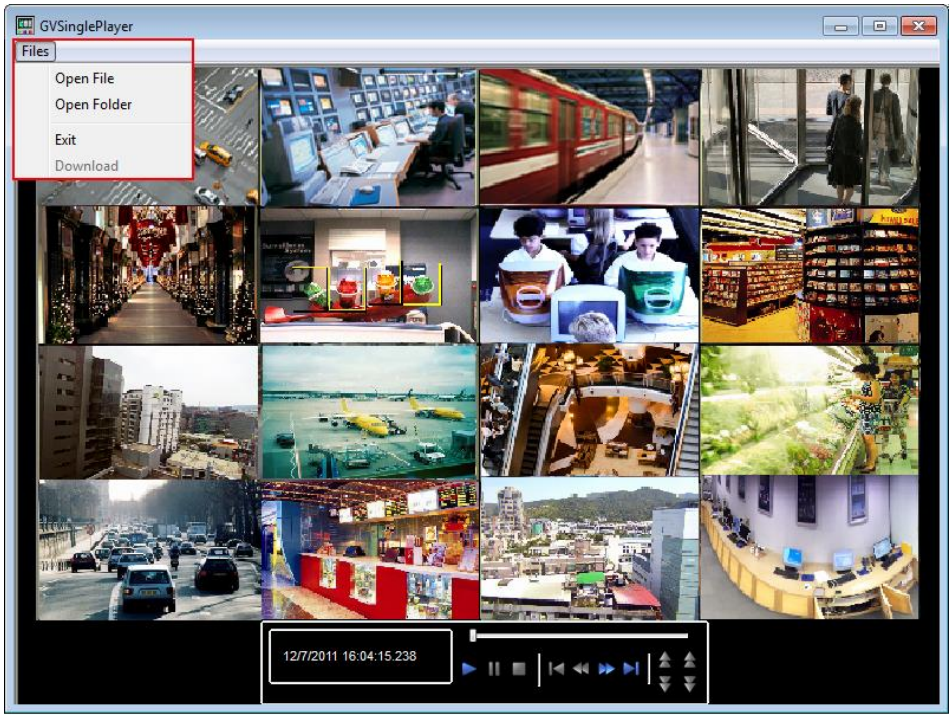
For details, see the *GV-Remote ViewLog V2 Guide*.

4.5 Single Player

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

4.5.1 Single Player Window

Click **Files** > **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** > **Open Folder** to select the folder that collects several camera recordings.



4.6 Specifications

Feature	Notes
Support for PIP View	Yes
Support for Focus View	Yes
Videos Exported as .avi Files	Yes
Object Search	Yes
Support for Fisheye View	Yes

Chapter 5

Backup, Deletion and Repair..... 234

5.1 Backing up Log Data 234

5.2 Backing up Recorded Files 235

5.3 Deleting Recorded Files 238

5.4 Repairing Damaged File Paths 239

5.5 Repairing Damaged Video Files 241

CHAPTER 5

Backup, Deletion and Repair

This chapter explains how to back up, delete, and repair video and audio files stored on the hard disk. Video files can be copied to external storage devices such as USB drives, external hard drives, or CD, DVD, or BD.

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** > **Toolbar** > **Tools** > **Advanced System Log**. The Open Database dialog box appears.
2. Specify a time range and click **OK**. Events recorded during the specified range are displayed on the Advanced Log Browser window.
3. Click **Backup** on the toolbar. The Customer Database Export dialog box appears.

   [Table Option] Select **All Tables** to back up all log data or **Current Table** for the log table you are currently at.

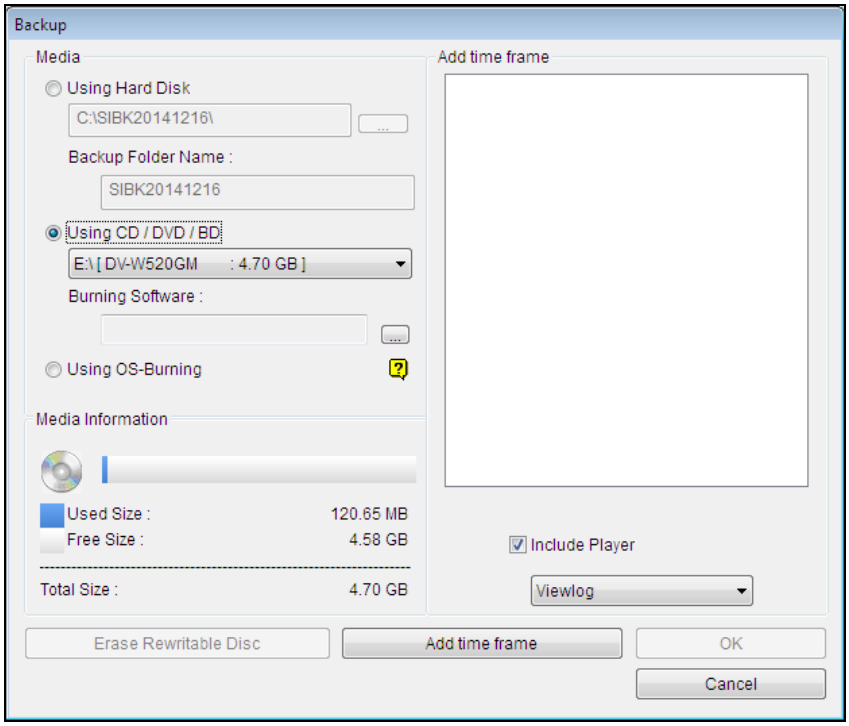
   [Export with Video/Audio data] Backs up video/audio attachments with log data.
4. Click **OK**. The Backup dialog box appears (see *Backing up Recorded Files* later in this chapter).
5. In the Media section, select the method and destination to back up the log files and click **OK** to back up.

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

1. Click **ViewLog** > **Toolbar** > **Tools** > **Backup**. This dialog box appears.



Backup dialog box

2. Select the destination media to back up files.

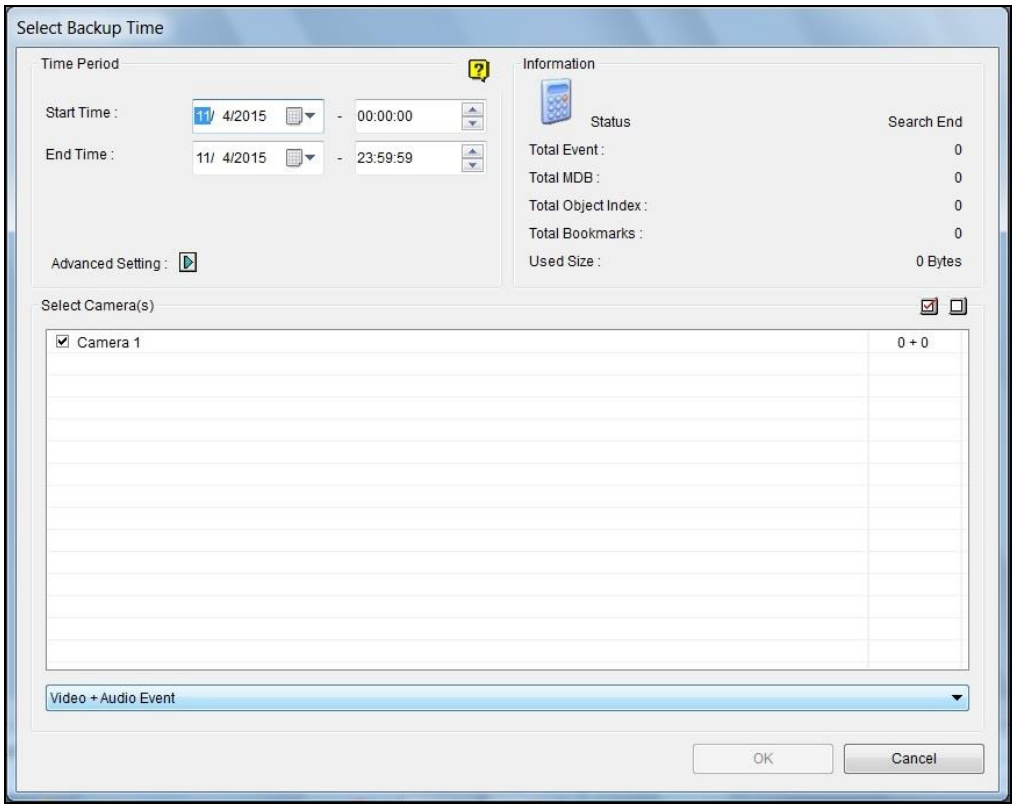
[Media]

- **Using Hard Disk:** 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 software.
  - Click the **[…]** button to assign the desired burning software (.exe file). After clicking **OK** on the Backup dialog box, the system will ask you to paste the backup files to the CDR-Writer program, and call up the assigned burning software for you to paste and backup files.
  - If Nero software of version 6.6.0.14 or later is installed, you can directly burn the files onto CD/DVD without assigning the burning software and pasting the backup files to the CDR-Writer program.
  - If Nero software of version 7.0 or later is installed, you can directly burn the files to blu-ray disc.

- **Using OS-Burning:** It burns files using the inbuilt software of the operation system onto the DVD, CD or blu-ray disc. Note that your hard disk needs at least 1 GB buffer space.

[Media Information] Indicates free and used space on CD/DVD media or the local disk.

3. Click the **Add Time Frame** button to specify the time range of recorded videos to be backed up and define which files to back up. The Select Backup Time dialog box appears.



[Time Period] Specify the time range of recorded videos to be backed up.

[Information] Indicates the number of backup files and their total size. (Total MDB refers to the System Log files.)

[Advanced Setting]: Click  to choose which files to back up:

- **Database Files:** Backs up the System Log files.
- **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.
- **Include daylight saving rollback events:** Backs up the events recorded during Daylight Saving Time.
- **Bookmarked files:** Backs up the bookmarked files.

[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 dropdown list:** Select the types of video events for backup.

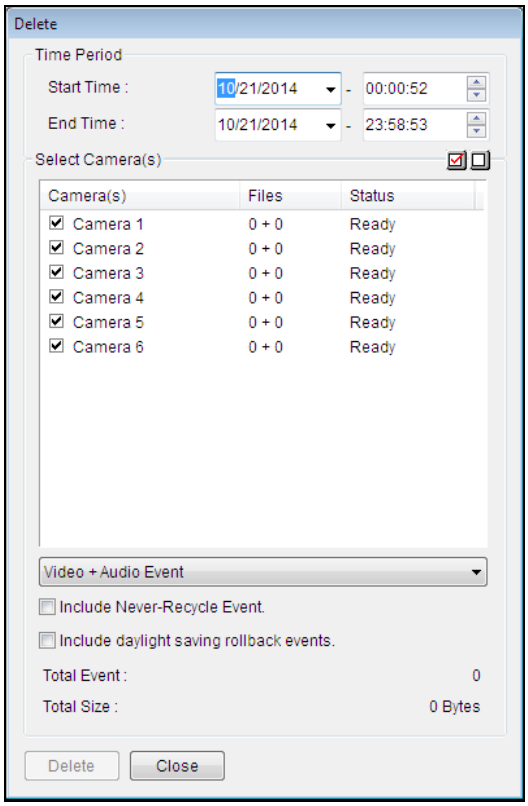
4. Click **OK** to add the time frame. You can repeat step 3 to create up to 10 periods of time.
5. To include the player to the backup files, select **Include Player** at the bottom right of the Backup dialog box and select **ViewLog** or **Single Player**. By default, **ViewLog** is selected. If no player is selected, you can only play the backup files at the computer installed with GeoVision codec.
6. Click **OK** in 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 the ViewLog player and Single Player, see *Chapter 4 Video Playback*.

5.3 Deleting Recorded Files

1. To delete files using the ViewLog, click **ViewLog** > **Toolbar** > **Tools** > **Delete**. This dialog box appears.



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 dropdown list to select the types of events to be deleted, e.g. video, audio or both together.
5. To delete the never-recycle events, select **Include Never-Recycle Event**.
6. To delete the events recorded during Daylight Saving Time, select **Include Day Light Saving Time Rollback Event**.
7. Click the **Delete** button.

Note:

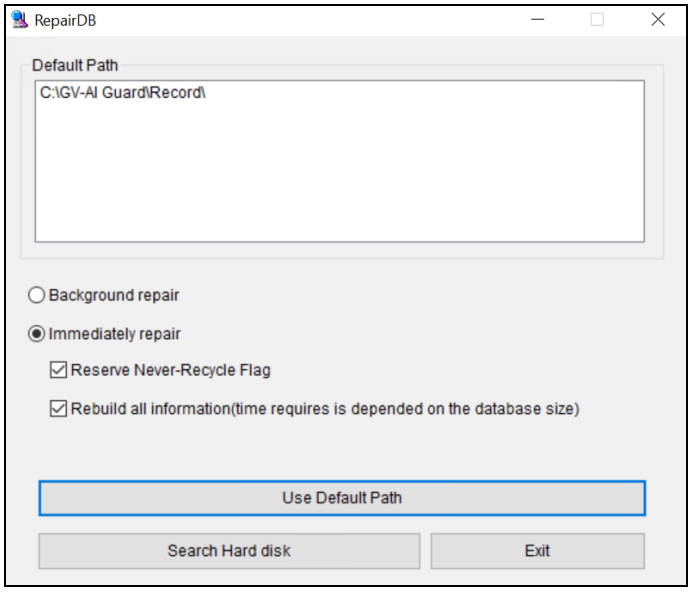
1. To view the history of file deletion, click **Home** > **Toolbar** > **Tools** > **System Log** > **Monitor Table**, and click the **Delete** tab.
2. To view the file paths and sizes of a camera's event recordings, right-click the camera and select **Event View** on the Delete dialog box.

5.4 Repairing Damaged File Paths

Use the Delete function (see *Deleting Recorded Files* earlier in this chapter) to correctly delete video and audio files. If you move or delete video files using Windows Explorer or Windows File Manager, the system will not be able to detect this change. However, as long as these files are still stored in the hard drives and are detectable by the Windows operating system, you can use the Utility to restore these misplaced and missing recorded files back to their default paths.

This Utility comes with the installation of the Main System. Follow these steps to repair the paths.

1. Go to the **Windows Start** > **All apps** > **GV-AI Guard folder** > **Repair Database Utility**.
2. When the Select Camera for Repair Database dialog box appears, select the cameras that require database repair and click **OK**. This dialog box appears.



3. Set **Background repair** for a quick scan of the files needing repairs. This function allows the utility to repair the files after the scan is completed while the system continues its operation. Select **Immediately repair** to thoroughly repair your recorded files while the system is closed.
4. If your recorded files exist only in the predefined recording path, click the **Use Default Path** button to rebuild the file path in the predefined recording hard drive only.
5. For **Immediately repair** only: If your recorded files scatter across different hard drives, click the **Search Hard Disk** button to allow more time to rebuild these file paths in the hard drives connected to the system.

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 any of the following scenarios occurs in the 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.
3. To see the Background Repair progress, click **ViewLog**  **> Repair Database**  (No. 9 in *ViewLog Window* in Chapter 4).

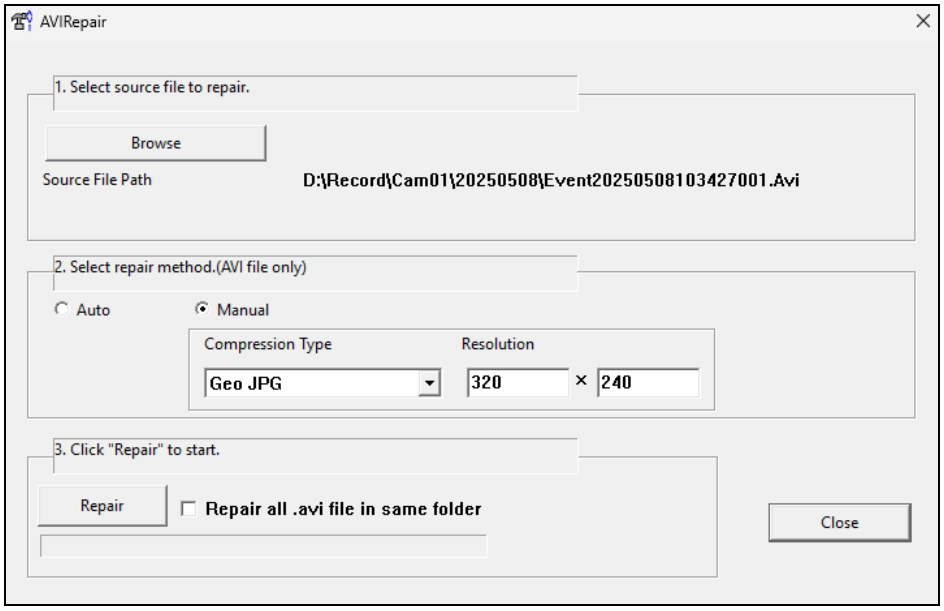
5.5 Repairing Damaged Video Files

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

Tip: If the computer was not shut down properly, the first thing you should do before starting the system is to run the **Repair Database Utility** (see *Repairing Damaged File Paths* earlier in this chapter). After running the Utility, go to the ViewLog and check video events. You should be able to play all video files at this step. However, if you see a question mark after clicking on a file, the problem may be that its recording process was interrupted. To repair the file, follow the steps below to run the **AVI Repair Utility**.

---

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



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, select **Auto** but it takes longer to repair with this selection.
4. Optionally select **Repair all .avi file in same folder**.
5. Click the **Repair** button to start.

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

Distorted Image **No Image** **lete Image**



7. When a complete image is displayed, click the arrow button to preview the file.
8. Click **Yes** to start the repair.
9. Click **Yes** to overwrite or **No** to save this file to another path. Note that if you choose **No** at this step, remember to run the **Repair Database Utility** again after exiting this program. For details, see *Repairing Damaged File Paths* earlier in this chapter.

Chapter 6

I/O Applications 244

6.1 Setting up I/O Devices 244

6.1.1 Adding I/O Devices 245

6.1.2 Setting up the Input and Output Devices 246

6.1.3 Latch Trigger 248

6.1.4 Keeping Last Toggle Status 250

6.1.5 Setting up PLC I/O devices 252

6.2 Advanced I/O Applications 254

6.2.1 Setting up Actions upon Input / Output Trigger 255

6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger 256

6.2.3 Setting up Momentary and Maintained Modes 257

6.2.4 Deactivating Alarm and Alert upon Input Trigger 258

6.2.5 Other I/O Application Functions 259

6.3 I/O Devices in Content List 260

6.4 Visual Automation 261

CHAPTER

6

I/O Applications

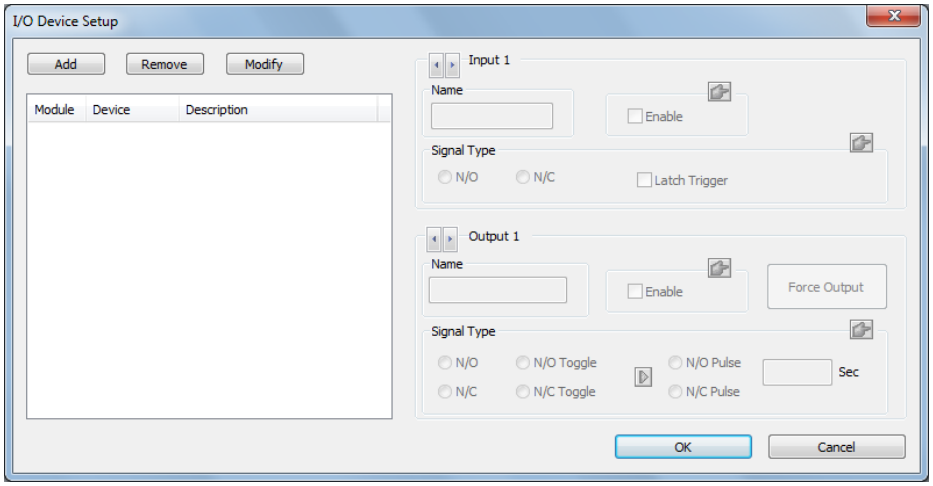
This chapter describes how to configure and control the system's I/O devices. I/O applications include the following features:

- Record video, send e-mail notifications and trigger output upon input trigger
- Move PTZ camera to a preset location upon 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 up I/O Devices

To connect the I/O device to the computer of the system, you may need additional devices: GV-NET Card, GV-NET/IO Card or GV-I/O Box. For details, visit the GeoVision Website.

To set up I/O devices on the system, click **Home** > **Toolbar** > **Configure** > **Accessories** > **I/O Device** (if available) > **I/O Device Setup**. The I/O Device Setup dialog box appears.



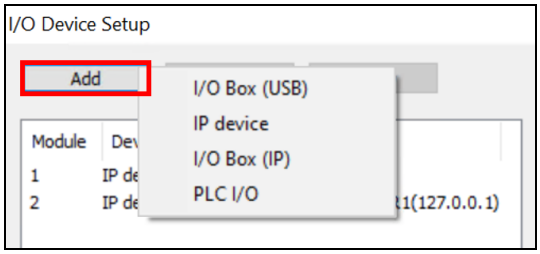
I/O Device dialog box

Note: The **I/O Device Setup** option appears only after at least one I/O device has been added.

Tip: To set up I/O devices, you can also expand **I/O Device** in the Content List and select **Configure** > **I/O Device Setup**.

6.1.1 Adding I/O Devices

To add an I/O device to the system, click the **Add** button in I/O Device Setup dialog box.



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

- **I/O Box (USB):** Select if the system is connected to 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.

- **IP Device:** The system can remotely control the I/O devices connected to GV-IP Devices through network connection. Select GV-IP Device with I/O devices installed and click the >> button.

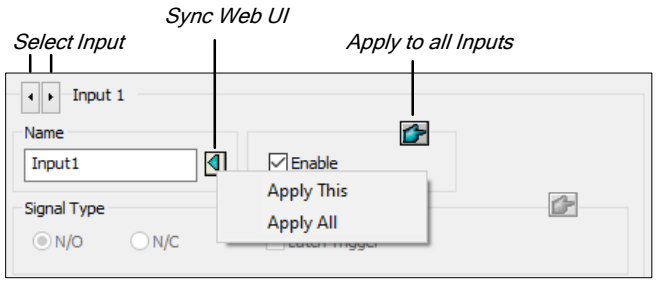
- **I/O Box (IP):** The system can remotely control the I/O devices connected to GV-I/O Box through network connection.
  1. Click the **Search** button to search for available devices under LAN or click the **Add** button to manually type the connection information of the device.
  2. Select the device and click the >> button. Type the **User Name** and **Password** if needed.

- **PLC I/O:** PLC I/O devices are supported. For details, see *Setting Up PLC I/O devices* later in this section.

6.1.2 Setting up the Input and Output Devices

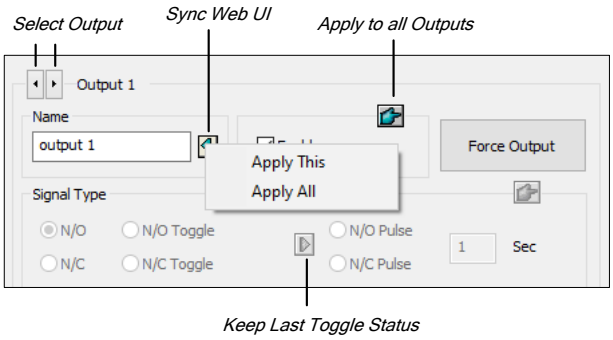
After adding the I/O device, enable the input and output devices. For GV-I/O Boxes connected through USB, you can configure the signal type on the system. For GV-IP Devices and GV-I/O Boxes connected through TCP/IP, you will have to configure the signal type on the device's Web interface.

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



- **Name:** Name each input pin. Click the left Arrow button and select **Apply This** to sync the name of the specified input pin with that on the I/O device's Web interface. Optionally select **Apply All** to sync all names of the input pins with the ones on the I/O device's Web interface.
- **Signal Type:** Select a signal type for your input device: N/O (normally open), N/C (normally closed), or Latch Trigger. For details on Latch Trigger, see *Latch Trigger* later in this section.

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

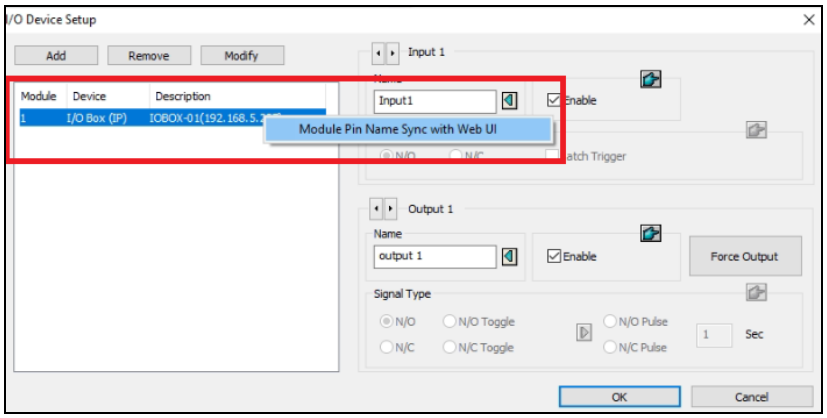


- **Name:** Name each output pin. Click the left Arrow button and select **Apply This** to sync the name of the specified output pin with that on the I/O device's Web interface. Optionally select **Apply All** to sync all names of the output pins with the ones on the I/O device's Web interface.
- **Force Output:** Click to test the 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 section.

Note:

1. PTZ camera and I/O devices cannot be assigned to the same port at the same time.
2. To sync all input / output pin names with those on I/O device's Web interface, right-click the I/O device on the list and select **Module Pin Name Sync with Web UI**.

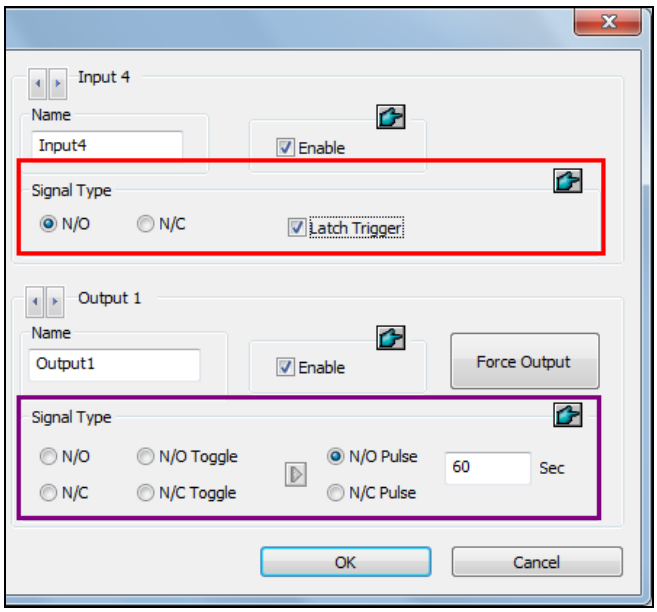


6.1.3 Latch Trigger

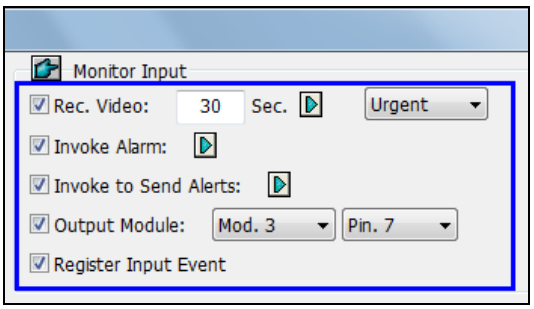
Instead of constant output alarm in N/O and N/C during the input trigger, the Latch Trigger option provides a momentary output trigger.

Setting up Latch Trigger

In the I/O Device Setup dialog box (see the dialog box in *Setting Up I/O Devices* earlier in this chapter) , select **Latch Trigger**.



I/O Device Setup



I/O Application Setting

Application Example

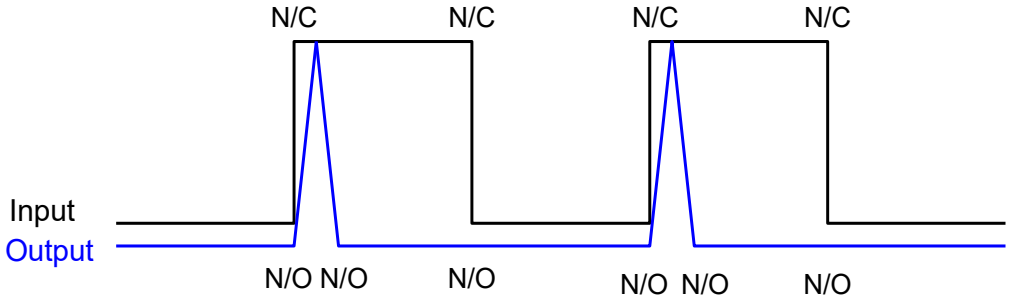
In the above scenario, Input 4 is set to N/O and Latch Trigger. When Input 4 is triggered:

- 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).
- 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.

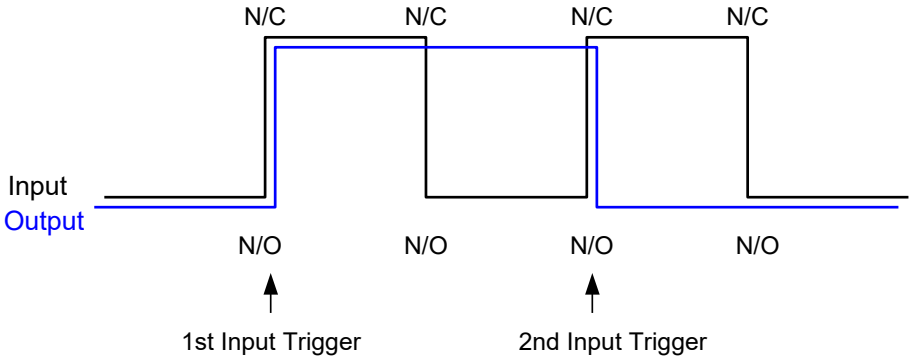
1. N/O (Normal Open) + Latch Trigger

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



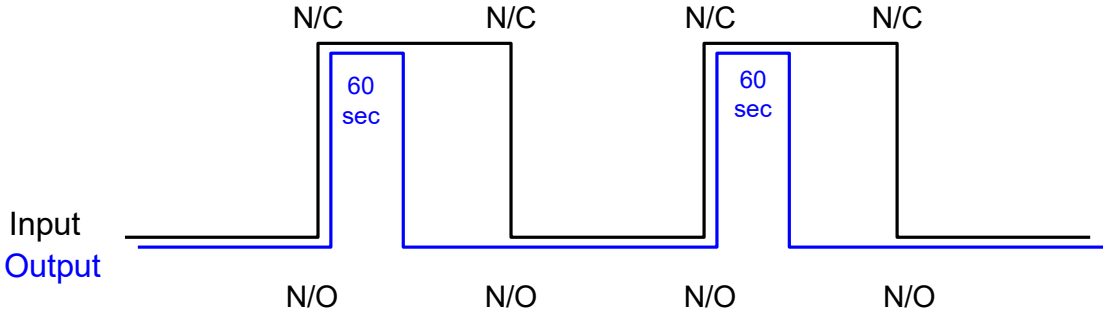
2. N/O Toggle + Latch Trigger

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.

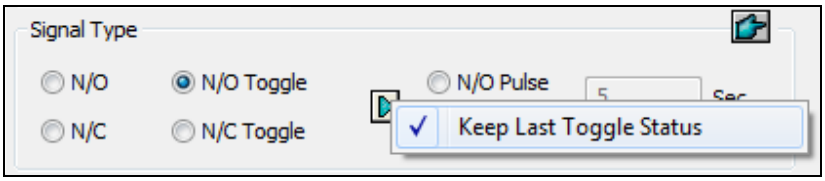


6.1.4 Keeping Last Toggle Status

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 Setup dialog box (see the dialog box in *Setting Up I/O Devices* earlier in this chapter), select **N/O Toggle** or **N/C Toggle**, and click the **Arrow** button on the right to select **Keep Last Toggle Status**.

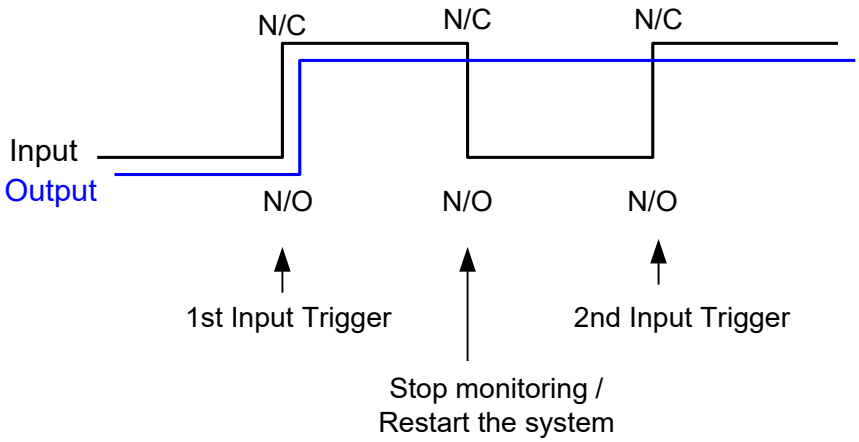


Application Example

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

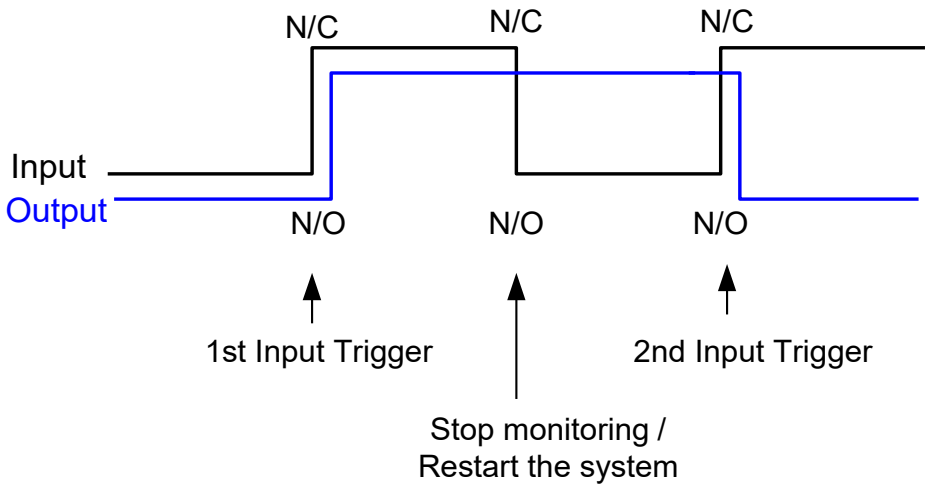
1. Input (N/O) + Output (N/O Toggle + Keep Last Toggle Status)

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



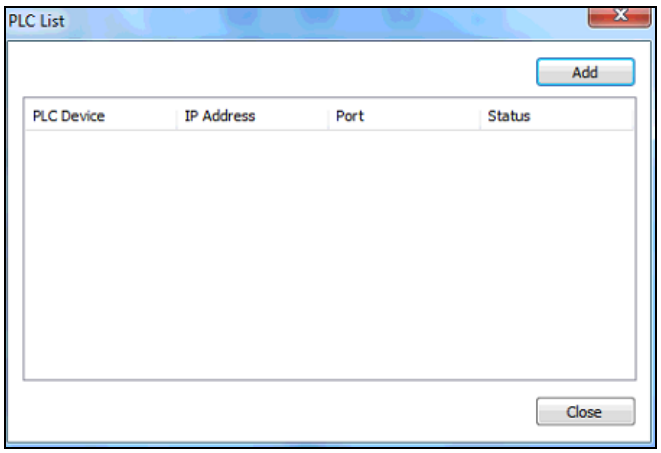
2. Input (N/O + Latch Trigger) + Output (N/O Toggle + Keep Last Toggle Status)

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.



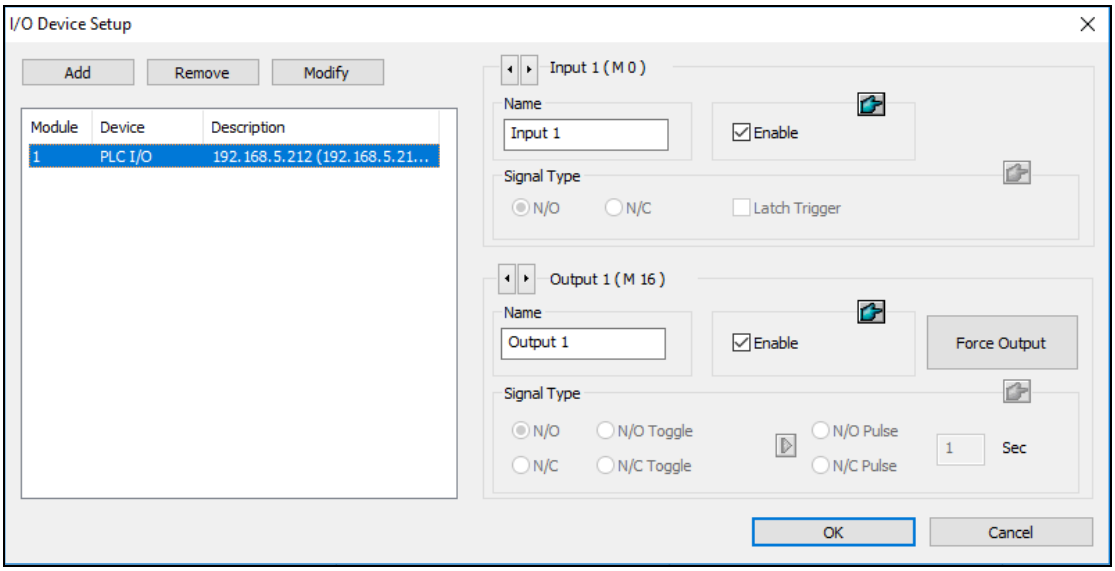
6.1.5 Setting up PLC I/O devices

1. To connect a PLC I/O device to the system, click **Home** > **Toolbar** > **Configure** > **Accessories** > **PLC Device Setup**. This window appears.



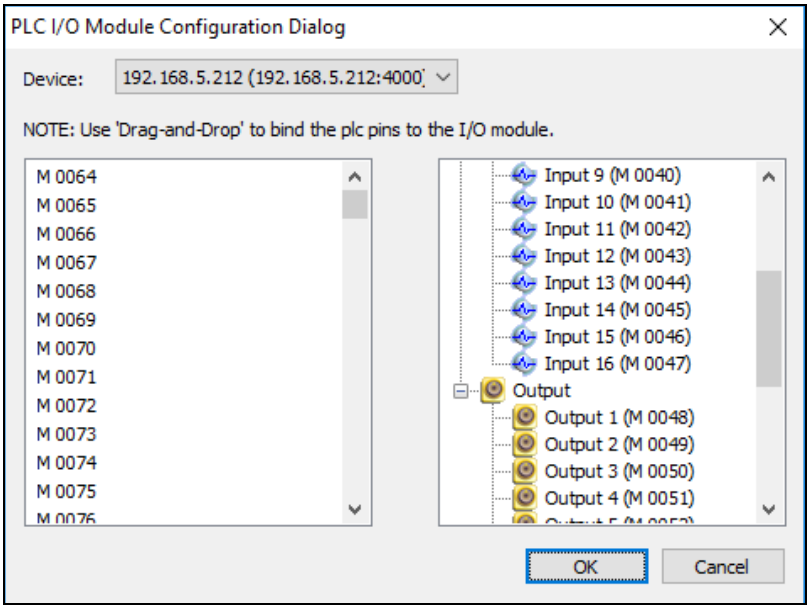
2. To add a PLC device, click the **Add** button, enter the following information: **Name**, **IP Address**, **Port**, **Password**, **M-Pin Range**, and **Connection Type**. The M-Pin Range supports up to 999,999 pins.

3. To bind the M-pins, click **Home** > **Toolbar** > **Configure** > **Accessories**, and select **I/O Device Setup**, When the I/O Device Setup dialog box appears, select the PLC device, click the **Add** button and select **PLC I/O**.



4. In the PLC I/O Module Configuration Dialog, drag the pins on the left-hand side to the I/O module on the right-hand side.

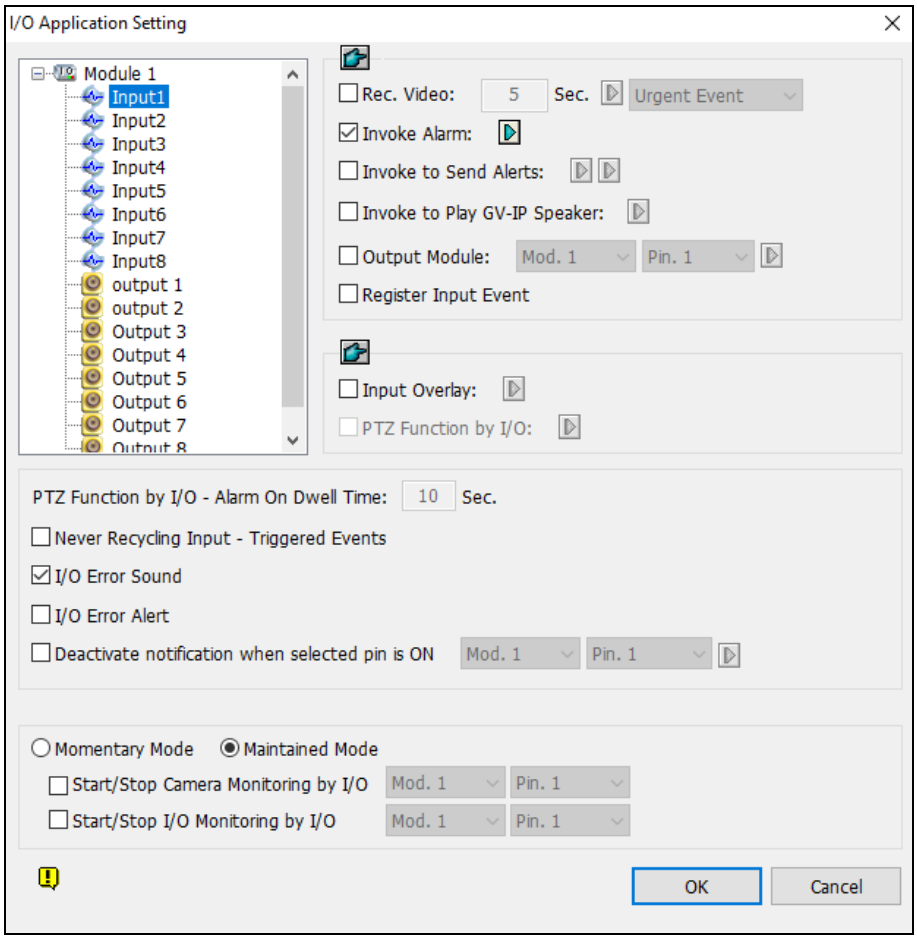
Note: Every Input/Output module can only support up to 16 pins. To use other pins, add more I/O modules.



6.2 Advanced I/O Applications

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

Click **Home** > **Toolbar** > **Configure** > **Accessories** > **I/O Device** (if available) > **I/O Application Setting**. This dialog box appears.



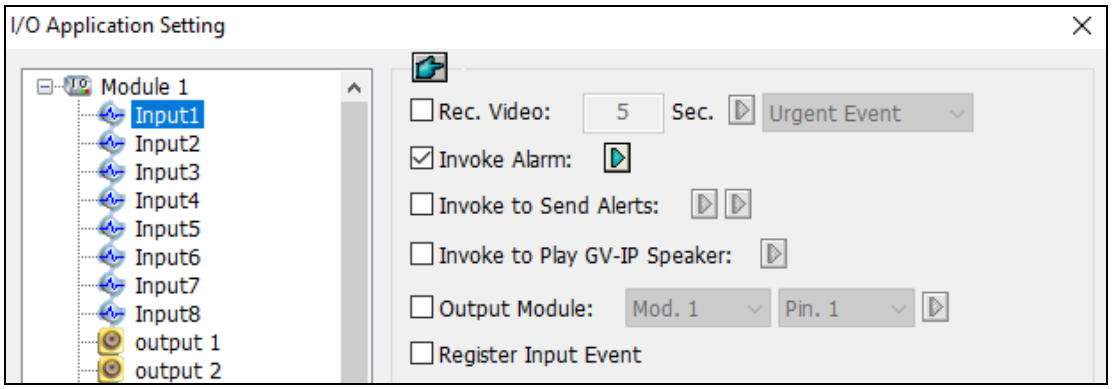
Note:

1. The **I/O Device** option only appears after at least one I/O device has been added.
2. To activate I/O functions after applying the settings, click **Home** > **Toolbar** > **Monitor** > **I/O Monitoring** or **Start All Monitoring**.

Tip: To configure I/O application settings, you can also expand **I/O Device** in the Content List and select **Configure** > **I/O Application Setting**.

6.2.1 Setting up Actions upon I/O Trigger

You can configure the system to perform specific actions when an input or output device is triggered. Select an I/O device on the left, and then click the Finger button to apply the same settings to all I/O devices.

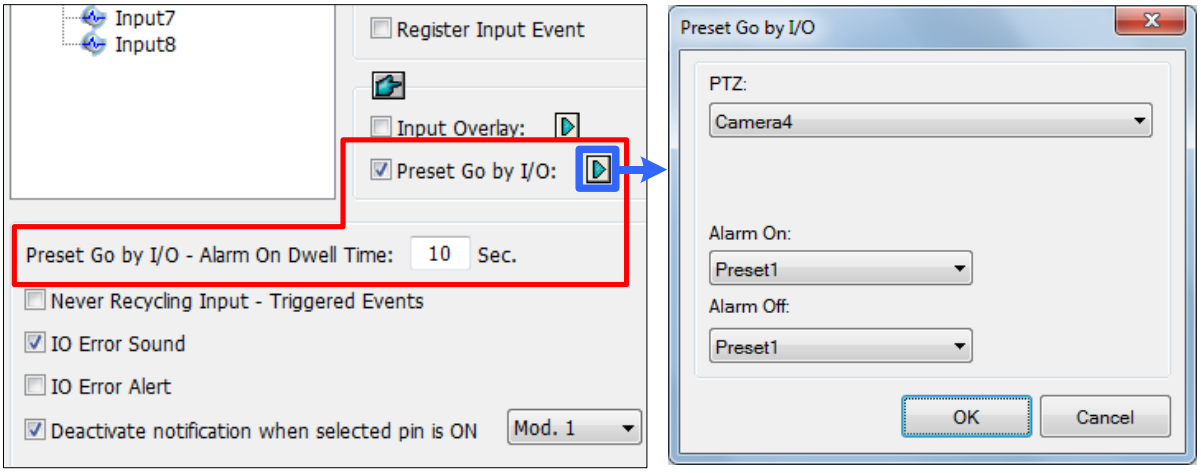


I/O Application Setting dialog box

- **Rec Video:** Records one or multiple videos when an input is triggered. Specify the recording duration, and click the **Arrow** button to select the cameras for recording. Use the dropdown list to choose between Urgent Event and General Event frame rate settings. For details on setting up Urgent and General Events, see *Configuring Abnormality Settings* in Chapter 2.
- **Invoke Alarm:** Activates a computer alarm when an input is triggered. Click the **Arrow** button to select an alarm sound.
- **Invoke to Send Alerts:** Sends email notifications when triggered by an I/O device. Click the first **Arrow** button to select the associated camera channel for video to be sent. Click the second **Arrow** button to specify the recipient's email address. To attach a video to the email, it is required to first enable **Attach Image Setup** in the email setup. See *Setting up E-Mail Notifications* in Chapter 1.
- **Invoke to Play GV-IP Speaker:** Activates the GV-IP Speaker to play audio files when triggered by an input or output device. Click the **Arrow** button to select a GV-IP Speaker and assign an audio file and play mode.
- **Output Module:** Triggers the specified output module when an input is activated. Use the dropdown lists to select the output module and pin number. Click the **Arrow** button to enable Delay for Deactivation and configure the Delay Time.
- **Register Input Event:** Registers input trigger events into the System Log. Each event is labeled with ID, time, device name (camera or input device), corresponding module of the device, and event for later retrieval. For details on the System Log, see *System Log* in Chapter 1.

6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger

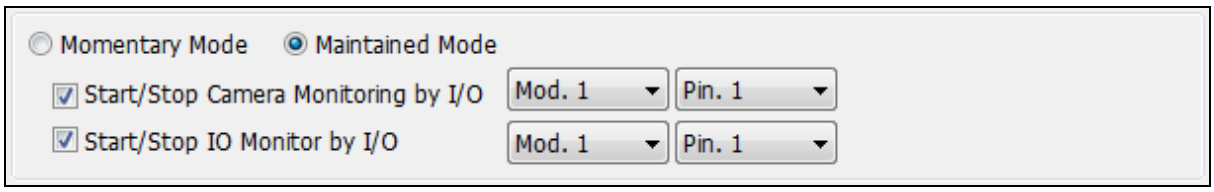
This feature allows you to move the PTZ camera to preset points when an input is triggered. Select an input number to be set up.



- **PTZ Function by I/O:** Enable the option and click the **Arrow** button to select your PTZ camera from the dropdown list.
- **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.
- **PTZ Function by I/O - Alarm On Dwell Time:** Specify the amount of time (in seconds) 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 up Momentary and Maintained Modes



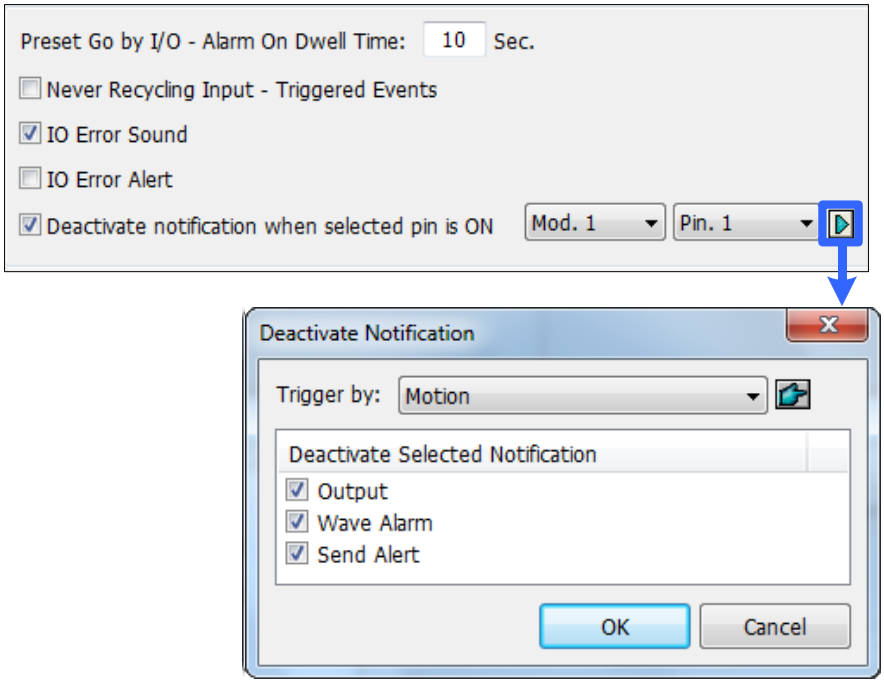
[Momentary Mode] Push button switches that are normally open and stay closed as long as the button is pressed. Momentary switches allow turn-on or turn-off from multiple locations.

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



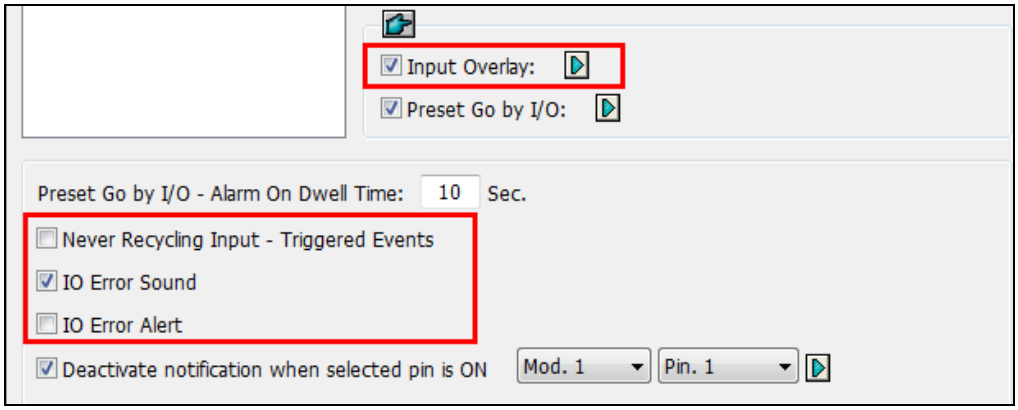
[Deactivate notification when selected pin is ON] When an assigned input module is activated, all designated alarms and alerts will be disabled. Assign an installed input module and a pin number for the application.

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

- **Triggered by:** Select an alert condition from the dropdown 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, I/O error alerts, and whether to recycle input-triggered events. Select an Input number to configure.



[Input Overlay] Select to overlay the name of an input device on live video for alert or save the name to video files upon the input trigger. To map cameras with the input device, click the **Arrow** button to select the camera.

To overlay the name of a triggered input on live video:

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**.
2. In the dialog box that appears, select **Text Overlay Setting** under the Video Analysis tab, select the camera, and click **Setting**.
3. Select **Print on screen (Only for I/O alarm)** or **Print on video file**. Up to 5 input names can be stamped on one camera channel when inputs are triggered.

[Never Recycling Input-Triggered Events] When selected, the system will not recycle the files recorded by the input trigger if the disk space is full.

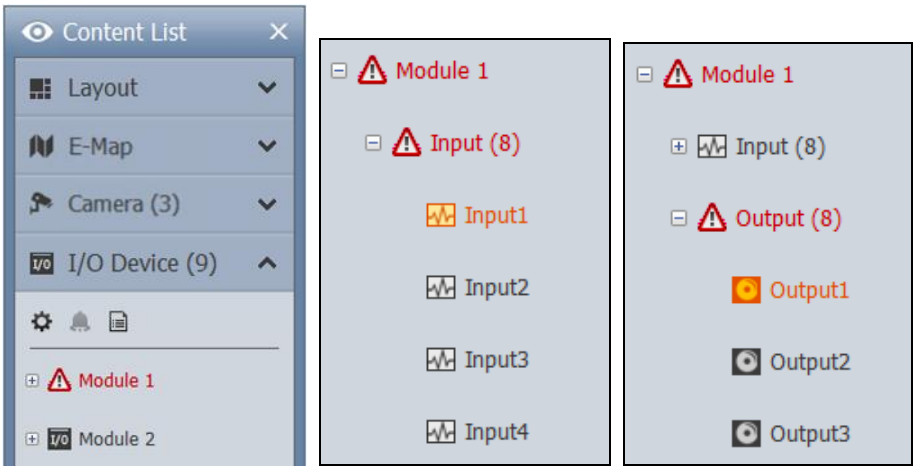
[I/O Error Sound] Enabled by default. The computer alarm will sound if the connected I/O device is not detected.

[I/O Error Alert] When enabled, the system will send e-mail notifications if the connected I/O device is not detected. To configure the e-mail server, see *Setting up E-mail Notifications* in Chapter 1.

6.3 I/O Devices in Content List

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

1. To display the Content List, click **Home** > **Toolbar** > **Content List** .
2. Click **I/O Device** to see the I/O devices added to the system. When an input or output is triggered, its icon will light up in the I/O Device list.

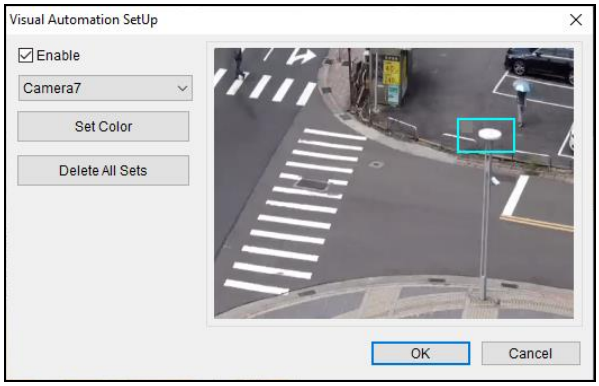


3. You can force the output device to be triggered by clicking its icon . Another way to trigger an output is to select an output and click the **Force Output** button .
4. To manually turn off a triggered output, right-click the triggered output in the list and click **Reset**.

6.4 Visual Automation

The Visual Automation helps you automate any electronic device by triggering the connected output. 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** > **Toolbar** > **Configure** > **Accessories** > **I/O Device** (if available) > **Visual Automation Setting**. This dialog box appears.



2. Select a camera from the dropdown list, and select **Enable**.
3. Drag a region on the camera view. A dialog box appears.
4. Select the connected module and output device. Type a **Note** to help you identify the device.
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.

On the main screen, move the cursor to the camera view with the Visual Automation settings, and click **Tools** > **I/O Automation**. Next, click the region 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.



Tip: To access Visual Automation settings, you can also expand **I/O Device** in the Content List and select **Configure** > **Visual Automation Setting**.

Chapter 7

Remote Viewing.....263

7.1 Remote Viewing using a Web Browser 264
7.2 WebCam Server Settings 267
7.2.1 General Settings 267
7.2.2 Server Settings 268
7.2.3 Video Settings 269
7.2.4 Audio Settings 270
7.2.5 JPG Settings 271
7.2.6 UPnP Settings 272
7.2.7 Network Port Information 273
7.2.8 Mobile Service 274
7.3 Single View Viewer 275
7.3.1 Adjusting Video Quality 277
7.3.2 Control Panel 278
7.3.3 Configuring Single View Viewer Options 279
7.3.4 PTZ Control Panel 282
7.3.5 Visual PTZ Control 283
7.3.6 I/O Control 284
7.3.7 Visual Automation 285
7.3.8 Picture-in-Picture View 286
7.3.9 Picture-and-Picture View 287
7.4 Multi-Window Viewer 288
7.5 JPEG Image Viewer 289
7.6 Remote Playback and Query 290
7.6.1 Event List Query 290
7.6.2 Remote Playback 291
7.7 Download Center 292
7.8 Remote ViewLog 293
7.9 GV-Cloud 294
7.10 GV-Edge Recording Manager 296
7.11 Mobile Phone Applications 297

CHAPTER

7

Remote Viewing

With a Web browser, you can remotely view live video, download and play back video files, as well as controlling PTZ cameras and I/O devices, through the WebCam Server.

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

OS	64-bit	Windows 7 / 8 / 8.1 / 10 / Server 2008 R2 / Server 2012 R2 / Server 2016 / Server 2019
CPU		4th Generation i5-4670, 3.4 GHz
Memory		8 GB RAM
Hard Disk		80 GB
Network		TCP/IP
Web Browser		IE 7.0 or later Chrome V38.0.2125.111 or later Firefox 30.0 or later Edge V20 or later
DirectX		9.0c

Note: Some remote functions may not be supported by non-IE browsers. However, users can download the **Web Viewer** from non-IE browsers to access the full functions of the WebCam Server.

7.1 Remote Viewing using a Web Browser

The system has a built-in WebCam Server that allows you to remotely view and manage the camera images from the system using a Web browser. Different browsers have slightly different user interfaces.

Note:

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

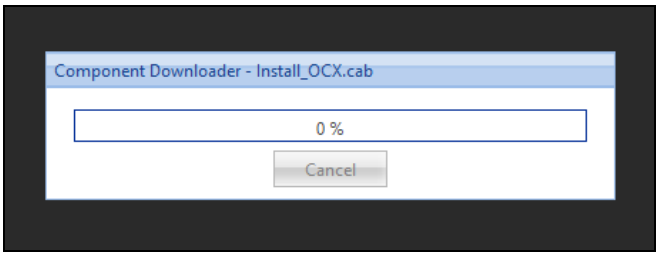
---

1. To enable the WebCam Server on the system, click **Home** > **Toolbar** > **Network** > **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 a remote computer, open a Web browser and type the IP address or domain name of the system. The WebCam Login dialog box appears.

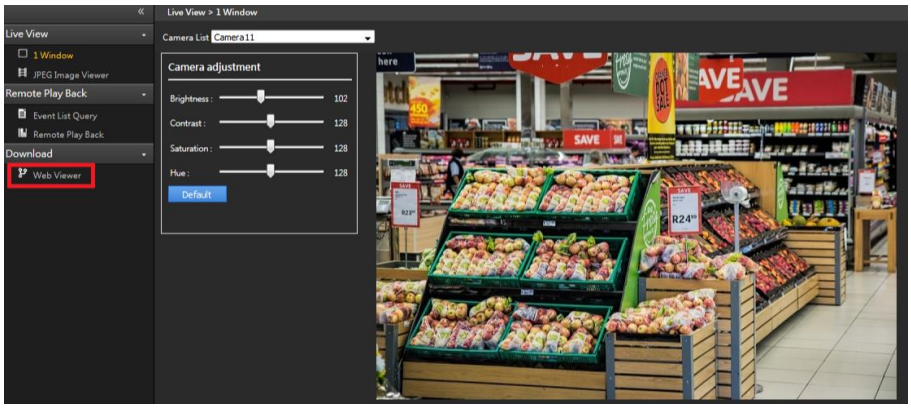
Note: If the default HTTP port 80 has been changed, type a colon and the port number after the IP address, for example, **Http://192.168.3.199:81**.

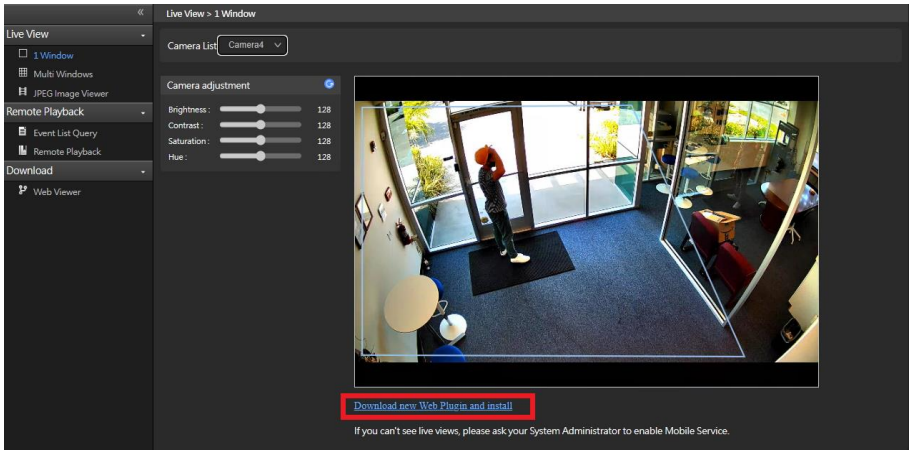
---

3. Type the user ID and password of the system.
4. Click **Login**. When accessing the remote viewer for the first time, you may need to download and install different files for different browsers.
   a. For **Internet Explorer**, download and install the plugin from the pop-up window.



b. For **Google Chrome**, **Microsoft Edge** or **Mozilla Firefox**, download and run **Web Viewer** from the left menu. After the connection to GV-AI Guard is established using the Web Viewer, you can enjoy complete functions of the WebCam Server. Optionally, you can also click and download the Web Plugin from the link below the live view window to access complete functions on the Web browsers once the connection to GV-AI Guard is set up.





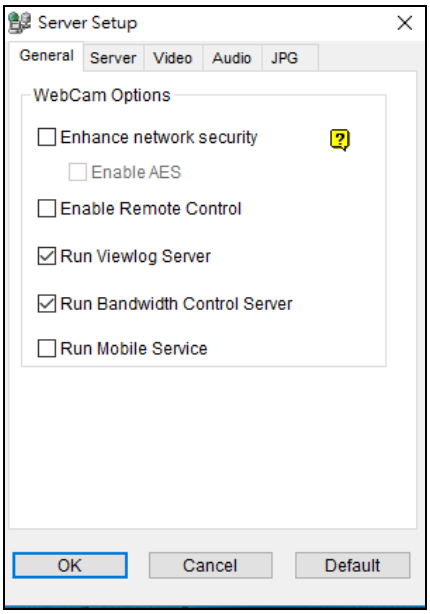
WebCam Server Features

Name	Description
Live View	Accesses different types of live view viewers. See *Single View Viewer*, *Multi-Window Viewer* and *JPEG Image Viewer* later in this chapter.
Remote Playback	Accesses remote playback options. See *Playing Back Events* later in this chapter.
Remote ViewLog	Accesses the Remote ViewLog. See *Remote ViewLog* later in this chapter.
Remote eMap	Accesses E-Maps remotely set up at the system. See *E-Map Application* in Chapter 8.
Download	Accesses the Download Center. This function offers optional viewing programs to be downloaded to the local PC. See *Download Center* later in this chapter.

7.2 WebCam Server Settings

To enable and configure the built-in WebCam Sever, click **Home** > **Toolbar** > **Network** > **WebCam Server**.

7.2.1 General Settings



The Server Setup (General) dialog box

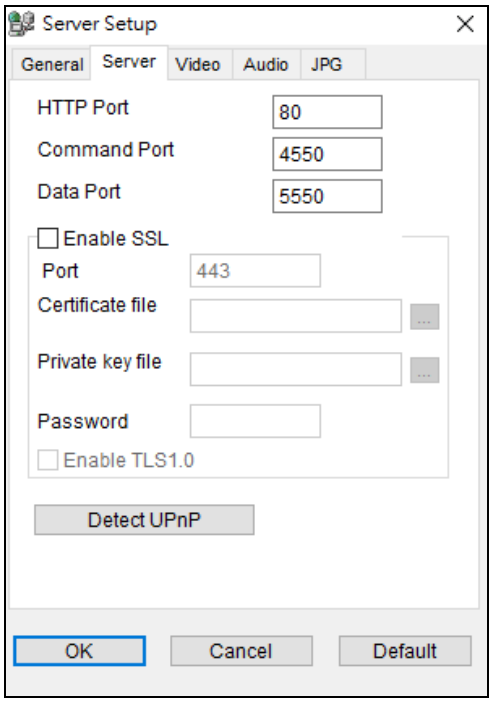
- **Enhance network security:** If enabled, a word verification step is required for each WebCam Server's login.

  ⊙ **Enable AES:** Select to add an additional security protection for live streaming between the system and WebCam Server.

- **Enable Remote Control:** Select 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 to enable the **Bandwidth Control Server**. For details, see *Bandwidth Control Application* in Chapter 9.
- **Run Mobile Service:** Select to enable the mobile function to connect to GV-Eye and GV-Edge Recording Manager (MAC Version).

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

7.2.2 Server Settings

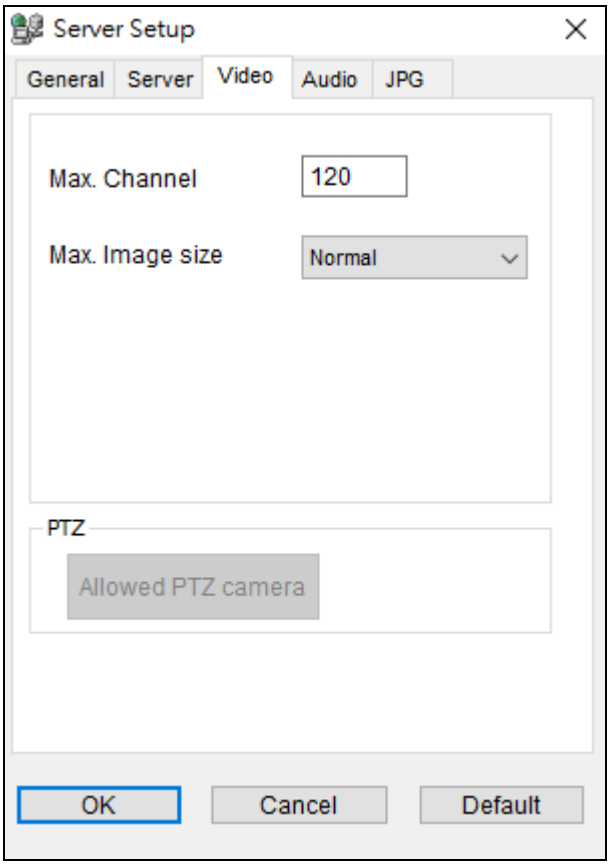


The Server Setup (Server) dialog box

- **HTTP Port:** Used to access the Internet. By default, it is 80.
- **Command Port:** Used to access WebCam. By default, it is 4550.
- **Data Port:** Used to transfer data over the Internet. By default, it is 5550.
- **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 further enable TLS 1.0 protocol when using SSL protocol, select **Enable TLS 1.0**.
- **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.

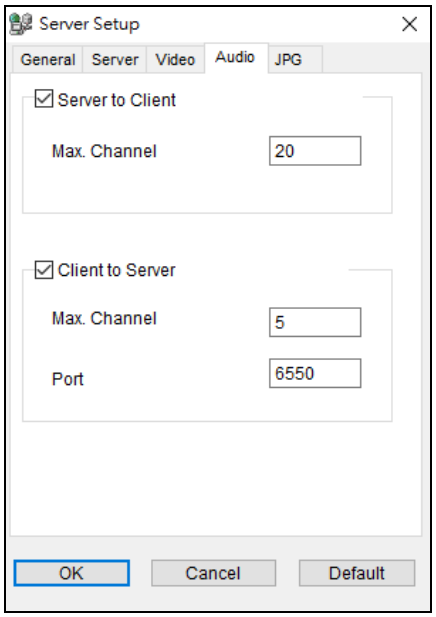
7.2.3 Video Settings



- **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 **Large** (640 x 480 or 704 x 480) and the **Actual Size** of that IP camera.
- **Allowed PTZ camera:** Controls 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



[Server to Client] Allows a remote computer to access live audio from the system.

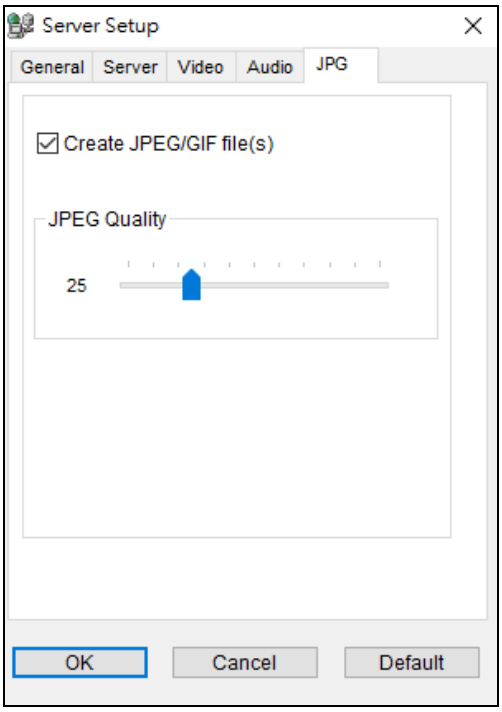
- **Max. Channel(s):** Enter the maximum number of channels allowed to access live audio, with the upper limit of 40 channels.

[Client to Server] Allows a remote computer to speak to the system.

- **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 the Internet.



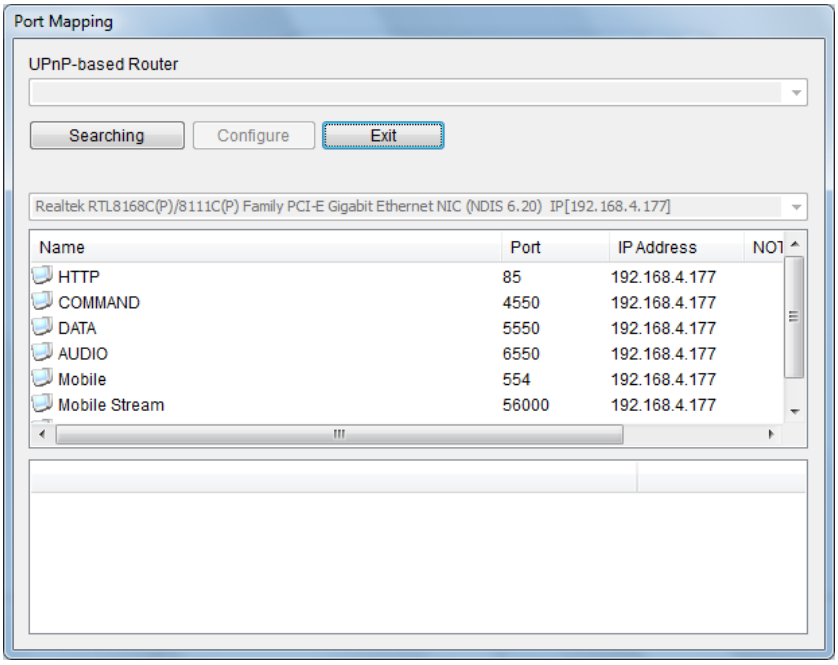
- **Create JPEG/GIF file(s):** You can access the JPEG images through WebCam Server, and adjust the image quality. Bigger number results in better image quality and bigger image file size.

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** > **Toolbar** > **Network** > **WebCam Server**. The Server Setup dialog box appears.
2. Click the **Server** tab and click **Detect UPnP**. This dialog box appears.



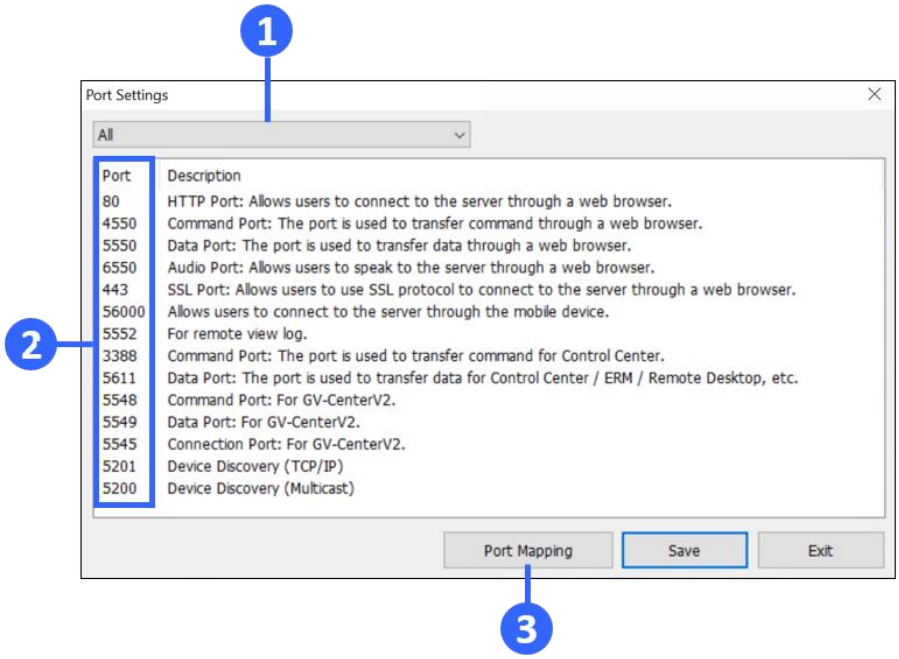
3. Click **Searching** to search the UPnP-enabled routers.
4. If your server is installed with multiple routers, select one from the UPnP Router dropdown list.
5. If you server is installed with multiple network adapters, select one from the dropdown list under the Searching button.
6. Click **Configure**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

Note: If you don't use the default ports, modify them in the Server Setup (Server) dialog box (see *7.2.2 Server Settings*) and then click **OK**. Re-open the dialog box and follow the above steps to configure your router.

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** > **Toolbar** > **Network** > **Network Port Information**. This dialog box appears.



The controls on the Port Settings:

No.	Name	Description
1	Filter	Select the application type for the port from the dropdown list.
2	Port	Displays the port value for different applications. Double-click the port to modify its port value.
3	Port Mapping	Employs UPnP (Universal Plug and Play) to allow automatic port configuration on the router. See the previous subsection *UPnP Settings*.

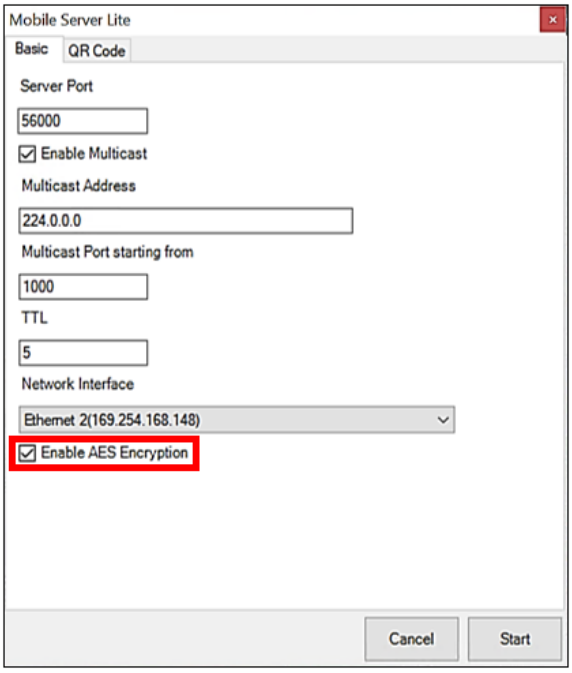
7.2.8 Mobile Service

Mobile Service allows remote connection and video streaming from the system by other applications, namely GV-Eye, GV-Edge Recording Manager – Mac version and the multicast of GV-Control Center. You can also add additional security protection for live streaming between the system and the connected application using AES Encryption.

For details on configuring multicast on GV-Control Center, see *Multicast Setting*, Chapter 9, in the *GV-Control Center User's Manual V4*.

To add AES Encryption:

1. After connecting to GV-Edge Recording Manager / GV-Control Center / GV-Eye, on the main screen of the system, click **Home** > **Toolbar** > **Network** > **Mobile Service**.
2. In the Basic settings, select **Enable AES Encryption**.

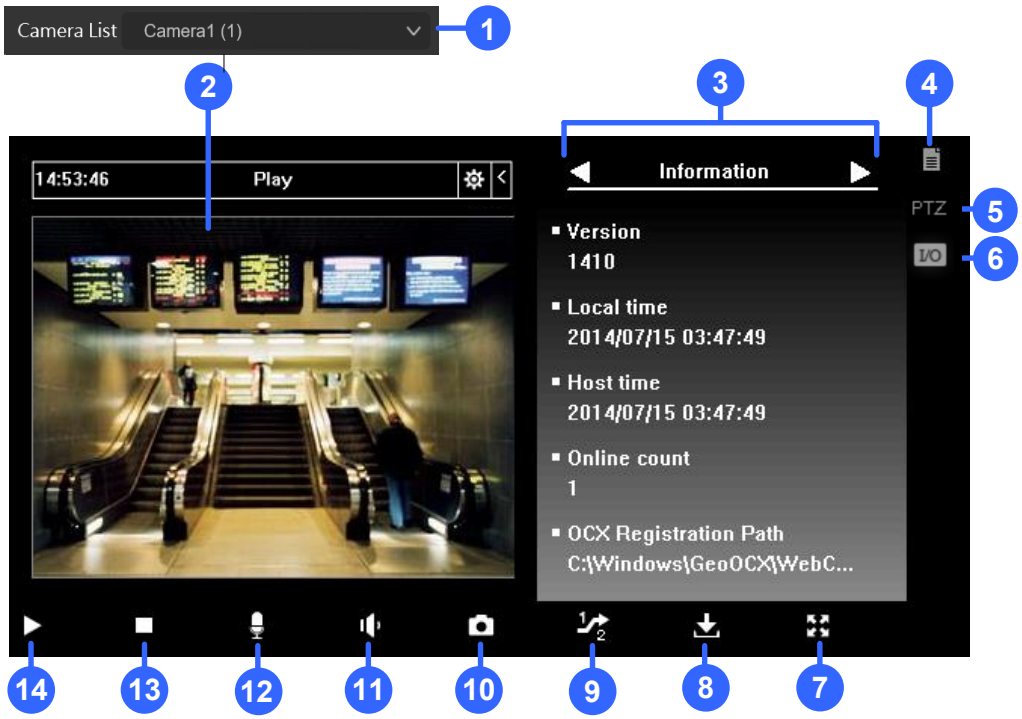


Note: The AES Encryption function is only compatible with

- GV-Edge Recording Manager V1.3.0.0 or later
- GV-Control Center V3.5.0.0 or later
- GV-Eye V2.5 or later
- WebCam Server V17.1 or later

7.3 Single View Viewer

After logging into the WebCam Server successfully, you can see the single live view from the system.



The controls in the Single View Viewer:

No.	Name	Description
1	Change Camera	Selects the desired camera for display.
2	Live View	Right-clicking on live view allows you to instantly access some useful functions. The Resolution option can display a resolution indicator at the bottom right corner of the video.
3	Control Panel	See *Control Panel* later in this chapter.
4	Options	See *Alarm Notification, Video and Audio Configuration, Server List, Show Camera Name*, and *Image Enhancement* later in this chapter.
5	PTZ Control	See *PTZ Control* and *Visual PTZ Control Panel* later in this chapter.
6	I/O Control	See *I/O Control* later in this chapter.
7	Full Screen	Switches to full screen view. The maximum video resolution configured on the WebCam Server will be applied. See *Video Settings* in *WebCam Server Settings* earlier in this chapter.
8	File Save	Saves video to a local computer in .avi format.

9	Change Quality	See *Adjusting Video Quality* later in this chapter.
10	Snapshot	Takes a snapshot of the live view.
11	Speaker	See *Video and Audio Configuration* later in this chapter.
12	Microphone	See *Video and Audio Configuration* later in this chapter.
13	Stop	Terminates the connection to the remote GV-AI Guard.
14	Play	Connects to the remote GV-AI Guard.

Displaying Full-Screen Live View on Other Monitors

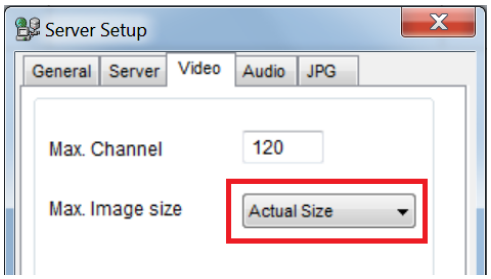
Using the IE browser, you can display up to 10 full-screen channels with multiple monitors installed. Right-click the live view and select a designated monitor to bring full-screen live view. The full-screen live view appears on the designated monitor immediately.

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

7.3.1 Adjusting Video Quality

To adjust the live view quality to have megapixel resolution in the Single View Viewer:

1. Select **Actual Size** on the system. Click **Home** > **Toolbar** > **Network** > **WebCam Server** > the **Video** tab > select **Actual Size** in the Max. Image Size option.



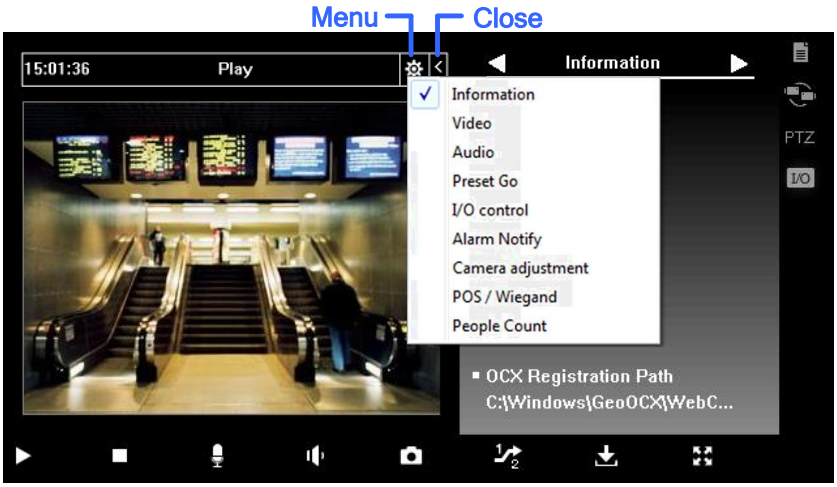
2. On the Single View, click the **Change Quality** button (see No. 9, *Single View Viewer* earlier in this chapter). You will have the option of megapixel resolution now.

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**. For details on the fisheye settings, see *Fisheye View* in Chapter 2.

7.3.2 Control Panel

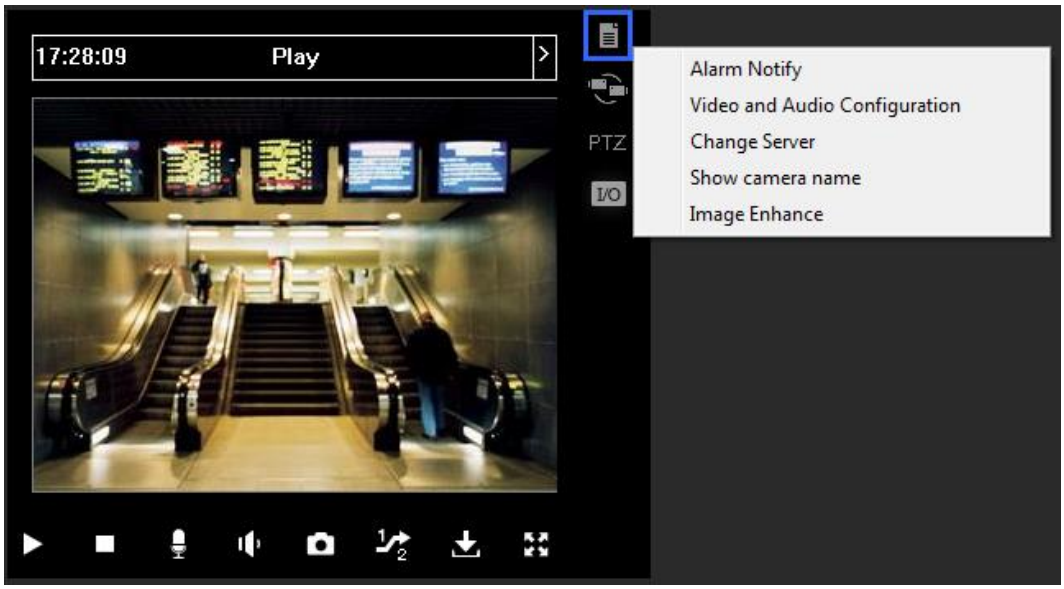
A control panel can be opened next to the live view by clicking the **Menu** button and selecting any of the options. To change the pages of the control panel, use the right and left arrow buttons on the panel, or click the **Menu** button to directly make selection.



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 system.
Alarm Notify	Displays the captured images by sensor triggers and/or motion detection. See *Alarm Notification* later.
Camera Adjustment	Remotely adjusts image quality by moving the slider to the desired values.
POS/Wiegand	Not functional.
People Count	Views the counts of Object Counting along with live view. Once the counts are logged into the system, **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 **Option** button located on the right of the live view.



Alarm Notification

Up to four captured images can be shown in the control panel upon motion detection or input trigger.



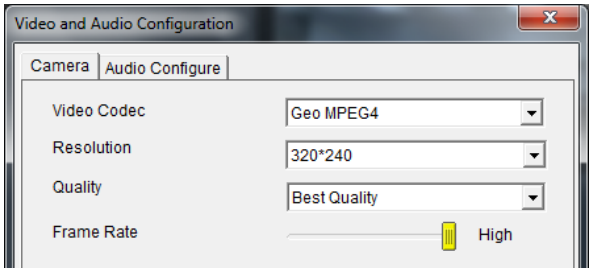
1. Click the **Option** button, and select **Alarm Notify.** The Alarm Notify dialog box appears.
   - **Motion Notify:** The captured images are displayed in the control panel of the Single View upon motion detection.
   - **I/O Alarm Notify:** The captured images are displayed in the control panel of the Single View upon input-triggered detection.
   - **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.

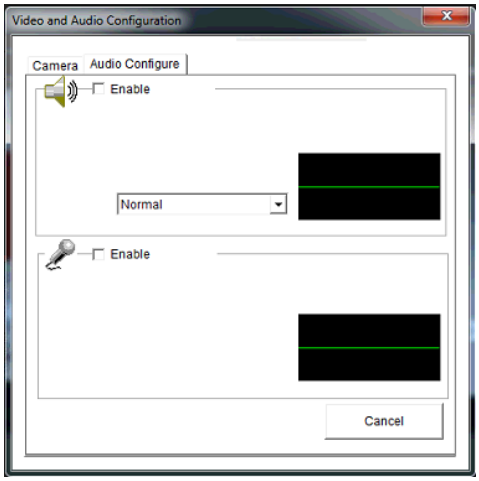
- **File Path:** Assigns a path to save the snapshots.

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**.





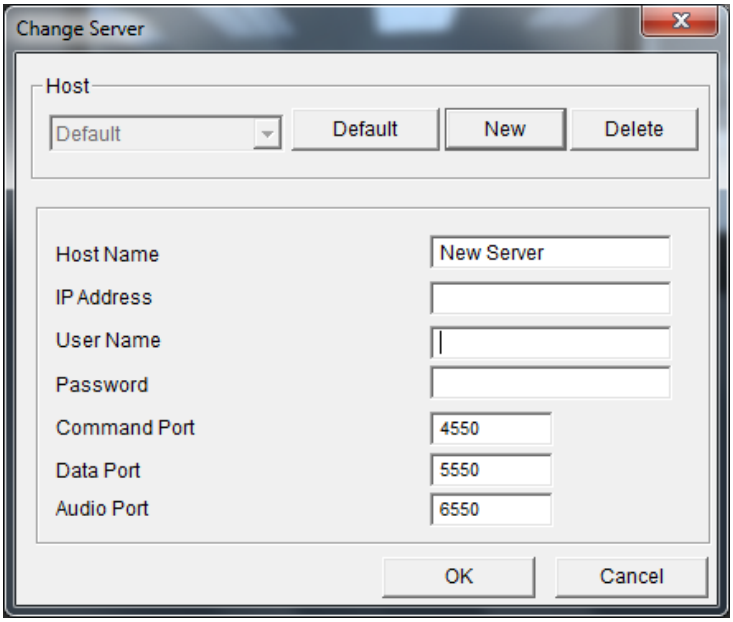
[Camera] Change the video codec, quality and frame rate. The resolution options depend on the maximum image size set on the connected system. For details, see *Video Settings* in *WebCam Server Settings* earlier in this chapter.

[Audio Configure] 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 (see *7.2.4 Audio Settings*) 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.

Server List

You can add the connection information of multiple GV-AI Guard systems to the WebCam Server for quick access later. Click the **Option** button > **Change Server** to display the following dialog box.



To add a GV-AI Guard system to the dropdown list, click the **New** button and type its connection information. Leave all port settings as defaults at **4550**, **5550**, and **6550** respectively unless otherwise necessary. Click the **OK** button. Then the created GV-AI Guard system will appear in the Host dropdown list.

Show Camera Name

To show camera name on top-left corner of the live view, click the **Option** button and select **Show Camera Name**.

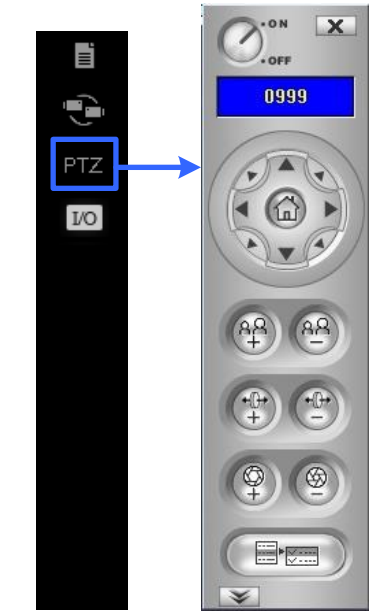
Image Enhancement

To enhance the image quality of live view, click the **Option** button and select **Image Enhance**.

- **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:** Enabled by default to enhance image quality. Some graphics cards might not support DirectDraw and can produce distorted frames. In this case, 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 (see No. 5, *Single View Viewer* earlier in this chapter) to bring up the 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 logon user and then to the next user in queue.

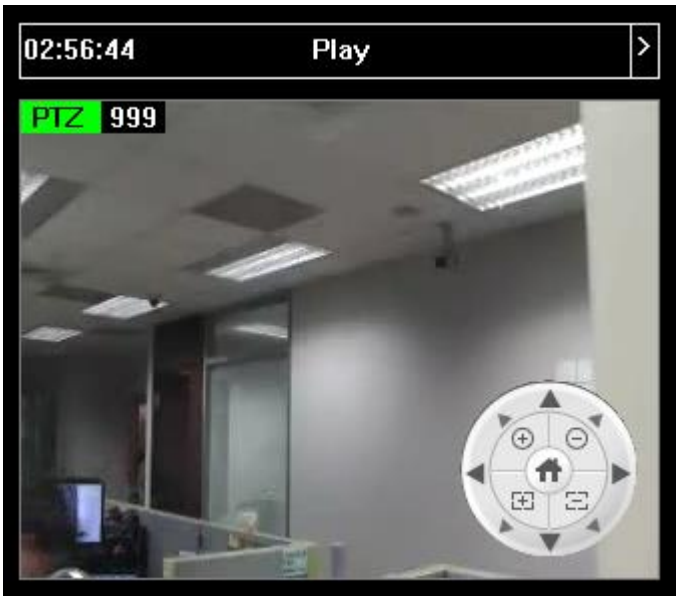
Each user will be given 60 seconds to control the PTZ camera. The Timer at the upper right corner informs the user of the remaining time of control or the total waiting time. The supervisor is given 666 seconds, which the highest priority to control the PTZ camera.

Click the  button to access additional PTZ functions. The functions available vary, depending on the PTZ models.

7.3.5 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:

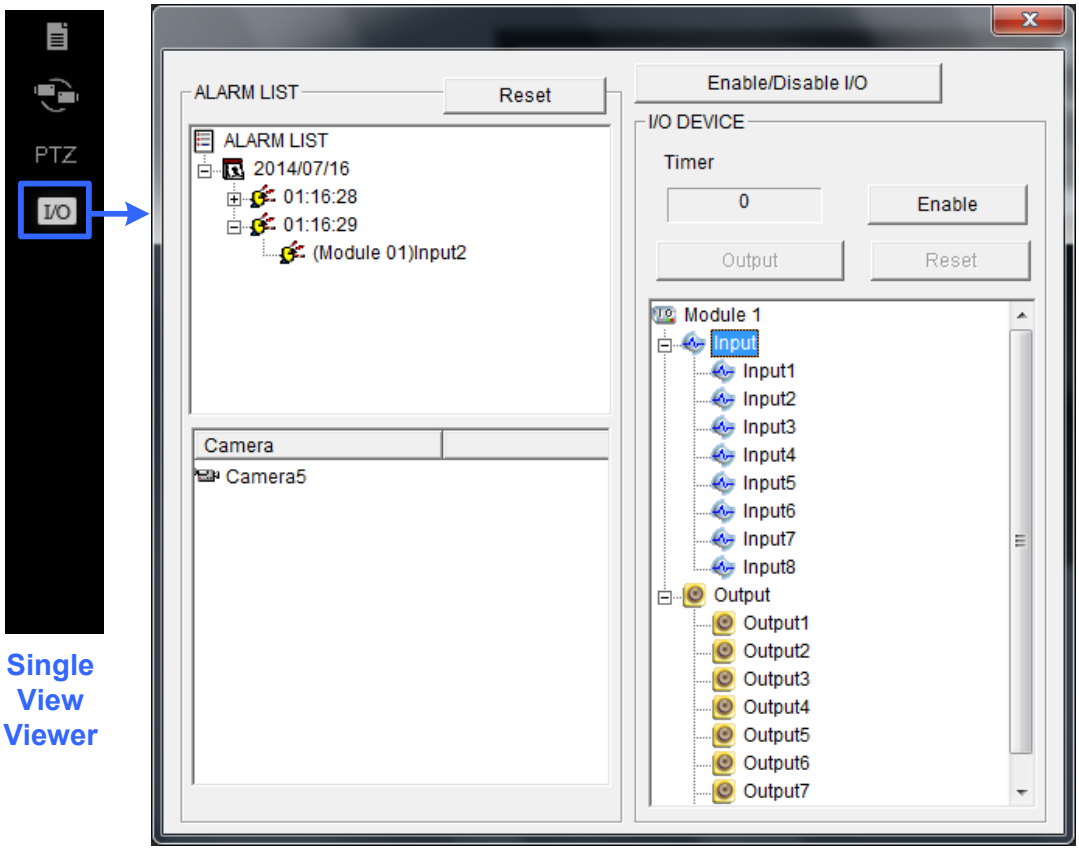
- **Random Move:** You can move the camera view to any direction by clicking on a desired direction. When you place the mouse cursor on the live view, a circular PTZ control panel appears. See *PTZ Control Panel and Auto Functions* in Chapter 1 for details on the circular PTZ control panel.



- **Center Move:** Only for GV-SD220, you can zoom in and out using the mouse scroll or by drawing a block directly on the live view.

7.3.6 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-AI Guard system. Click the **I/O Control** button at the right of the live view to bring out the I/O control panel.



Single View Viewer

I/O Control Panel

The alarm status shows the triggered inputs. Clicking the **Reset** button will clear the alarm list.

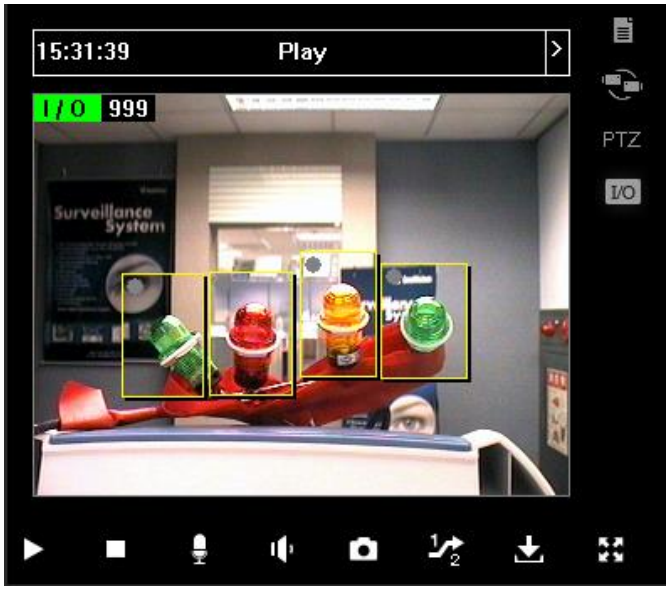
To force to trigger an output device, click the **Enable** button, highlight an output and then click the **Output** button. The Timer functions the same as in the PTZ control panel. Each user will be given 60 seconds of control time while the supervisor has 999 seconds. Clicking the **Stop** button 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 connected to the remote GV-AI Guard, click the **Enable/Disable I/O** button. Note that the **Enable Remote Control** option must be enabled beforehand in the Server Setup dialog box (see *General Settings* earlier in this chapter).

7.3.7 Visual Automation

If the Visual Automation function is enabled on the system, 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.



7.3.8 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 select **PIP**. An inset window of the camera view appears in the live view.



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.

7.3.9 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 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.

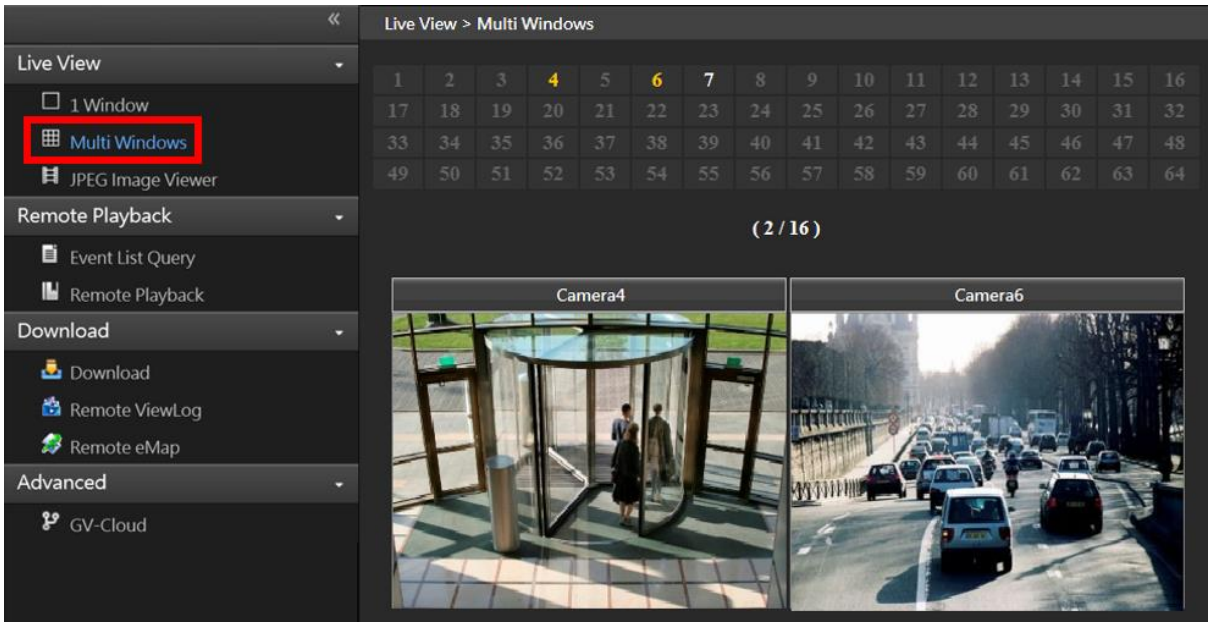


3. To exit the PAP view, right-click the live view and select **PAP** again.

7.4 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 GV-WebCam Server, and select **Multi Windows**.



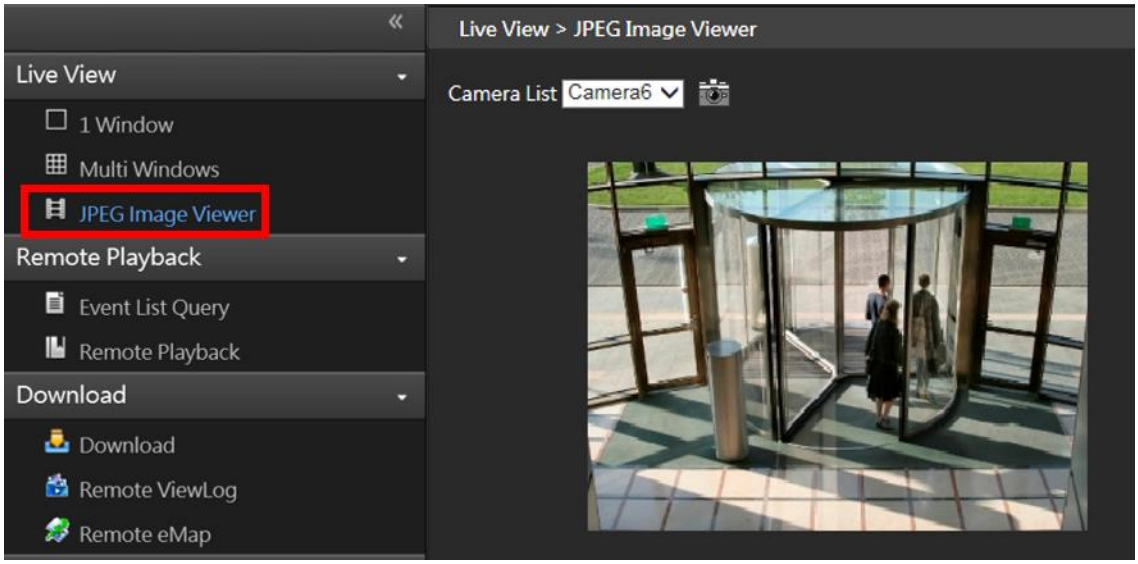
7.5 JPEG Image Viewer

JPEG Image Viewer is a cross-platform viewer, compatible with Mac OS and Microsoft IE browsers. Continuously receiving JPEG images from the system and limited to a single camera view, the viewer is an ideal tool for users with limited Internet bandwidth.

Note: To enable the JPEG Image Viewer, Java needs to be installed on the local PC.

To enable the viewer:

1. Click **Home** >**Toolbar** > **Network** > **WebCam Server**.
2. Disable **Enhance Network Security** under the General tab (see *General Settings* earlier in this chapter), and enable **Create JPEG/GIF File(s)** under the JPG tab (see *JPG Settings* earlier in this chapter).
3. Access the system using a Web browser.
4. On the left panel of GV-WebCam Server, click **Live View** and select **JPEG Image Viewer**. The JPEG Image Viewer appears.



7.6 Remote Playback and Query

7.6.1 Event List Query

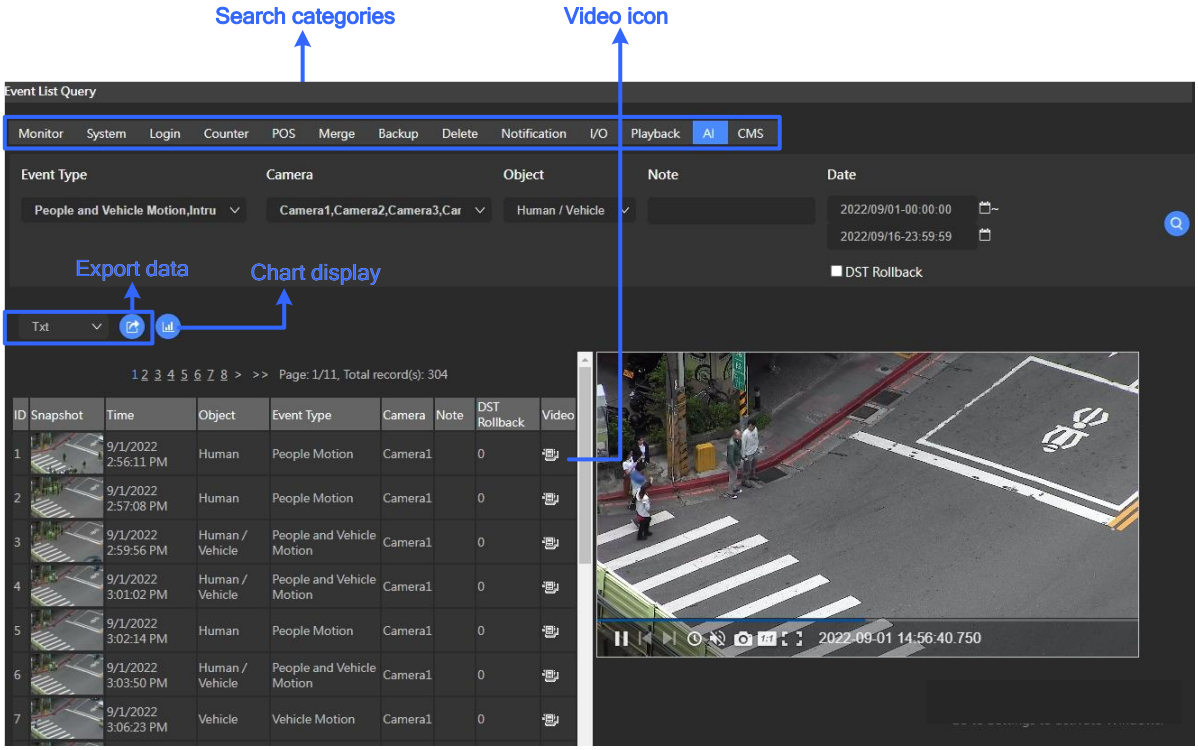
The Event List Query on the WebCam Server allows you to remotely search for events by defining event type and time. The search results can be displayed in text form or in a chart. You can also play back events instantly from the search results.

To allow remote access to the system and play back events,

- Ensure the WebCam Server with the **Run ViewLog Server** function (see *General Settings* earlier in this chapter) is activated on the system.

1. On the left panel of GV-WebCam Server, click **Remote Playback** and select **Event List Query**. The Query window appears.
2. On the top, select one of the following search categories: **Monitor**, **System**, **Login**, **POS**, **Merge**, **Backup, Delete, Notification, I/O, Playback, AI, AI Counter**, and **CMS**. Note that these categories are based on those of System Log in the Main System.
3. Define the search criteria such as Event Type, Device, Information, Date, etc. The selection of search criteria may vary, depending on search categories.

4. Click **Query**. The search results are displayed.



5. To play back the attached video, click the **Video** icon. For more playback features, right-click on the video image.
6. To graph the search results, click the **Chart** icon.
7. To export the search results, select one of the formats and click the **Export** icon.

7.6.2 Remote Playback

With the Remote Playback (RPB) function on the WebCam Server, you can play back the recorded files of the connected system.

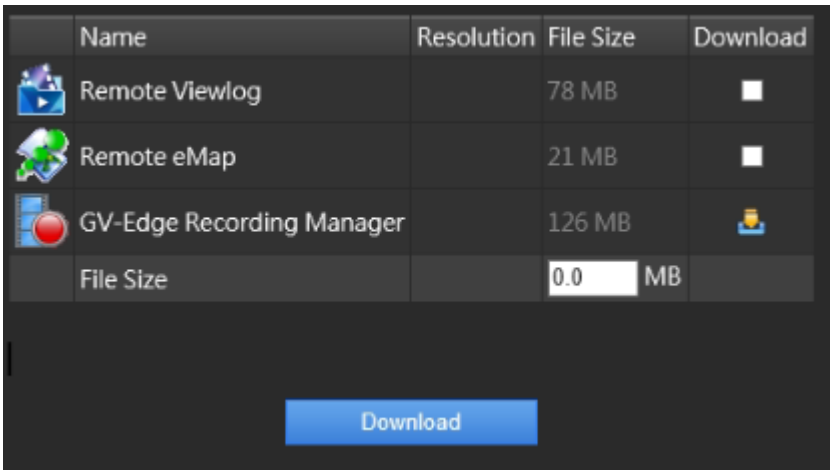
1. To allow remote access to the system, ensure the WebCam Server with the **Run ViewLog Server** function (see *General Settings* earlier in this chapter) is activated.
2. On the left panel of GV-WebCam Server, click **Remote Playback** and select **Remote Playback**. The Remote Playback page appears.
3. Select the desired camera, date, and time-segment file.
4. Click the **Play** button to start.

5. For additional playback features, right-click on the image to have the options of **Play Mode, Render** and **Tools.**

7.7 Download Center

The Download Center allows you to download Remote ViewLog, Remote eMap and GV-Edge Recording Manager.

1. On the left panel of GV-WebCam Server, click **Download** and select **Download**. This page appears.



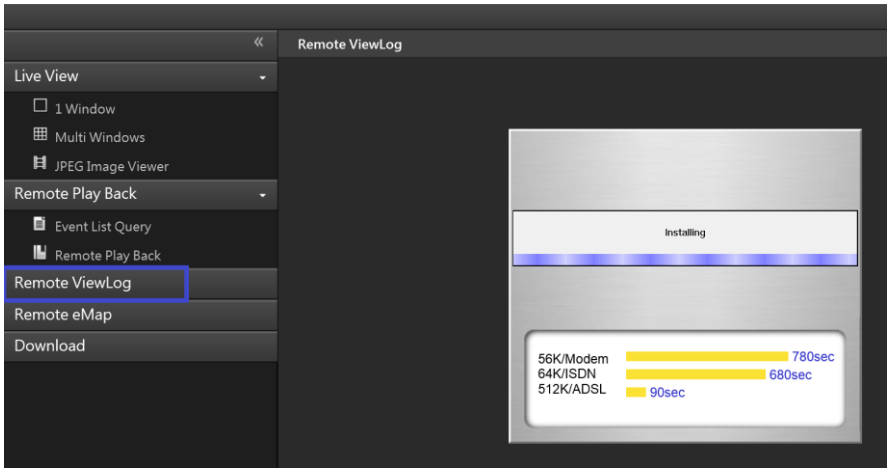
2. Check the desired programs. The **File Size** field will display the total file size of the selected programs.
3. Click **Download** and follow the on-screen instructions to install the programs. When the installation is complete, the message "*Install Complete*" will be displayed.

7.8 Remote ViewLog

Through WebCam Server, you can remotely play back the recorded files by using the ViewLog player.

Note: The integration of AI events from **GV-AI Guard** to Remote ViewLog is not supported.

1. To allow remote access to the system, ensure the WebCam Server with the **Run ViewLog Server** function (see *General Settings* earlier in this chapter) is activated.
2. On the left panel of GV-WebCam Server, click **Remote ViewLog**. Remote ViewLog will be installed on your PC if it is not already.

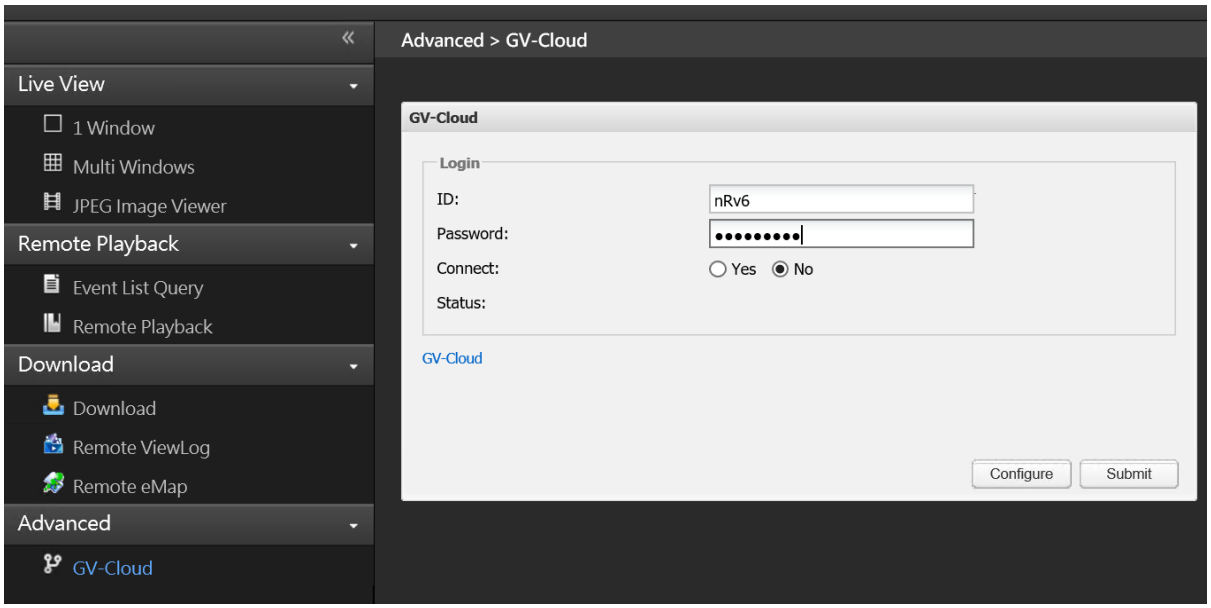


3. Execute GV-Remote ViewLog and create a Remote ViewLog account on the Add Remote Viewlog Account dialog box.
4. After creating an account, the Add New Host dialog box appears.
5. In the Host Type, select **DVR / NVR / VMS**. Type the **Location Name**, **IP Address**, **Account** and **Password** of the system. Only modify the default port 5552 if necessary.
6. Click **OK**. The events available will be listed in the Event List.

For details on ViewLog player, see Chapter 4.

7.9 GV-Cloud

To connect GV-AI Guard to GV-Cloud via GV-WebCam Server, select **Advanced > GV-Cloud** from the left menu. The GV-Cloud page appears.



To connect to GV-Cloud and configure advanced settings, follow the steps below.

1. To configure advanced settings related to connection to GV-Cloud, click **Configure**. The Configure dialog box appears. For details, see *Configuring Advanced Settings* in Chapter 2 of the *GV-Cloud VMS User's Manual*.
2. To connect to GV-Cloud, type a **Host Code** and **Password** created on GV-Cloud VMS in the *ID* and *Password* fields, respectively. For details, see *Creating Hosts* in Chapter 2 of the *GV-Cloud VMS User's Manual*.
3. Set **Connect** to **Yes**.
4. Click **Submit** to apply the settings and start connecting to GV-Cloud.
5. It may take some time for the connection to be established. To verify the connection in GV-Cloud VMS, check the icon color next to the host on the GV-Cloud VMS Hosts page. For details, see *Connecting GV-VMS or GV-AI Guard* in Chapter 2 of the *GV-Cloud VMS User's Manual*.
6. To check the updated connection status in GV-WebCam Server, click **GV-Cloud** in the left menu to refresh the page. If the status hasn't updated yet, wait a moment and try refreshing again.

Note: To configure advanced settings, you must first disconnect from GV-Cloud by setting **Connect** to **No**, and then clicking **Submit** to apply the change. To confirm the disconnection, click **GV-Cloud** in the left menu to refresh the page. The Configure button will become available once the disconnection is confirmed.

7.10 GV-Edge Recording Manager

GV-Edge Recording Manager is designed for remote live viewing and playback of GeoVision IP devices and software. GV-Edge Recording Manager brings live view and allows remote control of GV-IP Camera, GV-Video Server, and GV-SNVR, as well as GV-DVR / NVR / VMS and GV-Recording Server, together under one management interface.

Note: The integration of AI events from **GV-AI Guard** to GV-Edge Recording Manager is not supported.

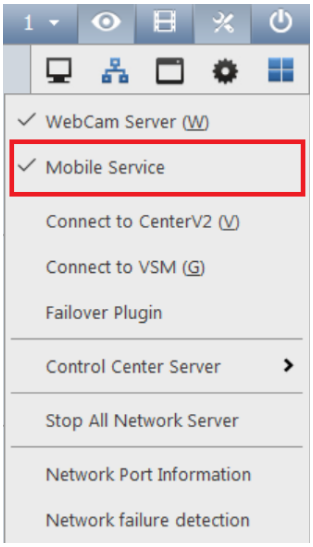
For details on GV-Edge Recording Manager, please visit our website:

- GV-Edge Recording Manager (Windows Version)
- GV-Edge Recording Manager (Mac Version)

- **GV-Edge Recording Manager (Windows Version):** Make sure that **Remote ViewLog Service** and **Control Center / ERM Service** are enabled on the system.
- **GV-Edge Recording Manager (Mac Version):** Make sure that **Webcam Server** and **Mobile Service** are enabled on the system.



Windows version



Mac version

Note:

1. **Mobile Service** has the same function as **Run Mobile Service** (WebCam Server > General Tab).
2. To add additional security protection of the live streaming between the system and GV-Edge Recording Manager through AES encryption, see *Mobile Service* earlier in this chapter.

7.11 Mobile Phone Applications

With a smartphone, you can access live view and play back recordings from the system using GV-Eye mobile app. GV-Eye can be downloaded from App Store or Android Market.

Note: The integration of AI events from **GV-AI Guard** to GV-Eye is not supported.

For details, see the *GV-Eye Installation Guide*.

Chapter 8

E-Map Applications 299

8.1 The E-Map Editor 299

8.1.1 The E-Map Editor Window 300

8.1.2 Creating E-Map 301

8.1.3 Creating E-Map for a Remote Host 304

8.2 Starting E-Map 305

8.2.1 Setting up the Popup Map 306

8.3 3D E-Map Display 307

8.3.1 3D E-Map Display 307

8.3.2 Utilizing 3D E-Map Icons 308

8.4 Remotely Accessing E-Map 309

8.4.1 The Remote E-Map Window 310

8.4.2 Accessing E-Maps of Multiple Hosts 311

8.4.3 Configuring the Remote E-Map 312

8.4.4 Viewing Event List and Playing back Videos 314

8.5 E-Map Server 314

8.5.1 Installing E-Map Server 314

8.5.2 The E-Map Server Window 315

8.5.3 Setting up E-Map Server 316

8.5.4 Connecting to E-Map Server 316

CHAPTER 8

E-Map Applications

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 the system, 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 the system. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **E-Map Editor**. The E-Map Editor window appears.



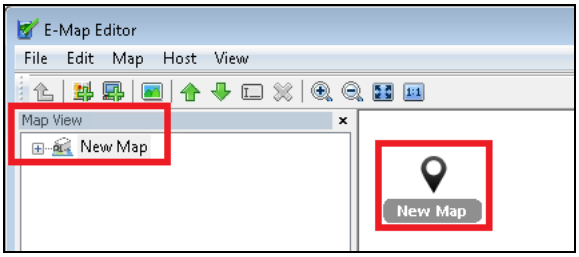
The controls in the E-Map Editor window:

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 & 8	Zoom In / Out	Enlarges / 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 the 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 E-Map

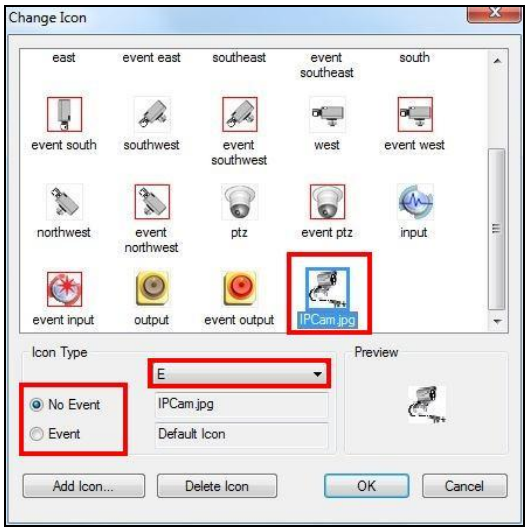
1. To create an E-Map, click **Add Map** on the toolbar. A New Map file is created in Map View and the Floor Plan window separately.



2. Click the **New Map** file in Map View, and click the **Load Map** button (see No. *4, 8.1.1 The E-Map Editor Window*) to import a graphic file. The file opens in the Floor Plan window.
3. Drag and drop the icons from Host View (see No. 13, *8.1.1 The E-Map Editor Window*) onto the map in the Floor Plan window.
4. To change the orientation of the default camera icon, right-click the camera from the Host View, and select an orientation.
5. To change the camera / IO icon to your own, right-click the camera / IO from the Host View, and add your own icon.

Note: Make sure the icon file is of 32 x 32 pixels or smaller.

6. Define the condition that the icon appears by selecting **No Event** or **Event** and select the icon orientation using the dropdown list. You can set different icons for an event and no-event situation. In this example, the icon of IPCam.jpg appears on the map when no event occurs and when an event occurs, the icon changes to the default one.



7. Click **File** in the window menu and select **Save to AI Guard** to save the file to the GV-AI Guard folder, or select **Save to File** to save the file to a desired path.

Advanced Settings

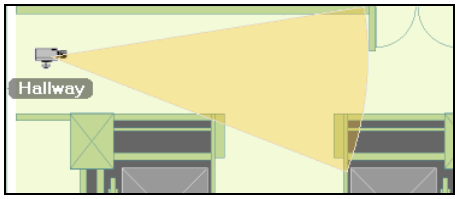
Optionally, you can have the following settings on your created E-Map.

Note: The changes in the orientation of camera icons will not be reflected on the 3D E-Map.

A. View Zone

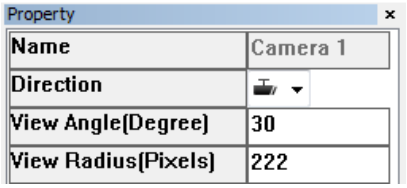
The View Zone function illustrates the monitored area of each camera on the E-Map.

1. In the E-Map Editor window, click to highlight a camera icon, and select **Edit View Zone**. A fan-shaped view zone appears.



2. Move the mouse to adjust the size and direction of the view zone.

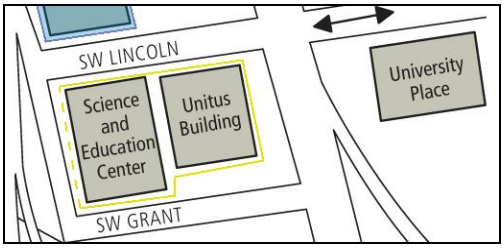
3. Right-click the map and select **Finish** to finalize the zone.
4. You can also adjust the property of the view zone from the Property menu.



B. Polygonal Map

The Polygonal Map function helps you quickly locate a triggered device. Draw an area on the map and it will flash when any device within the area is triggered.

1. In the E-Map Editor window, click to highlight a map, and select **Edit Polygonal Map** or **Edit Polygonal IO**.
2. Click on the map to start drawing a polygonal shape, indicated by a yellow dotted line.



3. After closing the shape, right-click the map and select **Finish**.

The enclosed area will be colored in blue. When a device placed within the polygonal map is triggered, the blue area will flash in blue and red.

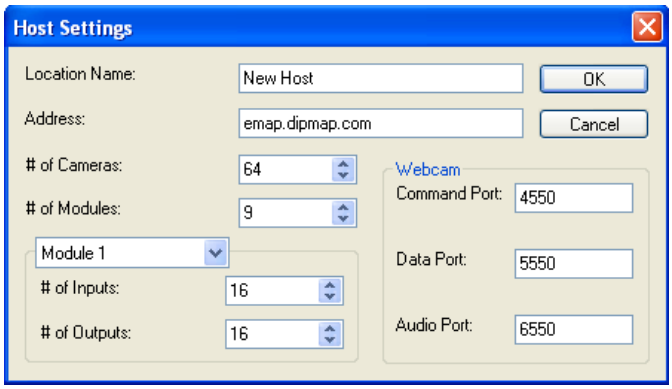
8.1.3 Creating E-Map for a Remote Host

Aside from for the local host (GV-AI Guard), E-Maps can also be created for remote host(s). 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-DVR / NVR / VMS, GV-IP Devices, GV-Video Server and GV-Compact DVR.

---

1. Click **Add Host**  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, which varies depending on the host.



3. Type the necessary information, such as IP address and the number of cameras, and click **OK**.
4. Follow the instructions in *Creating an E-Map* earlier in this chapter to create an E-Map for the remote host.

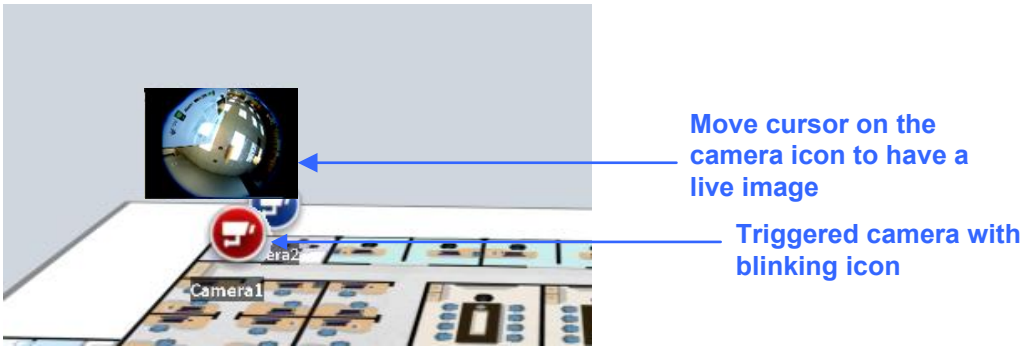
8.2 Starting E-Map

After an E-Map is created, you can start the E-Map on the system and monitor through the E-Map. When any camera and/or I/O device on it is triggered, the corresponding icon will blink as an alert.

1. On the **Content List**, expand the **E-Map** folder and drag the created E-Map to the live view grid. The E-Map is displayed.



2. When any camera or I/O device on the E-Map is triggered, its corresponding icon will blink red. Hover the cursor over the icon to see the live view of the camera or click the icon to see the full view.

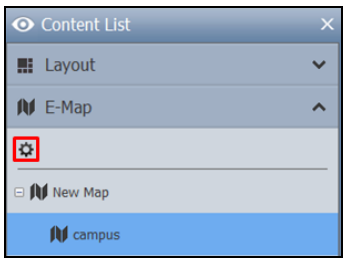


Note: If you have created the E-Maps for multiple hosts, you can see these map files in the Content List. However, these maps won't function on the system but only work on the Remote E-Map. See *Accessing E-Maps of Multiple Hosts* later in this chapter.

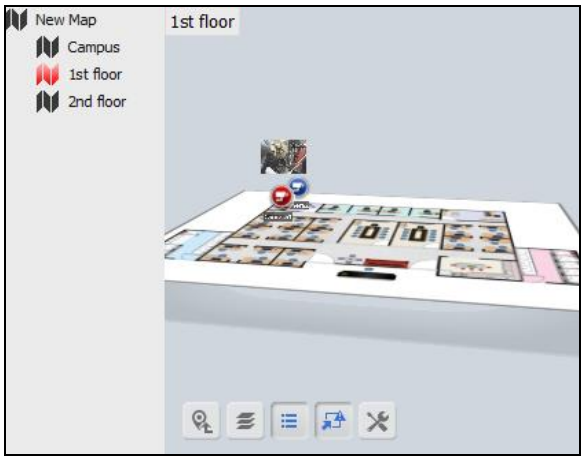
8.2.1 Setting up the Popup Map

When multiple E-Maps are being monitored simultaneously, the popup function can be enabled for monitoring convenience. Once any camera or I/O device is triggered, its corresponding E-Map will pop up, replacing the current E-Map.

1. In the Content List, click the **Configure** button under E-Map and select **E-Map Popup Settings**.



2. Select the 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 popup.
3. At the bottom of the E-Map grid, click **E-Map Auto Pop-up** to enable the function.

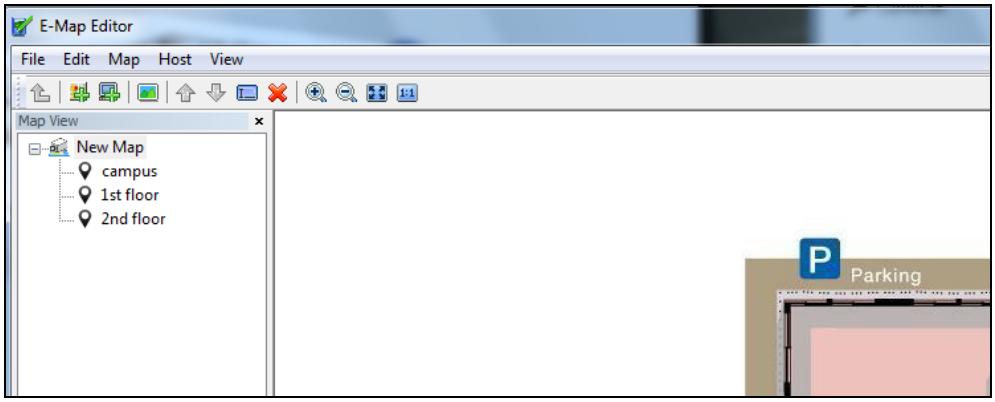


8.3 3D E-Map Display

8.3.1 3D E-Map Display

The E-Map can display the monitoring area in 3D view, meaning you can zoom in and out with the mouse wheel, and rotate the view as you wish.

1. Create an E-Map by following the instructions in *Creating an E-Map* earlier in this chapter. To build multiple layers of maps, create another subfolder under the E-Map folder, as illustrated below.



2. After creating an E-Map, click **Home** > **Toolbar** > **Content List** on the system.
3. Expand the **E-Map** folder and drag the created E-Map to the live view grid
4. To zoom in / out of the monitoring area, simply scroll the mouse wheel up or down.
5. To adjust the angle of view, click and hold on the E-Map and move in any direction as desired.
6. To move up or down the building view (see No. 2, *Utilizing 3D E-Map Icons* later in this section), right-click on the E-Map and scroll the wheel.

8.3.2 Utilizing 3D E-Map Icons

The 3D E-Map display comes with a set of icons for settings and control. Place the mouse cursor on the E-Map to see the icons below.



No	Icons	Functions
1	Move Up	Move to the main folder of the current E-Map.
2	Building View	Switch the floor plan to 3D view mode of the building.
3	Map List	Display the E-Map list.
4	E-Map Auto Popup	Enable this function to automatically pop up the related map whenever any device on it is triggered. See *Setting Up the Popup Map* earlier in this chapter.

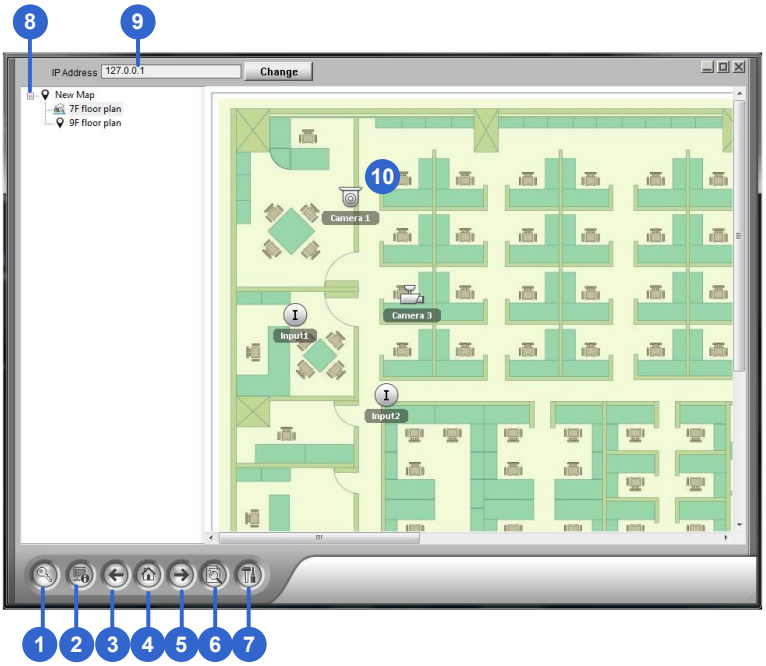
5	Tools 	Includes the following options: ■ **Auto Rotate:** Automatically rotates the E-Map anticlockwise. ■ **Icon Options:** ➢ **Always Show Live Video**: Always display the received live view on the E-Map. ➢ **Show Device Name**: Display the device name on the E-Map. This option is enabled by default. ➢ **Large Icons**: Change to large icons of cameras. By default, the large icons are used. ➢ **Small Icons**: Enable this option if you want to use small icons. ■ **Properties:** Show the E-Map name on the upper-left corner and change the font size of the E-Map name. ■ **Close:** Remove the E-Map display.

8.4 Remotely Accessing E-Map

You can remotely access and view E-Maps with a Web browser.

1. To allow remote access to E-Maps, click **Home**  > **Toolbar**  > **Network**  > **WebCam Server** on the system. The Server Setup dialog box appears.
2. Click **OK** to start the WebCam server.
3. Open the Web browser and type the address of the system. Once the connection is established, the Single View page appears.
4. On the left panel, click **Remote E-Map** under Download. The Login dialog box appears.
5. Type the login credentials of the system and click . The Remote E-Map window is displayed.

8.4.1 The Remote E-Map Window

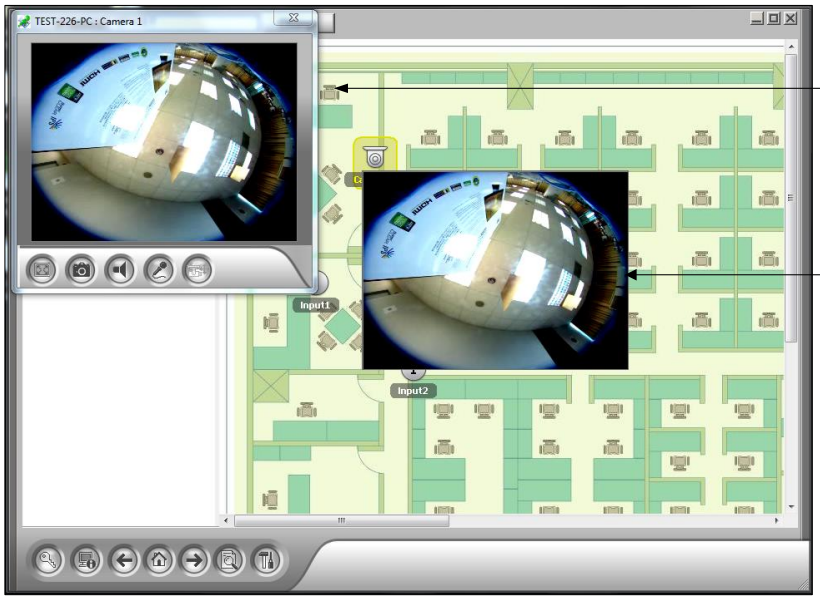


The controls in the window:

No.	Name	Description
1	Login	Logs up to 500 hosts.
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. See *Remote ViewLog Service* in Chapter 4.
7	Configure	Configures the advanced settings.
8	Tree List	Displays all created E-Map files and folders.
9	IP Address	Displays the IP Address of the connected host.
10	Camera / Input / Output Icon	When events occur, the corresponding icons will blink red. **Camera icon:** Move the cursor over the icon to view a live image. Click the icon to open a control panel for the camera. **Output Icon:** Click the icon to manually trigger the output device. .

Note: By default, E-Maps opened with Remote E-Map are displayed in 3D. To display the E-Maps in 2D view, click the **Configure** button (see No. 7 above) and select **Disable 3D eMap**.

Controls in the Camera Icon

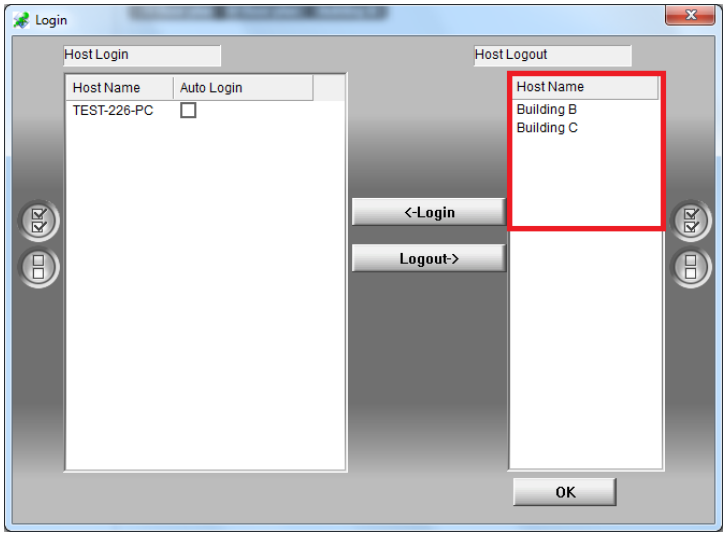


8.4.2 Accessing E-Maps of Multiple Hosts

If you have created E-Maps for multiple hosts, you can monitor these E-Maps remotely through a Web browser. Up to 500 hosts can be accessed at a time.

1. To start, click **Login**  on the Remote E-Map window. The Login window appears.

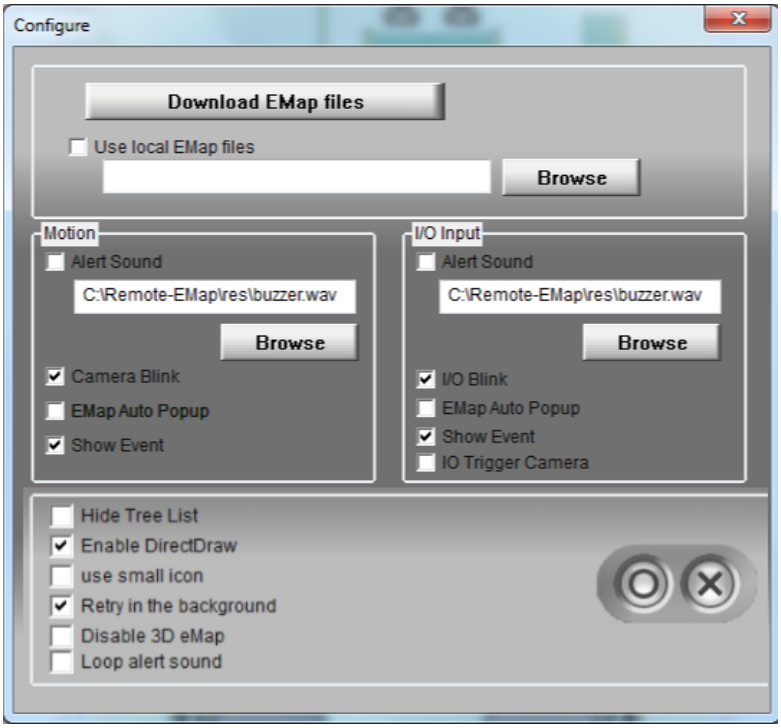
2. Select a host on the right panel and click **Login**. You are prompted for the required login info.



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.

8.4.3 Configuring the Remote E-Map

Click **Configure** on the Remote E-Map window. The Configure dialog box appears.



[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.

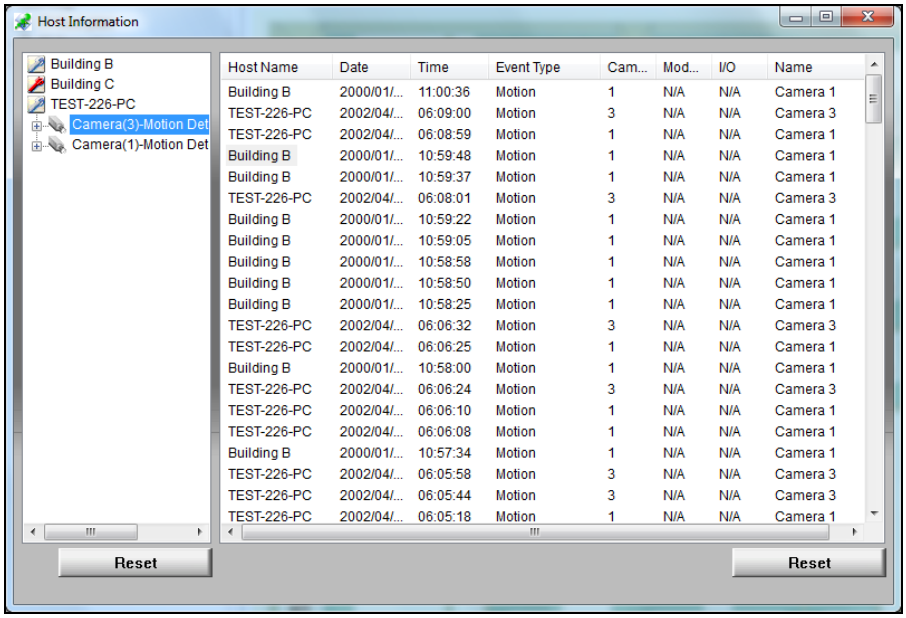
[Motion] / [I/O Input]

- **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.
- **E-Map Auto Popup:** When cameras or I/O devices are triggered, the associated map will pop up on the screen instantly when the Remote E-Map window is minimized.
- **Show Event:** Display the information of triggered events on the Host Information window.
- **I/O Trigger Camera:** When input devices are triggered, the associated d camera views will pop up. To enable this function, you must map input devices to cameras on the system first. See *Setting up Popup Live View* in Chapter 1.
- **Hide Tree List:** Select to hide the tree list.
- **Enable DirectDraw:** Enabled by default to speed up graphics rendering. Some graphics cards might not support DirectDraw and can produce distorted frames. In this case, disable the function.
- **Use Small Icon:** Use smaller icons for cameras and I/O devices.
- **Retry in the Background:** When the Remote E-Map is disconnected from the system, a warning message will pop up every 30 seconds. Select to hide the message and retry the connection in the background.
- **Disable 3D emap:** Disable the 3D e-map function.
- **Loop alert sound:** When **Alert Sound** is enabled, the assigned .wav file will be played repeatedly until it is turned off by the operator.

8.4.4 Viewing Event List and Playing back Videos

You can see a list of triggered events on the Host Information window and play back the desired video(s).

1. Click **Host Information** on the Remote E-Map window. The Host Information window appears.



2. For event playback, double-click any motion event on the left panel. The player appears.
3. Optionally right-click the image to access the advance functions of the player.

8.5 E-Map Server

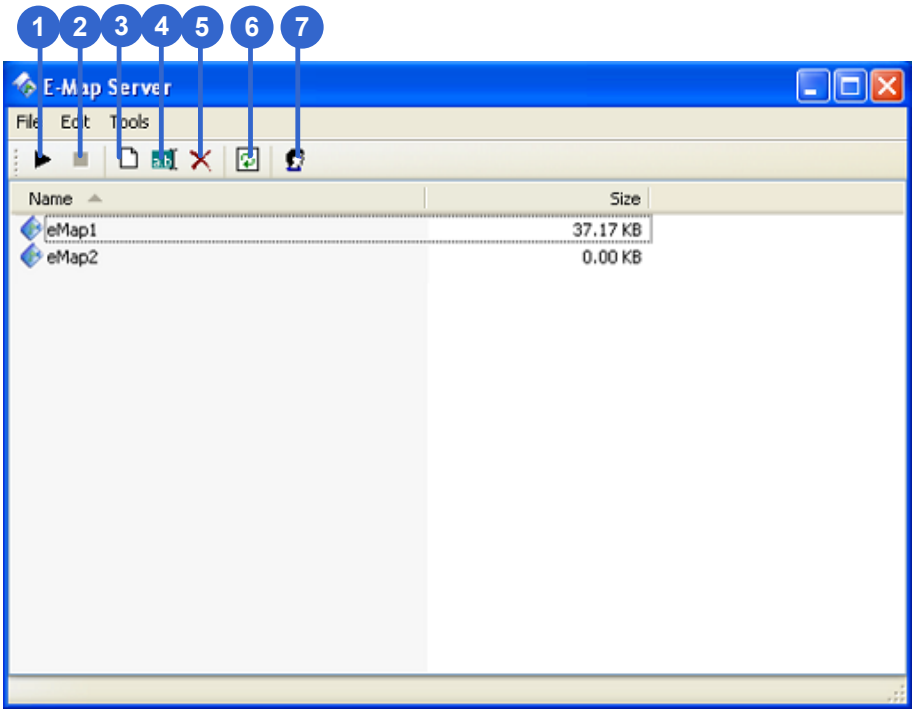
The E-Map Server is an independent program designed to create E-Maps for different hosts. With the E-Map Server, you can monitor different sites on electronic maps through any computer accessible to the network.

8.5.1 Installing E-Map Server

You can install GV-E-Map Server from the GeoVision Website.

8.5.2 The E-Map Server Window

Go to **Windows Start** > **All apps** > **E-Map Server folder** > **E-Map Server**. This window appears.



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.

8.5.3 Setting up E-Map Server

Before starting the E-Map Server, you must create E-Map files and user accounts.

- To create E-Map, click **New** (see No. 3, *The E-Map Server Window* earlier in this section). See *Creating an E-Map* earlier in this chapter.
- To create a user account for the server, click **Accounts** (see No. 7, *The E-Map Server Window* earlier in this section).

8.5.4 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 the login info of the E-Map Server. You are prompted to select an E-Map (.emp) file.
3. Click **OK**. The Remote E-Map window appears.
4. Click **Login**  to log into the desired host. For details, see *Accessing E-Maps of Multiple Hosts* earlier in this chapter.

Note: To log into the system, make sure the WebCam Server is enabled. See *Remotely Accessing E-Map* earlier in this chapter.

Chapter 9

Useful Utilities 319

9.1 Dynamic DNS 319
9.1.1 Running Dynamic DNS 319
9.1.2 Registering and Starting Dynamic DNS 319
9.2 Watermark Viewer 320
9.2.1 Activating Watermark Protection 320
9.2.2 Running Watermark Proof 320
9.2.3 The Main Window 321
9.3 Windows Lockup 322
9.3.1 The GV-Desktop Screen 322
9.3.2 GV-Desktop Features 323
9.3.3 Token File for Safe Mode 326
9.4 Authentication Server 327
9.4.1 Installing the Server 327
9.4.2 The Main Window 328
9.4.3 Creating Clients 329
9.4.4 Creating User Accounts 331
9.4.5 Importing Groups and Users from Active Directory 334
9.4.6 Starting Authentication Server 337
9.4.7 Connecting to Authentication Server 339
9.4.8 Remote Access from Control Center and Remote E-Map 341
9.5 Fast Backup and Restore 344
9.5.1 Running the FBR Program 344
9.5.2 Plugin Component 345
9.5.3 Customizing the Features 346
9.5.4 Backing up and Restoring Settings 347
9.6 Bandwidth Control Application 350
9.6.1 Installing the Bandwidth Control 350
9.6.2 The Main Window 351
9.6.3 Allowing Remote Control 352
9.6.4 Connecting to WebCam Server 353
9.6.5 Controlling a Specific WebCam Server 354
9.6.6 Setting up the Bandwidth 355

9.6.7 Block List Setup 356
9.6.8 General Setup 357
9.7 Language Setting 358
9.7.1 Installing the MultiLang Tool 358
9.7.2 Revising the Translated Text 359
9.7.3 Setting up the UI Language to English 362
9.8 GV-SD Card Sync Utility 363
9.8.1 Installing the Utility 363
9.8.2 Setting up the Utility 364
9.8.3 The Main Window 367
9.9 The Media Man Tools Window 368
9.9.1 The Media Man Tools Window 368
9.9.2 Viewing Disk Drive Status 369
9.9.3 Adding a Disk Drive 371
9.9.4 Removing a Disk Drive 372
9.9.5 Logging in Automatically at Startup 373
9.9.6 Setting up LED Panel 373
9.10 Alert Notifications through SNMP Protocol 376
9.11 Local and Remote Backup 377
9.11.1 Remote Backup 377
9.11.2 Local Backup 377
9.11.3 Advanced Settings 379
9.11.3.1 Advanced Settings for Local Backup 379
9.11.3.2 File Transfer Settings for Local Backup 381
9.12 Report Generator 383
9.13 GV-Cloud VMS 383

CHAPTER 9

Useful Utilities

GV-AI Guard supports some advanced utilities to enhance the system performance in a security network.

9.1 Dynamic DNS

GV-Dynamic DNS maps your GV-AI Guard server's dynamic IP address to a fixed domain name and updates it every 10 minutes. This keeps the server accessible even when its IP address changes.

For more information, see the *GV-Dynamic DNS Service V2 Installation Guide*.

9.1.1 Running Dynamic DNS

GV-Dynamic DNS Service is included in the installation of the system. To access the service, go to **Windows Start** > **All apps** > **GV-AI Guard folder** > **DNS Client V2.** The DNSClient V2 dialog box appears.

9.1.2 Registering and Starting Dynamic DNS

To register a domain name and start the DDNS service, refer to the following sections in the *GV-Dynamic DNS Service V2 Installation Guide*:

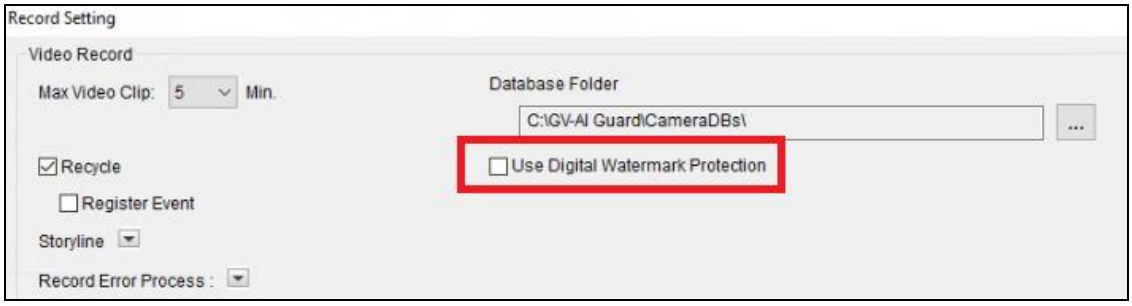
- Registering Domain Name with DDNS
- Starting Dynamic DNS

9.2 Watermark Viewer

GV-AI Guard can embed digital watermarks in video streams for authentication purposes. 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 system, to further verify the authenticity of the recording.

9.2.1 Activating Watermark Protection

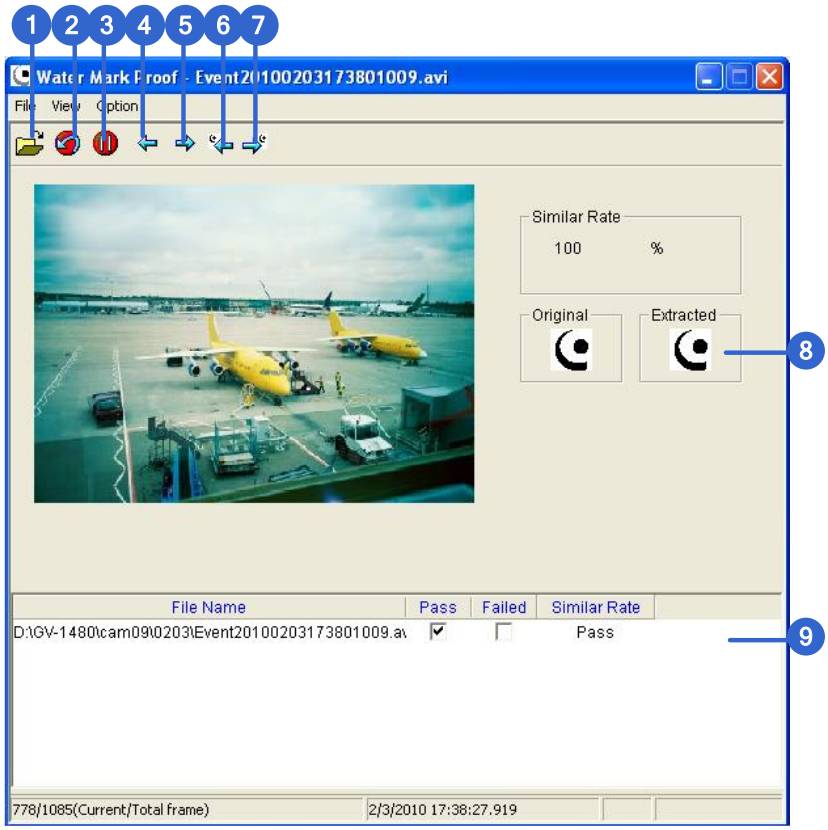
To enable the watermark protection, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting**, and select **Use Digital Watermark Protection**. The system will digitally sign videos during the recording.



9.2.2 Running Watermark Proof

1. Locate the GV-AI Guard 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 (see No. 9, *The Main Window* later in this section). 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.
3. To play the recording, double-click the listed file on the window.

9.2.3 The Main Window



No.	Name	Description
1	Open File	Opens the recorded file.
2	First Frame	Goes to the first frame of the file.
3	Play	Plays the file.
4	Previous Frame	Goes to the previous frame of the file.
5	Next Frame	Goes to the next frame of the file.
6	Previous 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

GV-Desktop helps you secure your computer while away from your workstation. You can lock up the Windows desktop while launching a customized GV-Desktop. In GV-Desktop, users are limited to run GV-AI Guard and only selected programs.

9.3.1 The GV-Desktop Screen

GV-Desktop is included in the installation of the system. Go to **Windows Start** > **All apps** > **GV-AI Guard** > **Key Lock Utility**. The GV-Desktop screen appears.

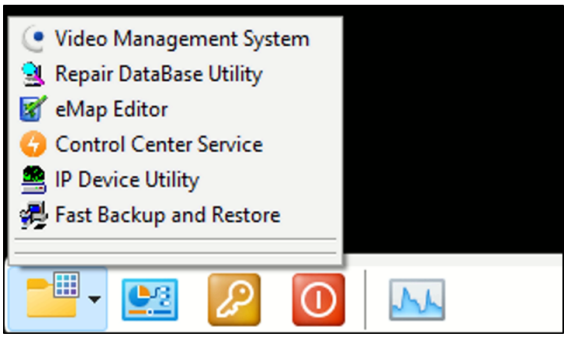


No.	Name	Description
1	Programs	Accesses programs.
2	Settings	Adds programs to the programs menu.
3	Log Off	Logs off GV-Desktop.
4	Shut Down	Shuts down the computer.
5	Task Manager	Views the tasks currently running on your computer.

9.3.2 GV-Desktop Features

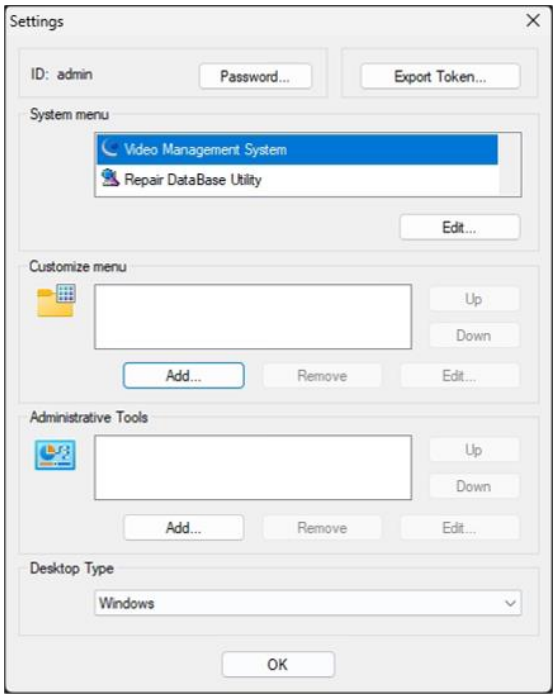
Programs

Click the **Programs** button (see No.1, *The GV-Desktop Screen* earlier in this section) to see the program menu. The default programs are Video Management System (GV-AI Guard), Repair Database Utility, E-Map Editor, Control Center Service, IP Device Utility, and Fast Backup and Restore. To add or remove new programs to the menu, see the following subsection *Settings*.



Settings

Click the **Settings** button (see No.2, *The GV-Desktop Screen* earlier in this section) and type the valid ID and password. This window appears.



GV-Desktop Settings dialog box

[Password] Change the password. For **Allow Removing Password System**, see *Account and Password* in Chapter 1.

[Export Token] See *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-AI Guard from the dropdown menu. The selected desktop will launch the next time when you log into the computer.

Log Off

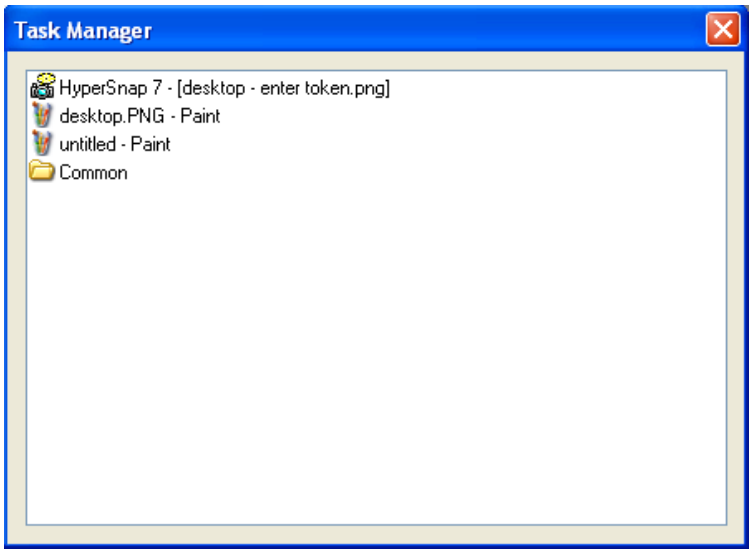
Click the **Log off** button (see No.3, *The GV-Desktop Screen* earlier in this section) to log off GV-Desktop with a valid ID and password.

Shut Down

Click the **Shut Down** button (see No. 4, *The GV-Desktop Screen* earlier in this section) to shut down your computer with a valid ID and password.

Task Manager

Click the **Task Manager** button (see No. 5, *The GV-Desktop Screen* earlier in this section) 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 the desktop, double-click the program listed in Task Manager.



9.3.3 Token File for Safe Mode

This option in the Settings section lets you export a token file. In case you start Windows in Safe Mode and in the status of GV-Desktop, this token file allows you to exit from GV-Desktop and enter Windows desktop. To export a token file, follow the steps below.

Exporting the Token File

1. Click the **Export Token** button (see *Settings, GV-Desktop Features* earlier in this section). The Enter Token Code appears.
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 GV-Desktop. You will be prompted to locate the stored token file and type the configured token code.
2. When the Settings window (see *Settings, GV-Desktop Features* earlier in this section) appears, select **Windows** in the Desktop Type field and exit from the window.
3. Click the **Log Off** button to log off 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

GV-Authentication Server is a password and account management system for multiple GV-AI Guard systems. Through the Authentication Server, the administrator can create the accounts with different access rights to a group of GV-AI Guard systems. Once any GV-AI Guard is connected to the Authentication Server, the previous password settings in local GV-AI Guard will be invalid. Local GV-AI Guard will submit to the full control of the Authentication Server.

Note:

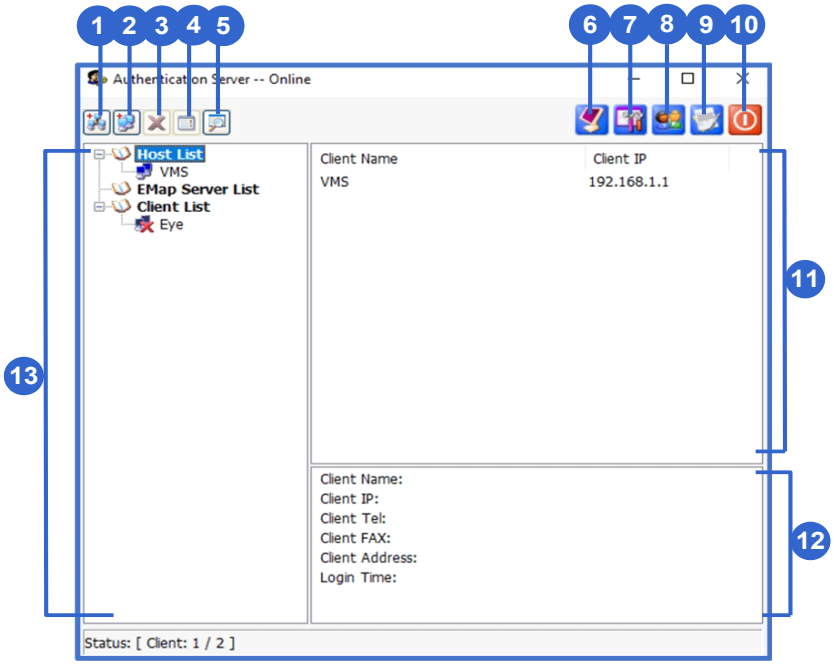
1. In addition to GV-VMS / DVR / NVR where the Authentication Server acts as a password and account management system, the Authentication Server also supports E-Map Server, GV-Control Center, GV-Edge Recording Manager and GV-Eye app to allow users to access a specified group of GV-VMS / DVR / NVR hosts through an Authentication user account.
2. GV-Eye V2.8.0 or later and GV-Edge Recording Manager V2.1.0 or later support multiple GV-Authentication Server connections at a time.

9.4.1 Installing the Server

You can install **GV-Authentication Server** from **Utility** in the GeoVision Website.

9.4.2 The Main Window

Go to **Windows Start** > **All apps** > **AuthServer folder** > **AuthServer**. This window appears.

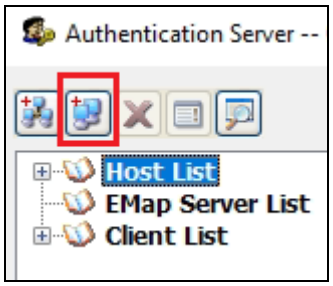


No.	Button	Description
1	Add An Area	Creates an Area group.
2	Add A Client	Creates a client account.
3	Delete An Area / Client	Deletes an existing group or client.
4	View/Edit A Client	Select a client from the Client List, and click to view / edit it.
5	Find A Client	Finds an existing client.
6	Start/Stop 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.
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 clients.
12	Client Information	Lists the information of the selected client.
13	Client List	Lists the created clients.

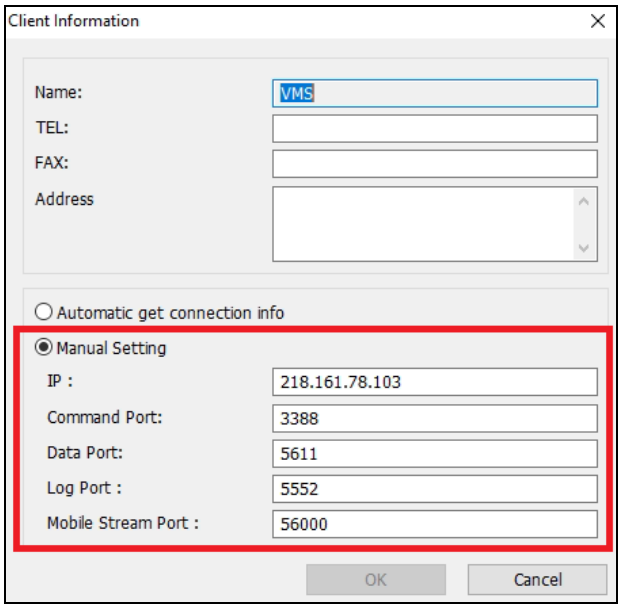
9.4.3 Creating Clients

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-AI Guard clients, follow the steps below.

1. To create a client, highlight the **Host List** from the left panel and click the **Add A Client** button . The Client Information dialog box appears.

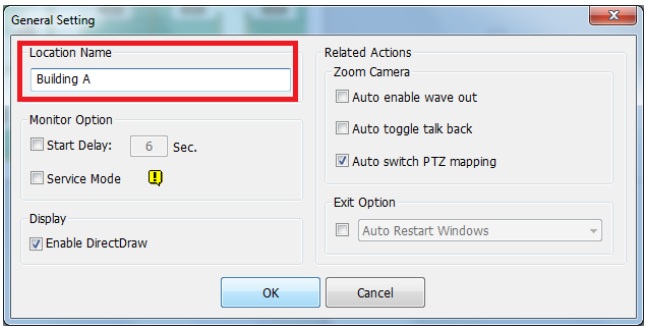


2. Type the client's information and select **Automatic get connection info**. The **Name** must match that of the local GV-AI Guard.
3. Optionally select **Manual Setting** and type the IP address of GV-Authentication Server. Keep the default ports or modify them if necessary.



4. Click **OK**.

Tip: To view the name of your GV-AI Guard system, select **Toolbar** > **Configure** > **System Configure** > **General Setting**.



General Setting dialog box

5. To create another client, repeat the steps above.
6. You can also arrange multiple clients under a group by highlighting a list and clicking the **Add An Area** button (see No. 1, *The Main Window* earlier in this section). The created group appears under the selected List.

9.4.4 Creating User Accounts

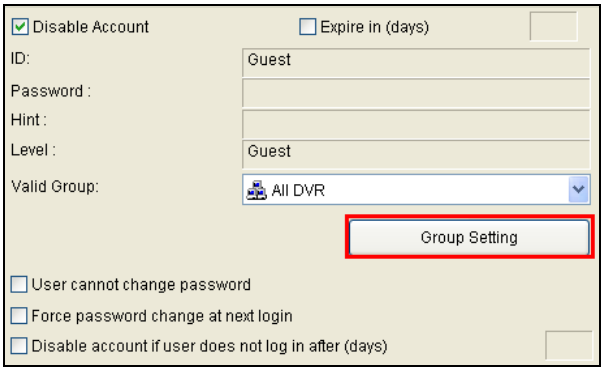
To create user accounts with different access rights and assign the user accounts to a group of GV-AI Guard clients, follow the steps below.

1. Click the **Account Setup** button (see No. 8, *The Main Window* earlier in this section) 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.

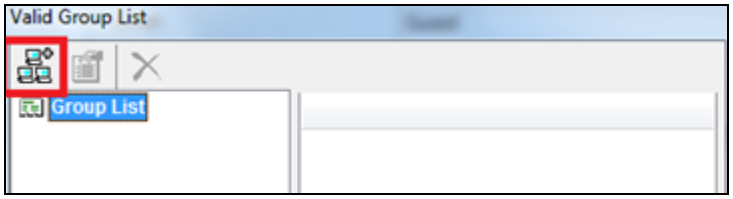
Note: The Administrator has the authority of changing the password of any accounts.

---

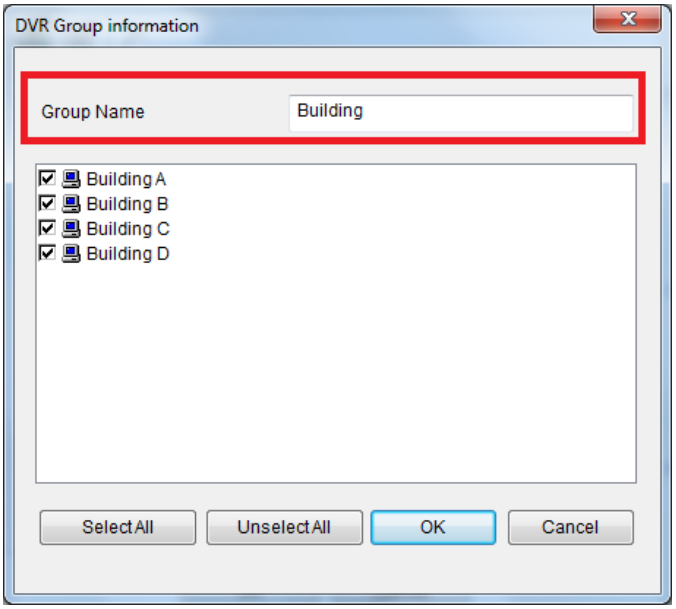
3. To assign the created user to a group of GV-AI Guard clients:
   A. Click the **Group Setting** button.



   B. In the Valid Group List window, click the **New Group** button.

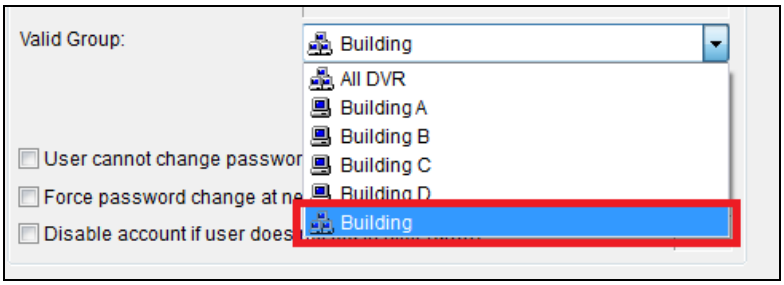


C. In the DVR Group Information window, name the group, select the desired GV-AI Guard clients to be added to the group. Click **OK**.



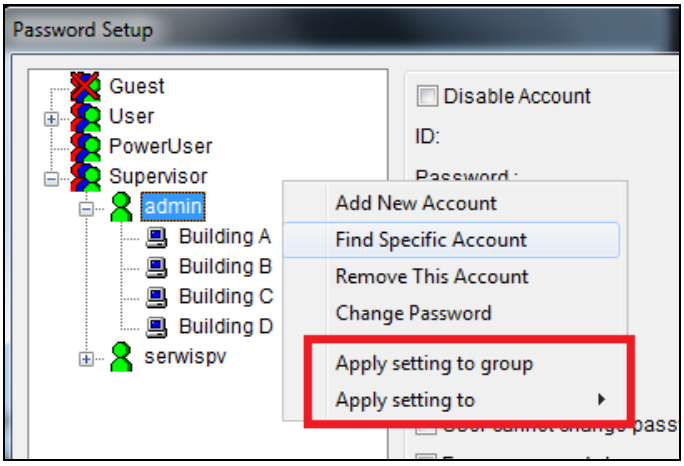
D. Click **OK** again to return to the Password Setup window.

E. Use the **Valid Group** dropdown list to select the created group. The user will be able to log in the assigned GV-AI Guard clients.

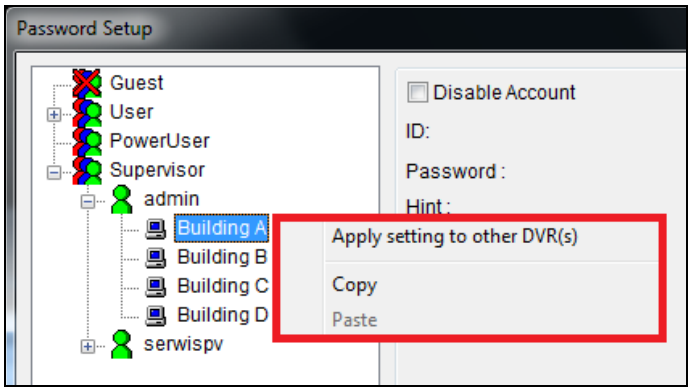


4. Optionally use the following functions to arrange the user and client accounts.

   A. Right-click a user account to have two options. The **Apply setting to** option will apply the same settings to a specific user account. The **Apply setting to group** option will apply the same settings to all user accounts under the same account level.



   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.



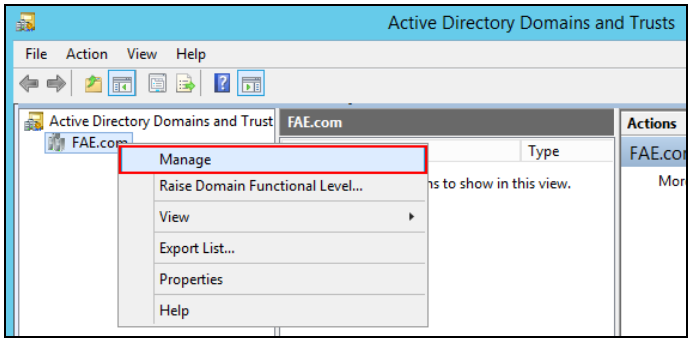
9.4.5 Importing Groups and Users from Active Directory

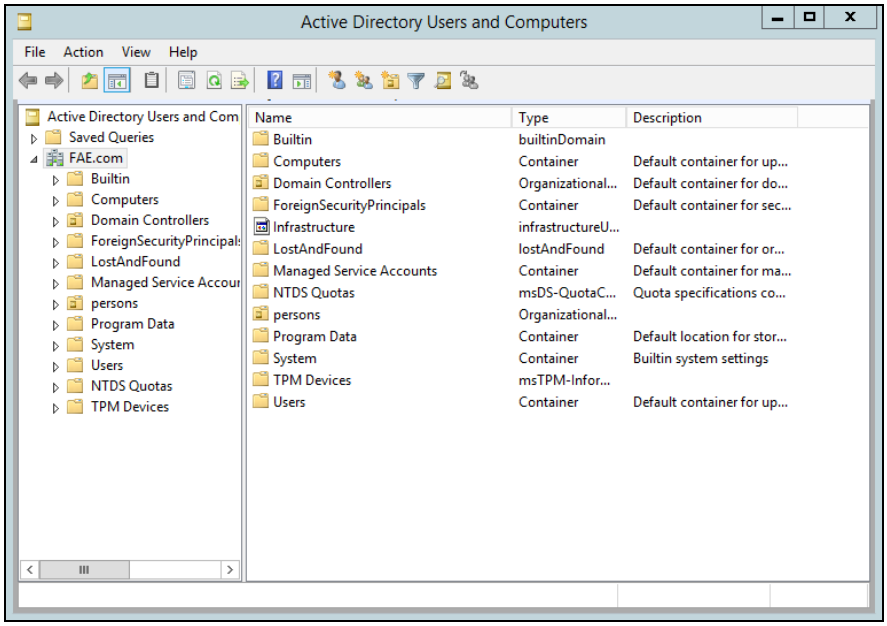
To create user accounts efficiently, you can import groups and users from Microsoft's Active Directory to the Authentication Server. You will need to install Active Directory on Windows Server and set up users into groups before following the steps below.

Note: User accounts in Active Directory need to be grouped into Groups settings first as only groups can be imported into Authentication Server.

---

1. Run **Active Directory Domains and Trusts** in Windows Server by clicking the **Start** menu and opening **Administrative Tools**.
2. Right-click your local Active Directory system and select **Manage**. The Active Directive Users and Computers dialog box appears.





3. On the **View** menu, select **Advanced Features**.

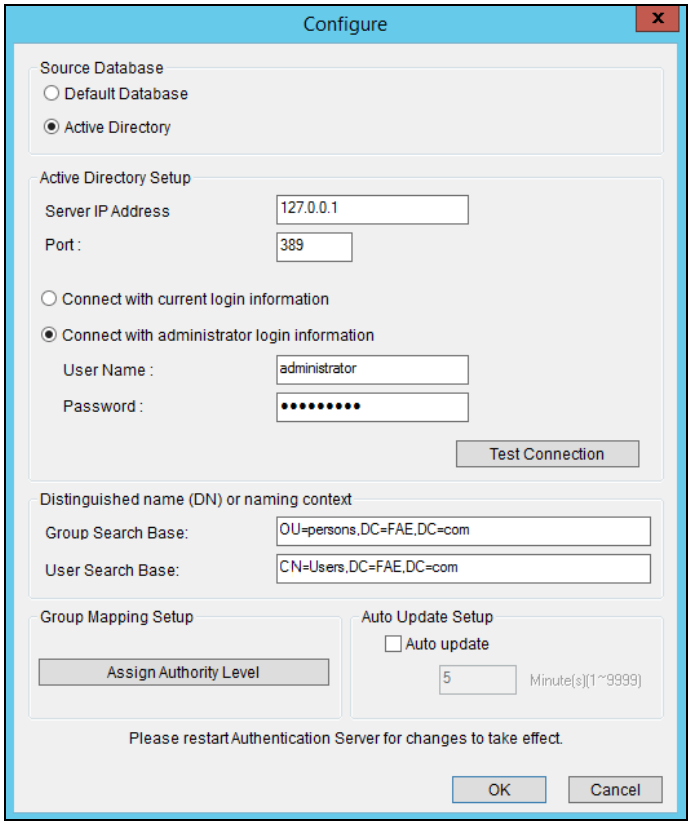
4. Right-click the folder saved with the user accounts or groups and select **Properties**.

Tip: You can change the query parameters or show all items for each folder by clicking **View** and selecting **Filter Options**.

---

5. Select the **Attribute Editor** tab, double-click the attribute **distinguished Name** and copy the value like **OU=persons, DC=FAE,DC=com**. You will need to paste the value at *step 8, C* to assign the folder to import the user accounts or groups.

6. In the Authentication Server, click the **Account Setup** button (see No. 8, *The Main Window* earlier in this section) and select **Active Directory Setup.** This page appears.



7. Under Source Database, select **Active Directory** to enable the function.

8. To connect to the server with Active Directory:

   A. Type the **Server IP Address** and the **Port** number of the server.

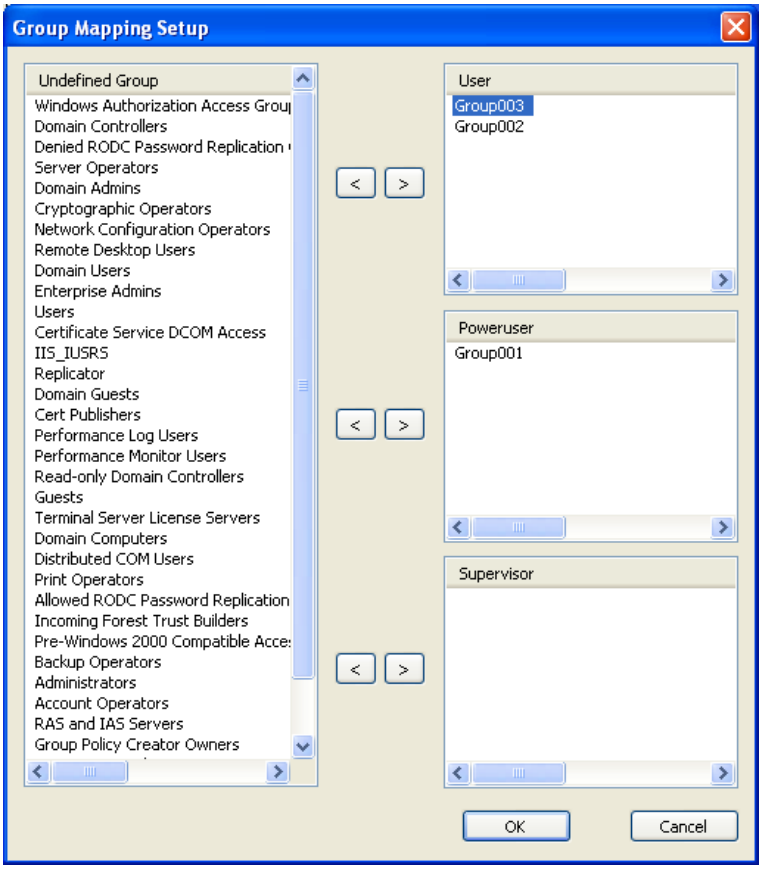
   B. To log into the server using your current login credentials, select **Connect with the current login information**. To log into the server using the login credentials of its administrator, select **Connect with administrator login information**.

   C. Paste the value of distinguished name you copied at step 5 respectively to **Group / Users Search Base**.

   D. Click **Test Connection** to see if you can connect to the server with Active Directory.

9. 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.



   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.

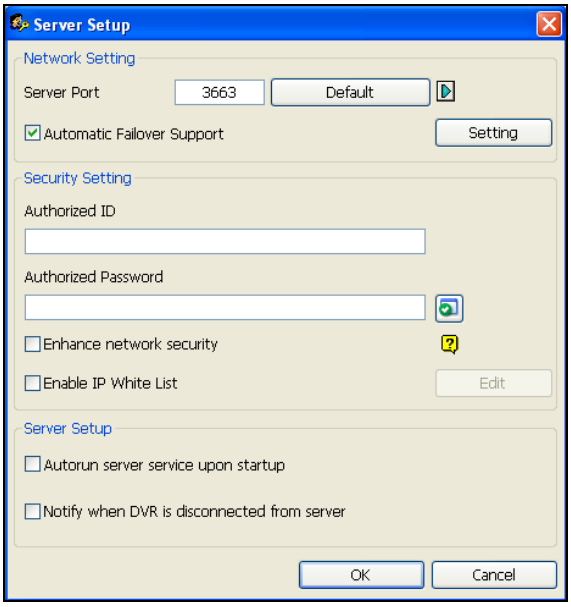
10. To automatically update changes to user data in Active Directory, click **Auto Update** and specify the update frequency in minutes.

11. Click **OK** and restart the Authentication Server to apply the settings.

9.4.6 Starting Authentication Server

To configure and start the Authentication Server, follow the steps below.

1. Click the **Server Setup** button (see No. 7, *The Main Window* earlier in this section). This dialog box appears.



2. Under Security Setting, type the **Authorized ID** and **Authorized Password** which will be used for the GV-AI Guard client to log into the Authentication Server.
3. Click **OK** to apply the settings.
4. Click the **Start/Stop Service** button (see No. 6, *The Main Window* earlier in this section) 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. If 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, 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 the Authentication Server.
- **Enable IP White List:** Click **Edit** to create a list of IP addresses only which are allowed to establish connection with the Authentication Server.

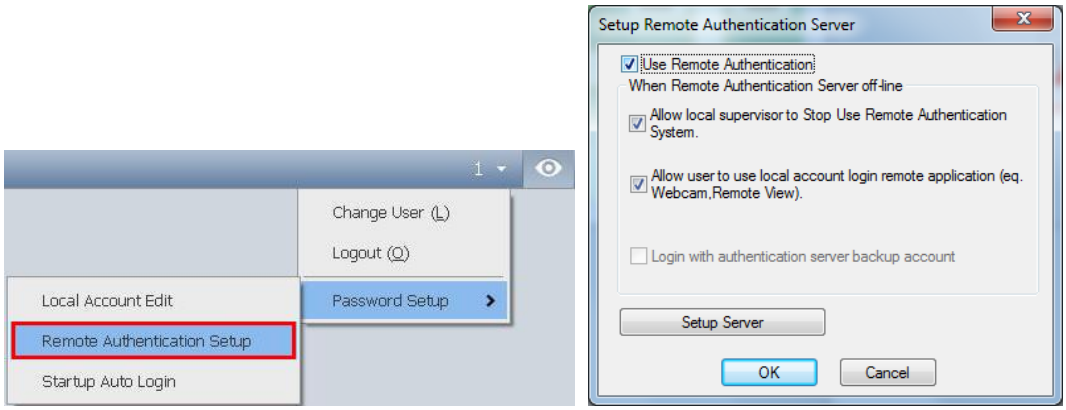
[Server Setting]

- **Auto run server service upon startup:** Starts the service automatically upon the startup of Authentication Server.
- **Notify when DVR is disconnected from server:** Notify the Authentication Server with a popup window when GV-AI Guard is disconnected with the Authentication Server.

9.4.7 Connecting to Authentication Server

To configure the system in order to access the Authentication Server remotely, follow the steps below.

1. On the main screen, click **User** > **Password Setup** > **Remote Authentication Setup**. The Setup Remote Authentication Server dialog box appears.



2. Select **Use Remote Authentication** and optionally select:

   [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 fails with the Authentication Server. Note if the option is disabled and the connection fails with the Authentication Server, the local supervisor will not be able to log into the system, 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**. The Remote Authentication dialog box appears.
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 system will be invalid.

7. On the main screen of GV-VMS, click **User** > **Change User** to call up the Login dialog box. The icon indicates that the connection is established.



Login dialog box

As long as the Authentication Server works, the Login dialog box will appear upon starting the system. Type the user account created on the Authentication Server to log into the system.

Note: The disconnection icon will appear on the Login dialog box (see Step 7 above) 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 does not match the location name of the system (see the General Setting dialog box in *Creating Clients* earlier in this section).
3. The network connection encounters traffic problem.

9.4.8 Remote Access from Control Center and Remote E-Map

The Authentication Server supports E-Map Server, GV-Control Center to allow users to access a specified group of GV-AI Guard hosts through an Authentication user account.

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-AI Guard 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 client accounts of E-Map Servers and Control Servers under their separate lists on the Authentication Server window.

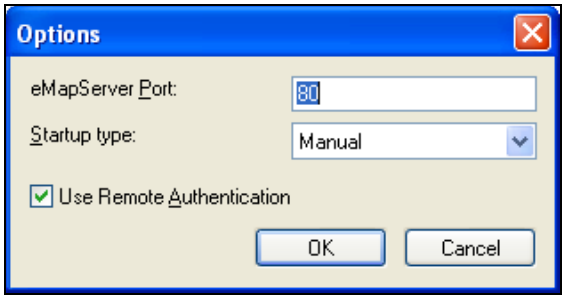
1. In the Client List field, click the E-Map Server List or Control Center List and click the **Add A Client** button (see No. 2, *The Main Window* earlier in this section). The Client Information dialog box appears.
2. Type the name and information of the E-Map Server or Control Center. The name does 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

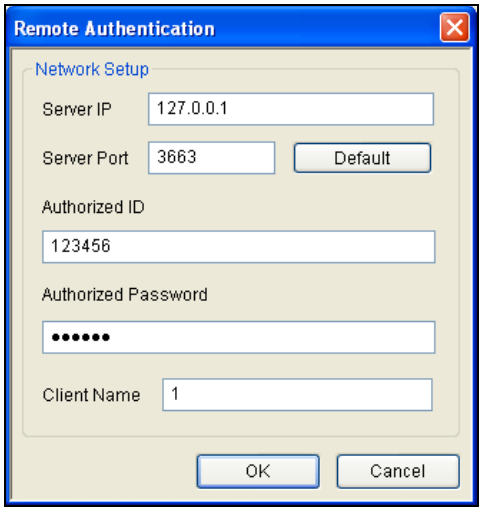
The E-Map Server can access the account settings of the Authentication Server.

1. Run the **E-Map Server**. For details, see *E-Map Server* in Chapter 8.

2. In the E-Map Server window, click **Tools** on the menu bar, and select **Options**. This dialog box appears.



3. Select **Use Remote Authentication**.
4. 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.
5. Click **OK** to apply the settings.
6. In the E-Map Server window, click **Tools** on the menu bar and select **Remote Authentication**. This dialog box appears.



7. 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**.
8. In the E-Map Server window, click **Tools** on the menu bar and select **Start Service** to start the E-Map Server.
9. When you log into the E-Map Server, type the user ID and password created on the Authentication Server. A list of assigned GV-AI Guard clients to the user will be displayed.

Accessing from GV-Control Center

GV-Control Center can access account settings of GV-Authentication Server. For details, see *Authentication Server* in Chapter 9 of the *GV-Control Center User's Manual V4* or *Authentication Server* in Chapter 9 of the *GV-Control Center User's Manual V3*.

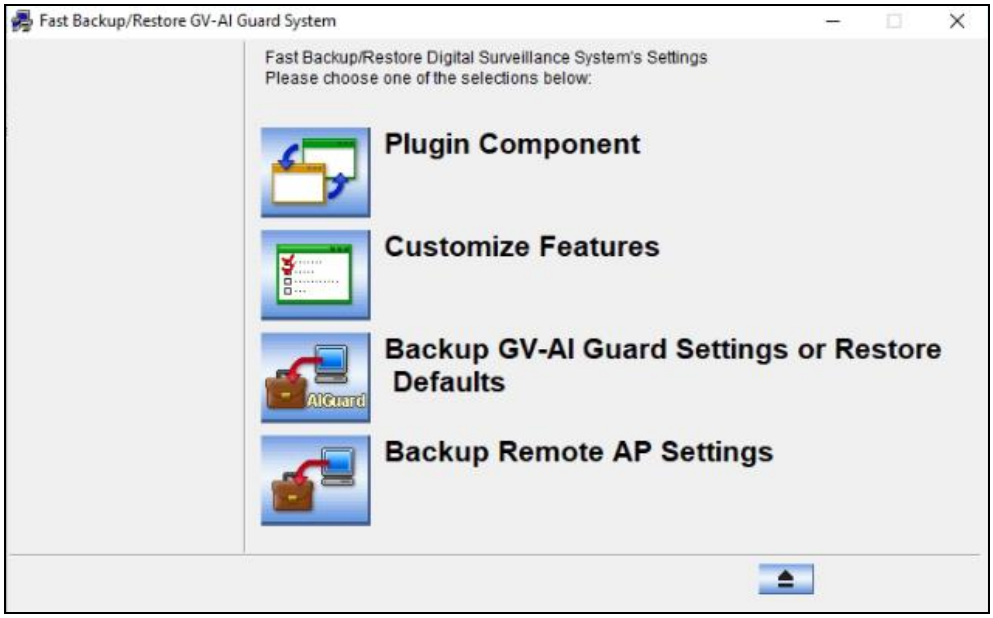
9.5 Fast Backup and Restore

With the Fast Backup and Restore (FBR) solution, you can change interface skin and customize features to suit personal preference, as well as backing up and restoring your configurations in the system.

9.5.1 Running the FBR Program

To run the FBR program, follow the steps below.

1. Go to **Windows Start** > **All apps** > **GV-AI Guard folder** > **Fast Backup & Restore Main System**. This window appears.



Fast Backup and Restore window

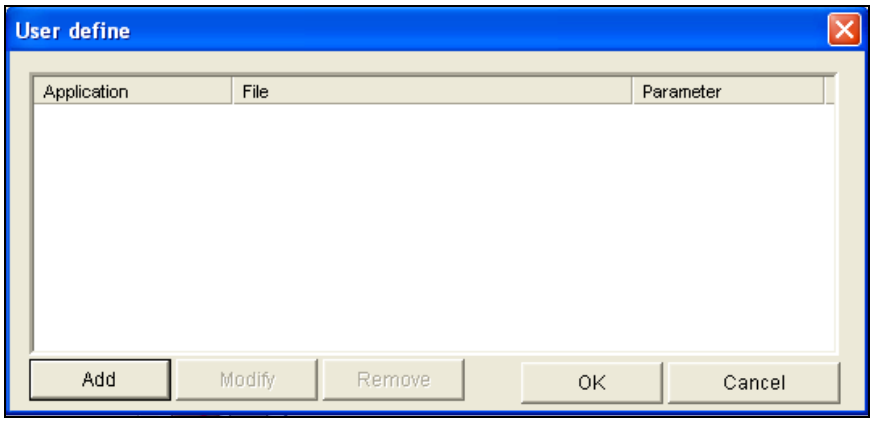
2. The first time you click any button, type a valid ID and password for the system when prompted.

After this, you can start configuring the settings.

9.5.2 Plugin Component

You can add programs to the system to expand the applications.

1. In the Fast Backup and Restore window (see the window in the previous subsection), click the **Plugin Component** icon. This dialog box appears.



2. Click **Add**. The Add New Item dialog box appears.

Note: For some applications, type **/FBR** in the Parameter column if necessary.

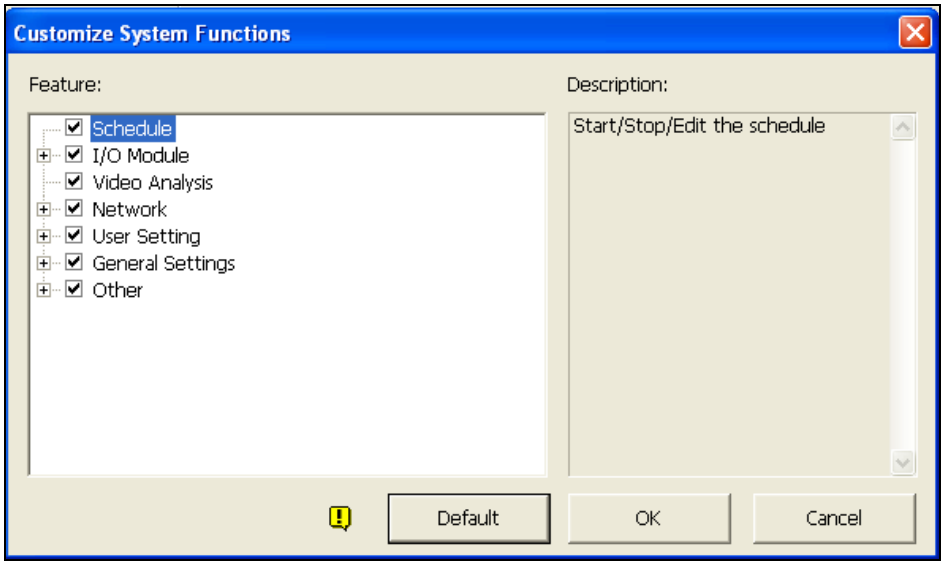
---

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 system, click **Home** > **Toolbar** > **Tools** > **Plugin**, and select a 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 Fast Backup and Restore window (see the window in *Running the FBR Program* earlier in this section), click **Customize Features**. This dialog box appears.



2. Expand the folder and click the function you want to disable in the system.
3. Click **OK** to save the settings.
4. Restart the system for the settings to take effect.

9.5.4 Backing up and Restoring Settings

You can back up the configurations you made in the system, and restore the backup data to the current system or import it to another system.

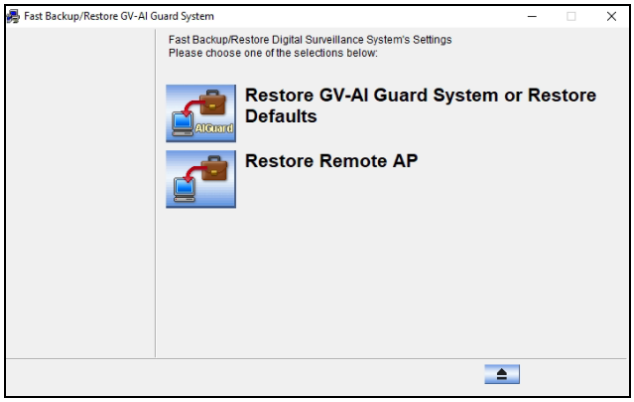
Backing up the settings

1. In the Fast Backup and Restore window (see the window in *Running the FBR Program* earlier in this section), click **Backup GV-AI Guard Settings or Restore Defaults** > **Backup Current System**.
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 GV-AI Guard 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.

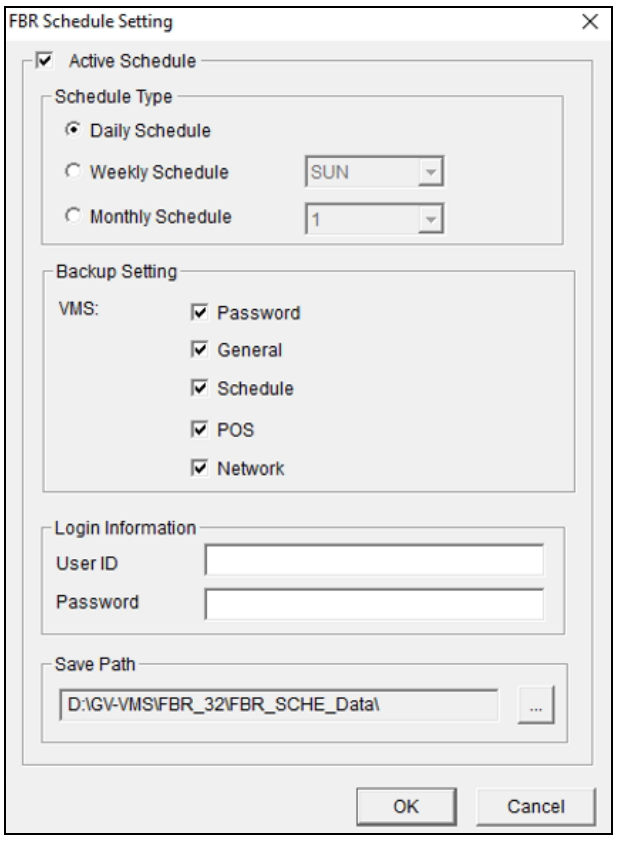


2. Click **Restore GV-AI Guard System** and select which backup settings you want to restore.
3. Click the **Next Step** button  to start restoring.
4. When the restoration is complete, the “Successfully Restore GV-AI Guard System Settings” message will appear.

Scheduling Configuration Backup

You can now set up a regular schedule with password protection to back up the system configurations you made.

1. Go to **Windows Start** > **All apps** > **GV-AI Guard folder** > **Fast Backup & Restore Main System**.
2. Click **Backup GV-AI Guard Settings or Restore Defaults** > **Schedule Setup**.
3. Select **Active Schedule**.



4. Select a desired schedule type.
5. Select desired options for backup.
   - **Password:** Back up all the user accounts and password settings of the system.
   - **General:** Back up all the settings of video analysis, IP devices, system configurations, Content List, E-Map, GV-Keyboard / GV-Joystick, and System Log.
   - **Schedule:** Back up the recording schedule configuration.
   - **POS:** Back up POS settings.
   - **Network:** Back up the network configuration for connections to GV-Vital Sign Monitor (VSM) and GV-Center V2.

6. Type a user ID and password in the Login Information section. The ID and password must be identical with that of a user account created in the system. You will need to use this ID and password to restore the backup file.
7. Locate a path to save the backup contents.

Restoring Defaults

To restore the system default, click the **Backup GV-VMS Settings or Restore Defaults** icon in the Fast Backup and Restore window (see the window in *Running the FBR Program* earlier in this section), 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. It has the following features:

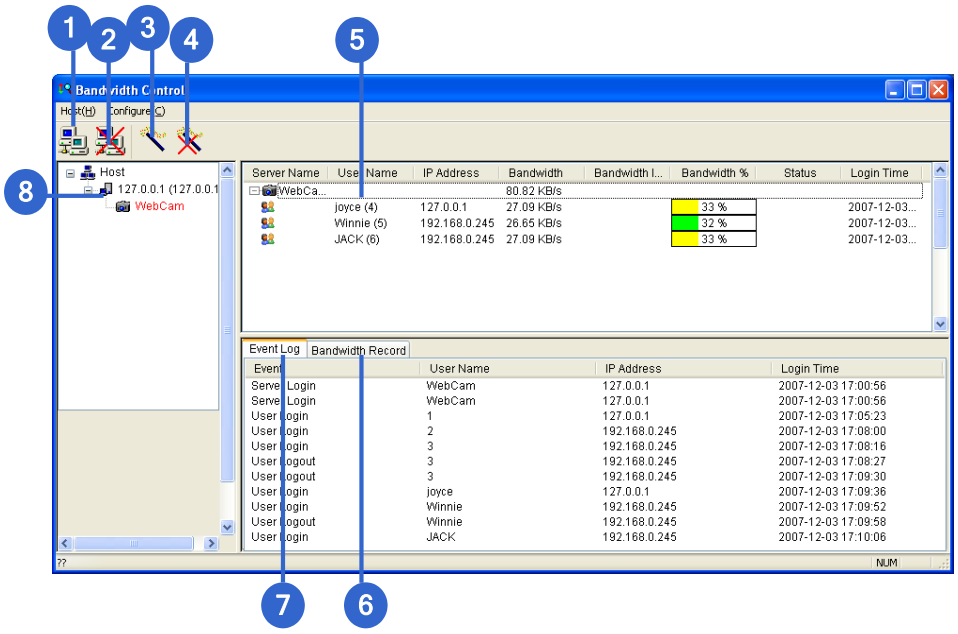
- Manage up to 5 GV-AI Guard systems
- Get bandwidth usages of every Webcam Server and every user
- Set bandwidth thresholds for specific users and IP addresses
- IP black and white list
- Kick unwanted users

9.6.1 Installing the Bandwidth Control

You can install **GV-Bandwidth Control Client Site** from **Utility** in the GeoVision Website.

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.

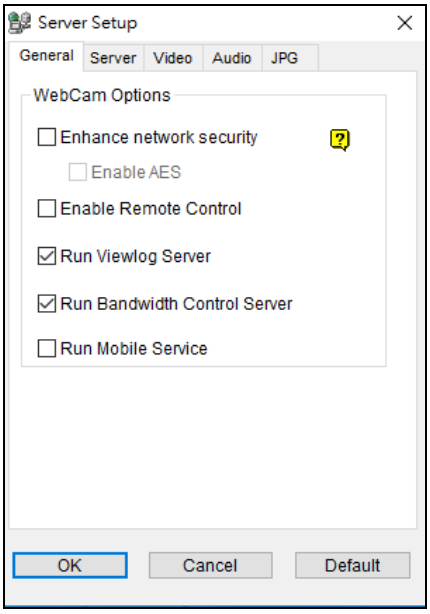


No.	Name	Description
1	Connection	Builds the connection to a WebCam Server.
2	Disconnect	Stops the connection to a WebCam Server.
3	Get Control	Obtains the right to remotely control WebCam Servers.
4	Give Up Control	Ceases controlling WebCam Servers and users.
5	User List	Displays the connected users 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.

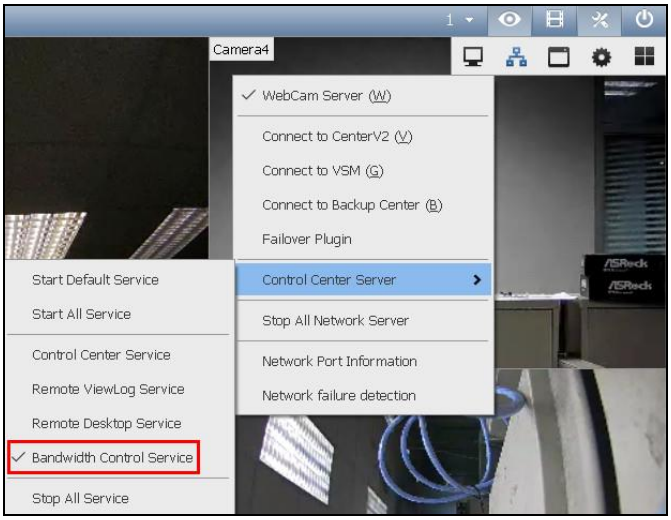
9.6.3 Allowing Remote Control

To allow the remote bandwidth control to the WebCam Server, follow the steps below.

1. On the main screen, click **Home** > **Toolbar** > **Configure** > **Network** > **WebCam Server**. This dialog box appears.

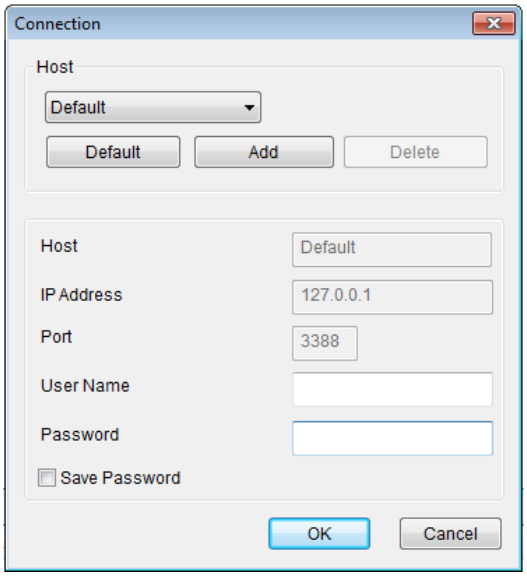


2. Under the **General** tab, select **Run Bandwidth Control server**. After this option is enabled, on the Control Center Server option list, the **Bandwidth Control Service** is marked with a check.



9.6.4 Connecting to WebCam Server

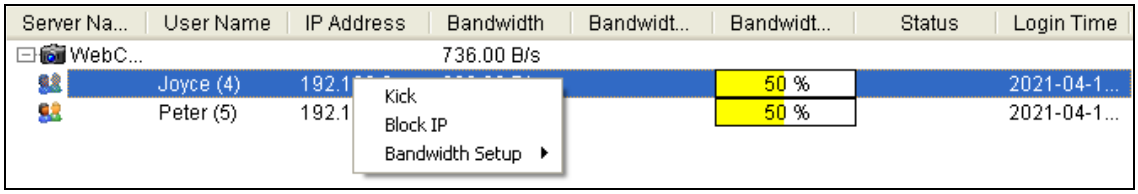
1. Click the **Connection** button (see No. 1, *The Main Window* earlier in this section) on the toolbar. This dialog box appears.



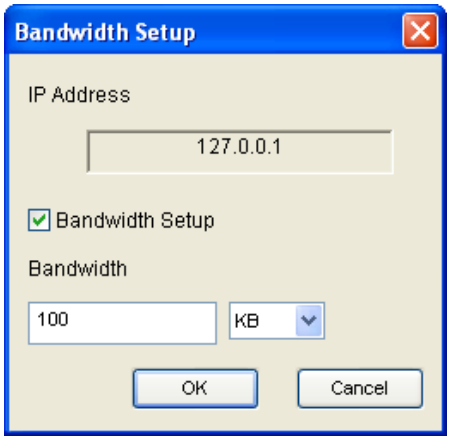
2. To add a WebCam Server to be connected to, click **Add**.
3. Type the host name, IP address, user name and password of the WebCam Server. Modify the port if necessary.
4. Click **OK**. After the connection is established, the WebCam Server shows up in the Host List.
5. You can add up to 10 WebCam Servers by repeating above steps.
6. To stop the connection, select the host and click the **Disconnect** button (see No. 2, *The Main Window* earlier in this section). 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 (see No. 4, *The Main Window* earlier in this section), the user no longer controls the WebCam Server. Whoever clicks the **Get Contro**l button (see No. 3, *The Main Window* earlier in this section) first has access to bandwidth settings. For bandwidth settings, see *Controlling a Specific WebCam Server* later in this section.

9.6.5 Controlling a 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:



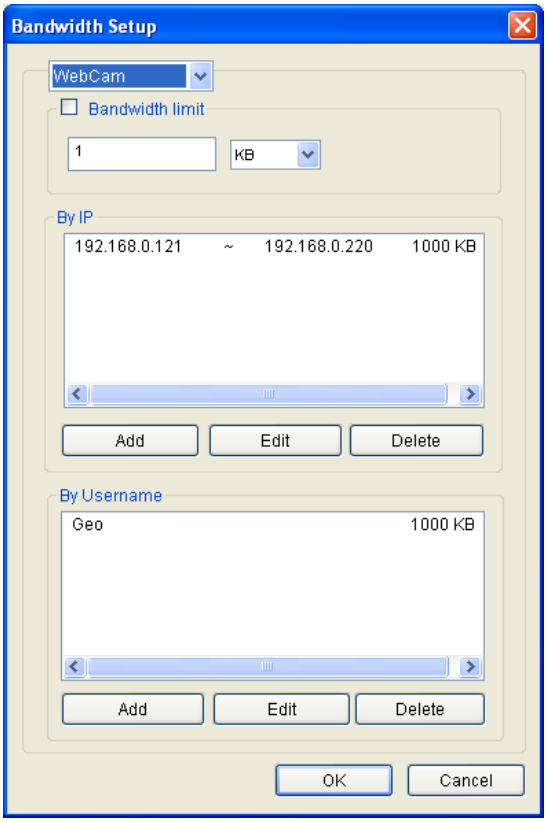
- **Kick:** Disconnect the user from the WebCam Server.
- **Block IP:** Prohibit the user from connecting to the WebCam Server. To use the function, the **Enable IP Black List** option (see *Block List Setup* later in this section) must be selected first.
- **Bandwidth Setup:** Select **By Username** 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**.



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.



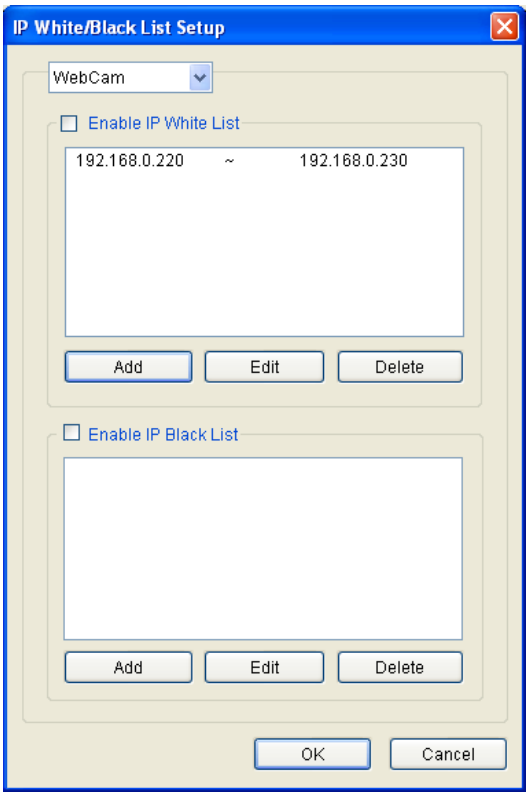
- **Bandwidth limit:** Select to define the total bandwidth that the WebCam Server will be allowed to use on your network.
- **By IP:** Click **Add** and specify an IP address or a range of IP addresses and its bandwidth limit.
- **By Username:** Click **Add** and specify the user name and its bandwidth 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.

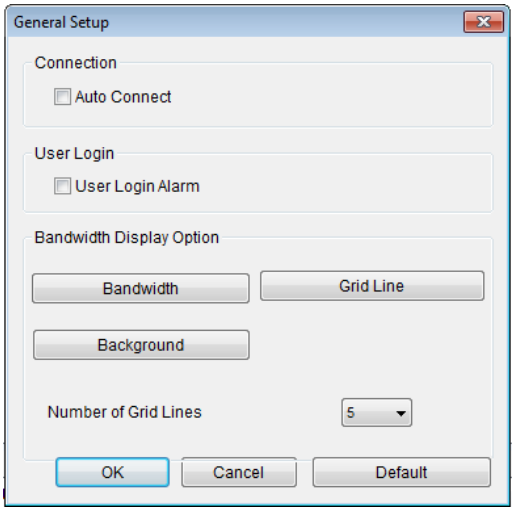


3. Select a desired type of block list and click **Add** to define the IP addresses.
   - **Enable IP White list:** Allow the defined range of IP addresses to establish the connection to the WebCam Server.
   - **Enable IP Black list:** Prohibit the defined range of IP addresses from establishing the connection to the WebCam Server.
4. Click **OK** to apply the settings.

9.6.8 General Setup

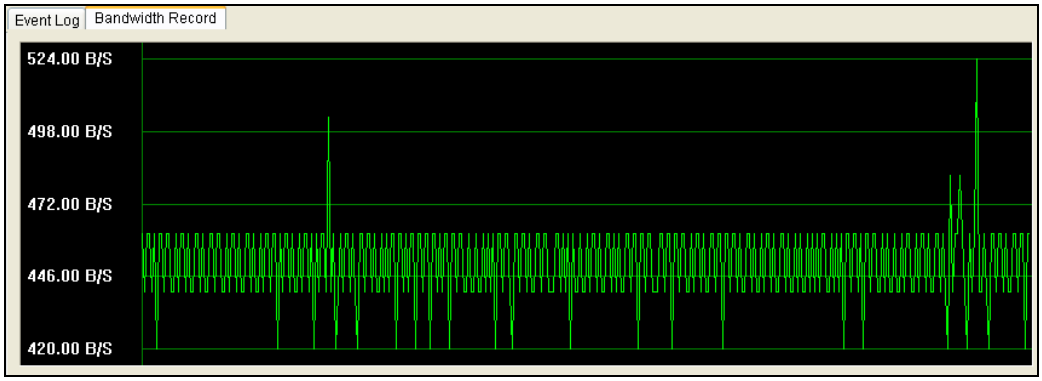
You can set up sound alarm for user log-in, or change the real-time graph display of network traffic.

Click **Configure** on the menu bar and select **General Setup**. This dialog box appears.



- **Auto Connect:** Enable the application to connect to previously connected hosts automatically next time the application restarts,
- **User Login Alarm:** Enable the computer alarm on when a user logs in.
- **Bandwidth Display Option:** Set the color of bandwidth save, grid lines of the graph and the background color of the graph.
- **Number of Grid Line:** Set the number of grid lines to be displayed on the graph.

You can click the Bandwidth Record tab in the Bandwidth Control window to view the network traffic in graph.



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, 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.

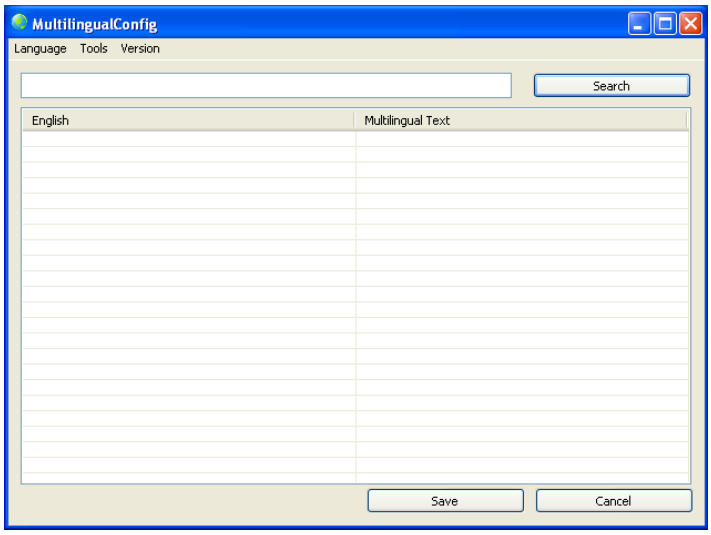
9.7.1 Installing the MultiLang Tool

You can install **GV-MultiLang Tool** from **Utility** in the GeoVision Website.

9.7.2 Revising the Translated Text

Revising the Translated Text

1. After completing the installation, close all GeoVision applications, go to **Windows Start** > **All apps** > **MultilingualConfig folder** > **MultilingualConfig**. This dialog box appears.

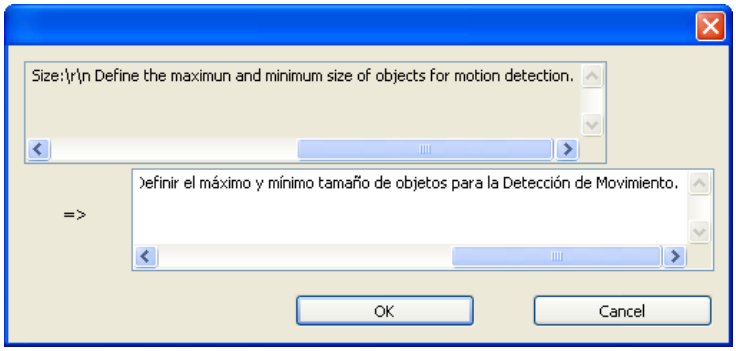


2. Click **Language** and select the language of the text you want to revise.
3. Click **Version** to select the version of the system that you want to revise.
4. In the **Search** field, type all or part of the text in English or the target language and click **Search**. The results are displayed.

Note: The search is case sensitive.

---

5. Double-click the text you want to revise. This dialog box appears.



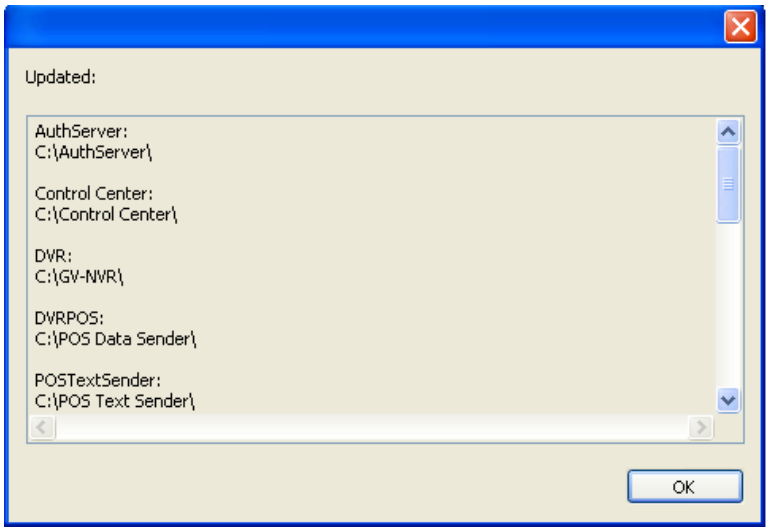
6. Revise the translated text and click **OK**.

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.



Note: The system will automatically locate the corresponding files on your computer and replace with the revised translation for the following applications: GV-AI Guard, 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.

Exporting the Revised Text

1. To export the revision as an executable file, click **Tools** > **Export** > **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.

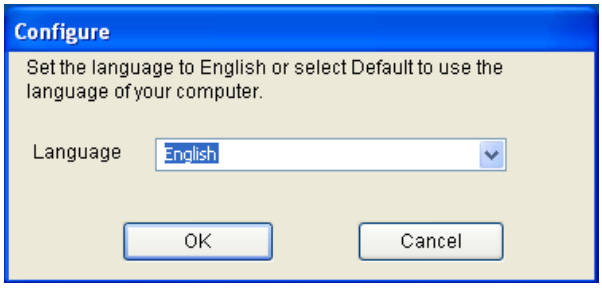
9.7.3 Setting up the UI Language to English

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-AI Guard
- 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 **GV-Set Language tool** from **Utility** on the GeoVision Website.

1. In the Configure window, select **English** from the Language dropdown list.



2. Click **OK** and restart your GeoVision software or application to enable the English UI.

9.8 GV-SD Card Sync Utility

GV-SD Card Sync Utility allows you to download videos from the memory card inserted in GV-IP Camera. When the connection between GV-IP Camera and the system is lost, recordings are automatically saved to the memory card inserted in GV-IP Camera. To automatically synchronize and download recordings from the memory card to a local folder, install and execute the utility on the system.

Note:

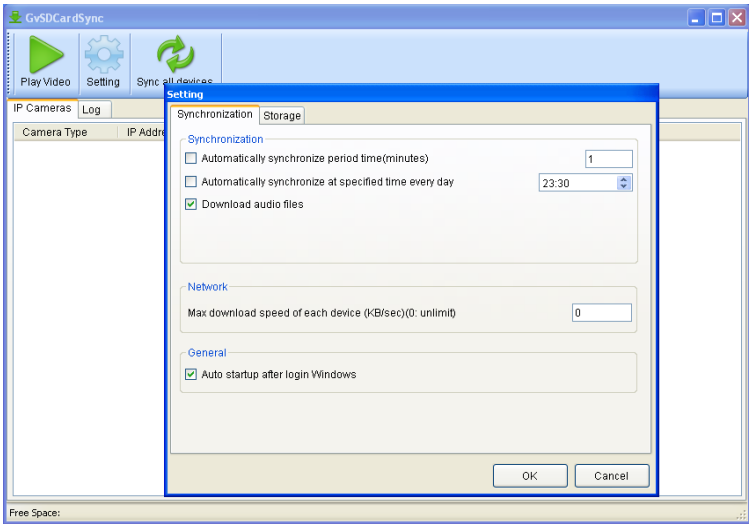
1. GV-SD Sync Card Utility is only supported by GV-IP Cam H.264 V1.11 or later, GV-IP Cam H.265 V1.00 or later, GV-BX2600 V1.00 or later, GV-PPTZ7300 V1.01 or later, and GV-SD2411 / BX12201 / FER12203 V1.01 or later.
2. It is recommended to keep GV-SD Card Sync Utility running in the background to automatically synchronize and download videos.
3. Besides the syncing SD card using GV-SD Card Sync Utility, the system also supports the **Sync recording from camera SD card when reconnected** function; see *Setting up Recording Settings for Individual Cameras* in Chapter 1.

9.8.1 Installing the Utility

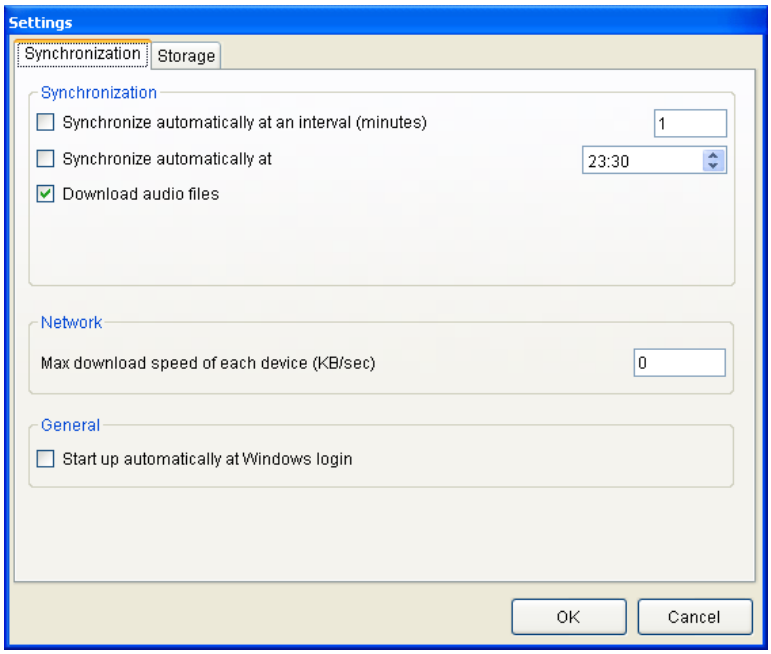
You can install **GV-SD Card Sync Utility** from **Utility** in the GeoVision Website.

9.8.2 Setting up the Utility

1. Run **GV-SD Card 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.



2. To configure synchronization, network and startup settings, select the **Synchronization** tab on the Setting window. This page appears.



[Synchronization]

- **Synchronize automatically at an interval:** Automatically synchronize videos from microSD cards to a local folder at the specified interval.
- **Synchronize automatically at:** Automatically synchronize videos from microSD 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.

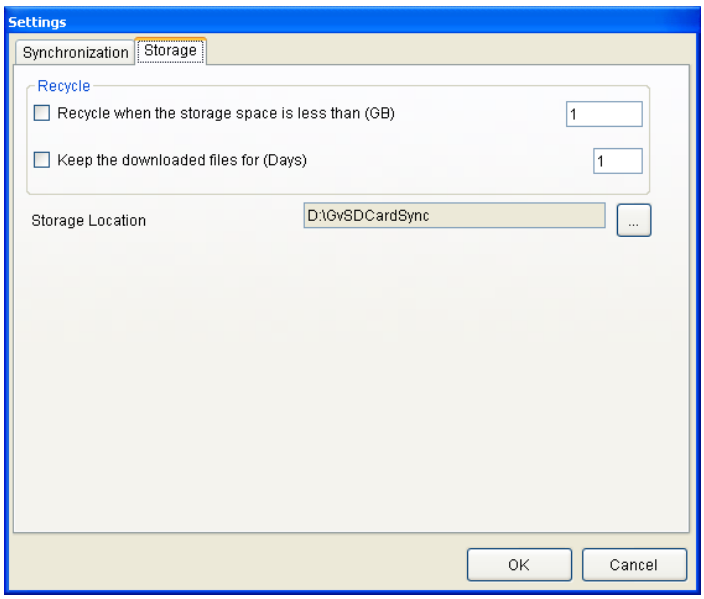
[Network]

- **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-SD Card Sync Utility when Windows starts up.

3. To configure the storage and recycling settings, select the **Storage** tab on the Setting window. This page appears.



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.

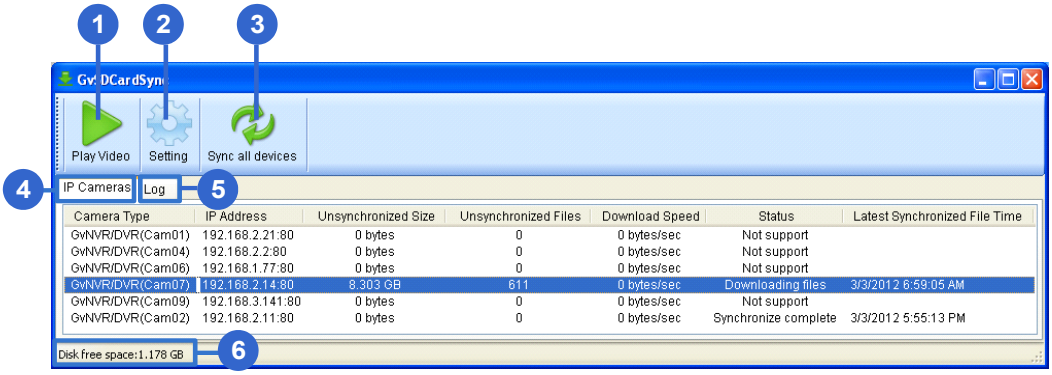
[Storage Location]

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.

9.8.3 The Main Window

After installing GV-SD Card Sync Utility, point to **Windows Start** > **All Apps** > **GV-SDCardSync** > click GvSDCardSync to launch the utility. This window appears.



No.	Name	Description
1	Play Video	Plays downloaded recordings of the selected GV-IP Cameras using the ViewLog player. See *Chapter 4 Video Playback*.
2	Setting	Configures settings of synchronization, network, storage location and recycling criteria. See *Setting up the Utility* 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 system,.
5	Log Tab	Displays up to 100 event entries. Once the entries are full, recycling will start from the oldest files.
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 GV-IP Camera.
2. The logs are deleted once the Utility is re-activated.

9.9 The Media Man Tools Window

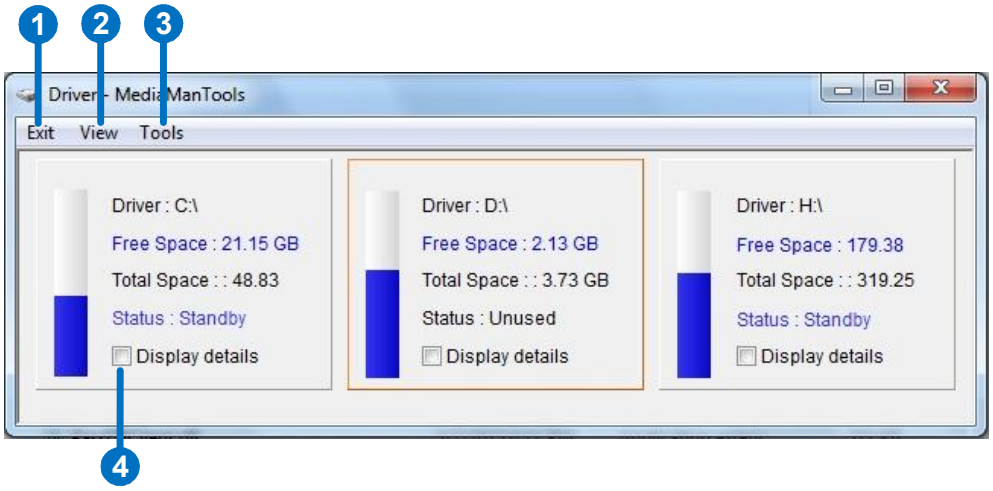
The program Media Man Tools provides a hot-swap feature, allowing a non-stop recording. You can add and remove a hot-swap or portable hard drive to the system without interrupting the monitoring. When the new drive is added, it will be configured to the recording path automatically.

Additionally, you can back up the ViewLog player and database files to play back at any computer.

Note: The minimum disk capacity for hot-swap feature is 32 GB.

9.9.1 The Media Man Tools Window

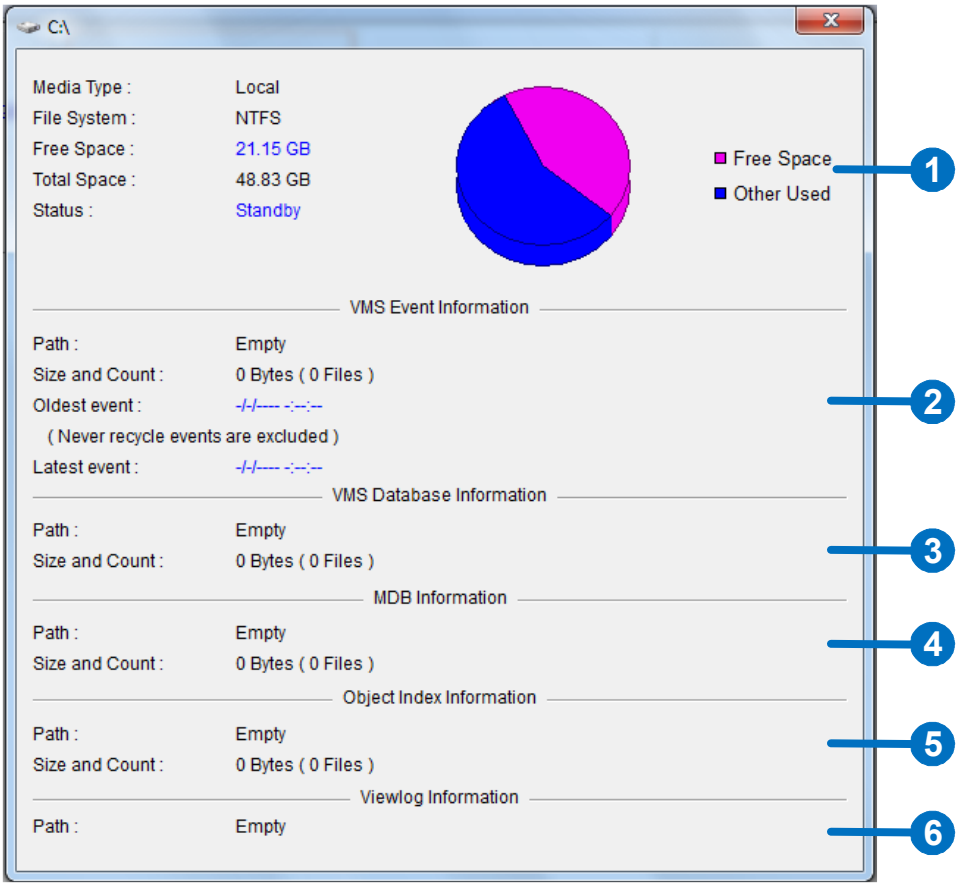
This program comes with the installation of the system. Locate the GV-AI Guard folder, and select **Hot Swap HDD Tool**. This window will appear.



No.	Name	Description
1	Exit	Closes or minimizes the Media Man Tools window.
2	View	Refreshes the disk drive status shown in this window.
3	Tools	Sets up the LED panel and automatically logs in the Media Man Tools window.
4	Display Details	Select the option to view the status and information of the disk drives. See *Viewing Disk Drive Status* later in this section.

9.9.2 Viewing Disk Drive Status

To view the detailed information of a drive, check **Display Detail**s in the desired drive section (see No. 4, *The Media Man Tools Window* earlier in this section). The status window will appear.



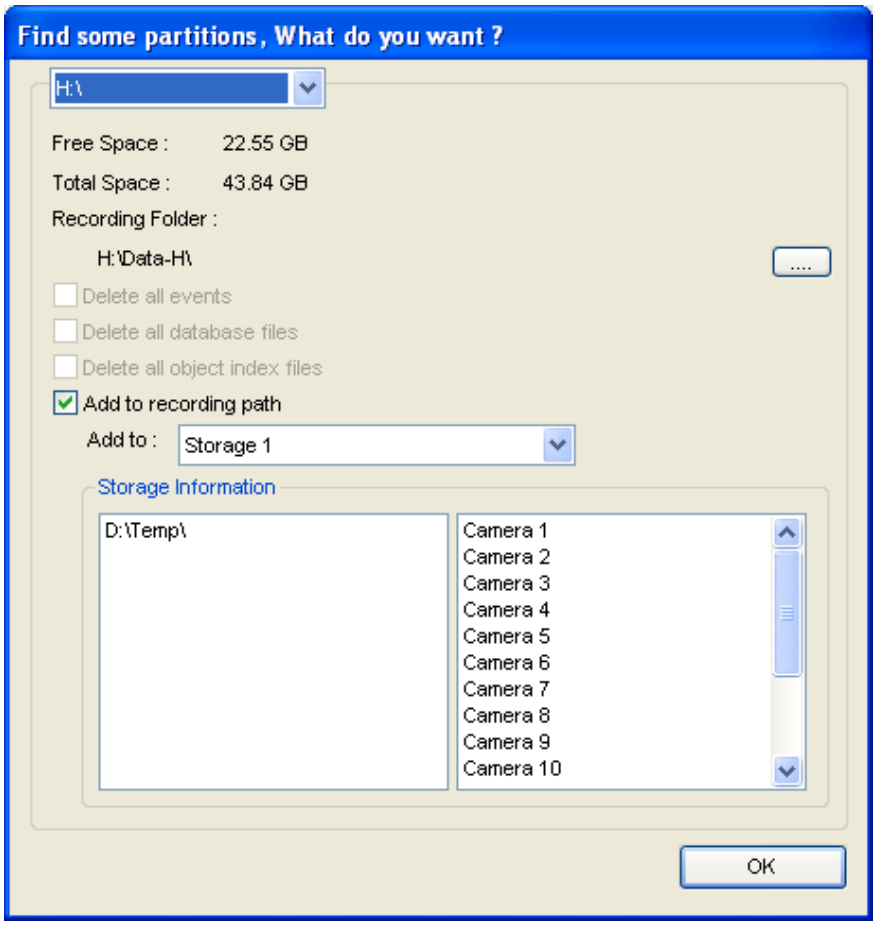
No.	Name	Description
1	Disk Properties	Indicates disk information. In “Media Type,” two messages may appear: ● **LAN:** indicates a network hard drive is connected. ● **Local:** indicates a local hard drive is connected. In “Status”, three messages may appear: ● **Standby:** indicates the hard drive already specified as the recording path. ● **Unused:** indicates the hard drive not specified as the recording path. ● **Recording:** indicates the files are being recorded to the disk.

No.	Name	Description
2	AI Guard Event Info	Indicates the path, size and number of recorded events; the dates of the oldest and latest events.
3	AI Guard Database Info	Indicates the path, size and number of the ViewLog Event List log files.
4	MDB Info	Indicates the path, size and number of System Log files.
5	Object Index Info	Indicates the path, size and number of Object Index files.
6	ViewLog Info	Indicates the location you have backed up the EZ ViewLog player.

Note: The AI Guard Event Info updates every minute. The MDB Info, AI Guard Database Info, Object Index Info, and ViewLog Info update as data changes.

9.9.3 Adding a Disk Drive

1. Locate the GV-AI Guard folder, and select **Hot Swap HDD Tools**.
2. Insert a hot-swap hard drive or plug a portable hard drive to your computer. This dialog box appears.



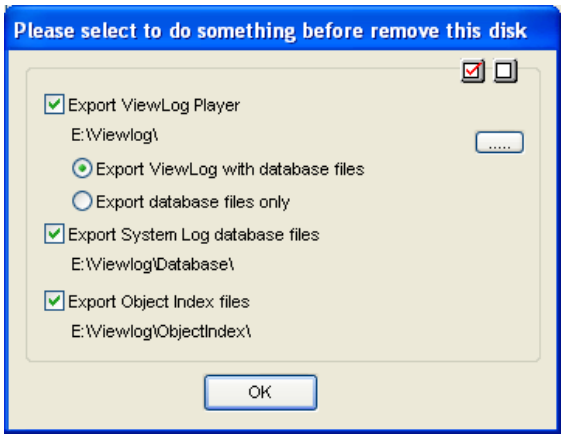
3. Select **Add to recording path** and select the storage group from the dropdown list.
4. If there are recording files saved on the hard drive, you may select the options of **Delete all events**, **Delete all database files** or **Delete all object index files**.
5. Click **OK** to automatically configure the hard drive to the recording path.

   To verify the hard drive is added successfully, check if the “Status” of the drive displays *Standby* (see *The Media Man Tools Window* earlier in this section).

Tip: To add a local drive to the recording path, right-click the desired drive on the Media Man Tools window (see *The Media Man Tools Window* earlier in this section) and select **Add for recording**.

9.9.4 Removing a Disk Drive

To remove a disk drive from the recording path, right-click the desired drive on the Media Man Tools window (see *The Media Man Tools Window* earlier in this section), and select **Remove from recording path**. This dialog box will appear. You can export related database files with the recordings on the hard drive. You can also export the ViewLog player which allows you to play back the recordings on any computer.



- **Export ViewLog Player:**
  - **Export ViewLog with database files:** Exports the ViewLog player together with ViewLog Event List log files (.db files), related to the recordings on the hard drive.
  - **Export database files only:** Exports ViewLog Event List log files (.db files) only if the ViewLog program already exits on the hard drive.
- **Export System Log database files:** Exports the System Log files (.mdb files), related to the recordings on the hard drive.
- **Export Object Index files:** Exports the Object Index files, related to the recordings on the hard drive.
- **[…] button:** If you want to change the default folder “Viewlog” created on the hard drive, click the button.

Note: Removing the hard drive will affect ViewLog database. To restore these events, add the hard drive back to the system and run **Repair Database Utility**.

9.9.5 Logging in Automatically at Startup

To automatically log in and minimize the Media Man Tools window at Windows startup, follow these steps:

1. Click **Tools** on the menu bar, and select **Auto login at Windows startup**. A dialog box appears.
2. Type the ID and password of the system for automatic login in the future.
3. If you want to minimize the Media Man Tools window to the system tray at startup, select **Auto minimize at startup**.
4. Click **OK**.

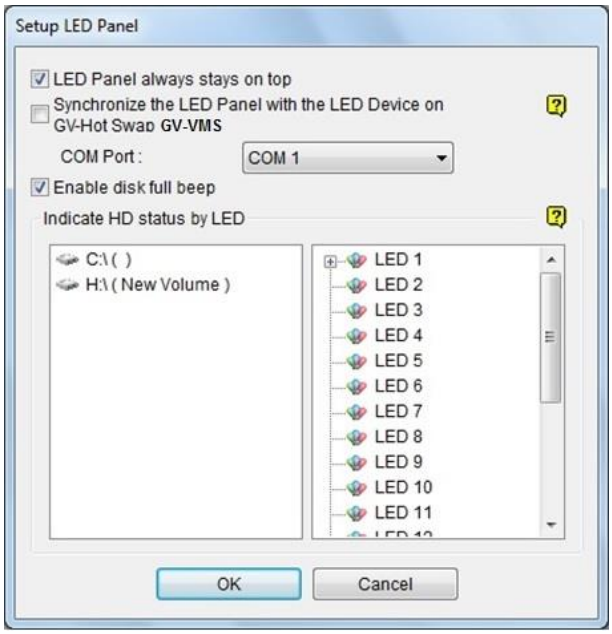
9.9.6 Setting up LED Panel

A LED panel on the screen provides a quick indication of the activity status of hard disk drives.



LED Color	Description
Gray	No HDD is assigned to this LED.
Green	A HDD is assigned to this LED.
Red	The HDD is full.
Flashing Green	The system is recording or the video / audio files are played back in ViewLog.
Flashing Red	The HDD is recycling.

1. Click **Tools** on the menu bar on the Media Man Tools window, and select **Setup LED Panel**. This dialog box appears.



- **LED Panel always stays on top:** Makes the LED panel stay on top of other windows when the Media Man Tools window is minimized.
- **Synchronize the LED Panel with the LED Device on GV-Hot Swap VMS:** For GV-Hot Swap VMS System only. If enabled, the LED device installed on the front panel of GV-Hot Swap VMS System will synchronize with the LED panel on the screen.
- **Enable disk full beep:** When the hard disk drive is full, the system makes the beeping sound. Note this function only works when the motherboard is equipped or installed with a PC speaker.

2. By default, only the hard disk drive that stores video and audio files will be assigned to LED. If you want to re-assign the hard disk drive or assign other drives to LEDs, freely move the hard disk drive to the desired LED on the tree.
3. Click **OK** to apply the settings, and minimize the Media Man Tools window to display the LED panel on the screen.
4. If you want to return to the Media Man Tools window, right-click the LED panel and select **Switch to the setup window**.

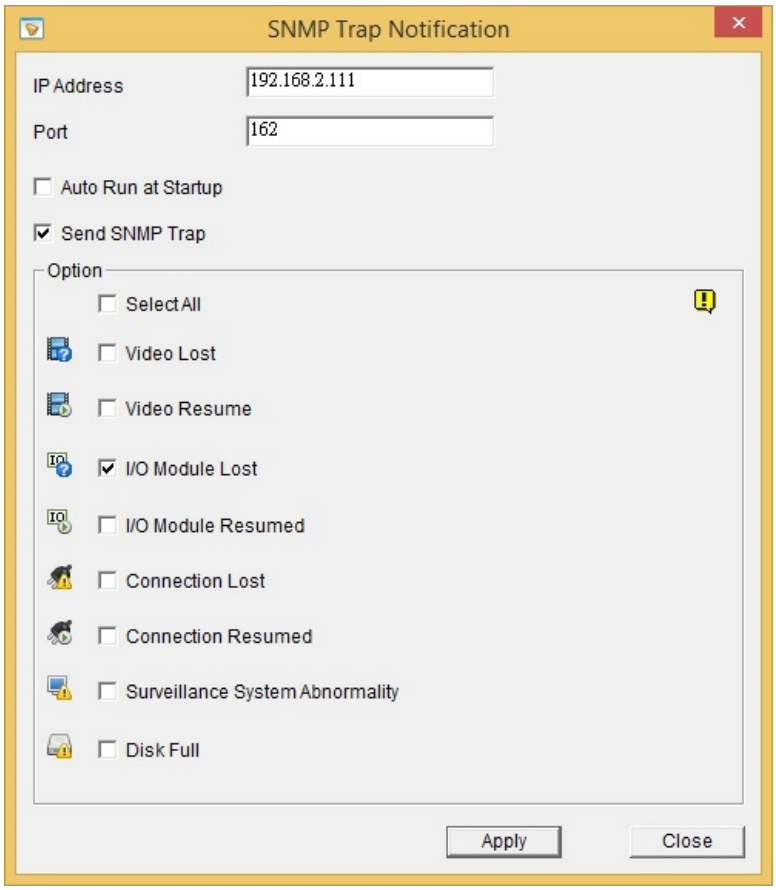
Note:

1. Because the LEDs are designed to indicate the video and audio files are being written or read, it is not recommended to assign the HDDs that store log files to the LEDs.
2. If the HDD that stores log files is assigned to a LED, make sure the log files are not being written (the LED turns red) before you remove it. Otherwise, the log files might be lost during the removal. The default location for data storage is D:\Record\<camxx or audxx folder> for recorded files, D:\CameraDBs\ for event database files, and C:\GV-AI Guard\Database for system logs.

9.10 Alert Notifications through SNMP Protocol

You can send alert notifications to SNMP-compatible software by using the SNMP Trap Notification utility.

1. Select **Windows Start** > **All apps** > **GV-AI Guard folder** > **SNMPTrapNotification.exe**. This dialog box appears.



2. Type the **IP address** of the software that will be receiving the alert notification, and modify the **Port** if needed.
3. To run SNMP Trap Notification upon system startup, select **Auto Run at Startup**.
4. Select **Send SNMP Trap** to enable the function.
5. Under Option, select the types of notifications you want to send to the software.
6. Click **Apply**.

9.11 Local and Remote Backup

The system can back up recorded files to any connected hard disk drives or GV-Backup Center over the Internet. A copy of recorded files will automatically be backed up to the assigned path or GV-Backup Center.

Note: You can only choose either **Local Backup** or **Remote Backup** (with GV-Backup Center). The two backup methods cannot be applied at the same time.

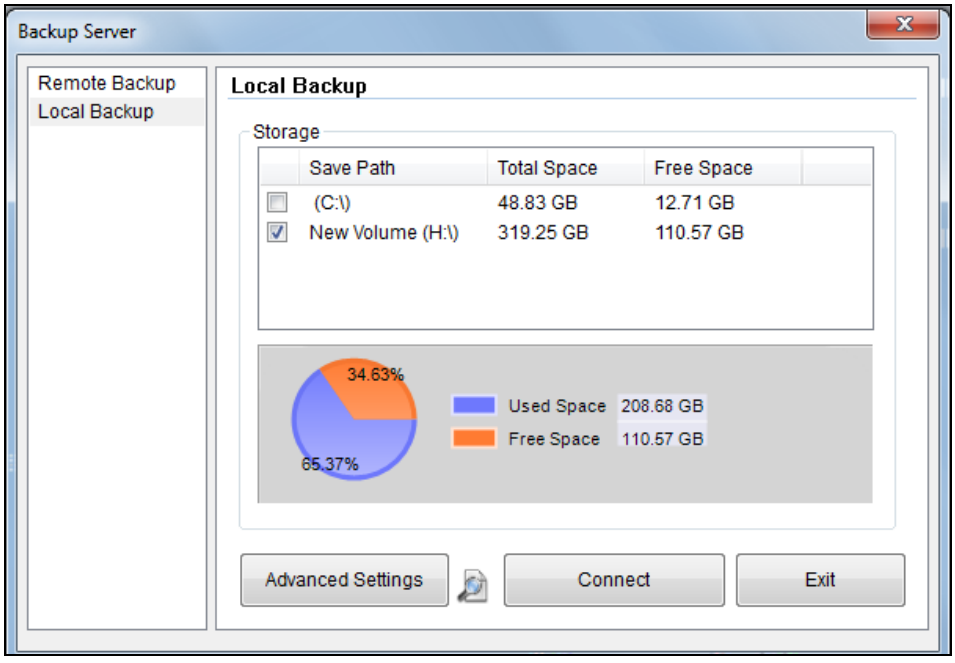
9.11.1 Remote Backup

To back up with GV-Backup Center, see *Connecting GV-VMS* in Chapter 3 in the *GV-Backup Center User's Manual*.

9.11.2 Local Backup

To connect to a hard disk drive, follow the steps below:

1. Click **Home** > **Toolbar** > **Network** < **Backup Center**. The Backup Server dialog box appears.

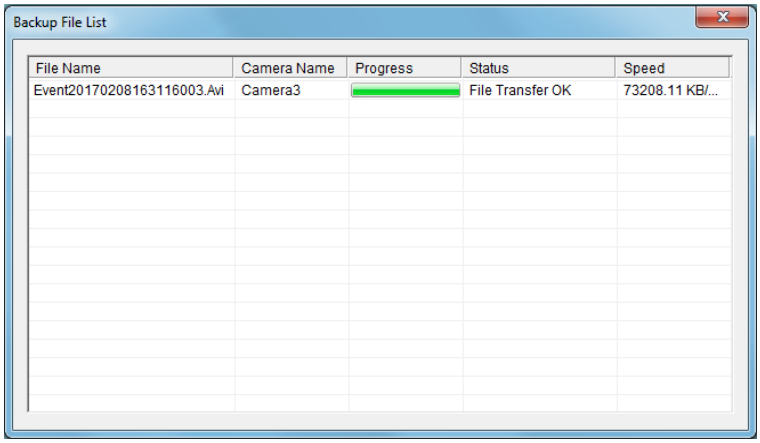


2. Select **Local Backup** in the left pane.

3. Specify in which hard drive you want to back up your files. If you assign multiple hard drives, when the first hard drive is full, the files will be backed up to the second hard drive.
4. For **Advanced Settings**, see the following subsection *Advanced Settings* for details.
5. To configure file backup schedule and transfer time, see *File Transfer Setting for Local Backup* later in this section.
6. Select your desired storage path and select **Connect** to back up files.
7. On the Windows taskbar, right-click on the **Geo Backup Client** icon. Three options are available:



- **Status**: "Connected" indicates that Local Backup is successfully activated.
- **Backup Status**: Indicates the status of file backup.
- **Playback**: Opens the ViewLog player for playback.



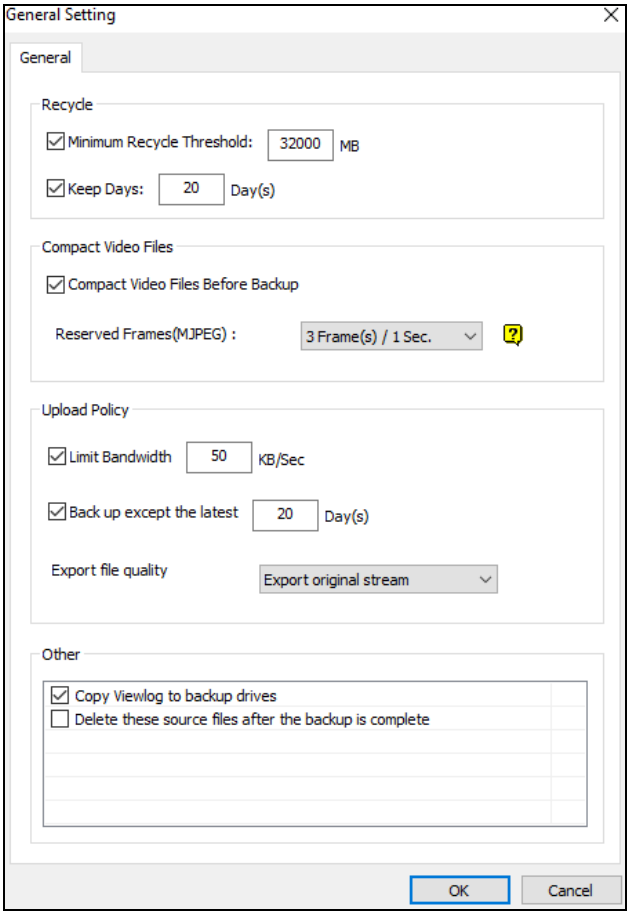
Note:

1. You can also click  on the first setting page of Local Backup to open the ViewLog player.
2. Be sure to assign different Local Backup storage paths from those of GV-AI Guard.

9.11.3 Advanced Settings

Advanced Settings for Local Backup

Click **Home** > **Toolbar** > **Network** > **Backup Center**, select **Local Backup** in the left panel, and then select **Advanced Settings** > **General Setting**. The General Setting dialog box appears.



[Recycle]

- **Minimum Recycle Threshold:** Specify a minimum free space of your local storage for file recycling.
- **Keep Days:** Specify the number of days to keep the download files at the local hard drive.
- **Compact Video Files Before Backup**: Compact the recorded video files before backing up.
  - If the recorded video is compressed with H.265 or H.264 codec, it will be compacted into key frames only.

- If the recorded video is compressed with MJPEG codec, you can use the **Reserved Frames (MJPEG)** option to specify the number of frames.

[Upload Policy]

- **Limit Bandwidth xx KB/Sec:** Specify a bandwidth limit when uploading files.
- **Back up except the latest xx Day(s):** Specify to exclude the latest number of days during backup.
- **Export file quality**: Select the desired file quality from the following options:
  - **Export original stream:** Export files in both main and sub stream.
  - **Export main stream:** Export files in main stream.
  - **Export main key stream:** Export files with only key frames in main stream.
  - **Export sub stream:** Export files in sub stream.
  - **Export sub key stream:** Export files with only key frames in sub stream.

[Other]

- **Copy Viewlog to backup drives**: Copy the ViewLog player to the assigned backup drives.
- **Delete these source files after the backup is complete**: Delete the recorded files in the system after the files are successfully backed up.

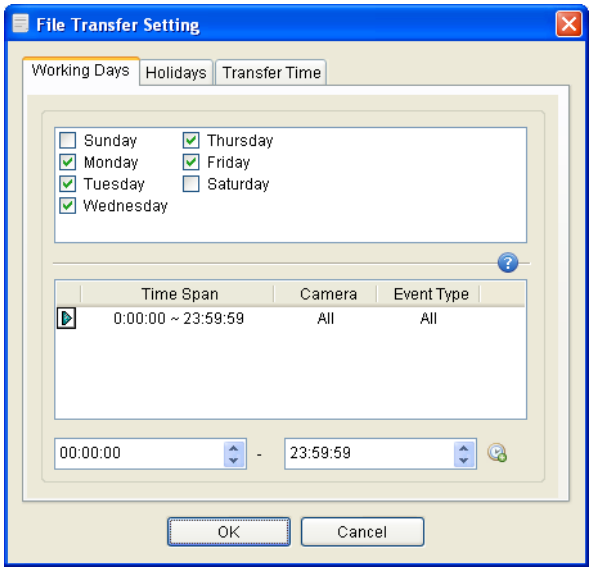
File Transfer Settings for Local Backup

Click **Home** > **Toolbar** > **Network** > **Backup Center**, select **Local Backup** in the left panel, and then select **Advanced Settings** > **File Transfer Setting**. The File Transfer Setting dialog box appears.

The File Transfer Setting allows you to specify the recordings to back up and transfer time.

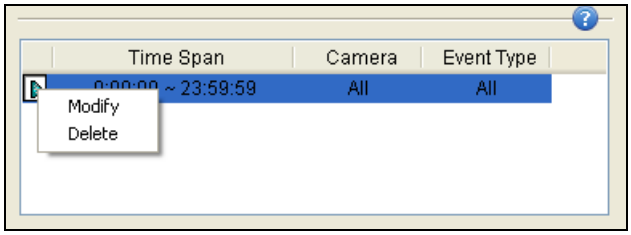
In this setting dialog box, you can define the following backup rules:

- The day of recordings to be transferred.
- The time period of recordings to be transferred.
- The type of recordings to be transferred, including motion detection, I/O trigger or all types of events.
- The time to back up the files.

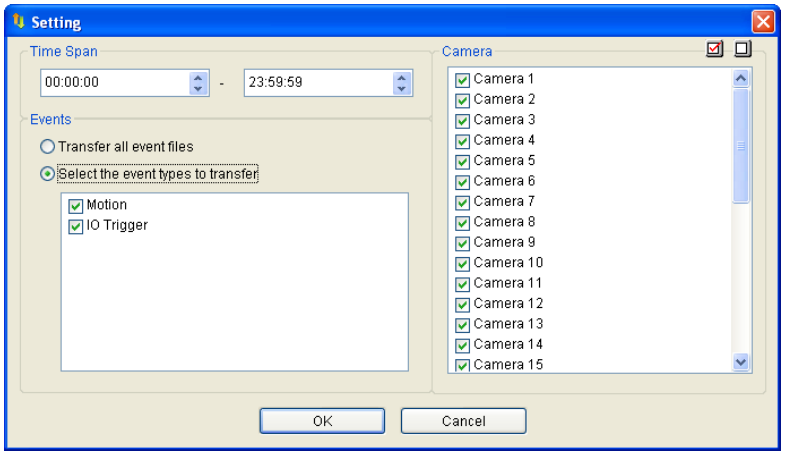


[Working Days] Define up to 10 backup rules to specify which recordings, including which type, which time period and on which working days they were recorded to be transferred to the assigned hard disk drive.

1. Select the day, including Monday to Sunday.
2. Click the arrow button before Time Span and select **Modify**.

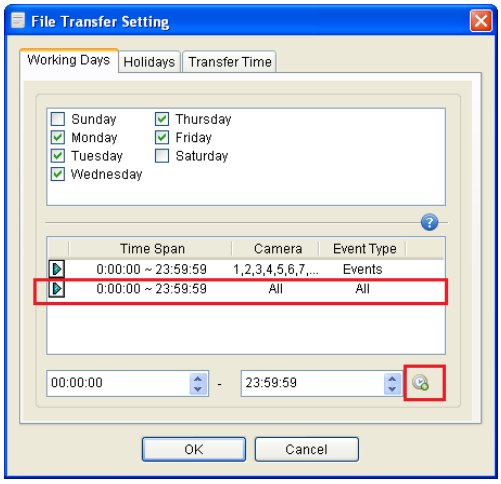


3. In this dialog box, select the **Camera** whose recordings you want to back up, specify the **Time Span** of the recordings to be backed up, and select the **Events** that you want to back up – All Events, Motion Events, or I/O Trigger Events.



4. Click **OK**. The backup settings are created.

5. To define another backup rule, click the  button. A new Time Span is created.



6. Click the arrow button, select **Modify**, and follow step 3 to define the backup rule.

[Holidays] Define up to 10 backup rules for non-working days, which include which non-working day, which camera, and which type of recording to be transferred to the assigned hard disk drive. For how to set up a rule, see the instructions in the above **[Working Days]**.

[Transfer Time] Define the daily time, from 00:00:00 to 23:59:59, to back up the files from the hosts to the assigned hard disk drive.

9.12 Report Generator

Report Generator is a useful utility that allows users to generate daily and/or weekly reports, in MDB or HTML format, for recording data of GV-AI Guard without requiring additional installation.

For details, see the *Report Generator User's Guide*.

9.13 GV-Cloud VMS

To connect to GV-Cloud VMS, see *Connecting GV-VMS or GV-AI Guard* in Chapter 2 in the *GV-Cloud VMS User's Manual* for details.

Chapter 10

Point-Of-Sale (POS) Application 385

10.1 Displaying Transactions on the Screen 386

10.2 Setting up Text Overlay 387

10.3 Filtering Transactions for a Product Item 388

10.4 Triggering Transaction Alarms 390

10.5 Mapping Codepage 392

10.6 Coloring Transactions of a Product Item 393

10.7 Displaying Receipt Details of a Transaction 396

10.7.1 Setting Up Receipt Display Conditions 396

10.8 Filtering Transactions by a Keyword 402

10.9 Searching for POS Events 405

10.9.1 Advanced Search Panel 406

CHAPTER 10

Point-Of-Sale (POS) Application

A POS device can be integrated to the system with transaction data overlaid on video channels. Transaction alerts can be triggered to notify you of transaction events. Video searches can be performed based on a specific transaction item or a specified time period.

GeoVision provides three POS integration solutions to meet a variety of needs.

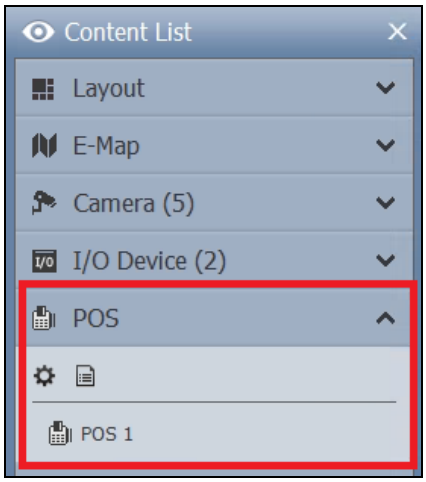
1. Direct POS Integration
2. GV-Data Capture Box Integration
3. Graphic Mode POS Integration

Please check the flowchart to find out which solution is suitable for you.

10.1 Displaying Transactions on the Screen

You can display transaction data on any of screen divisions without displaying live view.

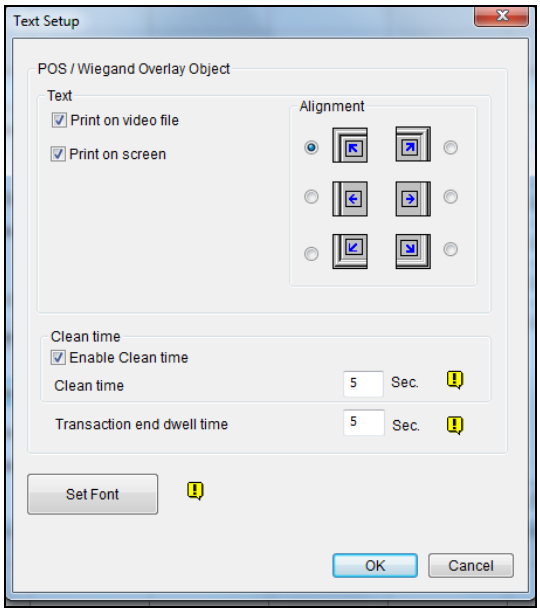
1. To set up a POS device, go to **Home** > **Toolbar** > **Configure** > **Accessories** > **POS Device Setup**. The POS device appears in the Content List. For details on setting up a POS device, check the flowchart.
2. Drag and drop the created POS device to any of screen divisions. Once the transaction on the POS starts, the data will be displayed on the screen.



Tip: To set up POS devices, you can also expand **POS** in the Content List (No. 9 in *Main Screen* in Chapter 1) and select **Configure** .

10.2 Setting up Text Overlay

To change the text font and position of the transaction data on the live view and recorded files, click the **Text Setup** button on the POS Server Setup dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Accessories** > **POS Device Setup** > select one POS device on the list > click the **Modify** button).



POS Text Setup dialog box

Tip: To set up POS devices, you can also expand **POS** in the Content List and select **Configure** .

[Text]

- **Print on video file:** Displays POS data on recorded videos.
- **Print on screen:** Displays POS data on transaction scenes.
- **Alignment:** Select the position of the text overlay on the screen.

[Clean Time]

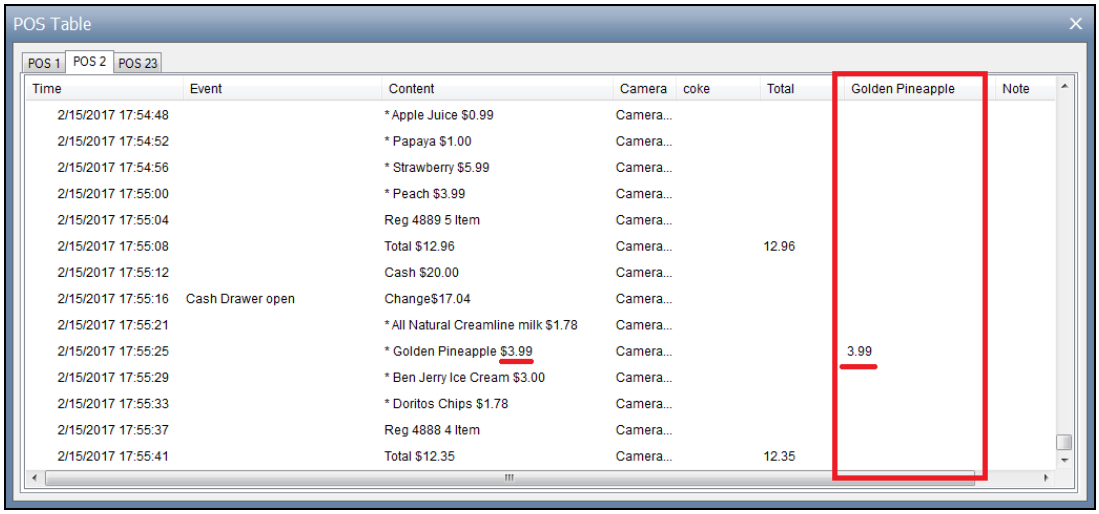
- **Clean time:** Specify the amount of time in seconds after which the system has not received the transaction data from the POS device, i.e., the cashier stops entering the transaction data. The already-displayed POS data will be hidden from live view.
- **Transaction end dwell time:** Specify the amount of time in seconds that POS data stays on the live view before the next transaction.

[Set Font] Click the button to set up the font for POS data.

10.3 Filtering Transactions for a Product Item

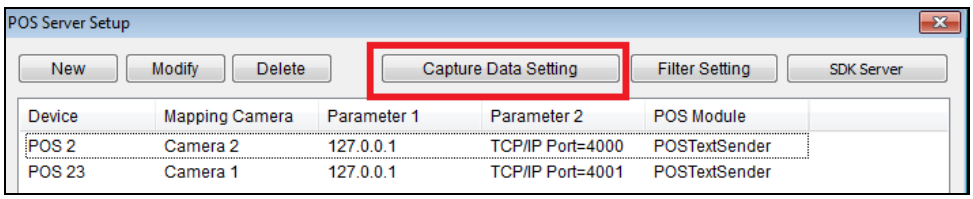
The POS Field Filter allows you to create a separate column in the System Log for a transaction item. The feature filters the transactions and highlights the item's price in the newly created column.

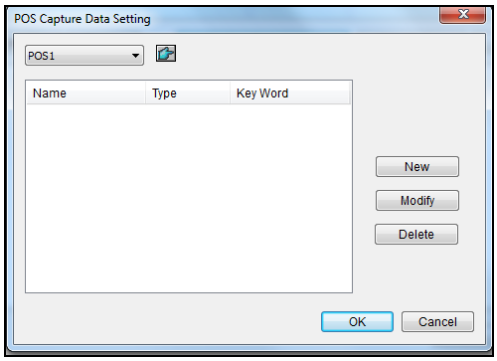
In the following example, the transaction item is "Golden Pineapple," and its transaction data stands out in the System Log to catch your eye.



To set up the function, follow the steps below:

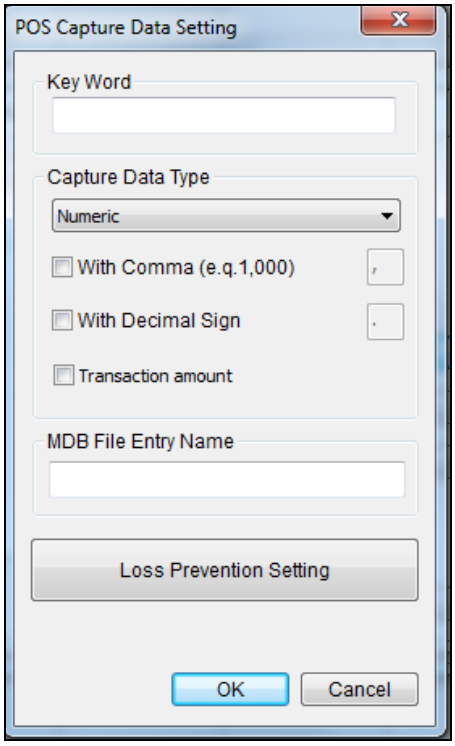
1. On the POS Server Setup dialog box, select a POS device, and select **Capture Data Setting**. The POS Capture Data Setting dialog box appears.





2. Select a POS device from the dropdown list for setup.

3. Click the **New** button and select **Caption Data**. This dialog box appears.



[Key Word] Type a keyword matching exactly a transaction item in the receipt. The field is case sensitive.

[Capture Data Type] Select the type of data followed by the specific transaction item: **Numeric**, **Currency** or **Text**. If the transaction item is followed by a price amount, select **Numeric** or **Currency**. If it is followed by alphabets, select **Text**. Any defined amount or text after the keyword will be brought out.

- **With Comma:** If there are commas in a price amount, e.g. $1,000, select the option.
- **With Decimal Sign:** If there are decimal signs in a price amount, e.g. $10.5, select the option.
- **With Space:** The option is only available when you select **Text**. If there is space among letters, select the option.

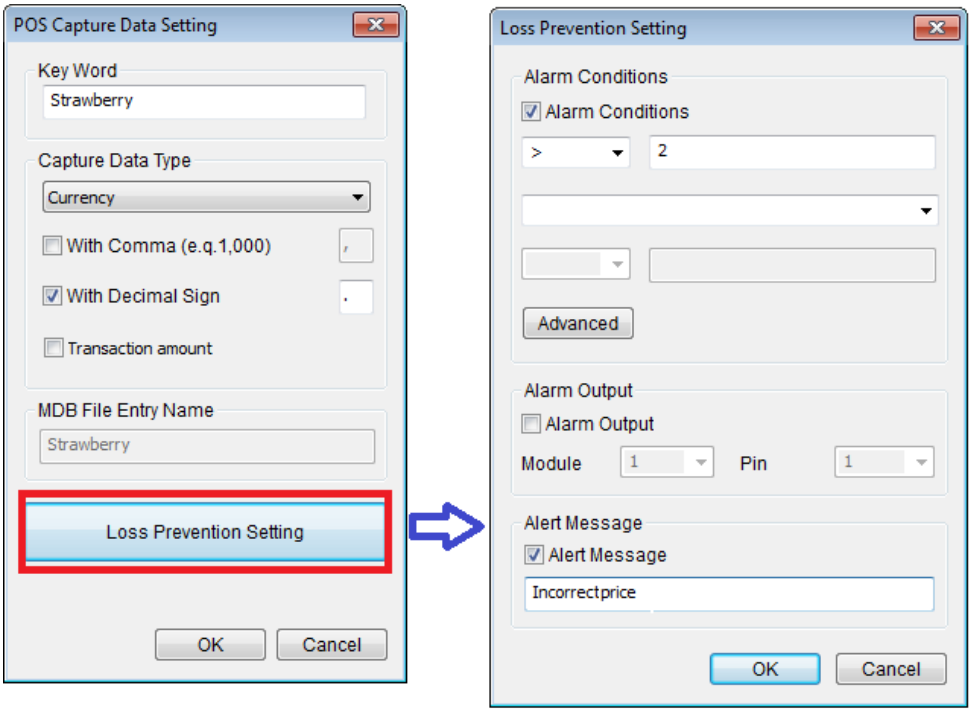
[MDB File Entry Name] Name the file to store the data.

4. Click **OK**.
5. Open the POS Table (**Home** > **Toolbar** > **Tools** > **System Log** > **POS Table**) to see the filtering results.

10.4 Triggering Transaction Alarms

When the abnormal transaction amount of an item occurs, this function can automatically activate the output device and send out E-Mail alerts. To set up this function, follow these steps:

1. Follow the steps in *Filtering Transactions for a Product Item* earlier in this chapter to define a transaction item first. Note that for this alarm function, a space between letters for the Keyword is not allowed.
2. Click the **Loss Prevention Setting** button. This dialog box appears.



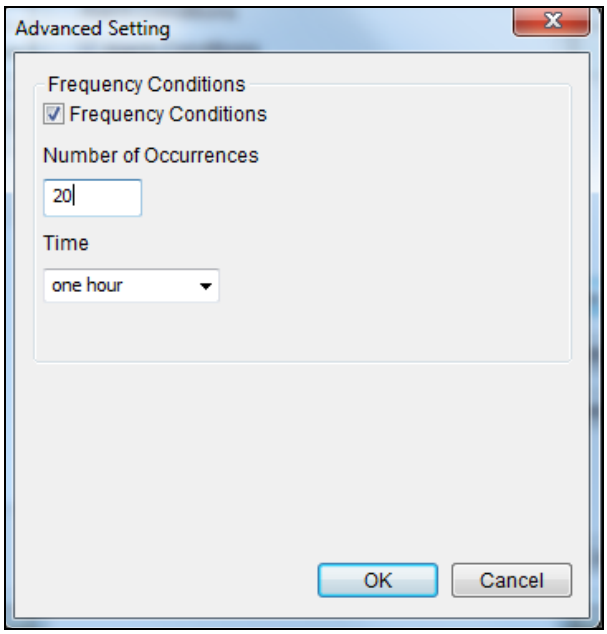
[Alarm Conditions] Define the price range for an alarm condition. For this example, when the price amount in a transaction is *greater than* (>) 2 dollars, the assigned alarm output and e-mail alert will be activated.

[Advanced button] See Step 3 below to define the alarm frequency.

[Alarm Output] Assign an installed output module. When the defined alarm condition is met, the output alarm will be triggered.

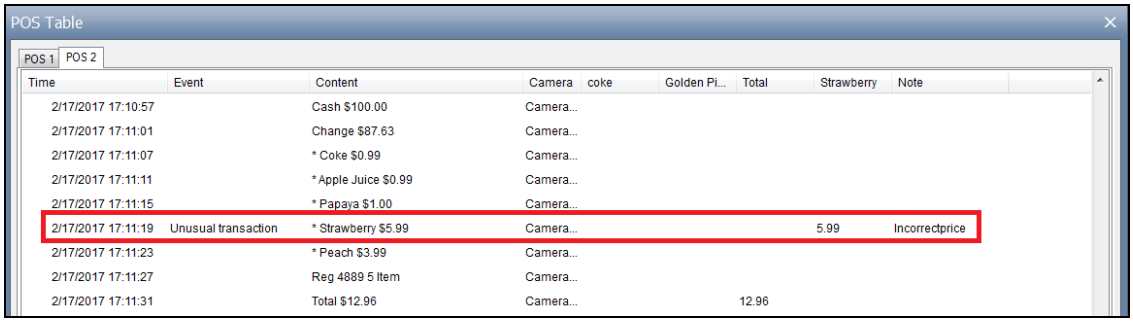
[Alert Message] Type an alert message (the space between letters is not allowed). When the defined alarm condition is met, the e-mail notifications will be sent. To configure the e-mail server, see *Setting up E-mail Notifications* in Chapter 1. In addition, the alert message will also be noted in the System Log.

3. To eliminate false alarms, configure alarm frequency.



- **Frequency Condition:** Enable to set up the number of event occurrences within a time period to trigger the alarm.
  - ⊙ **Number of Occurrences:** Specify the number of event occurrences.
  - ⊙ **Time Frame:** Select one of the time periods: **one hour**, **12 hours**, **one day**, **one week** or **one month**.

4. Open the POS Table (**Home** > **Toolbar** > **Tools** > **System Log** > **POS Table**). The transactions met the defined alarm conditions will be marked with “unusual transaction” event in the System Log.



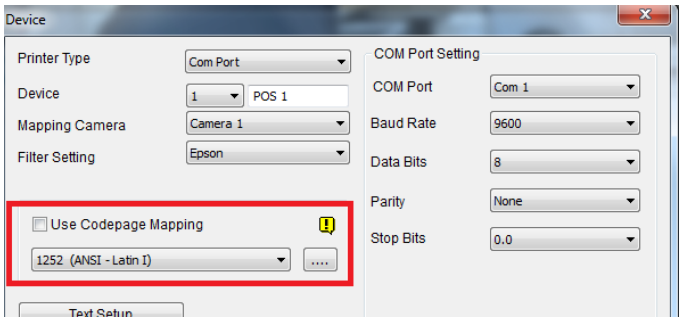
10.5 Mapping Codepage

This feature is to support the display of special characters and symbols. When transaction text incorrectly appears on the screen, a wrong character code may be used. To change a character code, follow the steps below.

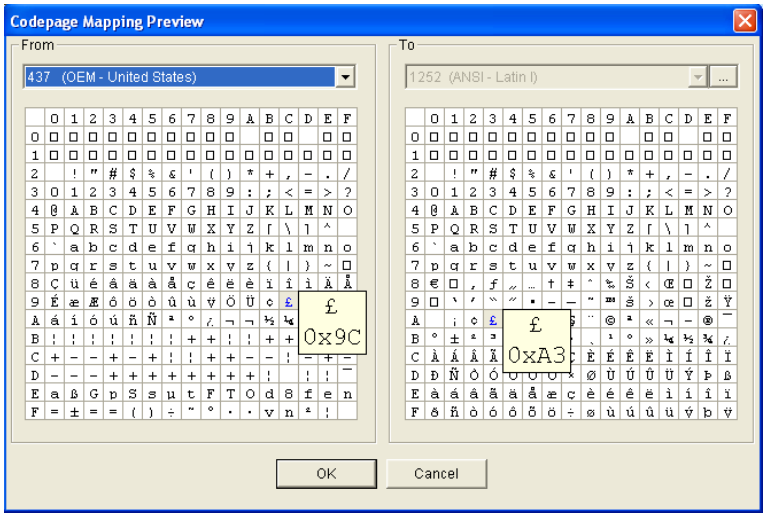
Note: When you cannot find a proper "Script" in the **Set Font** option in the POS Text Setup dialog box (see the dialog box in *Setting Up Text Overlay* earlier in this chapter), you may use the Codepage feature to fix the display issue of transaction text.

---

1. In the Device dialog box, select **Use Codepage Mapping** and select a character code from the dropdown list.



2. To verify the character code you selected, click the **[…]** button to preview its codepage.

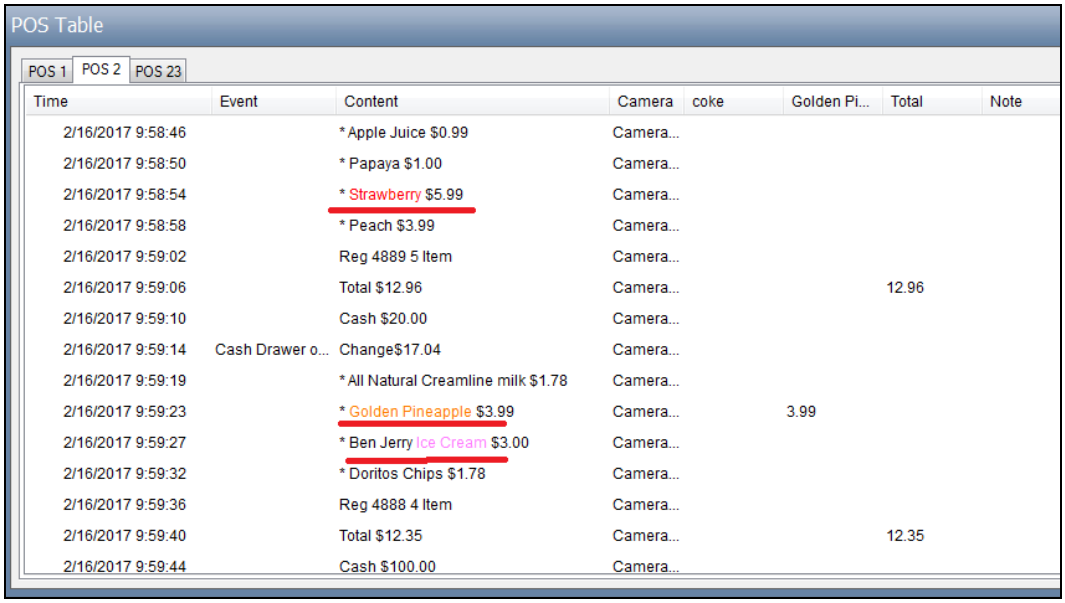


3. In the From field, select one symbol or character that are not displayed correctly. In this example, you can see its previous character code (From side: Ox9C) has been transferred to the default equivalent (To side: OxA3).

10.6 Coloring Transactions of a Product Item

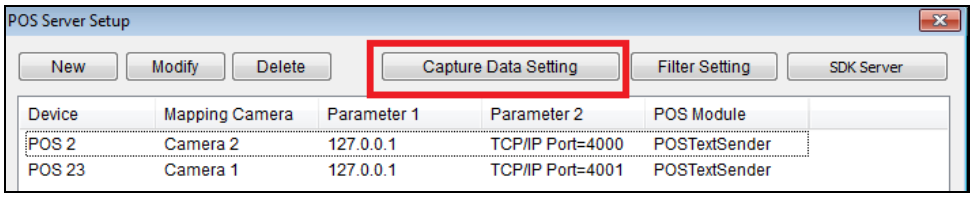
You can highlight a desired transaction item in any color. When the transaction item is identified, its text will have an outstanding color than others on the live view, and the alarm and e-mail alerts can be triggered at the same time. For example, if the liquor is prohibited for sale in the midnight, a seller can use this feature to prevent from any unintentional sale.

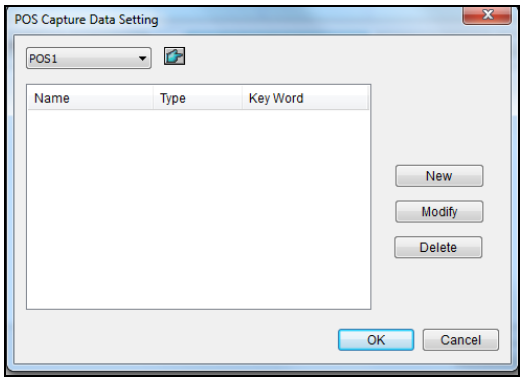
The identification will be recorded in the System Log for later retrieval as well. In this example, the transaction item “Strawberry” is colored red, “Golden Pineapple” is orange, and “Ice Cream” is pink whenever these transaction items appear.



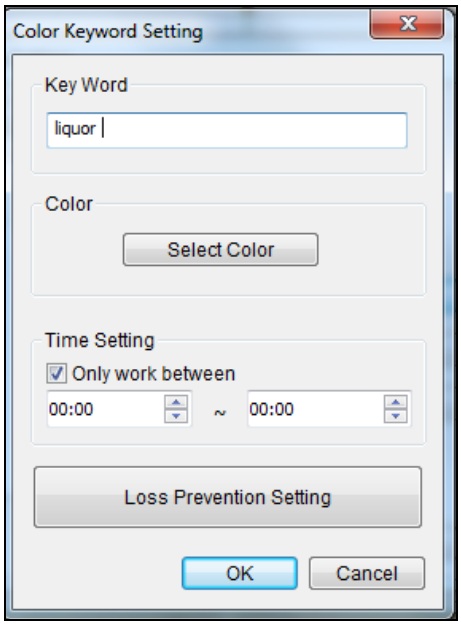
To configure the coloring feature, follow the steps below:

1. On the POS Server Setup dialog box, select **Capture Data Setting**. The POS Capture Data Setting dialog box appears.





2. Click **New** and select **Color Keyword**. This dialog box appears.



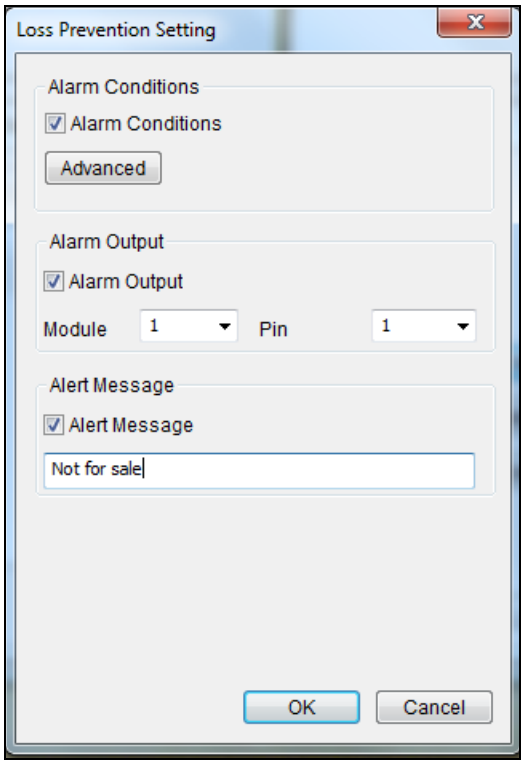
[Key Word] Type the keyword to be identified in the transactions. The field is case sensitive.

[Color] Select a color to show on the keyword.

[Only work between] Specify the period of transactions to identify the keyword.

Note: You can set up to 32 keywords for identification.

3. To trigger an alarm when the keyword is detected during the transactions, click the **Loss Prevention Setting** button. This dialog box appears.



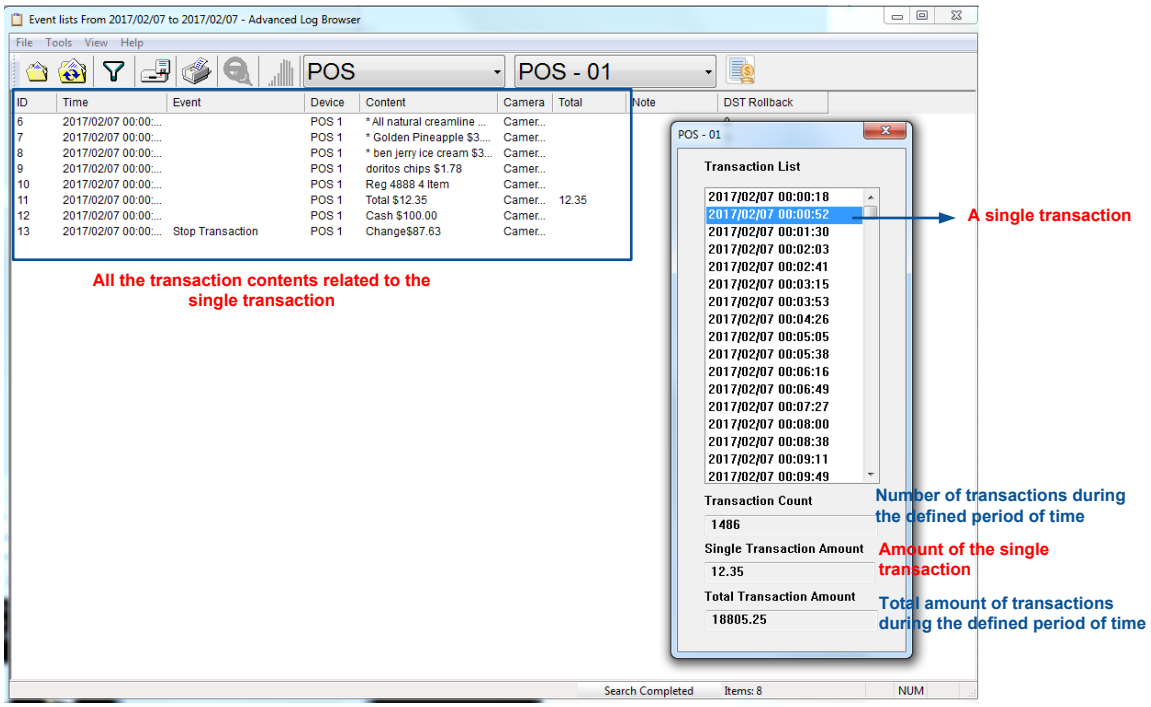
- **Alarm Conditions:** Enable the alarm when the defined text is detected. To configure alarm frequency, click the **Advanced** button. For details, see Step 3, *Triggering Transaction Alarms* earlier in this chapter.
- **Alarm Output:** Assign an installed output module. When the defined alarm condition is met, the output alarm will be triggered.
- **Alert Message:** Type an alert message. When the defined alarm condition is met, e-mail notifications will be sent. To configure the e-mail server, see *Setting up E-mail Notifications* in Chapter 1.

4. Click **OK**.

When the keyword is identified in the transactions, the identification not only appears on the live view, but also is recorded in the System Log (**Home** > **Toolbar** > **Tools** > **System Log** > **POS Table**).

10.7 Displaying Receipt Details of a Transaction

You can find out receipt details of a single transaction, so you will know the amount of the transaction, as well as the total number and total amount of all transactions during a defined period of time.



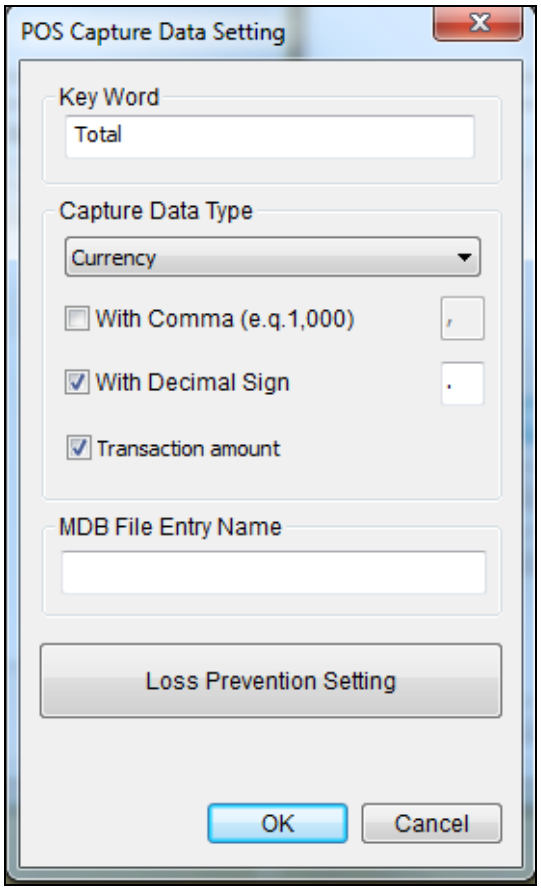
10.7.1 Setting Up Receipt Display Conditions

To have the feature, you need to define the format of how the amount of a transaction is shown and how a transaction ends on the receipt. Follow the 3 steps below to complete the settings:

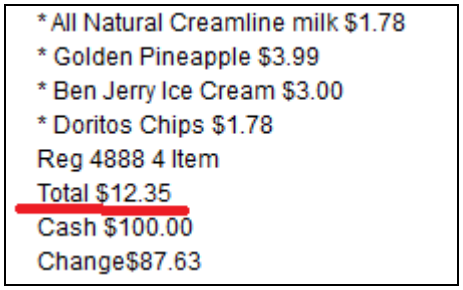
- *Step 1: Defining the Amount of a Transaction Shown on the Receipt*
- *Step 2: Define How a Transaction Ends on the Receipt*
- *Step 3: Displaying Receipt Details of a Transaction*

Step1: Defining the Amount of a Transaction Shown on the Receipt

1. On the POS Server Setup dialog box, select a desired POS device, and select **Capture Data Setting**. The POS Capture Data Setting dialog box appears.
2. Click the **New** button. This dialog box appears.



3. Take the following receipt as an example.



a. Type the **keyword** related to the amount of a transaction. In this example, the keyword is "**Total**" which is a prefix in the amount and appears in every receipt. Note the field is case sensitive.

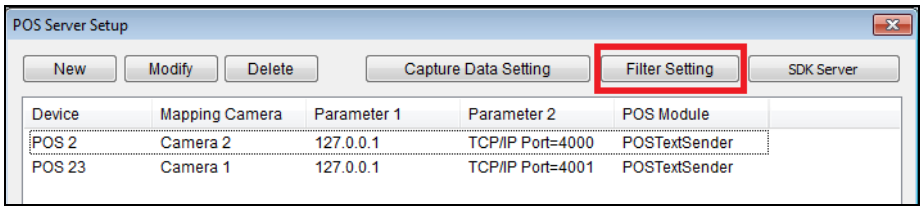
b. Under Capture Data Type, define if the total amount is attached with a currency symbol. In this example, select **Currency** because the currency symbol $ is used.

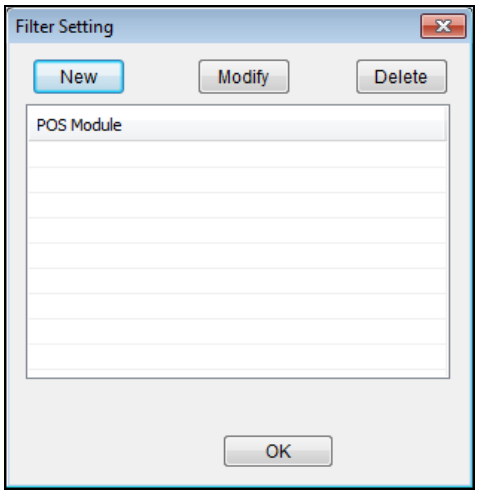
c. Select **With Comma** if there are commas in the total amount. Select **With Decimal Sign** if there are decimal signs in the total amount. In this example of "Total $12.35", select **With Decimal Sign**.

4. Select **Transaction Amount**, and click **OK**.

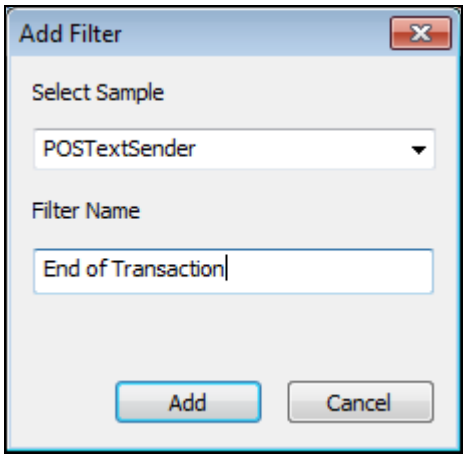
Step 2: Defining How a Transaction Ends on the Receipt

5. On the POS Server Setup dialog box, select the specific POS device, and select **Filter Setting**. The Filter Setting dialog box appears.





6. Click the **New** button. This dialog box appears.

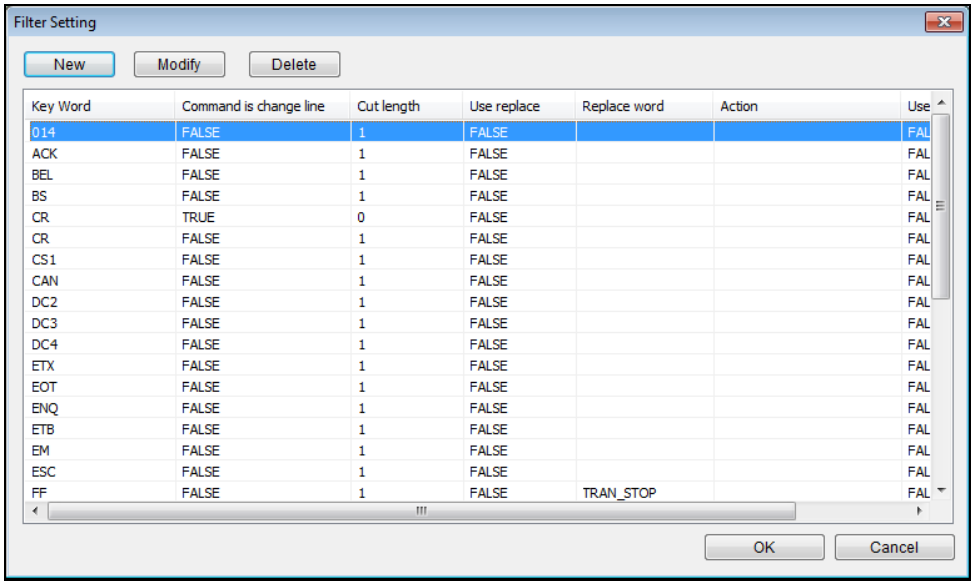


   a. Under Select Sample, select the type of printer attached to the POS device, or the GeoVision program installed in the POS device.

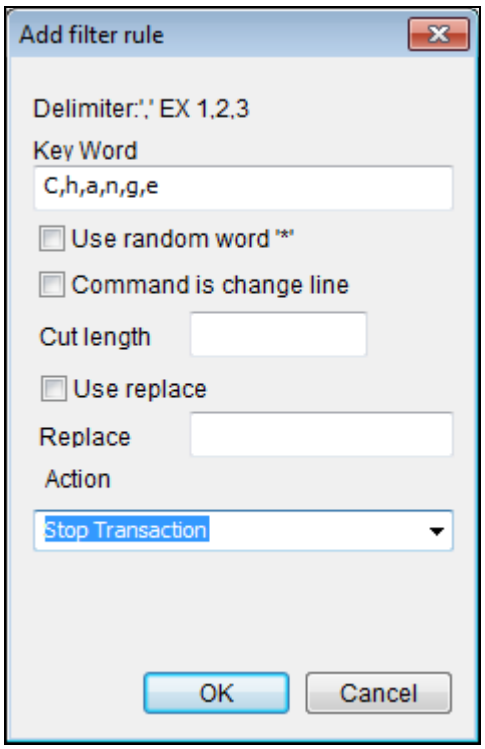
   b. Under Filter Name, name the filtering criteria. In this example, we will define how a transaction ends on a receipt, so we will name it “End of Transaction”.

7. Click the **Add** button. The Filter Name appears in the list.

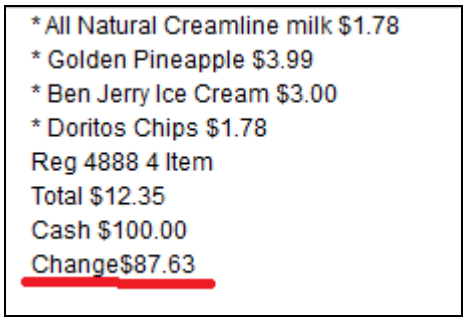
8. Select the created filter name and click the **Modify** button. This dialog box appears.



9. Click the **New** button. This dialog box appears.

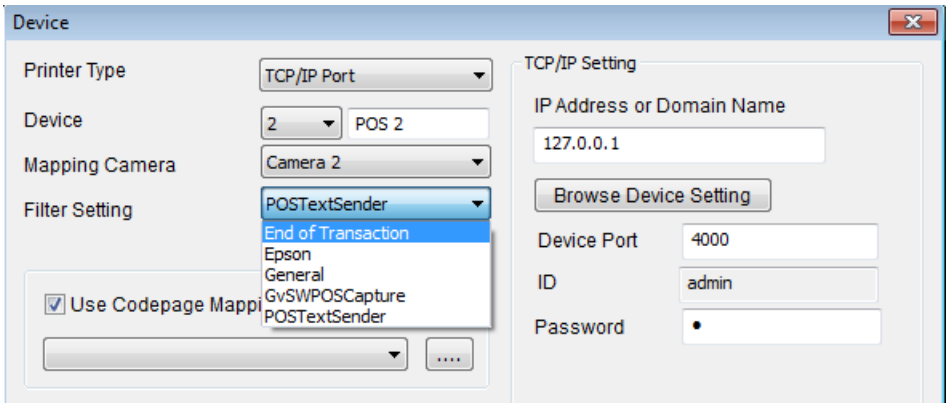


10. Type the **keyword** indicating the end of a transaction, and add comma (,) between every letter. In this example, the keyword is “Change” which appears at the end of every transaction, so type C,h,a,n,g.e.



11. Under Action, select **Stop Transaction**.
12. Click **OK** several times to return to the POS Server Setup dialog box.

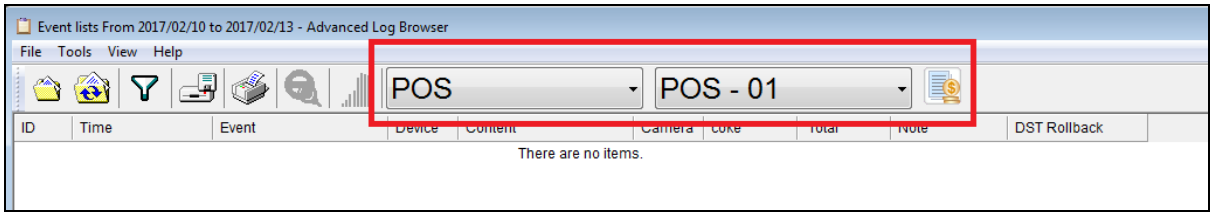
13. Select the POS device in the list applied for the filter setting, and click the **Modify** button. The Device dialog box appears.
14. Under Filter Setting, select the filter setting you set up for the end of a transaction. In this example, its “End of Transaction”.



15. Click **OK**.

Step 3: Displaying Receipt Details of a Transaction

16. Select **ViewLog** > **Toolbar** > **Tools** > **Advanced System Log**. The Open Database dialog box appears.
17. Define a period of time to retreive the POS data.
18. From the left side of toolbar, select **POS** data, select which **POS** device, and click to have a list of transactions during the defined period of time.

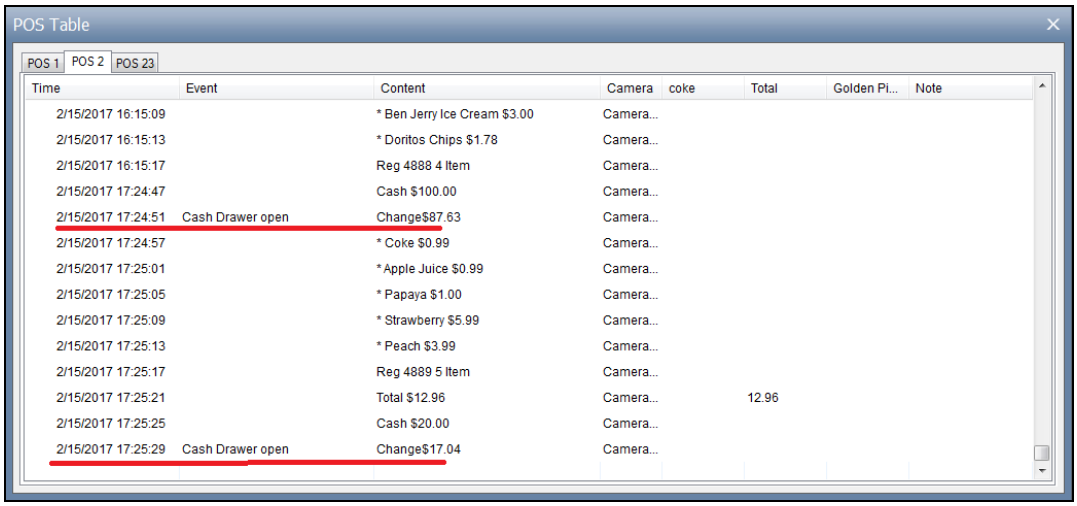


When you click a transaction on the List, its related receipt content will be displayed.

10.8 Filtering Transactions by a Keyword

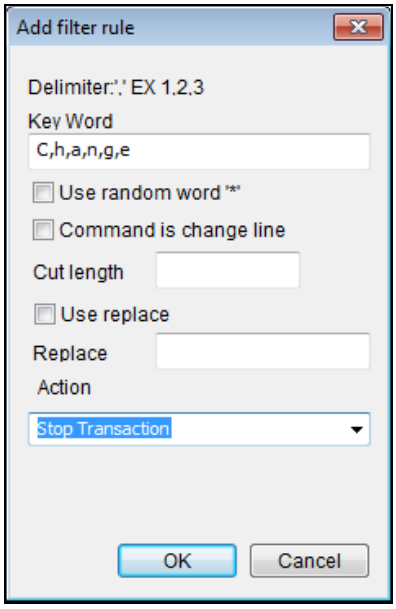
You can filter transactions by a keyword to have the following functions: to start a new line after the keyword, to remove unwanted text before the keyword, to replace a keyword with another, and/or to be noted as Event, such as Cash Drawer Open, in the System Log when the keyword appears.

For example, we define “Change” as the keyword, and specify it as “Cash Drawer Open” event. Whenever “Change” appears on the receipt, in the System Log, you will see not only the details of the transaction, but also an event “Cash Drawer Open” recorded.



To configure the function, follow the steps below:

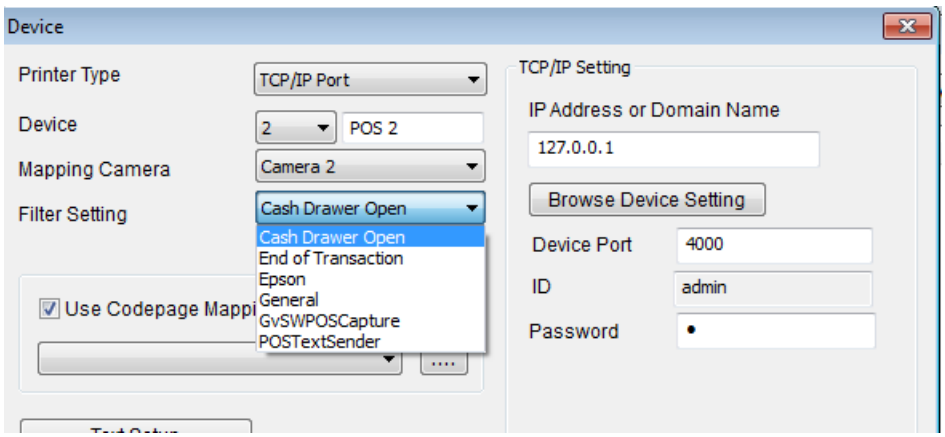
1. To open the following dialog box, follow Steps 5 to 8 in *Step 2: Defining How a Transaction Ends on the Receipt, Setting Up Receipt Display Conditions* earlier in this chapter.



2. Type the **keyword** and add comma (,) between every letter. In this example, the keyword is “Change”, so type C,h,a,n,g.e.
3. If the keyword has a random prefix, select **Use Random Word**, and type the symbol (*) before the keyword, e.g. *,C,h,a,n,g.e.
4. If you want the text to start a new line whenever the keyword appears, select **Command is change line.**
5. If you want to remove garbled text before the keyword, type the number of characters you want to remove in **Cut Length**.
6. If you want to replace the keyword with another, select **Use Replace** and type a desired word**.**
7. You can define an event to show in the System Log: Alert, Cash Drawer Open, Cash Drawer Close, Start Transaction, Stop Transaction, or Valid Transaction.
8. Click **OK** several times to return to the POS Server Setup dialog box.

9. Select the POS device in the list applied for the filter setting, and click the **Modify** button. The Device dialog box appears.

10. Under Filter Setting, select the filter setting you set up before. In this example, it is Cash Drawer Open.

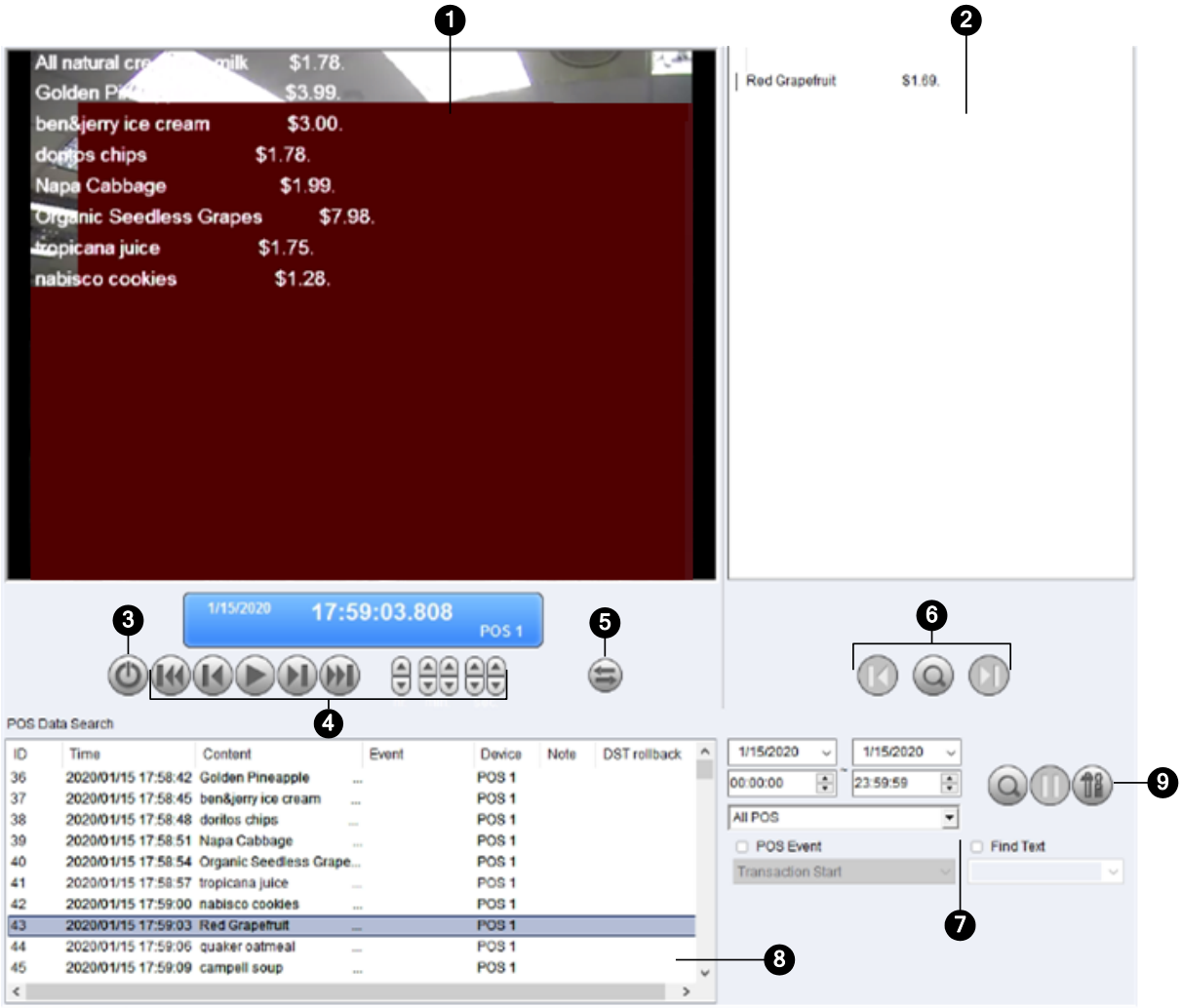


11. Click **OK**.

12. Open the System Log (**Home** > **Toolbar** > **Tools** > **System Log** > **POS Table**) to view the filtering results.

10.9 Searching for POS Events

With the POS Search function, users can instantly search for and play back the recordings of POS events from the ViewLog. To access this function, click **ViewLog** > **Toolbar** > **Tools** > **POS Search**. This window appears.



No.	Name	Description
1	Playback Window	Displays the recording of the POS event or content selected. Right-click on the window to have the options of **Play Mode**, **Render** and **Tools**
2	Transaction Window	Displays all POS transactions viewed while playing back on the Playback Window.
3	Exit	Click to close Quick Search screen
4	Playback Panel	Includes Play, Pause, Previous 10 frames, Next 10 frames and End buttons, as well as Time Period buttons to jump to 1 second, 10 seconds, 1 minute, 10 minutes and/or 1 hour later or earlier.

5	Expand / Shrink Dialog	Select **Expand/Shrink Dialog** to display the Transaction window or select **Advanced Search** to display the Advanced Search panel.
6	Find Condition	Click **Find Condition** to search for specific keywords and/or a type of POS transaction event forward or backward, starting from a date and time set. Use the Find Previous and Find Next buttons to jump from one search result to another.
7	Advanced Search Panel	See the following subsection *Advanced Search Panel*.
8	Search Results	Displays the search results by Advanced Search.
9	320<->640	Click to switch between 640 x 480 and 320 x 240 display.

10.9.1 Advanced Search Panel

To search for POS events with detailed criteria, click **Expand / Shrink Dialog** on the POS Search windo and select **Advanced Search**. The Advanced Search Panel appears.

1. Select the **Start / End Dates** and **Start / End Times** from the respective dropdown lists to specify the desired period of your POS search.
2. Select the POS devices you want to search for in the **POS Device** dropdown list.
3. Optionally select **POS Event** to search for a type POS transaction event.
4. Optionally select **Find Text** to type a keyword you want to search for.
5. After the desired conditions are set, click **Search**. The search results will be displayed at the left of the panel.