GeoVision inc
The Vision of Security

GV-VMS

User's Manual V20



VMS2013-UM-A

© 2026 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.

June 2026

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

[Warranty]

[Technical Support Policy]

Licensing for GV-VMS V20 Series

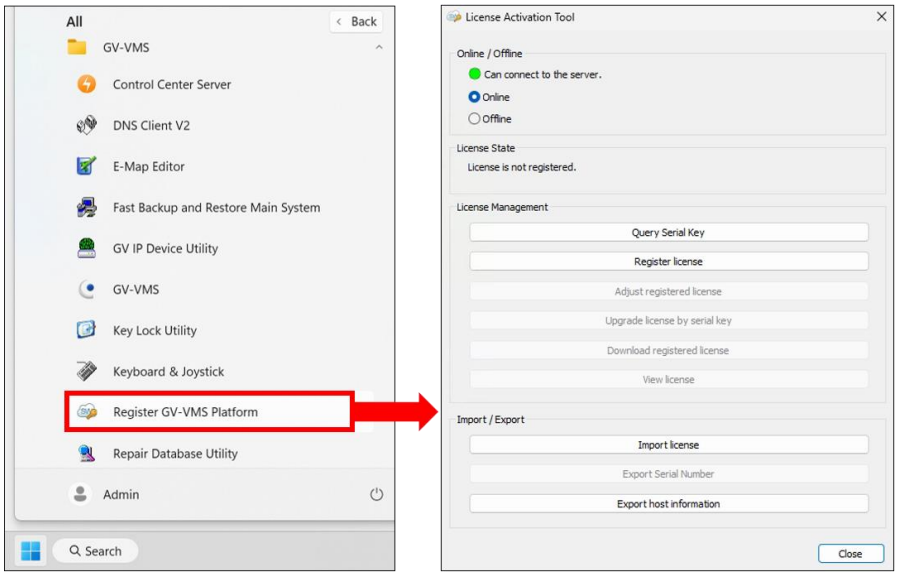
GV-VMS V20 series requires separate licenses for additional channel count, connecting to 3rd-party devices or HD DVRs, and enabling full AI functionality. For details, see *License* in Chapter 1.

Before starting GV-VMS, make sure your purchased GV-USB dongle or software license is inserted into or activated on the PC.

IMPORTANT: GV-VMS V17/V18 dongles and software licenses can be used with V20 or later without upgrade or re-registration.

For new licenses:

1. New software licenses must be registered using the **License Activation Tool** (**Windows Start** > **All apps** > **GV-VMS folder** > **Register GV-VMS Platform**) and the serial key. For details on software licensing, click here.



2. New dongle licenses require a dongle upgrade. For details on upgrading the GV-USB dongle, see *Chapter 8 Dongle Upgrade* in the *Quick Start Guide*.

V20.1 New Features

GV-VMS V20.1 supports the following new features. For details, refer to related sections.

- **GPU decoding with multiple AMD graphics cards**. See *GPU Decoding* (page v) for details.
- **Mask-compatible recognition** in the built-in face recognition engine (Local FR), enabling identification even when subjects are wearing masks.
- **Absence Event Detection** for triggering actions when no person, vehicle, or both is detected for a defined period. See *1.3.4 Setting Up Motion Detection* (page 29) for details.
- **Push notifications** via GV-Eye V3.6.0 or later, Telegram, and LINE. See *1.6.4 Setting Up Event Notifications* (pages 57-63) for details.
- **Multi-Factor Authentication (MFA)** for user login. See *1.7.2 Configuring Account Settings* (page 67) for details.
- **OAuth authentication integration** for e-mail services, enabling login-based authentication. See *1.6.4 Setting Up Event Notifications* (page 59) for details.
- **Time Synchronization Setup** window added, allowing users to configure Windows time synchronization settings directly within GV-VMS V20. See *1.2.2 Setting Up Time Synchronization* (page 13) for details.
- **Web Window function** for accessing web pages in the live view layout (GV-VMS Pro License, AI License, or GV-VMS V18 Platform License required). See *1.4.5 Setting Up Web Window* (page 45) for details.
- **Illumination Mode** option added to Video Settings in IP Device Setup, supporting switching the camera's light source between Infrared Light and White Light. See *2.2.2 Video Settings* (page 104) for details.
- **Stream Type** option (Main, Sub, or Both) added for scheduled Round-the-Clock and Motion Detection recording. See *1.8.1 Creating a Schedule with Setup Wizard* (page 76) for details.
- **Custom keyword** configuration added for 3rd-party events in IPCVA settings, enabling keyword mapping to AI events and keyword-based event exclusion. See *3.6.2 Setting Up Custom Keywords for 3rd-Party Events* (pages 178-180) for details.
- **Event snapshot download** function added in Event List and AI Query. See *1.4.1 Utilizing Live View Functions* (page 37) and *4.3.1 Performing an AI Query* (pages 204-205) for details.
- **Record List** added to ViewLog, enabling video event search by exact time. See *4.1.5 Searching Video Events with Record List* (page 191) for details.
- **Face Manager** option added in E-Map settings, enabling selection of face groups that trigger Recognition Events and Face Tracking on the E-Map. See *3.4.9 Tracking Recognized Faces* (page 163) for details.

- **Delete Group** function added in Face Manager Group Setup; not supported if Face Manager contains any GV-VD8700 (GV-Face Recognition Camera). See *3.4.2 Setting Up Face Groups* (page 153) for details.
- More feature support for **SIP function**:
  - Support for receiving calls from devices registered to the same SIP server, in addition to the original outbound dialing function.
  - Support for video calls.

  See *1.4.11 Setting Up SIP 2-Way Audio Communication* (pages 49-50) for details.
- **POS transaction integration with the GV-Cloud platform**, enabling search and video playback with POS text overlay. See *4.5 POS Transactions* (pages 35-36) in *GV-Cloud VMS User's Manual* for details.
- **Integration with Web Report on the GV-Cloud platform**, enabling Object Count (people and vehicle counting) and GV-3D People Count analytics data upload (GV-Cloud VMS V1.7.0 or later).
- Support for receiving Loitering events from GV-G Series IP Cameras. See *1. Camera's AI Events Supported by GV-VMS* (page 3) in *Camera Features Supported by GV-VMS V20*.
- Support for receiving Face Detection events from GV-BX2700-FD (IP camera).

GPU Decoding

GPU (Graphics Processing Unit) decoding can reduce CPU load and increase the total frame rate supported by GV-VMS. It can be performed by an onboard GPU, an external GPU, or both, under the following specifications. GPU decoding is performed by the GPU connected to each display.

Onboard GPU: GPU decoding is supported only when using the following CPUs:

For **H.264** Video Compression

- 2nd ~ 8th Generation Intel Core i3 / i5 / i7 Desktop Processors
- 9th ~ 14th Generation Intel Core i3 / i5 / i7 / i9 Desktop Processors
- Intel Core Ultra 5 / Ultra 7 / Ultra 9 Desktop Processors (Series 2)
- AMD processors with integrated graphics listed in this document

For **H.265** Video Compression

- 6th ~ 8th Generation Intel Core i3 / i5 / i7 Desktop Processors
- 9th ~ 14th Generation Intel Core i3 / i5 / i7 / i9 Desktop Processors
- Intel Core Ultra 5 / Ultra 7 / Ultra 9 Desktop Processors (Series 2)
- AMD processors with integrated graphics listed in this document

External GPU: GPU decoding is supported only when using:

- NVIDIA graphics cards with a compute capability of 3.0 or above and a memory of 2 GB or above. To look up the compute capability of the NVIDIA graphics cards, refer to: https://developer.nvidia.com/cuda-gpus
- AMD graphics cards listed in this document.

Note: Multiple external NVIDIA or AMD graphics cards are supported for GPU decoding. NVIDIA cards support up to 8 MP resolution.

Onboard GPU + External GPU: To have both the onboard and external GPU to perform GPU decoding, the GPUs must follow their respective specifications listed above.

Note:

1. If you have both onboard and external GPUs installed, the onboard GPU must be connected to a monitor for H.264 / H.265 GPU decoding.
2. For NVIDIA graphics cards, a CUDA compute capability of 5.0 or higher is recommended for optimal performance.

Software Specifications

GPU decoding is only supported under the following operating system, resolution, and codec.

Intel		2nd Gen	3rd ~ 4th Gen	6th ~ 14th Gen	Core Ultra Series 2
Operating System	**64-Bit**	Windows 10 / Windows 11 / Server 2016 / Server 2019 / Server 2022 / Server 2025			
Resolution		1 MP / 2 MP	1 MP / 2 MP / 3 MP / 4 MP / 5 MP / 8 MP / 12 MP	1 MP / 2 MP / 3 MP / 4 MP / 5 MP / 8 MP / 12 MP	
Codec		H.264		H.264 / H.265	
Note: For AMD GPUs, refer to AMD's official specifications for decoding support.					

Multi-Channel Playback

Multi-channel playback in ViewLog has been enhanced to improve video smoothness by increasing frame rates. However, playing back multiple channels at high resolution can increase CPU load, especially if the GV-VMS is performing other tasks simultaneously. This high load may result in dropped frames when playing back multiple recorded megapixel channels simultaneously.

To reduce CPU usage while maintaining smooth playback, consider the following:

1. Play back megapixel video in single view to minimize system load.
2. In multi-channel display environments, enable **Display Sub Stream Priority** in ViewLog, which prioritizes lower-resolution sub streams for display.

GDPR Practice

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

Login Credential Limitation

To increase security, your new password must meet the password requirements, including supported non-alphanumeric characters, length, and character categories. For details, see this technical notice.

Multi-Sensor Cameras

Each of the following multi-sensor cameras occupies multiple channels of GV-VMS when connected: GV-RMS32810 and GV-TMS20811 each occupy four channels, while GV-TMS8800 and GV-TMEB5800 each occupy two channels.

Contents

Licensing for GV-VMS V20 Series i

V20.1 New Features ii

GPU Decoding iv

Multi-Channel Playback v

GDPR Practice v

Login Credential Limitation v

Multi-Sensor Cameras v

Contents vi

1 Configuring Main System 3

1.1 Installing GV-VMS 3

1.1.1 License 3

1.1.2 Minimum System Requirements 6

1.1.3 Options 7

1.1.4 Minimum Network Requirements 7

1.1.5 Installing GV-VMS 8

1.2 Getting Started 10

1.2.1 Main Screen 11

1.2.2 Setting Up Time Synchronization 13

1.2.3 Adding Cameras 14

1.2.4 Accessing Live View 15

1.2.5 Enabling Recording 16

1.2.6 Playing Back Video 17

1.3 Recording Settings 18
1.3.1 Setting Up Global Recording Settings for All Cameras 19
1.3.2 Setting Up Recording Settings for Individual Cameras 21
1.3.3 Setting Up Video Storage Location 23
1.3.4 Setting Up Motion Detection 25
1.4 Live View and Layouts 32
1.4.1 Utilizing Live View Functions 32
1.4.2 Arranging Live View Layouts 41
1.4.3 Setting Up Zoom Window 42
1.4.4 Setting Up Scan Window 43
1.4.5 Setting Up Web Window 45
1.4.6 Setting Up Popup Window 46
1.4.7 Setting Up Focus View 47
1.4.8 Automatic Switch Among Different Live View Layouts 48
1.4.9 Adding GV-IP Decoder Box for Remote Monitor Display 48
1.4.10 Adding GV-IP Speaker for Broadcasting 48
1.4.11 Setting Up SIP 2-Way Audio Communication 49
1.5 Start Monitoring 52
1.6 System Configuration 53
1.6.1 Configuring General Settings 53
1.6.2 Customizing Startup Settings 55
1.6.3 Customizing Display Position and Panel Resolution 56
1.6.4 Setting Up Event Notifications 57
1.6.5 System Idle Protection 67
1.6.6 Configuring Fast Key Lock 68
1.7 Account and Password 69
1.7.1 Creating an Account 69
1.7.2 Configuring Account Settings 70
1.7.3 Changing or Retrieving Password at Login 73
1.7.4 Preventing Unauthorized System Termination 74
1.7.5 Setting Up a Startup Auto Login User 74
1.7.6 Setting Up Limits on Playback Time 75
1.8 Schedule 76
1.8.1 Creating a Schedule with Setup Wizard 77
1.8.2 Creating a Schedule Manually 81
1.8.3 Exporting and Importing Schedules 81
1.9 System Log 82
1.9.1 Setting Up System Log 82

1.9.2 Viewing System Log 84
1.10 AI Event Storage 86
1.10.1 Setting Up AI Event Storage 86
1.11 Other Functions 87
1.11.1 Popping Up Live View 87
1.11.2 Adjusting to Daylight Saving Time 88
1.11.3 Setting Up Network Failure Detection 89
1.12 QView 90
1.13 Storyline 91
1.13.1 Creating a Storyline in Live View 91
1.13.2 Creating a Storyline in Video Playback 93
1.13.3 Creating a Storyline in QView 93
1.13.4 Accessing a Storyline 93

2 IP Camera Setup 95

2.1 Adding IP Cameras 95
2.1.1 Adding Cameras Manually 97
2.1.2 Scanning for Cameras 99
2.1.3 Mapping GV-IP Cameras Using GV-IP Device Utility 100
2.1.4 Adding Cameras of Mobile Devices using GV-Live Streaming 100
2.2 Configuring Individual IP Cameras 101
2.2.1 General Settings 102
2.2.2 Video Settings 103
2.2.3 Video Stream Settings 104
2.2.4 Audio Settings 106
2.2.5 Abnormality Settings 107
2.2.6 Recording Settings 107
2.2.7 Advanced Settings 109
2.2.8 POE Switch Settings 110
2.3 Connection Through RTSP, ONVIF & PSIA 111
2.4 On-Demand Display 113
2.5 Wide Angle Lens Dewarping 115
2.6 Fisheye View 117
2.6.1 Setting Up Fisheye View 118
2.6.2 Setting Up a Third-Party Fisheye Camera 121

2.6.3 Object Tracking 122
2.6.4 Virtual PTZ Tour 123
2.7 PTZ Camera 125
2.7.1 Accessing PTZ Control Panel and Auto Functions 126
2.7.2 Setting Up Idle Protection and Advanced Functions 128
2.8 PTZ Object Tracking 130
2.8.1 Dual Camera Tracking 130
2.8.2 Single Camera Tracking 133
2.9 Panoramic PTZ Object Tracking 135
2.9.1 Accessing the Live View 136
2.9.2 Automatic Object Tracking 137

3 Video Analysis 142

3.1 Privacy Mask Protection 142
3.1.1 Setting Up a Privacy Mask 142
3.1.2 Granting Access Privileges to Recoverable Areas 144
3.2 Advanced Scene Change Detection 145
3.3 Text Overlay 147
3.4 Face Recognition 149
3.4.1 Enrolling Face Data 150
3.4.2 Setting Up Face Groups 153
3.4.3 Synchronizing Face Databases 154
3.4.4 Defining Access Schedule 155
3.4.5 Setting Up Recognition Alerts 158
3.4.6 Backing Up Face Database 159
3.4.7 Face ID – Live Recognition Profiles 160
3.4.8 Viewing and Searching for Face Recognition Events 160
3.4.9 Tracking Recognized Faces 161
3.4.10 Integrating Face Recognition to Access Control 164
3.4.11 Batch Enrolling Faces and Access Cards 168
3.5 Local Face Recognition 172
3.6 Video Analysis by Camera 175
3.6.1 Setting Up Video Analysis by Camera 175
3.6.2 Setting Up Custom Keywords for 3rd-Party Events 178

4 Video Playback 182

4.1 Playing Back on ViewLog 183
4.1.1 ViewLog Window 184
4.1.2 ViewLog Control Panel 186
4.1.3 Adjusting the Camera View 189
4.1.4 Bookmarking Video Events in ViewLog 190
4.1.5 Searching Video Events with Record List 191
4.1.6 Merging and Exporting Video 192
4.1.7 Saving, Printing & Copying Images 197
4.1.8 Adjusting Distorted Views 198
4.2 Object Search 199
4.3 AI Query 201
4.3.1 Performing an AI Query 202
4.4 Advanced Log Browser 207
4.4.1 Controls on the Advanced Log Browser 207
4.4.2 Filter Settings 209
4.5 Single Player 210
4.5.1 The Single Player Window 210
4.6 Specifications 211

5 Backup, Deletion, and Repair 213

5.1 Backing Up Log Data 213
5.2 Backing Up Recorded Files 214
5.3 Deleting Recorded Files 217
5.4 Repairing Damaged File Paths 218
5.5 Repairing Damaged Video Files 220

6 I/O Applications 223

6.1 Setting Up I/O Devices 223

6.1.1 Adding I/O Devices 224
6.1.2 Setting Up Input and Output Devices 225
6.1.3 Latch Trigger 227
6.1.4 Keeping Last Toggle Status 229
6.1.5 Setting Up PLC I/O devices 231
6.2 Advanced I/O Applications 233
6.2.1 Setting Up Actions upon Input or Output Trigger 234
6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger 235
6.2.3 Setting Up Momentary and Maintained Modes 236
6.2.4 Deactivating Alarm and Alert upon Input Trigger 237
6.2.5 Other I/O Application Functions 238
6.3 I/O Devices in Content List 239
6.4 Visual Automation 240

7 Remote Viewing 242

7.1 Remote Viewing Using a Web Browser 243
7.2 WebCam Server Settings 245
7.2.1 General Settings 245
7.2.2 Server Settings 247
7.2.3 JPG Settings 248
7.2.4 SDK Settings 249
7.2.5 UPnP Settings 251
7.2.6 Network Port Information 252
7.3 Mobile Service Settings 253
7.3.1 Basic Settings 254
7.3.2 QR Code Settings 255
7.3.3 RTSP Setting 256
7.4 Live View in Web Browsers 258
7.4.1 Functions on Live View 260
7.4.2 Picture-in-Picture View 261
7.4.3 Recording Video to File 262
7.4.4 Fisheye View 263
7.5 Remote Playback 264
7.6 Event List Query 265
7.7 Configure 267

7.7.1 Camera List 267
7.7.2 Server Information 268
7.7.3 Download Center 268
7.7.4 Connect to GV-Cloud 269
7.8 GV-Edge Recording Manager 271
7.9 Mobile Phone Applications 272

8 E-Map Application 274

8.1 The E-Map Editor 274
8.1.1 The E-Map Editor Window 275
8.1.2 Creating an E-Map 277
8.1.3 Creating an E-Map for a Remote Host 280
8.2 Starting E-Map 281
8.2.1 Setting Up Popup Map 282
8.3 3D E-Map Display 283
8.3.1 3D E-Map Display 283
8.3.2 Utilizing 3D E-Map Icons 284
8.4 Remotely Accessing E-Map 286
8.4.1 The Remote E-Map Window 287
8.4.2 Accessing E-Maps of Multiple Hosts 289
8.4.3 Configuring the Remote E-Map 290
8.4.4 Viewing Event List and Playing Back Videos 292
8.5 E-Map Server 293
8.5.1 Installing E-Map Server 293
8.5.2 The E-Map Server Window 294
8.5.3 Setting Up E-Map Server 295
8.5.4 Connecting to E-Map Server 295

9 Useful Utilities 298

9.1 Dynamic DNS 298
9.1.1 Running Dynamic DNS 298
9.1.2 Registering and Starting Dynamic DNS 298

9.2 Watermark Viewer 299
9.2.1 Activating Watermark Protection 299
9.2.2 Running Watermark Proof 299
9.2.3 The Main Window 300
9.3 Windows Lockup 301
9.3.1 The GV-Desktop Screen 301
9.3.2 GV-Desktop Features 302
9.3.3 Token File for Safe Mode 305
9.4 GV-Authentication Server 306
9.4.1 Installing the Server 306
9.4.2 The Main Window 307
9.4.3 Creating Clients 308
9.4.4 Creating User Accounts 310
9.4.5 Importing Groups and Users from Active Directory 313
9.4.6 Starting GV-Authentication Server 316
9.4.7 Connecting to GV-Authentication Server 318
9.4.8 Remote Access from Other Video Management Software / Mobile Application 320
9.5 Fast Backup and Restore 323
9.5.1 Running the FBR Program 323
9.5.2 Plugin Component 324
9.5.3 Customizing the Features 325
9.5.4 Backing Up and Restoring Settings 326
9.6 Language Setting 329
9.6.1 Installing the MultiLang Tool 329
9.6.2 Revising the Translated Text 330
9.6.3 Setting the UI Language to English 333
9.7 Alert Notifications Through SNMP Protocol 334
9.8 Local and Remote Backup 335
9.8.1 Remote Backup 335
9.8.2 Local Backup 335
9.8.3 Advanced Settings 337
9.9 Report Generator 341
9.10 GV-Cloud VMS 341

10 Point-Of-Sale (POS) Application..... 343

10.1 Displaying Transactions on the Screen 344
10.2 Setting Up Text Overlay 345
10.3 Filtering Transactions for a Product Item 346
10.4 Triggering Transaction Alarms 348
10.5 Mapping Codepage 350
10.6 Coloring Transactions of a Product Item 351
10.7 Displaying Receipt Details of a Transaction 354
10.7.1 Setting Up Receipt Display Conditions 354
10.8 Filtering Transactions by a Keyword 360
10.9 Searching for POS Events 363
10.9.1 Advanced Search Panel 364

Chapter 1

Configuring Main System 3

1.1 Installing GV-VMS 3
1.1.1 License 3
1.1.2 Minimum System Requirements 6
1.1.3 Options 7
1.1.4 Minimum Network Requirements 7
1.1.5 Installing GV-VMS 8
1.2 Getting Started 10
1.2.1 Main Screen 11
1.2.2 Setting Up Time Synchronization 13
1.2.3 Adding Cameras 14
1.2.4 Accessing Live View 15
1.2.5 Enabling Recording 16
1.2.6 Playing Back Video 17
1.3 Recording Settings 18
1.3.1 Setting Up Global Recording Settings for All Cameras 19
1.3.2 Setting Up Recording Settings for Individual Cameras 21
1.3.3 Setting Up Video Storage Location 23
1.3.4 Setting Up Motion Detection 25
1.4 Live View and Layouts 32
1.4.1 Utilizing Live View Functions 32
1.4.2 Arranging Live View Layouts 41
1.4.3 Setting Up Zoom Window 42
1.4.4 Setting Up Scan Window 43
1.4.5 Setting Up Web Window 45
1.4.6 Setting Up Popup Window 46
1.4.7 Setting Up Focus View 47
1.4.8 Automatic Switch Among Different Live View Layouts 48
1.4.9 Adding GV-IP Decoder Box for Remote Monitor Display 48
1.4.10 Adding GV-IP Speaker for Broadcasting 48
1.4.11 Setting Up SIP 2-Way Audio Communication 49
1.5 Start Monitoring 52
1.6 System Configuration 53
1.6.1 Configuring General Settings 53

1.6.2 Customizing Startup Settings 55
1.6.3 Customizing Display Position and Panel Resolution 56
1.6.4 Setting Up Event Notifications 57
1.6.5 System Idle Protection 67
1.6.6 Configuring Fast Key Lock 68
1.7 Account and Password 69
1.7.1 Creating an Account 69
1.7.2 Configuring Account Settings 70
1.7.3 Changing or Retrieving Password at Login 73
1.7.4 Preventing Unauthorized System Termination 74
1.7.5 Setting Up a Startup Auto Login User 74
1.7.6 Setting Up Limits on Playback Time 75
1.8 Schedule 76
1.8.1 Creating a Schedule with Setup Wizard 77
1.8.2 Creating a Schedule Manually 81
1.8.3 Exporting and Importing Schedules 81
1.9 System Log 82
1.9.1 Setting Up System Log 82
1.9.2 Viewing System Log 84
1.10 AI Event Storage 86
1.10.1 Setting Up AI Event Storage 86
1.11 Other Functions 87
1.11.1 Popping Up Live View 87
1.11.2 Adjusting to Daylight Saving Time 88
1.11.3 Setting Up Network Failure Detection 89
1.12 QView 90
1.13 Storyline 91
1.13.1 Creating a Storyline in Live View 91
1.13.2 Creating a Storyline in Video Playback 93
1.13.3 Creating a Storyline in QView 93
1.13.4 Accessing a Storyline 93

CHAPTER 1

Configuring Main System

1.1 Installing GV-VMS

1.1.1 License

GV-VMS V20 offers a flexible licensing model based on system size, devices, and features.

- **Channel count:** GV-VMS V20 supports a connection of up to 256 IP channels, with up to 64 GV-IP device channels available for free. Licenses are required for additional channels.
- **External devices:** Separate licenses are required for 3rd-party IP devices and HD DVRs.
- **AI features:** The AI License is required for full AI functionality.

License Status	Supported Features
No AI License	• AI camera events only
With AI License	• AI camera events • PVD events • Built-in face recognition (Local FR)

GV-VMS V20 License Requirements

<table>
<tr><th>Supported Devices</th><th>Channels</th><th>License Requirements</th></tr>
<tr><td rowspan="2">GV-IP Devices Only</td><td>≤ 64 ch</td><td>No license required.
Optional:
⊙ AI License</td></tr>
<tr><td>65 – 256 ch</td><td>License required:
● GV-VMS Pro License required, in increments of 32 ch.
GV-VMS Pro License
<table>
<tr><th>Levels</th><th>Total Channels</th><th>Additional Channels (Beyond free 64 ch)</th></tr>
<tr><td>#1</td><td>96 ch</td><td>32 ch</td></tr>
<tr><td>#2</td><td>128 ch</td><td>64 ch</td></tr>
<tr><td>#3</td><td>160 ch</td><td>96 ch</td></tr>
<tr><td>#4</td><td>192 ch</td><td>128 ch</td></tr>
<tr><td>#5</td><td>224 ch</td><td>160 ch</td></tr>
<tr><td>#6</td><td>256 ch</td><td>192 ch</td></tr>
</table>
Optional:
⊙ AI License</td></tr>
<tr><td rowspan="2">GV-IP Devices + 3rd-Party IP Devices</td><td>≤ 64 ch</td><td>Licenses required:
● 3rd-Party License for 3rd-party and UA-IP cameras, in increments of 1 ch.
● HD DVR License for GV-C Series IP cameras, GT-Y Series IP cameras (AI event integration not supported), and HD DVRs (GV-TXVL, UA-XVR, and UA-XVL series), in increments of 1 ch.
Optional:
⊙ AI License</td></tr>
<tr><td>65 – 256 ch</td><td>Licenses required:
● GV-VMS Pro License required, in increments of 32 ch.
GV-VMS Pro License
<table>
<tr><th>Levels</th><th>Total Channels</th><th>Additional Channels (Beyond free 64 ch)</th></tr>
<tr><td>#1</td><td>96 ch</td><td>32 ch</td></tr>
<tr><td>#2</td><td>128 ch</td><td>64 ch</td></tr>
<tr><td>#3</td><td>160 ch</td><td>96 ch</td></tr>
<tr><td>#4</td><td>192 ch</td><td>128 ch</td></tr>
<tr><td>#5</td><td>224 ch</td><td>160 ch</td></tr>
<tr><td>#6</td><td>256 ch</td><td>192 ch</td></tr>
</table></td></tr>
</table>

		• **3rd-Party License** for 3rd-party and UA-IP cameras, in increments of 1 ch. • **HD DVR License** for GV-C Series IP cameras, GT-Y Series IP cameras (AI event integration not supported), and HD DVRs (GV-TXVL, UA-XVR, and UA-XVL series), in increments of 1 ch. Optional: ⊙ **AI License**

IMPORTANT:

1. If you previously purchased the **GV-VMS V18 Platform License**, you can access all functions supported by the **AI License** after upgrading to GV-VMS V20.
2. If you previously purchased a **GV-VMS Pro License** for GV-VMS V17/V18, you will receive an additional 32 channels after upgrading to GV-VMS V20, increasing the total to **96 channels**.
3. If you previously purchased a **3rd-Party License** or **HD DVR License** for GV-VMS V17/V18, it remains valid in GV-VMS V20.
4. If two licensing dongles are used simultaneously, the total channel count is calculated as: **"64 ch" + "the Additional Channels for each selected GV-VMS Pro License level"**.

   For example, for Level #1 and Level #3:
   - 64 ch + (32 ch + 96 ch) = 192 ch

Note:

1. The licensing comes in two forms: *GV-USB dongle* and *software license*. The two are incompatible. If a GV-USB dongle is inserted into the computer with the system, please remove it before using software licensing.
2. Make sure your purchased GV-USB dongle or software license is inserted into or activated on the PC before running GV-VMS.
3. GV-USB dongle is available in internal and external models. The internal dongle is recommended for the Hardware Watchdog function, which restarts the PC when Windows is unresponsive.
4. For details on upgrading the GV-USB dongle, see *Chapter 8 Dongle Upgrade* in the *Quick Start Guide*.
5. GV-VMS automatically disables Memory Integrity on Windows 10/11 during installation. After the installation is complete, restart your PC to ensure a successful operation of GV-VMS.
6. When connecting HD DVRs using the **HD DVR** license, only **analog** channels are supported.
7. The Web Window function (for accessing web pages in the live view layout) requires a **GV-VMS Pro License**, an **AI License**, or a **GV-VMS V18 Platform License**.

1.1.2 Minimum System Requirements

Below are the minimum PC requirements for connecting GV-VMS with 64 and 256 channels of GeoVision and 3rd-party IP cameras (dual streams).

	GV-VMS (Up to 64 Channels)	GV-VMS Pro (Up to 256 Channels)
OS	64-bit Windows 10 / 11 / Server 2016 / Server 2019 / Server 2022 / Server 2025	
CPU	11th Generation i7-11700, 2.5 GHz	14th Generation i7-14700K, 3.4 GHz
Memory	16 GB RAM	32 GB RAM
OS HDD	SSD, ≥150 GB free space	
Processor Graphics	To obtain the maximum frame rate possible, see *GPU Decoding* specifications at the beginning of the manual.	

Note:

1. The following default sub stream settings are applied during initial setup based on the number of connected channels:
   a. If 1 to 32 channels are connected, all sub streams are set to 15 fps with a GOP of 30.
   b. If more than 32 channels are connected, all sub streams are set to 7 fps with a GOP of 14.
   These values help define the minimum system requirements and can be adjusted afterward.
2. When the number of connected channels exceeds 64, the databases (including the AI event database) must be stored on an SSD to achieve optimal access performance and system responsiveness.
3. To use the fisheye dewarping function, the graphics card must support DirectX 10.1 or above.
4. H.265 decoding and searching of face recognition events by face images require 6th Generation Intel Desktop Processor or above, which comes with onboard GPU.
5. Built-in face recognition (Local FR) requires 9th Generation Intel Desktop Processor or above, which comes with onboard GPU.
6. PVD motion detection requires 11th Generation Intel Desktop Processor or above, which comes with onboard GPU.
7. To expand PVD motion detection channels, ensure your PC has GV-AI Accelerator Module installed and meets the following system requirements. Without the GV-AI Accelerator Module, only up to 16 PVD channels are supported.
   a. For PVD motion detection of up to **48** channels: PC RAM of at least 16 GB and 11th Generation Intel Desktop Processor or above.
   b. For PVD motion detection of up to **64** channels: PC RAM of at least 32 GB and 13th Generation Intel Desktop Processor or above.
8. Only one unit of GV-AI Accelerator Module is supported.
9. The system requirements are determined in round-the-clock recording settings with live view only, while remote connections and video analysis are disabled.

1.1.3 Options

Optional devices can enhance your GV-VMS system's functionality and versatility. Check out the datasheet for possible alternatives.

1.1.4 Minimum Network Requirements

The data transmitting capacity of GV-VMS depends on the number of Gigabit connections available. The numbers of Gigabit network cards required to connect 256 channels are listed below according to the resolution and codec of the source video.

Codec	Resolution	Bitrate Used (Mbps)	Frame Rate (fps)	Gigabit Network Cards Required	Max. Channels Supported per Network Card
H.265	**2 MP**	0.88	30	1	Max. 256 ch / card
	4 MP	2.27	30	1	Max. 256 ch / card
	5 MP	2.93	30	2	Max. 128 ch / card
	8 MP	3.88	20	2	Max. 128 ch / card
	12 MP	4.15	20	2	Max. 128 ch / card
Note: The network requirements may vary depending on the bitrate of the streams.					

1.1.5 Installing GV-VMS

Before You Start

For optimal performance, refer to the following recommendations before installing GV-VMS:

- It is highly recommended to use separate hard disks; one for installing Windows OS and GV-VMS software, while the other for storing recorded files and system logs.
- When formatting the hard disks, select NTFS as the file system.
- When GV-VMS 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 note the total of recording frame rates that you can assign, as listed below:

Frame Rate Limit in a Single Hard Disk

Since the size of transmitted data from IP cameras may be quite large and reach beyond the transfer rate of a hard disk, you should note the total recording frame rates that you can assign, as listed below.

Frame Rate Limit in a Single Hard Disk (H.265)				
Video Resolution	**Bitrate (Mbps)**	**Max. Frame Rate / Channel (fps)**	**Max. Channels / Hard Disk**	**Total Frame Rate / Hard Disk (fps)**
2 MP (1920 x 1080)	0.88	30	32	960
4 MP (2588 x 1520)	2.27	30	32	960
5 MP (2560 x 1920)	2.93	30	32	960
8 MP (3840 x 2160)	3.88	20	32	640
12 MP (4000 x 3000)	4.15	20	32	640

Note:

1. The data above was determined using the listed bitrate, with enterprise-grade hard disks operating at 7200 RPM or higher and featuring an average read/write speed of over 200 MB/s to record 32 channels on a single hard disk.
2. If you upgraded from GV-VMS V17/V18, you can still use an enterprise-grade hard disk with 7200 RPM and an average read/write speed of over 110 MB/s to record 22 channels on a single hard disk.

The frame rate limit depends on the resolution of video sources. The higher the resolution, the lower the frame rate you can assign to a single hard disk. In other words, the higher the frame rate you wish to record, the more hard disks you will need. For detailed information on supported recording frame rates, see the user's manual of the IP camera that you plan to connect to.

Installing GV-VMS

1. Download GV-VMS by selecting **Primary Applications** from the dropdown list and clicking the **Download** icon next to **GV-VMS** on the GeoVision Website.
2. If you are using a USB dongle, insert the dongle into your computer. See *License* earlier in this section for connections requiring dongle licenses.
3. To install the USB driver, select **Drivers**, **F/W**, **Patch** from the dropdown list, and click the **Download** icon next to **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**.

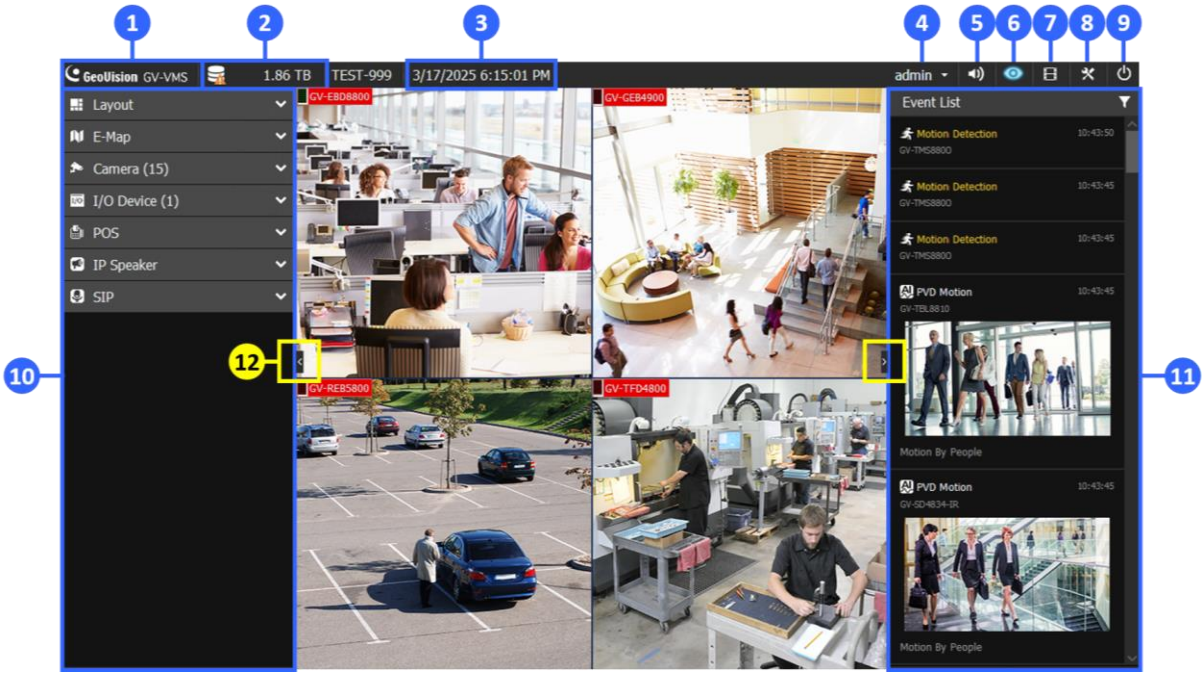


1.2 Getting Started

When you run GV-VMS 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 set up the following functions
   - **E-Mail List:** Enter e-mail addresses used to receive the password when forgotten.
   - **Auto Login:** Allows auto login as the current user whenever the system is launched.
   - **Allow Removing Password System:** It is recommended to select this option, allowing the removal of the password database once you forget passwords. For details, see the same option in *Account and Password* later in this chapter.
   - **:** Click to open the onscreen keyboard to enter the login information.
3. Click **OK**. The GV-VMS main screen appears, along with a dialog box.
4. To configure the system database, select **Default Database** for Microsoft Office Access Database or **Advanced** for Microsoft SQL Server.
5. Upon initial startup, GV-VMS displays the **Automatic Setup** dialog box to assist with adding IP devices quickly.

1.2.1 Main Screen



No.	Name	Description
1	Version Info	Click to display the version of the GV-VMS installed.
2	Storage Space	Displays the remaining storage space. When an HDD error occurs, an exclamation mark is displayed on the storage icon .
3	System Time	Displays the current system time. Right-click to access **Time Synchronization Setup**. See the following subsection *Setting Up Time Synchronization*.
4	Login ID	Click to manage accounts and passwords for accessing GV-VMS.
5	Audio	Click to control the volume of your PC.
6	Home	Shows the live view of connected cameras.
7	ViewLog	Shows a timeline of recorded events for playback.
8	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 GV-Software. • **Tools** : Enable audio broadcast, show / hide volume indicator, and open the System Log.

No.	Name	Description
		● **Configure** : Set up camera, recording, system, schedule, video processing, face manager, and I/O devices.
9	Exit	Click to minimize or exit GV-VMS.
10	Content List	When **Home** is selected: Access live view layouts, E-Map, and lists of cameras, I/O devices, POS systems, IP speakers, and SIP devices.
11	Event List	Displays monitored general / system events and detected AI / PVD events, including face / people / vehicle attributes. See *Event List* and *Instant Playback* in *Utilizing Live View Functions* later in this chapter. ● Use the **Filter** at the top of the Event List to display specific event types. ● Double-click an event to display its playback video in a 1x1 view and its playback timeline at the bottom of the Main Screen. ◆ If the camera is already displayed in the layout, or if it isn't displayed but an empty channel is available, playback appears on the Home page. ◆ If the camera is not displayed and all channels are occupied, playback appears on the Viewlog page.
12	Collapse / Expand	Click the and buttons on the sides of the Content List and Event List to collapse them.

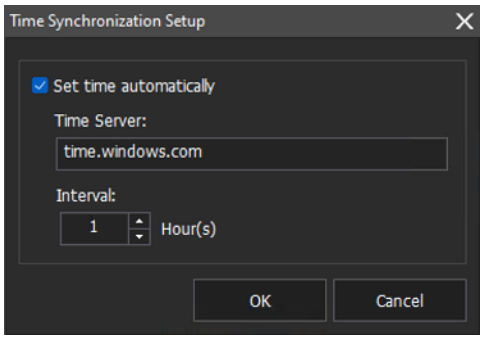
1.2.2 Setting Up Time Synchronization

GV-VMS uses the Windows operating system as its time source. With Time Synchronization Setup, users can configure Windows time synchronization settings directly within GV-VMS. Once configured, the Windows operating system automatically synchronizes its time with the designated NTP server at defined intervals, and GV-VMS follows the updated system time.

Note: The GV-VMS settings in this section correspond to Windows Date & time settings (**Windows** > **Settings** > **Date & time**). Any changes made in either GV-VMS or Windows are reflected in both interfaces.

To complete the setup, follow the steps below.

1. Right-click the **System Time** at the top of the main screen, and select **Time Synchronization Setup**. This dialog box appears.

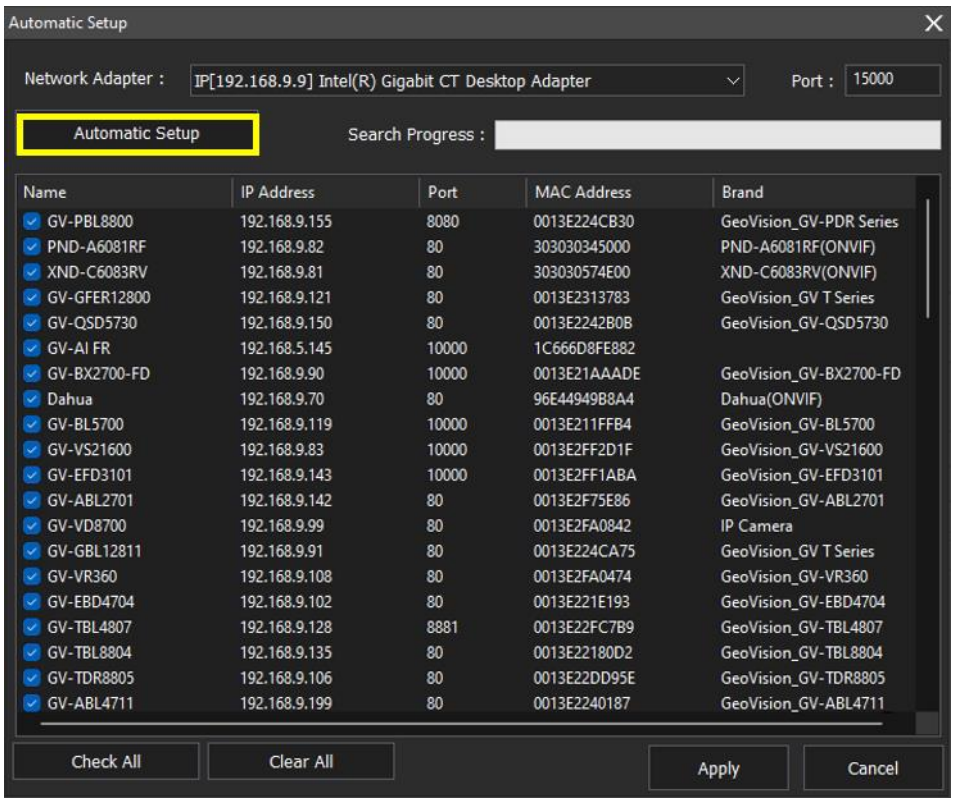


2. Enable **Set time automatically** to allow Windows to synchronize time automatically using an NTP server. This option is disabled by default.
3. Set the **Time Server** (NTP server). The default server for a Windows PC is time.windows.com, which can be changed if needed.
4. Set the synchronization interval (range: 1–999 hours).
5. Click **OK**. The system will immediately perform an initial synchronization within approximately 10–20 seconds.

1.2.3 Adding Cameras

To add cameras to GV-VMS, 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:

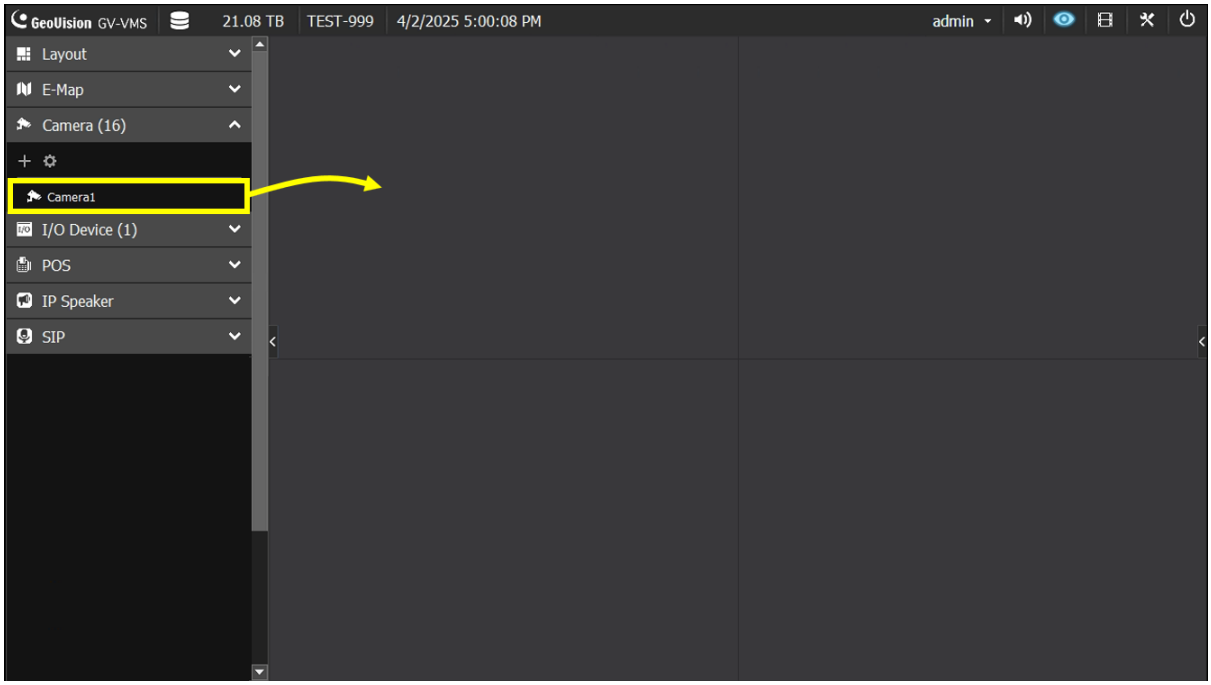
1. Double-click the camera to specify its login credentials. If you select **Apply All**, the login info will be applied to all selected cameras.
2. When cameras are added for the first time, they are automatically assigned to the live view grid.

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

1.2.4 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.

In the Content List under **Home** (No. 9 in *Main Screen* earlier in this section), click **Camera** to see the list of cameras added, and drag the desired cameras to the live view grid.



For details, see *Live View and Layouts* later in this chapter.

1.2.5 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:

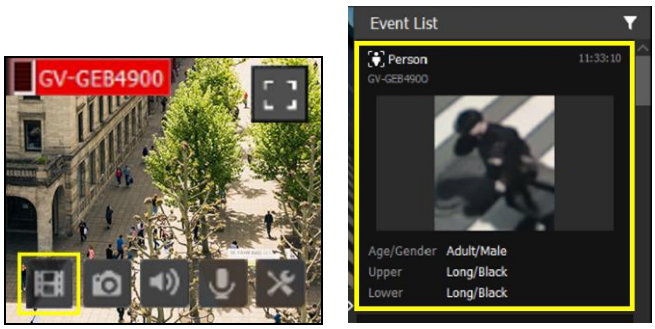
Default Recording Settings	
Recording Mode	Motion Detection
Resolution / Codec	The camera's current resolution / codec will be used.

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

1.2.6 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, or from the Event List by double-clicking an event.





For details, see *Instant Playback* in *Utilizing Live View Functions* later in this chapter.

ViewLog

For comprehensive playback functions, click **ViewLog** at the top right of the main screen.
For details, see *Chapter 4 Video Playback*.

1.3 Recording Settings

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

1.3.1 Setting Up Global Recording Settings for All Cameras

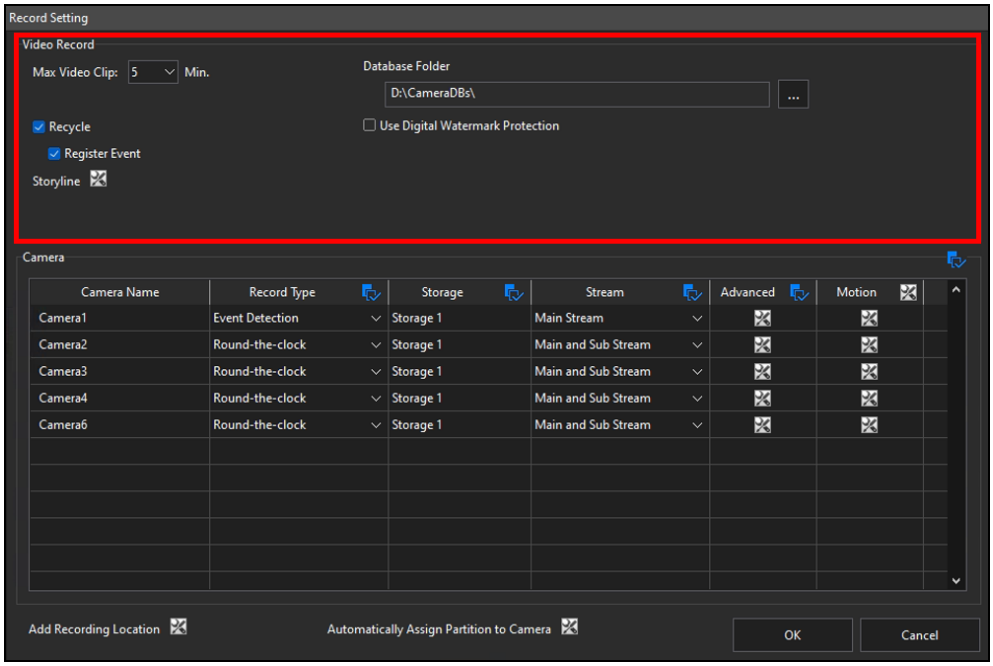
1.3.2 Setting Up Recording Settings for Individual Cameras

1.3.3 Setting Up Video Storage Location

1.3.4 Setting Up Motion Detection

1.3.1 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.



Recording Setting dialog box

[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 minutes**, a 30-minute event will be divided 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 D:\CameraDBs\StoryLine\. 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.

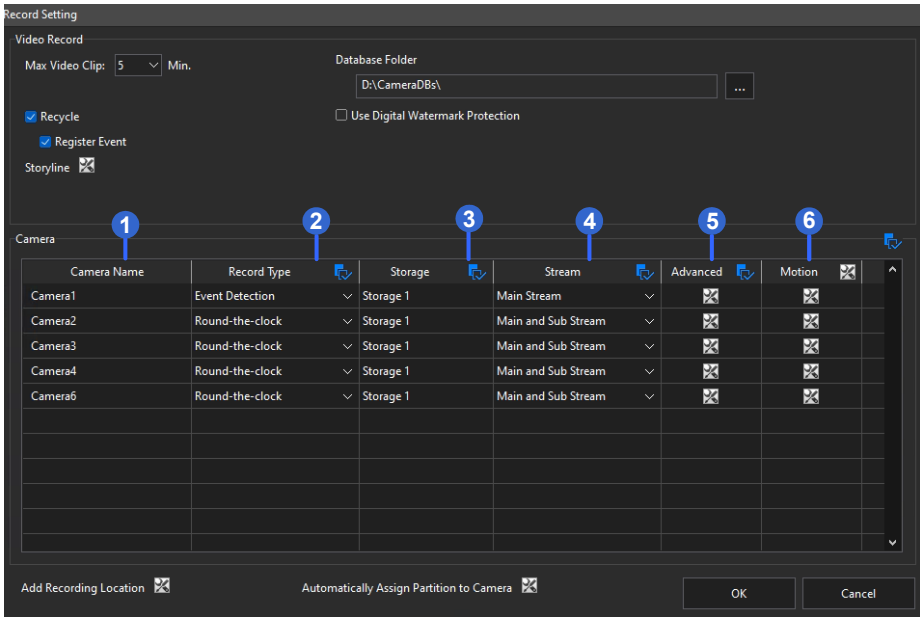
Note: To record a storyline, see *Storyline* later in this chapter.

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

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

1.3.2 Setting Up Recording Settings for Individual Cameras

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



1. Select the camera you want to configure.
2. Under **Record Type**, select **Disable**, **Event Detection**, or **Round-the-Clock**.
3. If there is more than one storage location, select a **Storage** to specify which storage group to store the recordings. For details, see *Setting Up Video Storage Location* later in this section.
4. Select the **Stream** you want to record. The default is set to **Main and Sub Stream** to record both streams simultaneously. Select **Main Stream** to record high-resolution videos. Select **Sub Stream** to record lower-resolution videos.
5. Under **Advanced**:

   [Sync recording from camera SD card when reconnected] When a camera is reconnected to GV-VMS after a disconnection, the function retrieves and restores recorded files from its SD card. ViewLog's Timeline displays recordings that have been synced from SD cards in yellow.

IMPORTANT: Do not change the camera's recording storage group settings at random (as described in Step 3). The changes may disrupt the recording file sequence, resulting in recording failures and unexpected recycling behavior.

Note: To sync a camera's recordings back to GV-VMS, it is required to enable related settings on both GV-VMS and a compatible camera. For details on compatible cameras and instructions, see the technical notice.

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

- **Post-Rec:** Keeps on recording for a specified duration after an event stops.
- **Pre-Rec:** Records video for a specified duration before an event starts. Set the number of video clips and the length (in seconds) of each clip. For example, if you set **3 video clips** at **5 seconds** each, the system will record 15 seconds (three 5-second files) prior to each motion or input event.
- **Urgent** / **General Event:** Select **Urgent Event** to record full frame rates or **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 section.

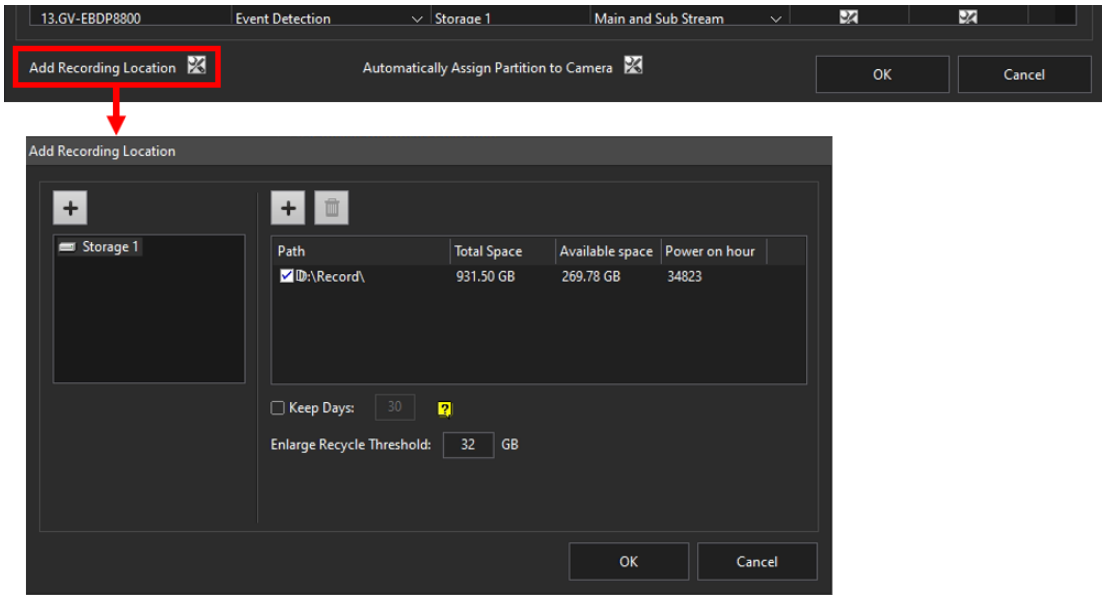
Note: You can define the frame rate of Urgent Event and General Event. For details, see **Recording Frame Rate Control** option in *Recording Settings* in Chapter 2.

1.3.3 Setting Up Video Storage Location

Add Recording Location

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

1. In the Recording Setting dialog box (see the dialog box in *Setting Up Global Recording Settings for All Cameras* earlier in this section), click next to **Add Recording Location**. This dialog box appears.



2. To add a storage folder for a storage group, click above Path and select a folder. Only 1 folder can be assigned as a 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. Click **OK**.

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.

Automatically Assign Partition to Camera

GV-VMS can automatically configure recording paths for numerous camera channels. After you configure the storage locations, each of your cameras will be evenly dispersed throughout the given recording paths.

1. In the Recording Setting dialog box (see the dialog box in *Setting Up Global Recording Settings for All Cameras* earlier in this section), click **Automatically Assign Partition to Camera**.
2. Select the desired recording paths (at least one) to store camera recordings and click **OK**.

1.3.4 Setting Up Motion Detection

The motion detection settings apply to both Round-the-Clock and Event Detection recording types. The following features are available to prevent false motion detection:

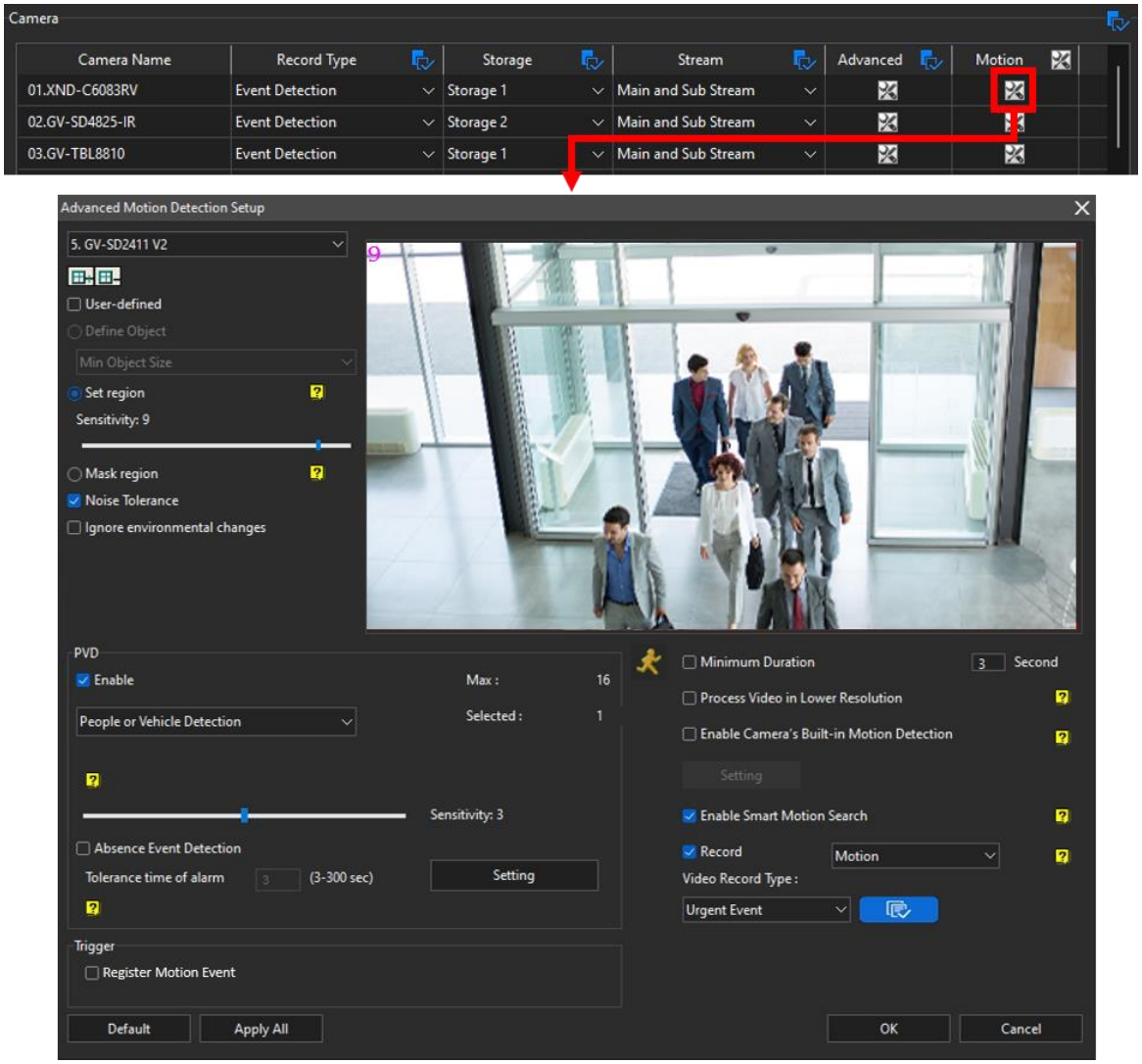
- **Object Size:** Set minimum and maximum object sizes to detect only those within the range.
- **Sensitivity:** Set up to 10 levels of motion detection sensitivity for each outlined area.
- **Mask Region:** Mask off unwanted areas for monitoring, such as movement from clouds or trees.
- **Noise Tolerance:** Ignore video noise under poor or changing lighting conditions.
- **Ignore Environmental Changes:** Ignore changes such as rain, snow, or tree movement.
- **Minimum Duration:** Set the minimum duration for motion to trigger an alarm.
- **PVD:** Detect only human or vehicle movement.

Note: To enable up to 64 PVD channels, ensure your PC has GV-AI Accelerator Module installed and meets the system requirements. For details, see *Minimum System Requirements* earlier in this chapter.

Tip: To quickly access the Advanced Motion Detection Setup dialog box, right-click a camera in the Content List under **Home**  (No. 9 in *Main Screen* earlier in this chapter), and then select **Motion Detection Setup**.

---

1. On the Recording Setting dialog box (see the dialog box in *Setting Up Global Recording Settings for All Cameras* earlier in this section), select a camera and click the button under **Motion**. The Advanced Motion Detection Setup dialog box appears.



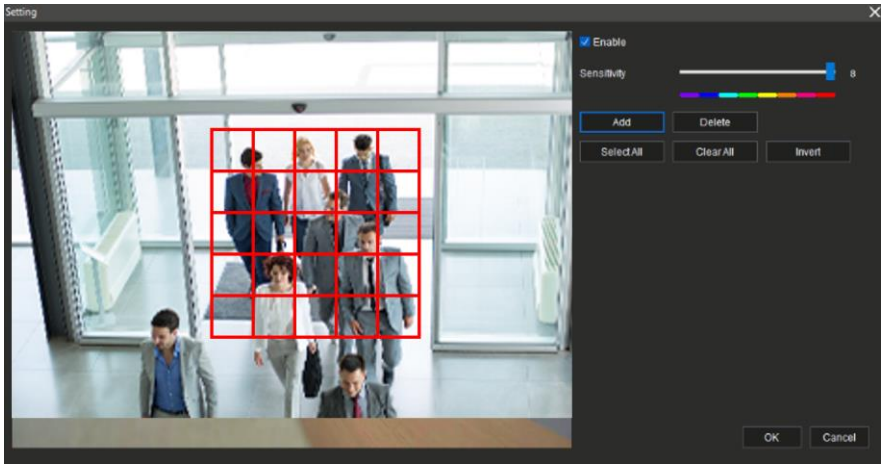
Advanced Motion Detection Setup dialog box

2. By default, the camera's built-in motion detection is used. Optionally deselect **Enable Camera's Built-in Motion Detection** to use GV-VMS's software motion detection rather than the camera's.

Note: By default, the cameras connected to GV-VMS use the camera's built-in motion detection, except for the GV-QSD series, GV-QFER series, and ONVIF cameras, which use software motion detection when connected.

The following steps (Steps 3 to 4) are for when the **camera's built-in motion detection** is used:

3. You can remotely adjust the camera's detection zones and sensitivity in GV-VMS by ensuring **Enable Camera's Built-in Motion Detection** is selected, and then clicking **Setting** under the option.
4. Add the detection area and adjust sensitivity. Note that the interface of the Setting dialog box varies depending on camera models.



Note:

1. Changes to the camera's built-in motion detection settings are applied to the camera immediately after saving.
2. This function is not supported by 3rd-party AI cameras.

The following steps (Steps 5 to 8) are for when **GV-VMS's software motion detection** is used:

5. You can refine motion detection by setting either Object Size or Region Sensitivity.

   - **Define Object:** Limit motion detection to objects within a given size range. Select **User-defined** and set the **Min. Object Size** and **Max. Object Size** from the dropdown lists.
   - **Set Region Sensitivity:** Set different detection sensitivities for different areas of the camera image.
     - To create new detection regions: Uncheck **User-defined**, select **Set region** (enabled by default), adjust the sensitivity level using the slider (default: level 9, range: 1–10), then click the **Add Mask**  button to create a new region with the selected sensitivity. You can create up to 10 regions.
     - To modify existing regions: Select a region, then drag it to reposition, or double-click on the image to add a vertex. You can drag a vertex to adjust the shape, or right-click a vertex and select **Delete** to remove it.
     - To remove regions: Click the **Cut Mask**  button to switch to Remove mode, then drag across a region to remove it.

     Note: Regions can be modified in both Add and Remove modes. In Remove mode, you can directly right-click a region to edit it without switching modes. After editing, click the **Cut Mask**  button again to continue removing regions.

   - **Mask Region:** To ignore motion in a certain region, uncheck **User-defined**, select **Mask Region**, then click **Add Mask** to create a new region. You can create up to 10 regions, modify existing regions, and remove regions, the same as the detection regions in *Set Region Sensitivity* above. Note that mask regions and detection regions can coexist on the image.

6. The following options are available to further reduce false alarms:

   - **Noise Tolerance:** Enable to ignore video noise.
   - **Ignore Environmental Changes:** Ignores environmental changes such as rain or snow. When selected, objects moving steadily and repeatedly in the same direction for over 1.5 seconds are filtered out and ignored.
   - **Minimum Duration:** Sets the minimum duration for motion to trigger an alarm. Specify the minimum duration in seconds (up to 60).

7. To reduce CPU load, optionally select **Process Video in Lower Resolution**. When enabled, GV-VMS compresses live view to a lower resolution before detecting motion, which reduces CPU load but may compromise accuracy.

8. To mark motion data while recording for later search in defined regions of interest, select **Enable Smart Motion Search**. For Smart Motion Search, see *Object Search* in Chapter 4.

The following steps (Steps 9 to 12) apply to both the **camera's built-in motion detection** and **GV-VMS's software motion detection**:

9. To set the recording type and frame rate, enable **Record**
   - **Record**: Select **Motion** to record any 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 recording.

[PVD]

10. Enable **PVD** (People and Vehicle Detection). Without the GV-AI Accelerator Module, only up to 16 PVD channels are supported.
    - **Dropdown list:** Select **People Detection**, **Vehicle Detection,** or both to only detect specific motion.
    - **Sensitivity:** Define the sensitivity for filtering out slow-moving objects. The larger the value, the more stationary the objects are.
    - **Absence Event Detection:** When enabled, recording starts only when the selected target (People, Vehicle, or both) is no longer detected, which triggers an absence event.
      - **Tolerance time of alarm:** Set the duration (3 to 300 seconds) that the selected target must remain undetected before an absence event is triggered.
11. Optionally, click **Setting** to configure the following options:
    - **Confidence:** Set the detection confidence for different objects from 1 to 95.
    - **Size Filter:** Set the detection size for people or vehicles. When the object is smaller than the set size, it will not be detected. This function helps prevent false alarms.
    - **Show Rect.**: Displays detection boxes around people and vehicles in the live view when detected.
    - **Mask:** Click the **+** / **-** buttons to add or remove the masks for blocking out certain areas to prevent detection. A maximum of 10 masks is applicable.

[Trigger]

12. Select the action to take when motion is detected.

    The trigger behavior depends 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 action is triggered by motion events using the camera's built-in motion detection.

- If **GV-VMS's software motion detection** is used (when Camera's Built-in Motion Detection is disabled), the action is triggered by motion events using GV-VMS's software motion detection.
- If **PVD (People and Vehicle Detection)** is enabled, the action is triggered only by PVD motion events.

Available trigger action:

- **Register Motion Event:** Log the motion event in the System Log.

13. Click **OK**.

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 sensitivity level of 9 with **Noise Tolerance** and **Process Video in Lower Resolution** functions enabled.
3. To define the frame rate of Urgent Event and General Event, see the **Record Frame Rate Contro**l option in *Recording Settings* in Chapter 2.
4. For the hardware specifications required for PVD motion detection, see *Minimum System Requirements* earlier in this chapter.
5. PVD Motion detection 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 valid person or vehicle detections. The detected PVD motion type (people or vehicle), confidence, and size will be displayed on the Event List and AI Query. For details, see *Event List* in *Utilizing Live View Functions* later in this chapter and *AI Query* in Chapter 4.

   Based on detection results, try different PVD settings (Confidence, Size Filter) to determine the confidence level that works best for your camera and application.

Event List:	**AI Query:**
	

6. The ratio for the minimum object size 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.

1.4 Live View and Layouts

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

1.4.1 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 *Audio Settings* 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 live view. ⊙ **Keep Image Ratio:** Locks the aspect ratio of the camera image. ■ **Close:** Removes the camera from the layout grid. The following options are available when the related function is enabled or supported: ■ **Storyline:** Records a sequence of short video clips of a specific incident. See *Storyline* later in this chapter.

	■ **Play Audio File:** ⊙ **Open:** After associating an IP speaker with the camera, select an audio file to be played through the speaker. For details on associating a speaker with a camera, see *section 3.3* in *GV-IP Speaker User's Guide*. ⊙ **Edit:** Configure whether the selected audio file repeats during playback. ■ **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* in Chapter 2. ■ **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 under **Home**  (No. 9 in *Main Screen* earlier in this chapter), right-click a camera to access the following options, when enabled or supported:

- **Monitor:** Starts monitoring the camera. See *Start Monitoring* later in this chapter.
- **Wave Out:** Enables live view audio. See *Configuring Audio Settings* in Chapter 2.
- **Talk Back Toggle:** Talks to the surveillance site from the PC. See *Configuring Audio Settings* in Chapter 2.

- **Video Process:** Opens the Video Processing dialog box. See *Chapter 3 Video Analysis*.
- **Motion Detection Setup:** Opens the Advanced Motion Detection Setup dialog box. See *Setting Up Motion Detection* earlier in this chapter.
- **Focus View Setup:** Creates up to 7 closed-up views in a camera. See *Setting Up Focus View* later in this chapter.
- **PTZ Setup:** Enables PTZ functions. See *PTZ Camera* in Chapter 2.
- **IP Device Setup:** Opens the IP Device Settings dialog box. See *Configuring Individual IP Cameras* in Chapter 2.
- **Fisheye Settings:** Opens the Fisheye Settings dialog box. See *Fisheye View* in Chapter 2.

Audio Broadcasting

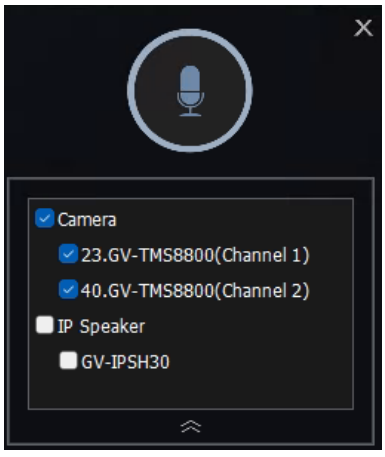
When necessary, the GV-VMS operator can broadcast audio to multiple cameras and GV-IP Speakers simultaneously with the speaker function.

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

---

1. Click **Home** > **Toolbar** > **Tools** > **Audio Broadcast**.

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 GV-VMS.

Event List

The Event List is designed for real-time monitoring, displaying both general and system events as well as detected AI and PVD events, including face, people, and vehicle attributes. Events appear in a cascaded view upon detection, with event type filters typically applied in advance to support timely monitoring and response.

If you prefer a text-based record of general and system events over real-time monitoring, the System Log provides fast access to recent event data. See *System Log* later in this chapter.

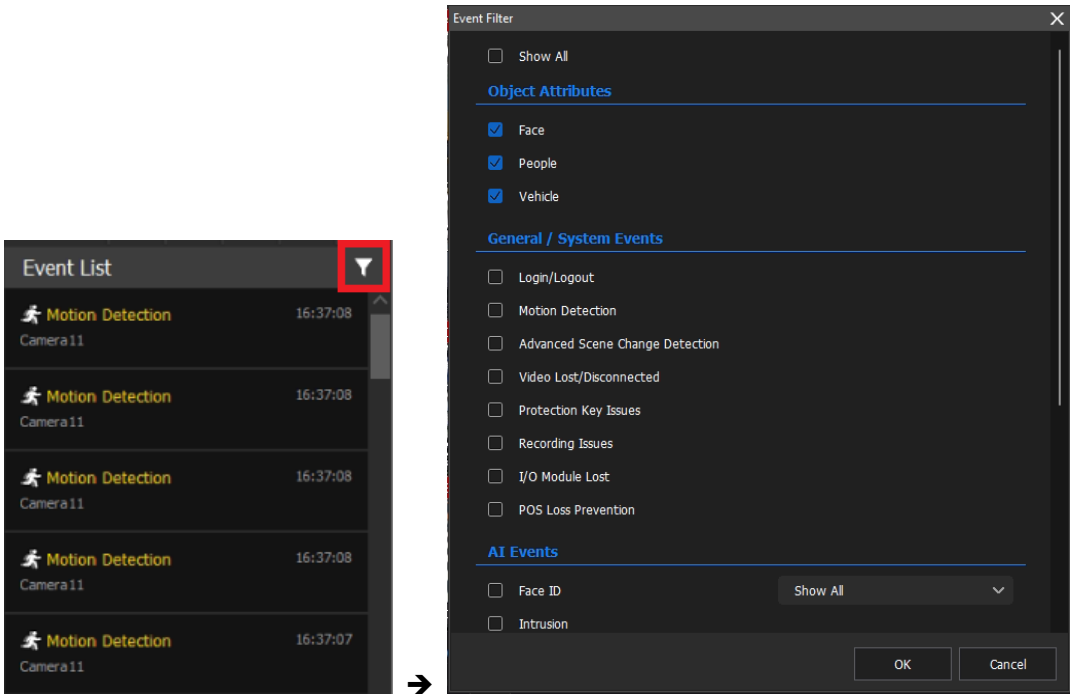
If you want to perform post-event advanced filtering of AI and PVD events – including face, people, and vehicle attributes – rather than monitor them in real time, see *AI Query* in Chapter 4.

Note:

1. Filtering by people and vehicle attributes is supported only on cameras that provide video metadata. For the list of supported GV-IP cameras, see *Camera's Video Metadata Supported by GV-VMS V20* in *Camera Features Supported by GV-VMS V20*.
2. Before AI and PVD events can appear in the Event List, ensure they are configured in advance using the IP Cam Video Analysis and Advanced Motion Detection Setup dialog boxes, respectively.
   - For AI event setup, including face, people, and vehicle attribute detection, see *Video Analysis by Camera* in Chapter 3. For face attributes, see **Face Detection**. For people and vehicle attributes, see **Video Metadata**, both under *Video Analysis by Camera*.
   - For PVD event setup, see *Setting Up Motion Detection* earlier in this chapter.

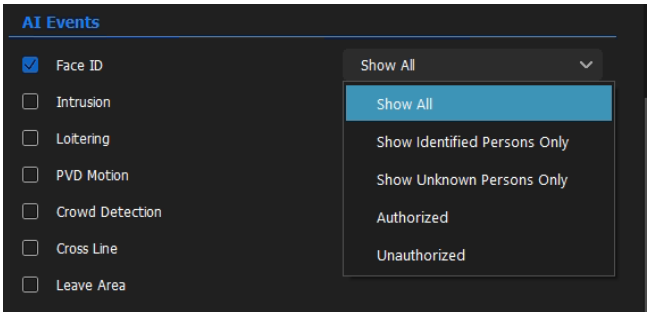
To display specific event types, follow the steps below.

1. Click **Filter** at the top of the Event List. The **Event Filter** dialog box appears.



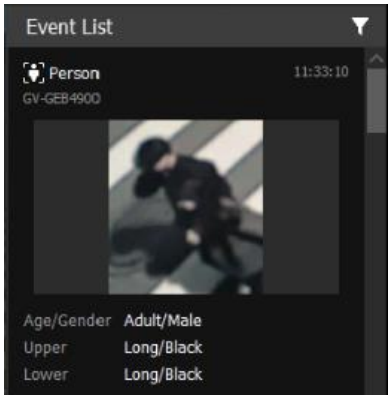
2. To filter the display, select event types in the following categories: *Object Attributes*, *General / System Events*, and *AI Events*.

   - **Face ID:** If you select Face ID under AI Events, you can further refine results by choosing *Show All*, *Show Identified Persons Only*, *Show Unknown Persons Only*, or other custom groups.



Note: In the Event Filter, to search for Local FR (GV-VMS's local recognition) events, select **Face ID** under AI Event; to search for Face Detection events, select **Face** under Object Attributes. For details on Local FR, see *Local Face Recognition* in Chapter 3.

3. Click **OK** to apply the filter. Events matching the selected types appear in the Event List upon detection.



Displayed details include event type, time, and camera model for all events:

- **AI Events:** Also include a captured image. For Face ID, attribute details such as Age/Gender are also included.
- **PVD Events:** Also include a captured image and motion detection type (People or Vehicle).
- **Face / People / Vehicle Attributes:** Also include a captured image and attribute details.

Click an event, hover your cursor over the enlarged image, and you can click **Save** to save the snapshot, click **Playback** to display its playback video in a 1x1 view and its playback timeline at the bottom of the Main Screen, or click **Live** to display the associated camera's live view in a 1x1 view. Alternatively, you can double-click the event to open its playback video directly. See the following subsection *Instant Playback*.

Instant Playback

The Home page provides direct access to playback video and the timeline, allowing users to watch live view and playback streams side by side with full playback controls and timeline access.

To access playback from camera channels:

Hover your cursor over the live view of the desired camera channel, and click **Instant Play** . The live view switches to playback in the same channel, and the playback timeline appears below. Select a time on the playback timeline and click **Play** to view the recording.

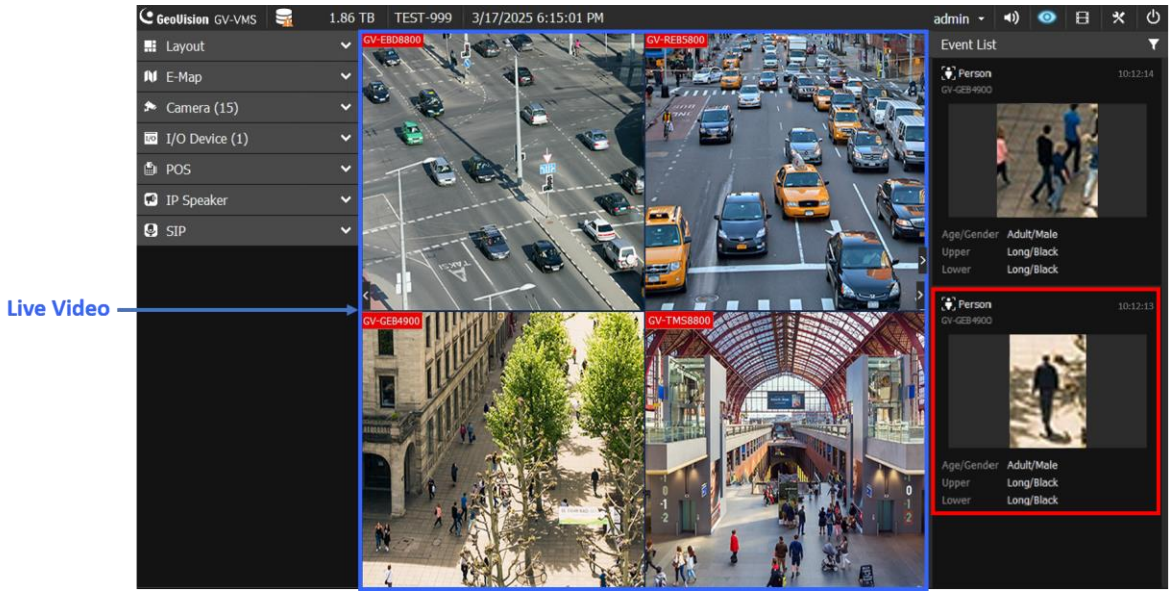


Icons	Functions
Back to Live View	Returns to Live View for a specific instant playback video
Return All to Live View	Returns to Live View for all instant playback videos on the Live View layout.

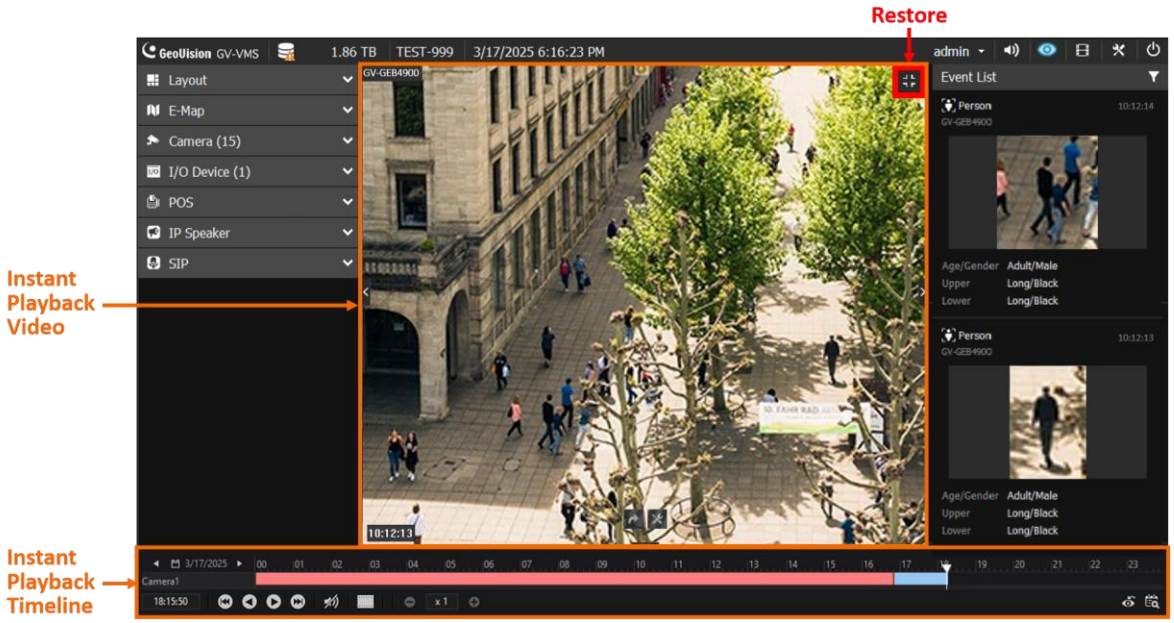
To access playback from the Event List:

Users can also play back video of detected events. To do this, follow the steps below.

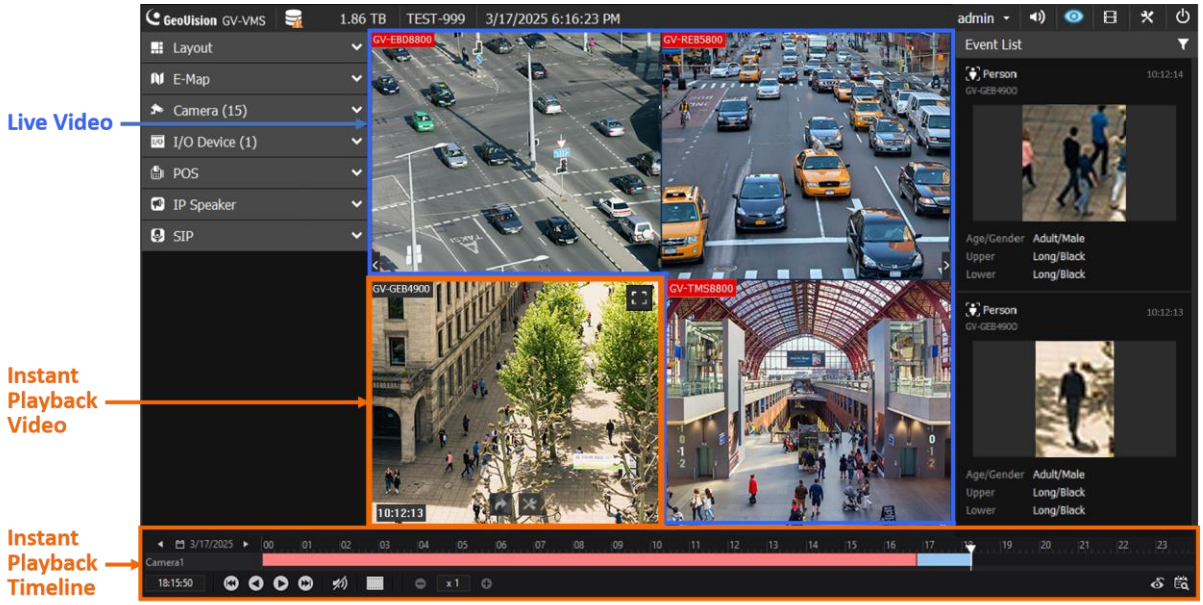
1. Filter for specific event types in the Event List. See the previous subsection *Event List*.
2. Use one of the following two methods:
   (a) Double-click the event in the Event List that you want to play back
   (b) Click the event in the Event List that you want to play back, hover your cursor over the enlarged image, and click **Playback** to play back its recording.



3. The event playback is displayed in the layout, zoomed in to a single channel (1x1 view), and the playback timeline appears below. Select a time on the playback timeline and click **Play** to view the recording.



4. To view the live and playback streams side by side, hover your cursor over the channel and click **Restore** at the top right. This displays both streams in the layout simultaneously.



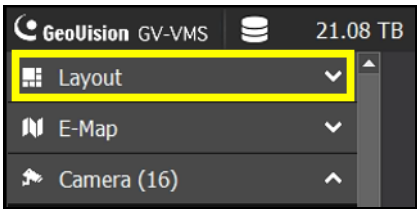
Note:

1. Instant Playback behavior depends on the camera's display status:
   (a) **If the camera is already displayed in the layout:** Double-clicking an event displays its playback on the Home page in a 1x1 view. After clicking the **Restore** button, the playback replaces the live view in the same channel on the Home page (see the steps above).
   (b) **If the camera is not displayed but there are empty channels in the layout:** Double-clicking an event displays its playback on the Home page in a 1x1 view. After clicking the **Restore** button, the playback opens in an empty channel on the Home page.
   (c) **If the camera is not displayed and all channels are occupied:** Double-clicking an event displays its playback on the ViewLog page in a 1x1 view. Clicking the **Restore** button closes the playback and returns you to the ViewLog page.
2. Instant playback is also supported for layouts distributed across secondary monitors.

For details on the playback preview window and timeline, see *ViewLog Control Panel* in Chapter 4.

1.4.2 Arranging Live View Layouts

1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Layout**.



2. Under **Layout**, click **Add**, and select **Add Layout**. The Add New Layout dialog box appears.
3. Name the new layout, 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 appears.
   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.

1.4.3 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, GV-VMS 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 under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Layout**, double-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.

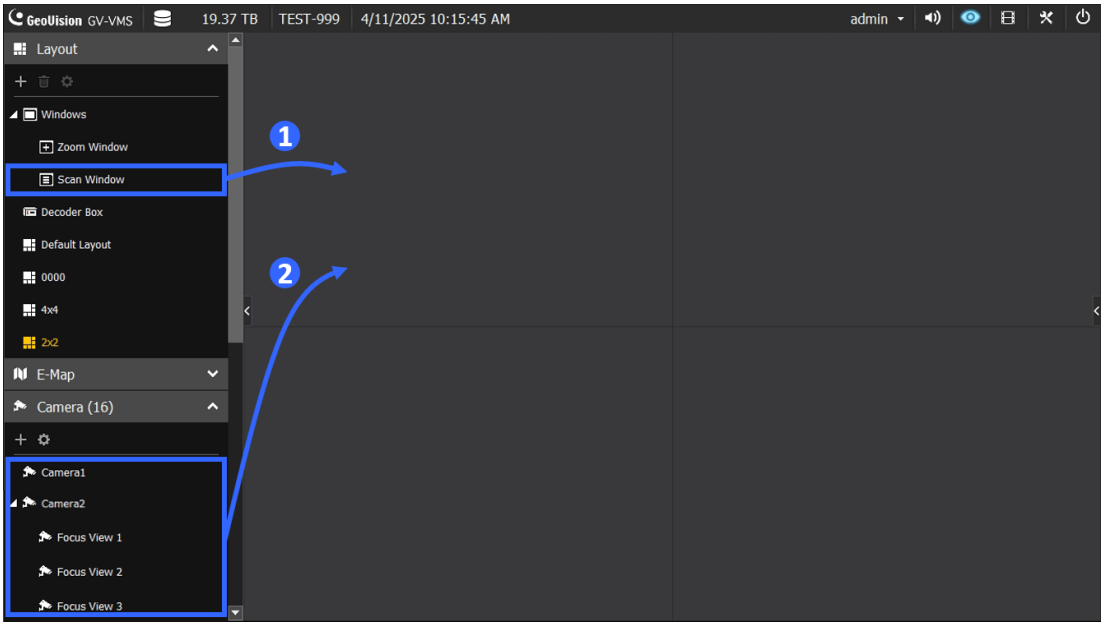
1.4.4 Setting Up Scan Window

You can assign multiple **cameras** or **focus views** to a Scan Window. Each camera or focus view will be displayed in the specified order for the duration of the Scan Interval. For details on focus views, see *Setting Up Focus View* later in this chapter.

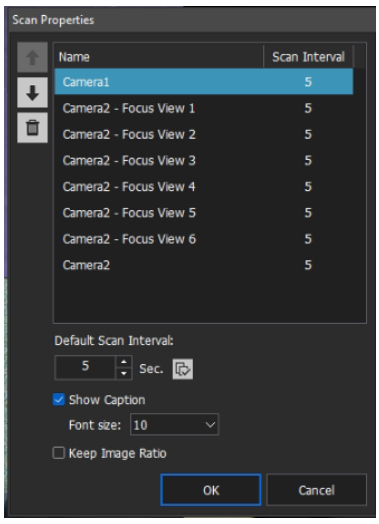
Note: Up to four Scan Windows can be created on each live view layout.

---

1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Layout**, double-click **Windows**, and drag **Scan Window** to a live view grid.
2. Drag multiple cameras or focus views 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 display order, select an item and click the **Up** and **Down** arrows.
5. To specify how long each item is shown in the live view, type a value in the **Scan Interval** field next to the item (default: 5 sec; range: 3 sec to 30 sec). Optionally, set the **Default Scan Interval** at the bottom of the dialog box, and click **Apply All** to apply this Scan Interval to all items.
6. To show the item name on 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**.

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. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Camera** > **Add** > **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 the Scan Window. For details on setting up a Scan Window, see *Setting Up Scan Window* earlier in this section.

1.4.5 Setting Up Web Window

You can display a Web page in a Web Window and interact with it directly from the Web Window.

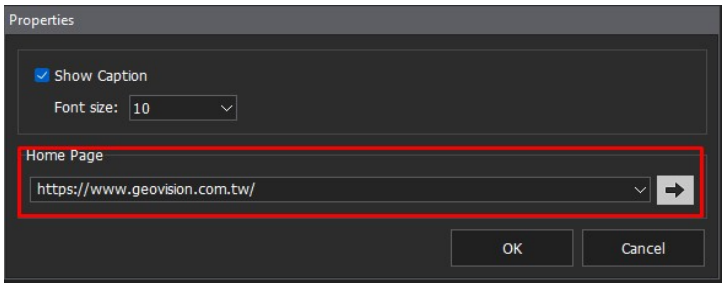
IMPORTANT: The Web Window function requires a **GV-VMS Pro License**, an **AI License**, or a **GV-VMS V18 Platform License**.

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

1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Layout**, double-click **Windows**, and drag **Web Window** to a live view grid.



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



3. In the **Home Page** field, type the **URL** of the Web page you want to display.

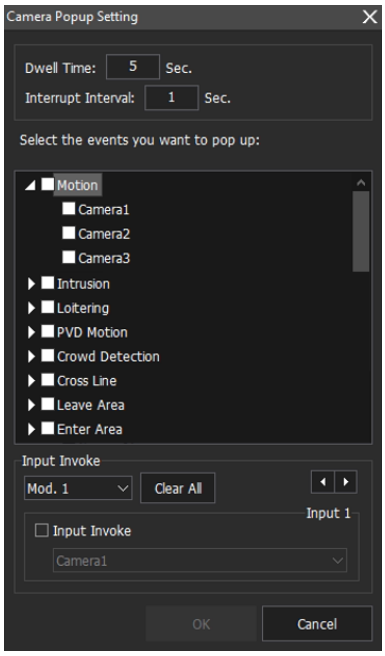
4. Click **OK**. The Web page appears in the Web Window. You can now navigate it directly



1.4.6 Setting Up Popup Window

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

1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **Layout** > **Add** > **Add Layout** to create a new layout.
2. After clicking **OK**, optionally 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 to be displayed in the Popup Window.



4. Rename the Popup Window if necessary, and drag the Popup Window from the Content List to the created layout.

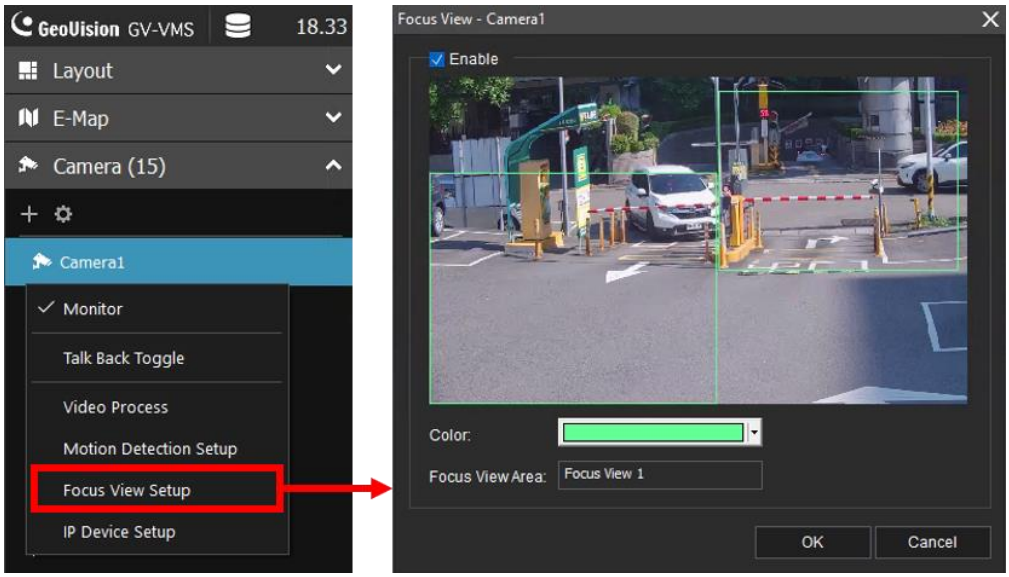
Tip:

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.

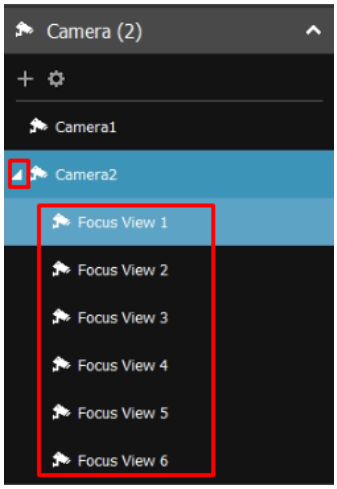
1.4.7 Setting Up Focus View

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 under **Home** (No. 9 in *Main Screen* earlier in this chapter), 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.

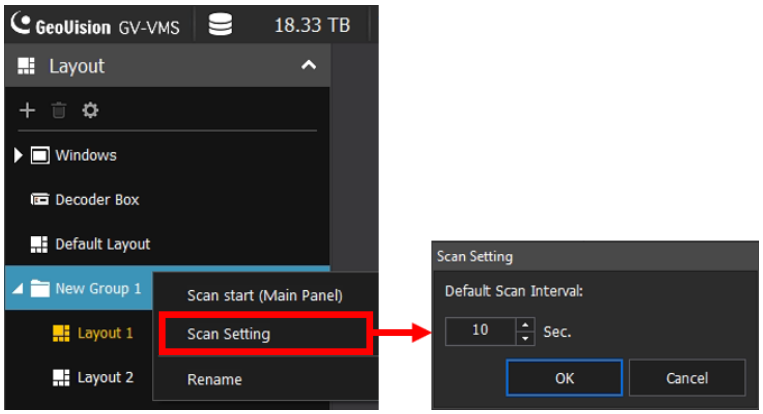


Note: This function is not supported on Fisheye and PTZ cameras.

1.4.8 Automatic Switch Among Different Live View Layouts

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

1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), create and group several layout templates.
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.

1.4.9 Adding GV-IP Decoder Box for Remote Monitor Display

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

1.4.10 Adding GV-IP Speaker for Broadcasting

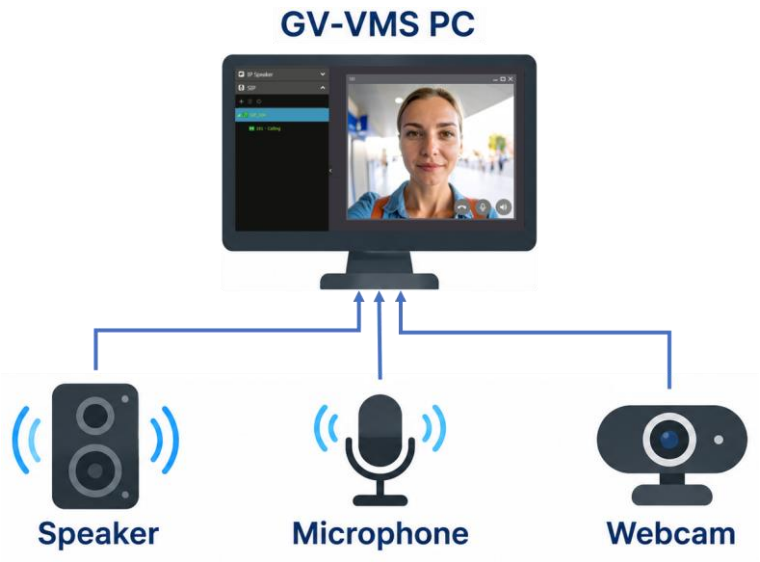
Users can add a GV-IP Speaker to GV-VMS for broadcasting. For details, see *Chapter 3 Adding to GV-VMS / GV-AI Guard* in *GV-IP Speaker User's Guide*.

1.4.11 Setting Up SIP 2-Way Audio Communication

Users can connect GV-VMS to a **SIP (Session Initiation Protocol)** server for dialing out to and receiving calls from devices connected to the same SIP server. Video calls are also supported.

Requirements for video calls:

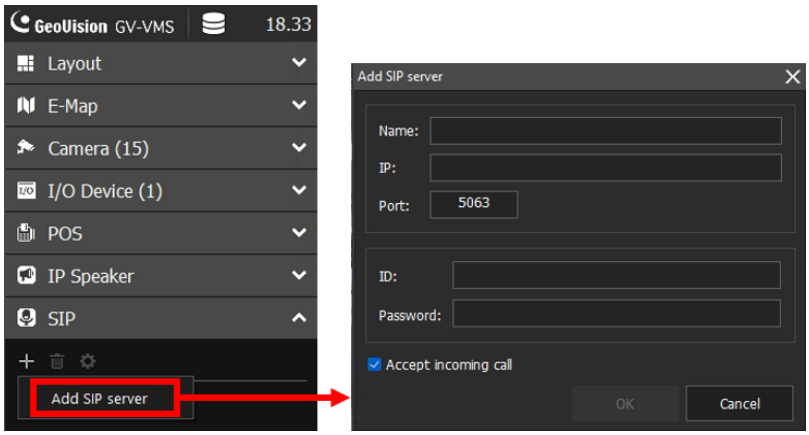
For video calls, the PC running GV-VMS must be equipped with a speaker, microphone, and webcam.



Note: The webcam refers to the camera connected to or built into the computer running GV-VMS. It is separate from the surveillance cameras managed by GV-VMS.

To add the SIP server:

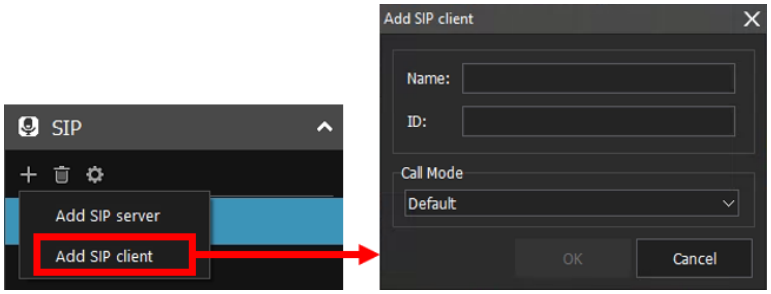
1. In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), click **SIP** > **Add** > **Add SIP Server**.



2. Type a name for the SIP server and its IP address. Modify the port if necessary.
3. In the ID and Password fields, type the ID that GV-VMS will use to identify itself on the SIP server, and a password for protection.
4. Optionally enable **Accept Incoming Call**. Click **OK**.

To add the SIP clients:

5. Select **SIP** > **Add** > **Add SIP Client**.



6. Type a name for the client device and its ID number as assigned on the SIP server.
7. Select a Call Mode (**Default**: Video + Audio; **Easy Mode**: Audio only), and click **OK**.
8. To add multiple client devices, repeat Step 5.

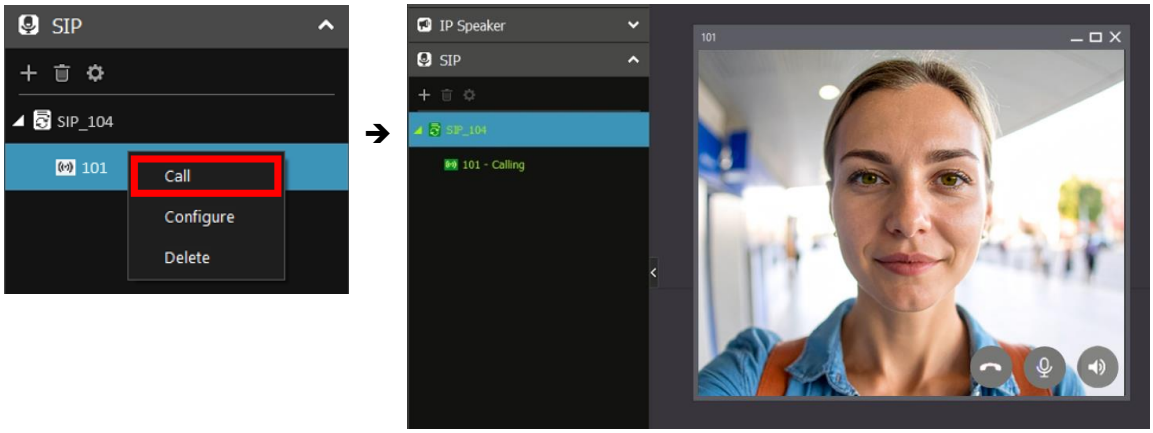
To place and receive calls:

Once all the desired client devices have been added, follow the steps below to place or receive calls.

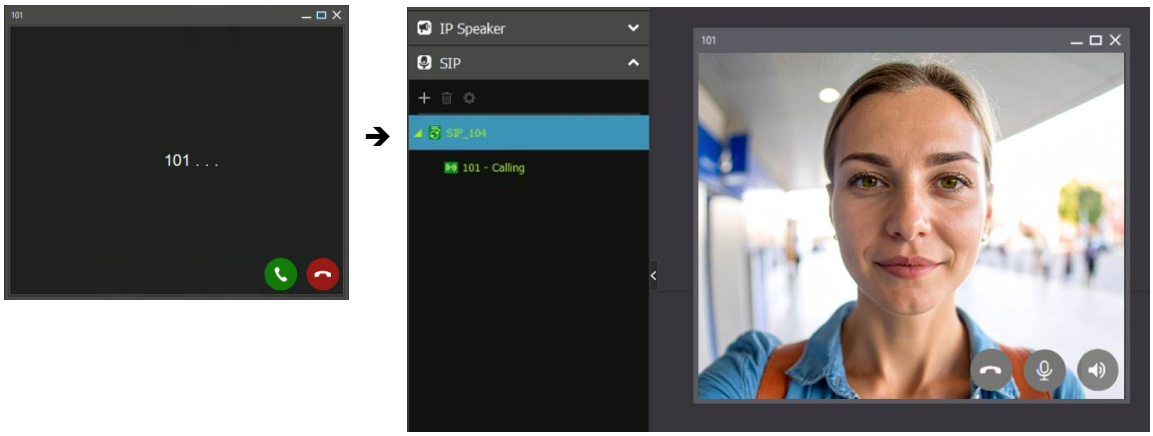
Note: To place and receive video calls, ensure that the **Default** call mode is selected in Step 7.

---

9. To place calls, right-click on any client and select **Call** to dial out to that client. After the client accepts, the call window appears.



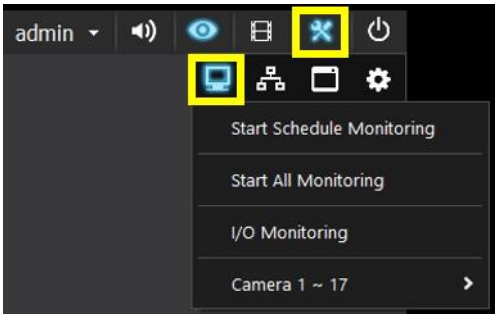
10. To receive calls, ensure that **Accept Incoming Call** is enabled in Step 4. When a call comes in, the incoming call window appears, showing the client's ID. Click the green **Answer** button to accept the call, or the red **Decline** button to reject it. After you answer, the call window appears.



1.5 Start Monitoring

After setting up the following functions, it is important to start monitoring in order for the functions 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:** If you want to start running a created schedule, select **Start Schedule Monitoring**. The schedule takes precedence over the current settings, and these functions will start and stop according to the schedule: Recording, Motion Event Trigger, PTZ Auto Functions, Video Analysis, I/O Monitoring, Network Connections with GV-WebCam Server / Edge Recording Manager / Center V2 / Vital Sign Monitor / Mobile Service, PTZ Object Tracking, and Audio Playback on GV-IP Speakers. For details, see *Schedule* later in this chapter.
- **Start All Monitoring:** Starts monitoring on all cameras to initiate recording and related functions.
- **I/O Monitoring:** Starts 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 #:** Starts monitoring of selected cameras. You can also start monitoring individual cameras by right-clicking the camera in the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter) and selecting **Monitor**.

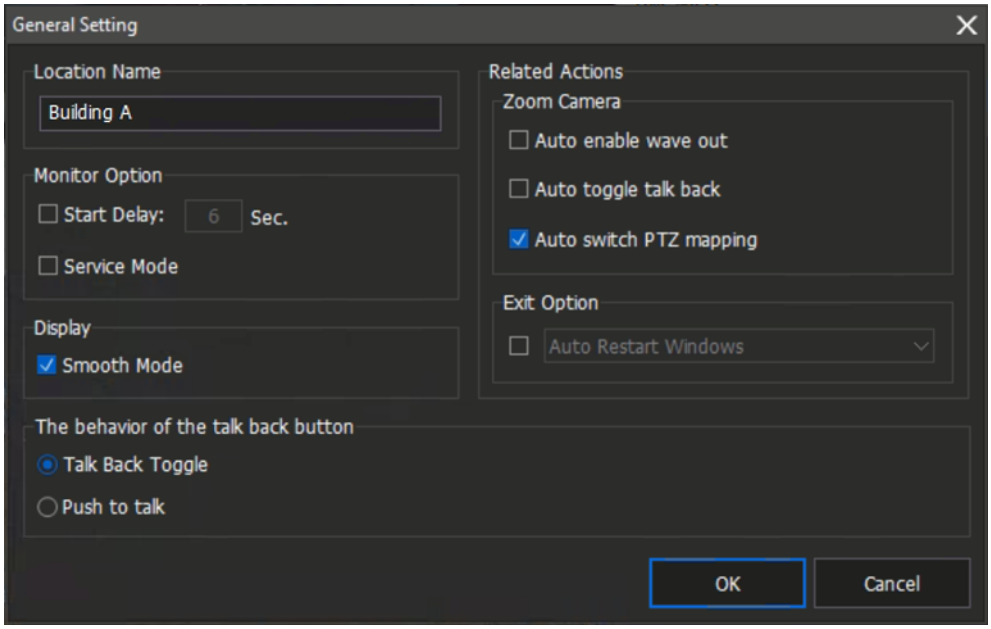
Note: Motion detection and input trigger will only be registered in the System Log if monitoring is started. You will also need to enable **Register Motion Event** in the Advanced Motion Detection Setup dialog box (see the dialog box in *Setting Up Motion Detection* earlier in this chapter) and **Register Input Event** in the I/O Application Setting dialog box (see the dialog box in *Setting Up Actions upon Input Trigger* in Chapter 6).

1.6 System Configuration

This section introduces system configurations.

1.6.1 Configuring General Settings

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



General Setting dialog box

[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 this mode, GV-VMS starts automatically upon PC startup and runs in the background without logging into Windows.

[Display]

- **Smooth Mode:** Enabled by default to ensure smoother video streaming.

[The behavior of the talk back button]

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

[Zoom Camera]

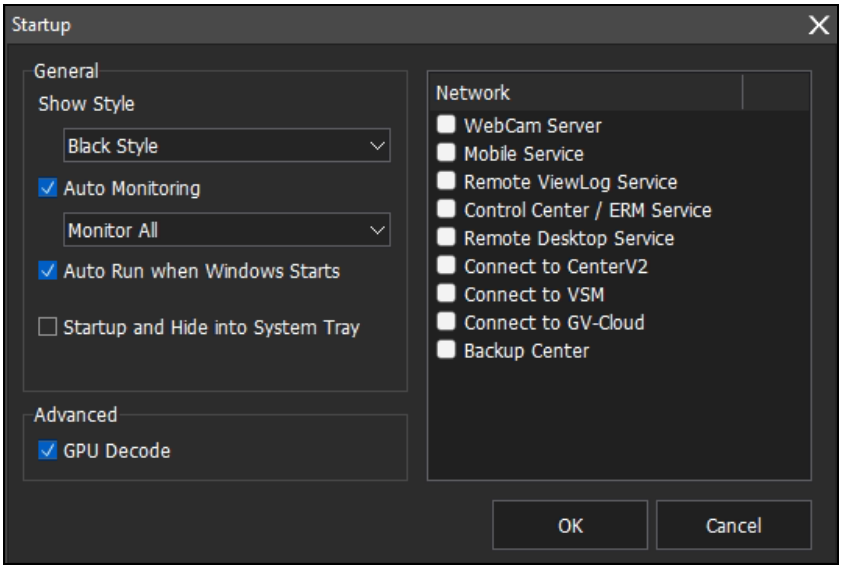
- **Auto Enable Wave Out:** Automatically enables Wave Out function of the camera in Zoom Window or in full screen. Note that the Wave Out function needs to be enabled in the Audio Setting page of the camera first.
- **Auto Toggle Talk Back:** Automatically enables Toggle Talk Back function of the camera. 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 GV-VMS. 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 GV-VMS.
- **Auto Shut Down Windows:** Shuts down Windows OS after exiting GV-VMS.

1.6.2 Customizing Startup Settings

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



[General]

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

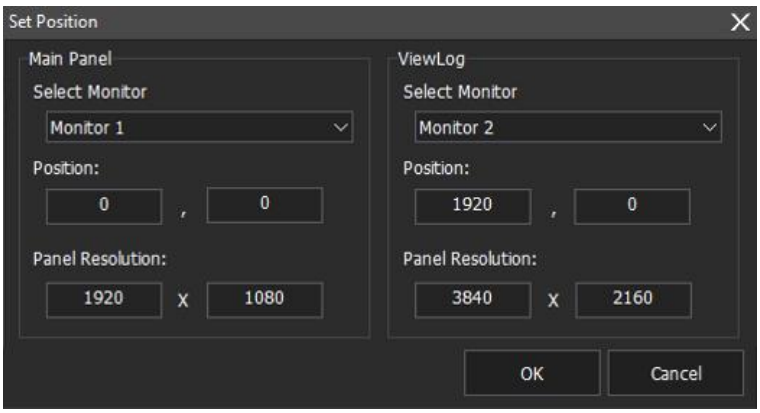
[Advanced]

- **GPU Decode:** Enabled by default, GPU (Graphics Processing Unit) decoding lowers CPU loading and increases the total frame rate supported by GV-VMS. 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**

1.6.3 Customizing Display Position and Panel Resolution

You can customize the display settings of GV-VMS 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 GV-VMS.

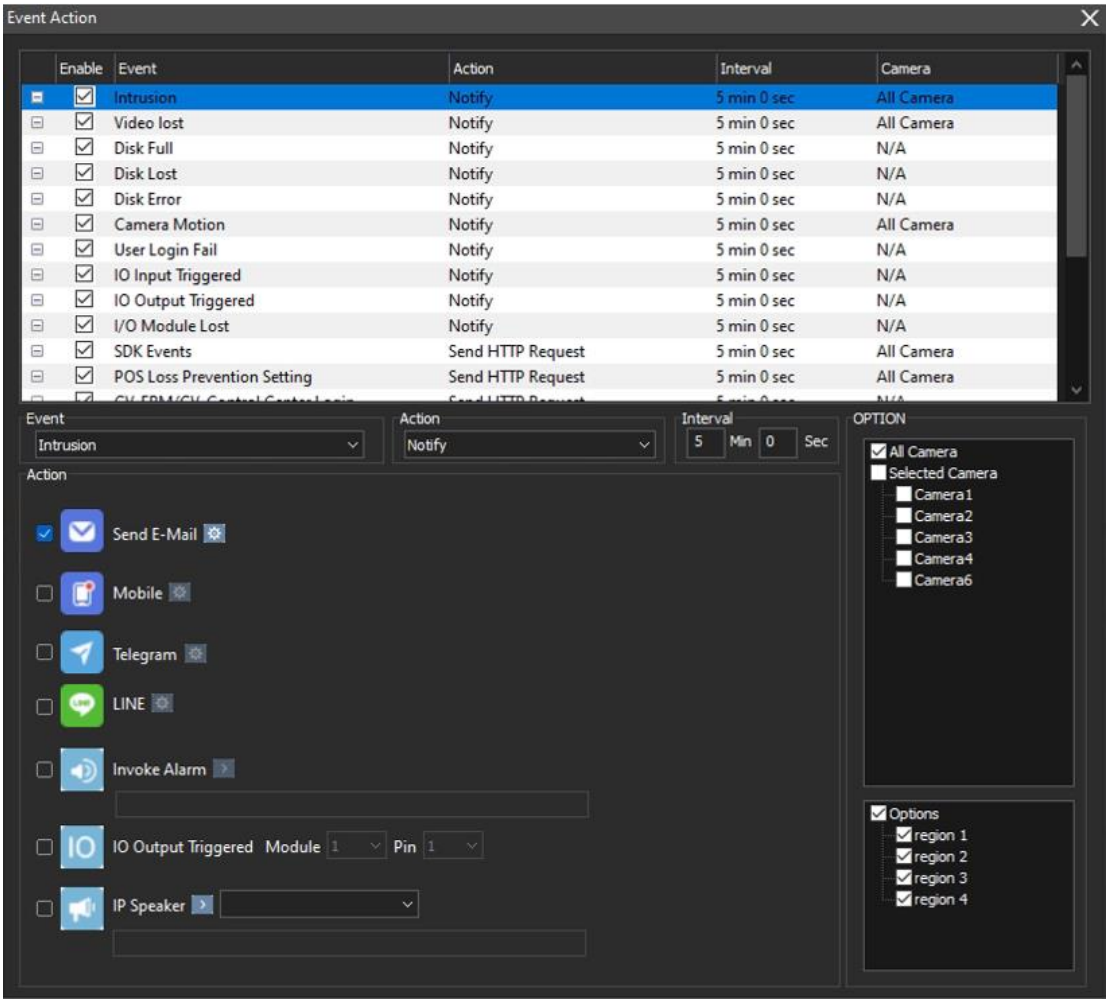
1.6.4 Setting Up Event Notifications

The following events can trigger e-mail notifications, computer alarms, selected output devices and IP speakers, and mobile apps such as GV-Eye, Telegram, and LINE:

Camera Motion, Video Lost, Disk Full, Disk Lost, Disk Error, Recording Error, User Login Fail, I/O Input Triggered, I/O Output Triggered, I/O Module Lost, SDK Events, POS Loss Prevention Settings, GV-ERM / GV-Control Center Login, Remote Login, Face ID, Intrusion, Counter, Loitering, PVD Motion, Crowd Detection, Cross Line, Leave Area, Enter Area, 3rd Party Events, Abnormal Audio Detection, Abnormal Temperature Detection, Absence Event Detection.

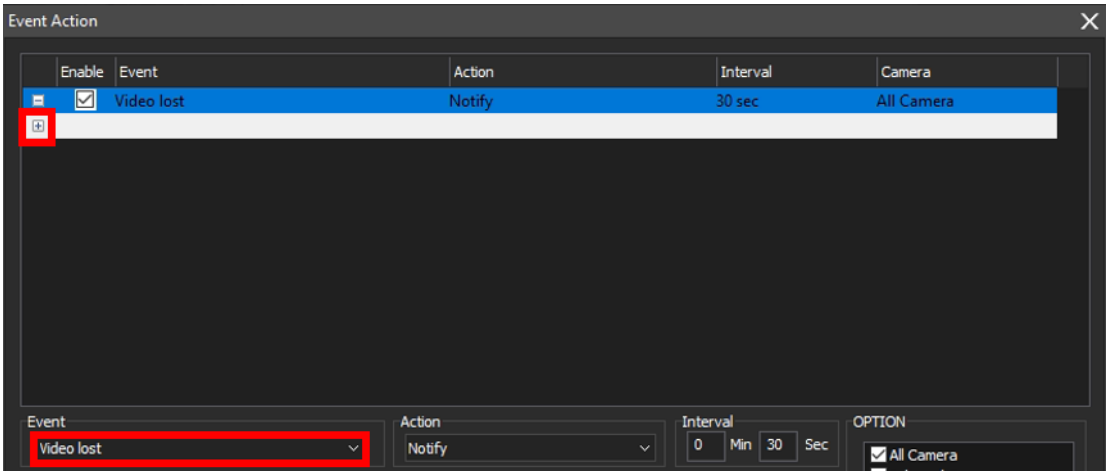
To set up event notifications, follow the steps below.

1. To receive notifications when an event occurs, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**. The Event Action dialog box appears.



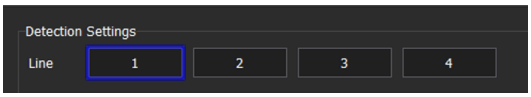
Event Action dialog box

2. Select an event, or click **+** to add a new event. Then select an Event Type from the dropdown list.



3. Enable the actions to take when the selected event is triggered.
   - **Send E-Mail:** Sends e-mail notifications. See *Setting Up E-mail Notifications* below.
   - **Mobile:** Sends push notifications to the GV-Eye mobile app. See *Push Notifications* in Chapter 5 of the *GV-Eye Installation Guide*.
   - **Telegram:** Sends push notifications to the Telegram mobile app. See *Setting Up Telegram Notifications* below.
   - **LINE:** Sends push notifications to the LINE mobile app. See *Setting Up LINE Notifications* below.
   - **Invoke Alarm:** Triggers the computer alarm and plays the selected sound file.
   - **IO Output Triggered:** Triggers an output device. Enable **IO Output Triggered** and select the output module and pin number. To set up output devices, see *Chapter 6 I/O Applications*.
   - **IP Speaker:** Enables a connected IP speaker for audio deterrence or announcements. See the *GV-IP Speaker User's Guide*.
4. Back in the Event Action dialog box, you can change the **Interval** (default: 30 sec; range: 0 sec to 59 min 59 sec), which defines the minimum time gap between repeated notifications for the same event to prevent excessive or duplicate alerts.
5. Select the cameras this event action applies to (only available for certain events).
6. Select the regions this event action applies to (only available for certain events), which are defined in **AI Cam Settings** (**Home** > **Toolbar** > **Configure** > **Video Process** > **IPCVA**) for events such as Intrusion and Cross Line. In AI Cam Settings, these regions are referred to as Detection Rules, Detection Regions / Lines, or Alarm Areas.

   In **AI Cam Settings**:

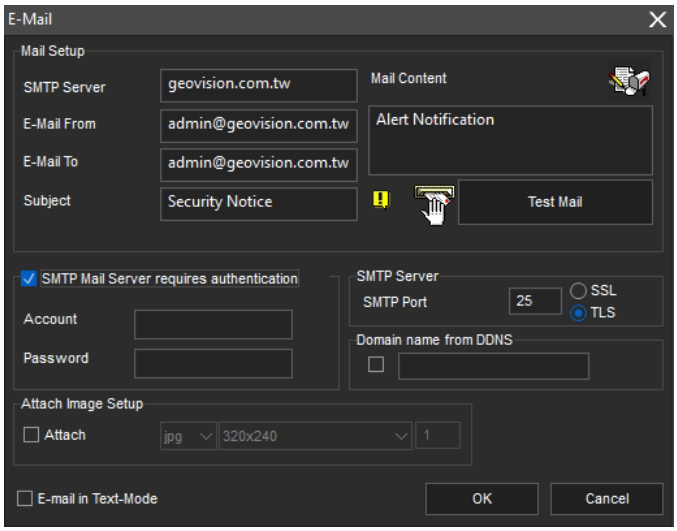


7. Select the face groups this event action applies to (only available for the Face ID event), which are defined in **Group Setup** (**Home** > **Toolbar** > **Configure** > **Face Manager**). See *Setting Up Face Groups* in Chapter 3.

Setting Up E-mail Notifications

To set up email notifications, follow the steps below.

1. In the Event Action dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**), enable **Send E-Mail**. If it's already enabled, click **Setup**. The E-Mail Setup dialog box appears.



2. 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, separate each e-mail address with a semicolon.

   For OAuth-supported e-mail services (e.g., Gmail), only the sender's e-mail address, recipient's e-mail address, and subject are required. The SMTP server will be filled in automatically.

3. Click **Test Mail** to send a test e-mail and check whether the setup is correct.

   For OAuth-supported e-mail services (e.g., Gmail), the system will open the login interface. After logging in, the test e-mail will be sent automatically.

   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 ports. In this case, check your e-mail provider for the SMTP port number. Select **SSL** or **TLS** if your e-mail server requires SSL/TLS authentication for connection.

4. Complete other optional settings as needed:

   - **Mail Content:** Type the e-mail content that will be included in all e-mail notifications.
   - **Domain Name from DDNS:** This option generates URL links in sent e-mails for remote video playback. For this function to work, type the fixed IP address or domain name of GV-VMS, and enable **WebCam Server**.
   - **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* in Chapter 2.
   - **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 GV-WebCam Server, click **Home** > **Toolbar** > **Network** > **WebCam Server**, and then click **OK**. For details, see *Remote Viewing Using a Web Browser* in Chapter 7.

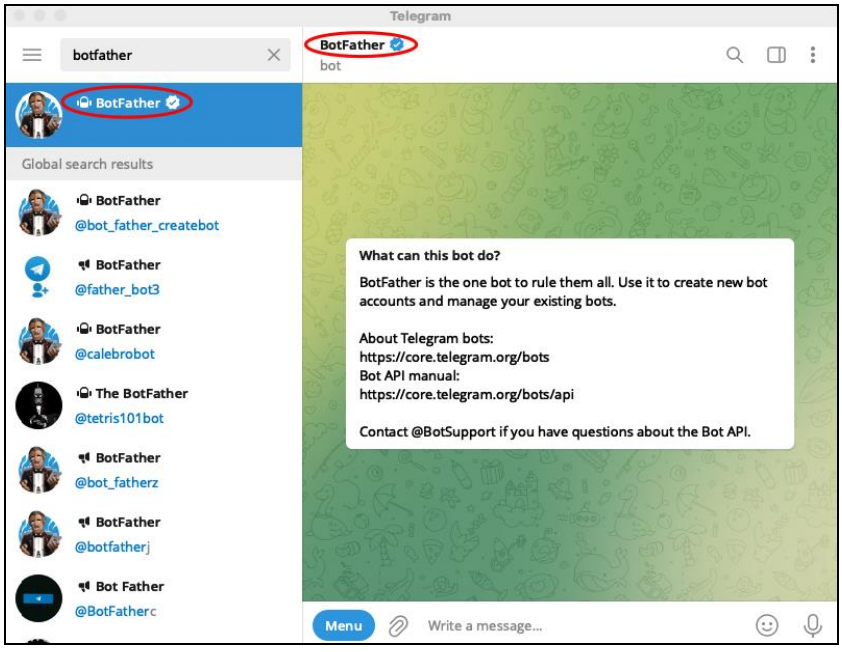
5. Click **OK** to save the settings.

Setting Up Telegram Notifications

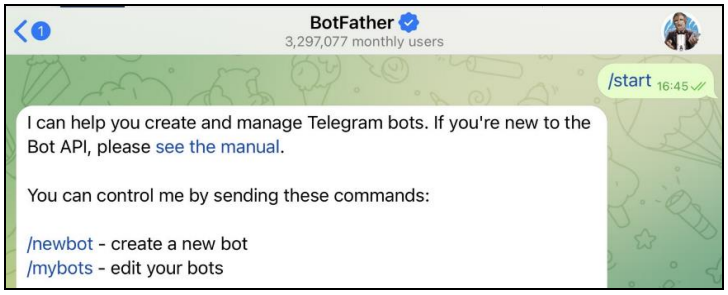
To configure the system to send Telegram notifications, follow the steps below.

Obtain the Bot Token and Chat ID in Telegram:

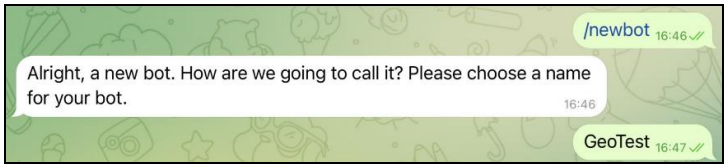
1. Search for **@BotFather** on Telegram, and then select the verified account to open the chat.



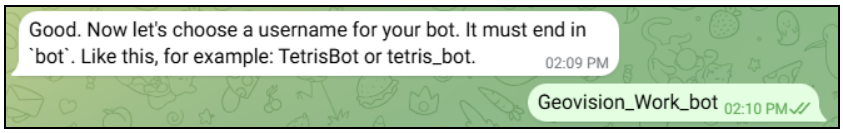
2. Type "`/start`" in the chat to start the conversation.

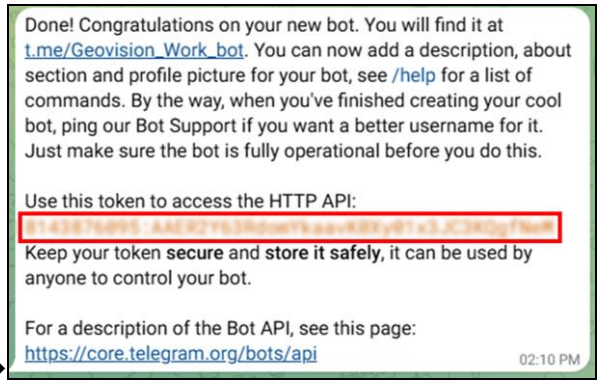


3. Type "`/newbot`" to create a new bot, and then type a name for the bot. This name is the display name. Different bots can have the same display name.

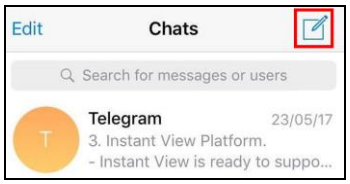


4. Type a username for the bot. The username must end in "`bot`". For example, "`VMS-V20_bot`". This username is the Bot ID and must be unique to each bot. After the bot is created, BotFather generates a bot token.



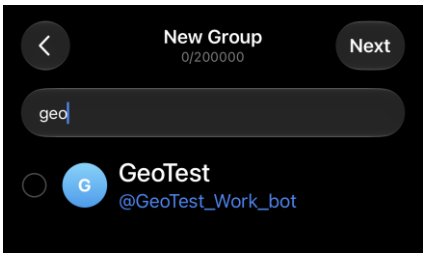
➔ 

5. Return to the chat list. Click  and then click **New Group** to create a group chat.



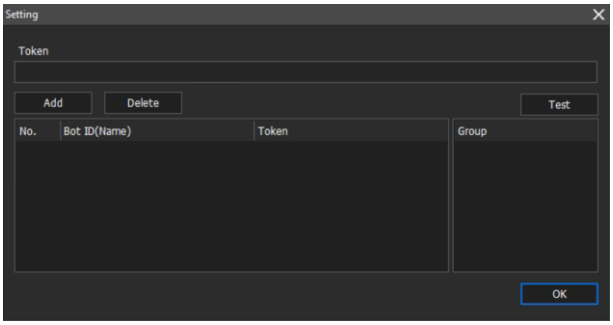
➔ 

6. Search for the bot you created by typing its username (defined in Step 4). Partial matches are supported. Select the bot and then click Next. Follow the on-screen instructions to create the group chat.

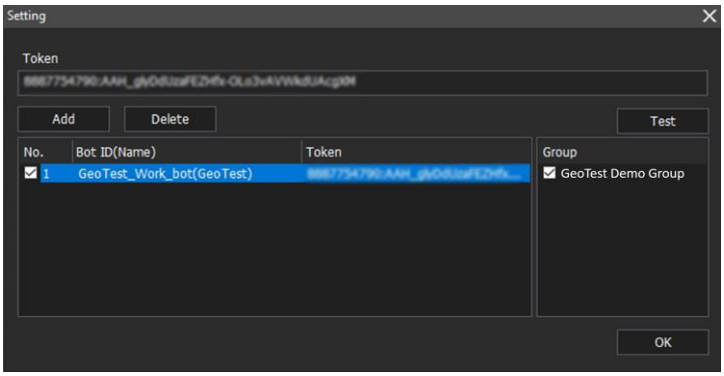


Apply the Token in GV-VMS:

7. In GV-VMS, go to the Event Action dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**), enable **Telegram** and click **Setup** . The Telegram dialog box appears.



8. Type the bot token obtained in Step 4 into the **Token** field.
9. Click **Add**. The bot is added to the list, and GV-VMS retrieves its Bot ID and Name using the bot token. Select the bot to view its available group chats on the right.
   - **Bot ID:** The username defined in Step 4.
   - **Name:** The display name defined in Step 3.
   - **Group:** The group chats available to the bot, created in Step 5.



10. Select the group chats that you want to send test messages to.
11. Click **Test**. GV-VMS sends a test message to the selected group chats. Open Telegram to verify that the messages are received successfully.
12. In GV-VMS, click **OK** to save the settings.

Setting Up LINE Notifications

To configure the system to send LINE notifications, follow the steps below.

Create LINE Official Account and Messaging API Channel:

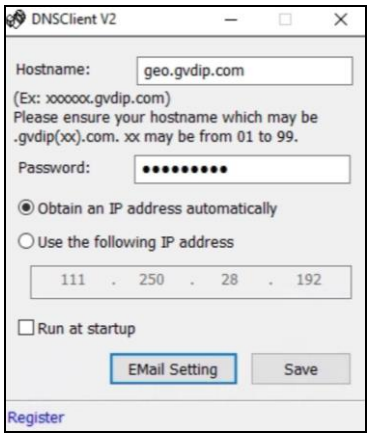
[LINE Official Account Manager]

1. Go to LINE Official Account Manager and create a new official account.
2. Go to the management page of your new official account, click **Settings** at the top right > **Messaging API** in the left menu, and click **Enable Messaging API**. This automatically creates a Messaging API channel for your account.

Set Up Webhook Endpoint:

[GV-Dynamic DNS Service V2 or other DDNS service]

3. To use LINE notifications, you must first register a domain name that points to the PC where GV-VMS is installed. The following example uses GV-Dynamic DNS Service V2. To access the service and register a domain name, follow the steps in *Dynamic DNS* in Chapter 9.



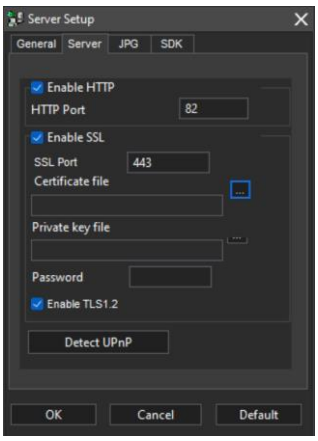
4. Copy the registered domain name.
   Example: `geo.gvdip.com`

[Certificate provider]

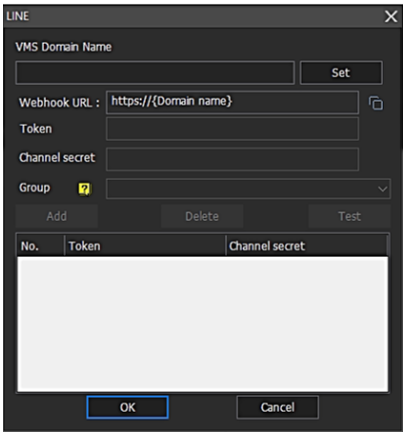
5. Obtain an SSL/TLS certificate and its corresponding private key for the registered domain name.

[GV-VMS]

6. Go to **GV-VMS**. Click **Home** > **Toolbar** > **Network** > **WebCam Server**. The Server Setup dialog box appears.
7. In the Server tab, select **Enable SSL**, verify that **Port** is set to 443, and click the **[…]** buttons next to **Certificate file** and **Private key file** to select the files obtained in Step 6.



8. Click **OK** to save the settings and enable GV-WebCam Server.
9. In the Event Action dialog box (**Home** > **Toolbar** > **Configure** > **System Configure** > **Send Alerts Approach Setup**), enable **LINE** and click **Setup**. This dialog box appears.

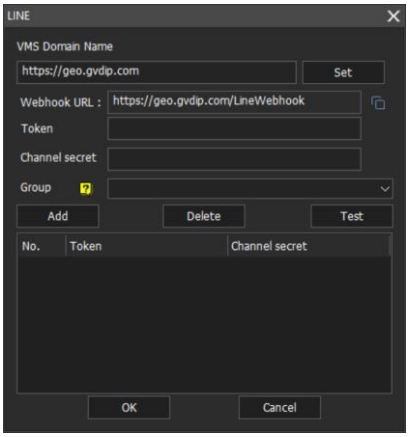


10. In the VMS Domain Name field, type "`https://`" followed by the domain name copied in Step 5. Example: `https://geo.gvdip.com`

11. Click **Set**. The Webhook URL is generated automatically in the following format:

    `https://<your_domain_name>/LineWebhook`

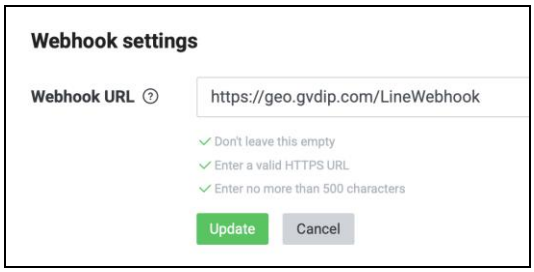
    Example: `https://geo.gvdip.com/LineWebhook`



12. Click the icon to copy the generated Webhook URL.

[LINE Developers Console]

13. Go to LINE Developers Console and log in to your official account.
14. Select your provider and Messaging API channel, go to the **Messaging API** tab, and click **Edit** under **Webhook settings** > **Webhook URL**. Paste the **Webhook URL** copied from GV-VMS in Step 13, and click **Update**.



15. To verify that the URL works, click **Verify**.
16. Enable **Use webhook** to allow the LINE Platform to send a request to your webhook URL when a user sends a message or adds your bot as a friend.
17. Optionally enable **Webhook redelivery** so that LINE retries failed requests.

Get and Paste Credentials into GV-VMS:

[LINE Developers Console]

18. In LINE Developers Console, go to the **Messaging API** tab, and click **Issue** under **Channel access token** at the bottom of the page.
19. Click the icon to copy the **Channel Access Token**.

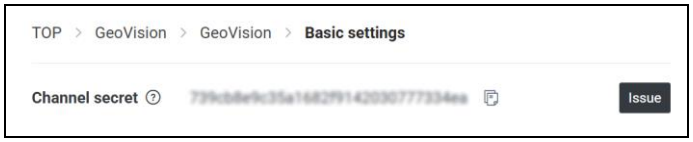


[GV-VMS]

20. Paste the **Channel Access Token** into the Token field in your GV-VMS LINE setup dialog box.

[LINE Developers Console]

21. In LINE Developers Console, go to the **Basic settings** tab.
22. Click the icon to copy the **Channel Secret**.



[GV-VMS]

23. Paste the **Channel Secret** into the Channel Secret field in your GV-VMS LINE setup dialog box.

Save and Activate Channels in GV-VMS:

[GV-VMS]

24. In your GV-VMS LINE setup dialog box, click **Add** to save and activate the channel.
25. Optionally add multiple channels by entering additional Channel Access Token and Channel Secret sets.
26. Click **OK** to save settings and close the setup window.

Add LINE Groups and Test Connection:

[GV-VMS]

27. To receive messages from LINE, enable the HTTP server. On the main screen, click **Home** > **Toolbar** > **Network** > **WebCam Server**, then click **OK**.

[LINE]

28. In the LINE app, have a user create a group.
29. Add the LINE Bot (your official account) to the group. If successful, the LINE Bot sends a message confirming that the group has been successfully added to the list. LINE then sends the group data to the HTTP server via the webhook URL, and the HTTP server retrieves and stores the group information.

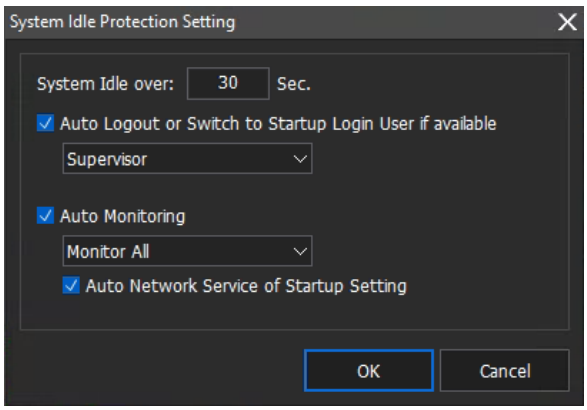
[GV-VMS]

30. Open the GV-VMS LINE setup dialog box.
31. Select the channel you added in Step 25. The group name is available in the Group dropdown list and is automatically selected for the channel.
32. Click **Test** to verify the connection. If successful, the LINE Bot sends a test message to the group chat.

1.6.5 System Idle Protection

The System Idle Protection automatically logs users off or starts monitoring after GV-VMS is idle for a set period of time.

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



System Idle Protection Setting dialog box

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

   If you have set up a Startup Auto Login User, GV-VMS will switch to the Startup Login User instead of logging out. See *Setting Up a Startup Auto Login User* later in this chapter.

3. To automatically start monitoring, select **Auto Monitoring**, and use the dropdown list to select **Monitoring All**, **Schedule Monitoring**, **I/O Monitoring** or **Camera Monitoring**. When Monitoring All is selected, both I/O Monitoring and Camera Monitoring will be enabled.

   - Select **Auto Network Service of Startup Setting** to enable network connections to the applications predefined in Startup. See *Customizing Startup Settings* earlier in this section.

4. In the **System Idle Over** field, type an idle time between 10 and 14400 seconds.

5. Click **OK**.

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

1.6.6 Configuring Fast Key Lock

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.

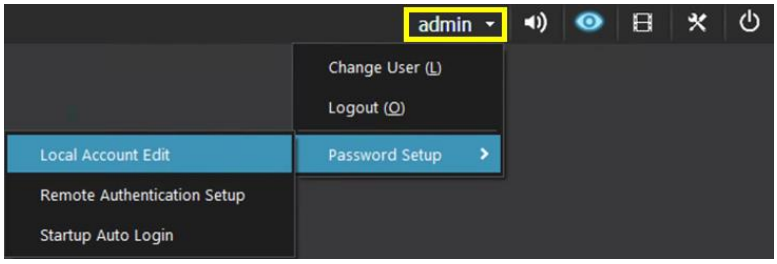
2. Select one of the four tabs: General, ViewLog, PTZ Control, and Network.

3. Clear the checkmark for the fast keys you want to disable. To restore the fast keys, select the checkbox again.

4. Click **OK** to apply your settings.

1.7 Account and Password

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



1.7.1 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.

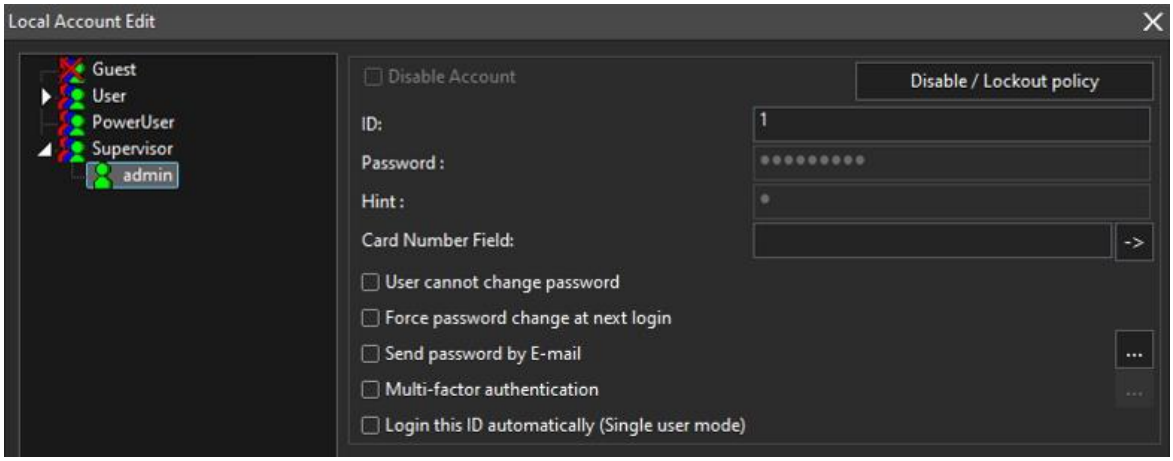
Note:

1. To increase security, your new password must meet the password requirements, including supported non-alphanumeric characters, length, and character categories. For details, see this technical notice.
2. When connected from GV-Control Center V3, the special character @ is not supported for the account ID and password of GV-VMS.

1.7.2 Configuring Account Settings

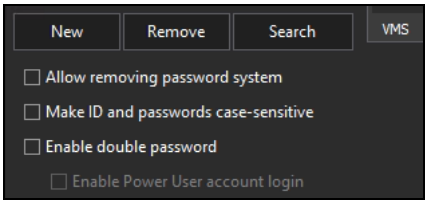
Local Account Edit

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. Supervisor accounts cannot be disabled.
- **Disable / Lockout policy:** Click to open the Configure dialog box. See the following subsection *Disable / Lockout Policy*.
- **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.
- **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 section.
- **Multi-factor authentication:** Requires the user to enter a verification code generated by an authentication app in addition to the account password at login. After enabling this option, scan the displayed QR code with an authentication app (e.g., Google Authenticator, Microsoft Authenticator). Type the verification code generated by the app to complete the setup. Note that enabling multi-factor authentication (MFA) disables the auto login and double password functions.
- **Login this ID automatically (Single User Mode):** Automatically logs into this account after you click **Login** at startup.

At the bottom of the dialog box 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.
- **Make ID and passwords case-sensitive:** Select to make all ID and passwords case-sensitive.
- **Enable double password:** When selected, after starting ViewLog, you will be required to enter two passwords from one of the following combinations:
  - ⊙ Supervisor + Supervisor
  - ⊙ Supervisor + Power User
  - ⊙ Power User + Power User
- **Enable Power User account login:** Select to enable Power User accounts to be used for the Double Password function.

Note:

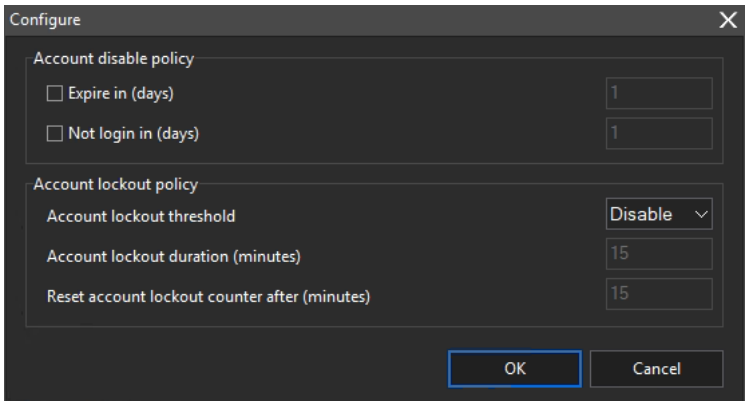
1. At least two Supervisor accounts must be created before you can enable the Double Password function.
2. Before running the utility ***PassUNINStall,*** you need to disable Service Mode on GV-VMS (see the General Setting dialog box in *Configuring General Settings* earlier in this chapter), and then close the system. After running the utility, restart GV-VMS.
3. The loss of passwords can be solved in the following two ways:
   - Retrieving password through e-mails.
   - Removing password database by using the utility *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 the Windows operating system once you lose the passwords.

Disable / Lockout Policy

The Disable / Lockout Policy enhances security by automatically disabling inactive or expired accounts and locking accounts after repeated failed login attempts. These settings help protect the system from unauthorized access.

In the Local Account Edit dialog box, select an account, and then click **Disable / Lockout policy**: The Configure dialog box appears.



[Account disable policy]

- **Expire in (days):** When enabled, the account will be disabled automatically after the set number of days. Enter a number from 1 to 9999. The countdown begins once this setting is saved.
- **Not login in (days):** When enabled, the account will be disabled automatically if the user does not log in within the set number of days. Enter a number from 1 to 9999.

[Account lockout policy]

- **Account lockout threshold:** Select the number of consecutive failed login attempts allowed before the account is locked. Choose a value between 1 and 20, or select **Disable** to turn off account lockout.
- **Account lockout duration (minutes):** When the Account Lockout Threshold is enabled, set how long the account remains locked once the threshold is reached. Type a value from 1 to 9999.
- **Reset account lockout counter after (minutes):** When the Account Lockout Threshold is enabled, this setting resets the count of consecutive failed login attempts to 0 if no additional failed attempts occur within the specified time. Type a value from 1 to 9999.

Note: This setting resets the failed-attempt counter only before the account is locked. Once the account is locked, it will remain locked for the full Account Lockout Duration and cannot be unlocked by this setting.

1.7.3 Changing or Retrieving Password at Login

You can change or retrieve passwords of GV-VMS 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.

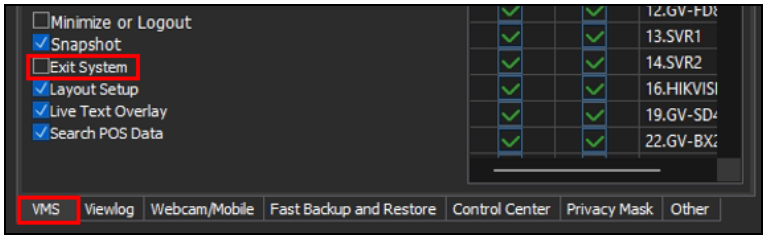
- If you are a supervisor but do not remember your ID, separate passwords will be sent to all supervisor e-mail accounts after you click the **Send Password** button.
- If you remember your ID but forgot your password, enter your ID and click **Send Password**. The password will be sent to your e-mail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

1.7.4 Preventing Unauthorized System Termination

To restrict a non-supervisor account from exiting or restarting the system, click the **account ID** at the top right of the main window, and click **Password Setup** > **Local Account Edit**. The Password Setup dialog box appears.

Select a user from the user list to display its properties.

Select the **VMS** tab at the bottom, and deselect the **Exit System** option to restrict the user from quitting or restarting the system.



1.7.5 Setting Up a Startup Auto Login User

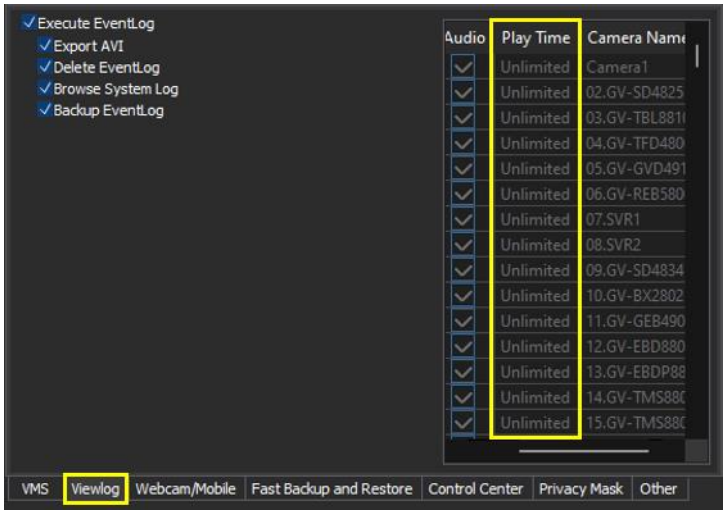
The function is to automatically log in a user account with limited access rights after system startup.

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 the dialog box in *System Idle Protection* earlier in this chapter), GV-VMS will switch to the Startup Auto Login account after it is idle for the set period of time.

1.7.6 Setting Up Limits on Playback Time

1. To restrict the playback time of camera channels, in the Local Account Edit dialog box, select an 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.

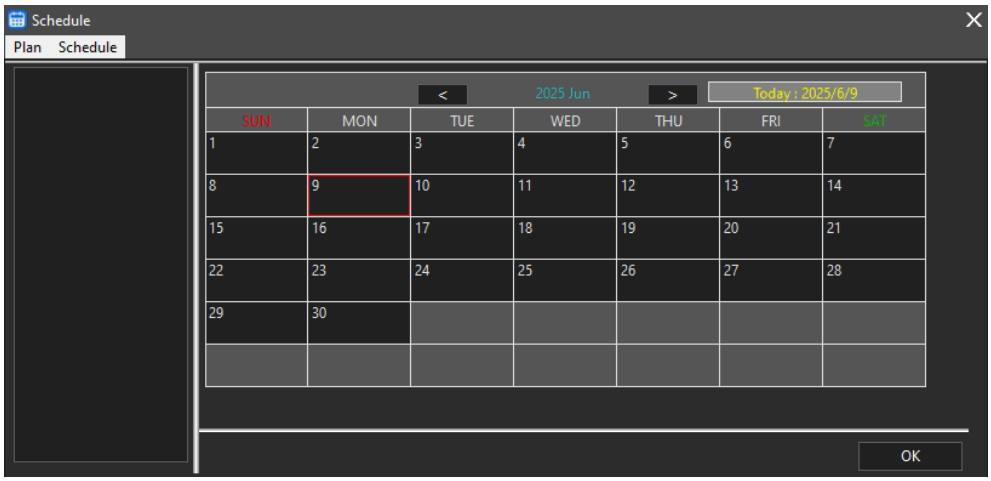
Note: The Setting Limits on Playback Time is based on the time when the user logged into the account. To reset, please log out and log in again.

1.8 Schedule

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

- Recording
- Alert upon motion detection
- PTZ Auto functions
- Video processing
- I/O monitoring
- Network connections to GV-WebCam Server, GV-Edge Recording Manager, GV-Center V2, GV-Vital Sign Monitor, and Mobile Service.
- PTZ object tracking
- Audio playback on GV-IP Speakers

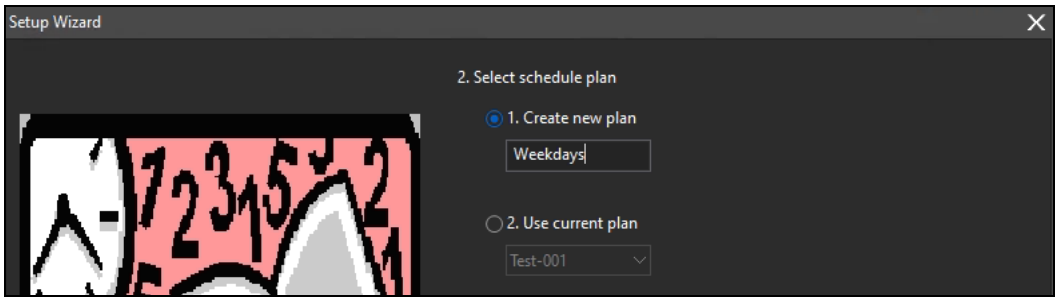
Click **Home** > **Toolbar** > **Configure** > **Schedule Edit**. The Schedule dialog box appears.



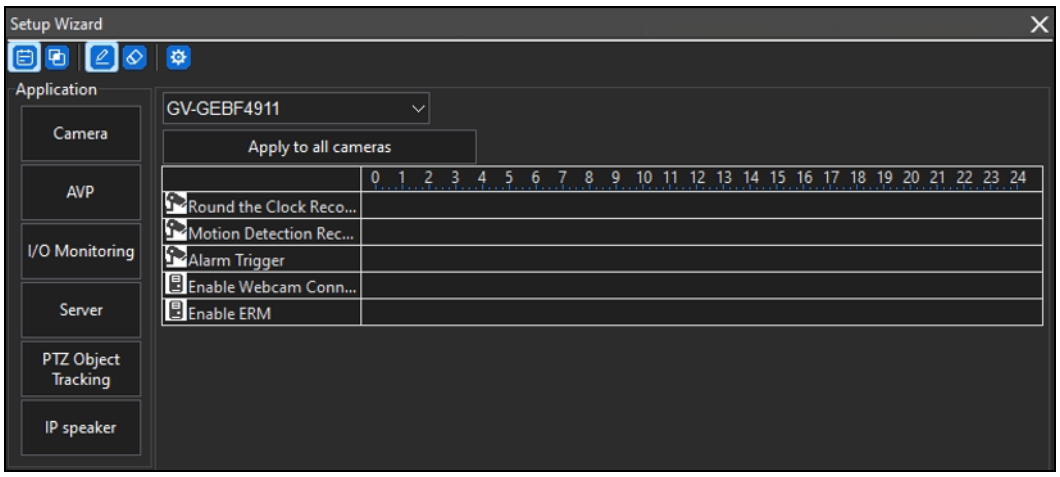
1.8.1 Creating a Schedule with Setup Wizard

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

1. In the Schedule dialog box, click **Schedule** and select **Setup Wizard**. The Setup Wizard dialog box appears.
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.



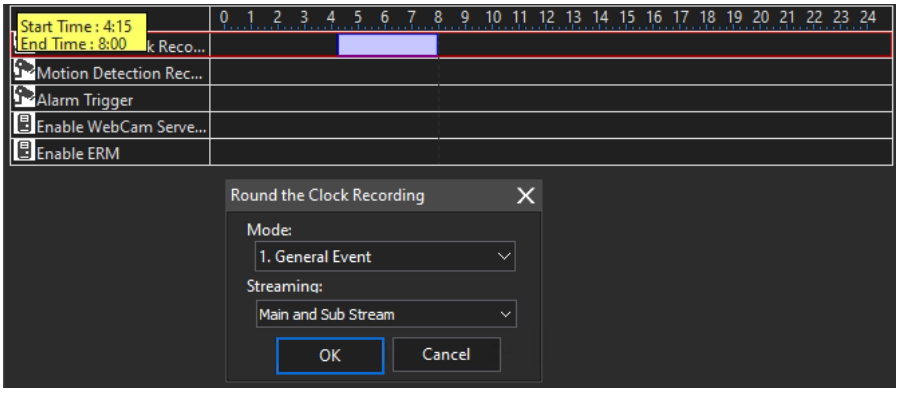
5. When the **Include** button is selected, you will start with an empty timeline. Click the **Add** button and drag across the timeline to enable the function during the specified time. Use the **Erase** button when you want to disable the function.
6. You can also click the **Exclude** button and start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

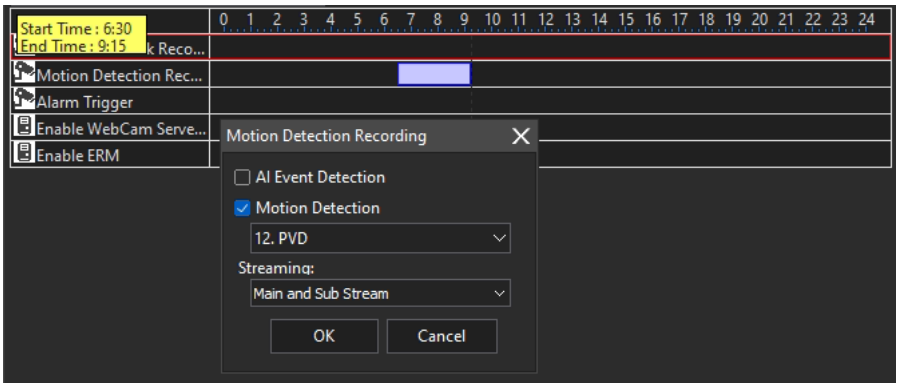
     - **Round-the-Clock Recording:** When highlighting the timeline, select the frame rate settings of **General Event** or **Urgent Event**, which will be applied once the schedule monitoring is started. Also select the Stream Type of **Main and Sub Stream**, **Main Stream**, or **Sub Stream**.



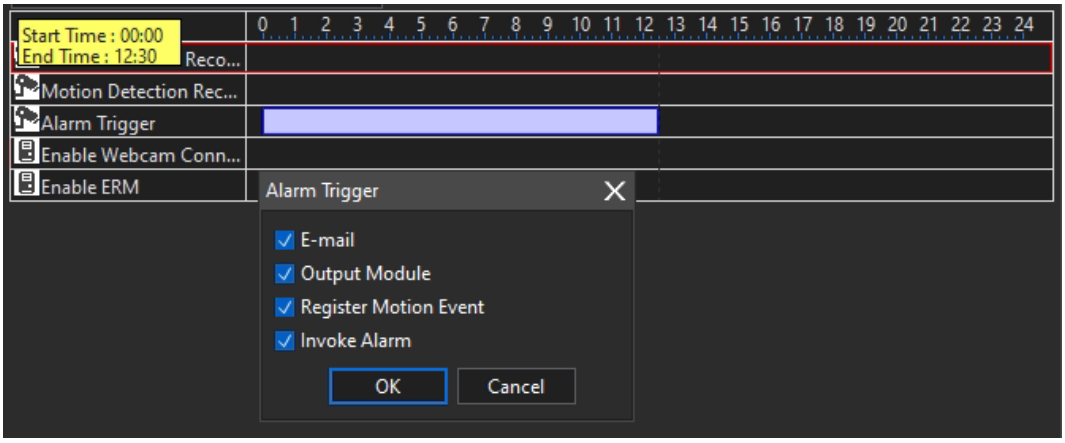
     - **Motion Detection Recording:** When highlighting the timeline, select **AI Event Detection** (triggered from AI-capable GV IP cameras) or **Motion Detection**.

       - For Motion Detection, you can further select different **Sensitivity** levels, **User Defined** to apply the sensitivity level set in the Advanced Motion Detection Setup dialog box (see the dialog box in *Setting Up Motion Detection* earlier in this chapter), or **PVD** to enable people / vehicle detection.

     Also select the Stream Type of **Main and Sub Stream**, **Main Stream**, or **Sub Stream**.



- **Alarm Trigger:** When highlighting the timeline, select **E-mail**, **Output Module**, **Invoke Alarm**, or **Register Motion Event** for the desired actions upon alarms.



- **PTZ:** When highlighting the timeline, select a PTZ Auto function to be enabled during that time.
- **Enable Webcam Connection:** Grant streaming access for GV-WebCam Server within the highlighted time periods.
- **Enable ERM:** Grant streaming access for GV-Edge Recording Manager within the highlighted time periods.

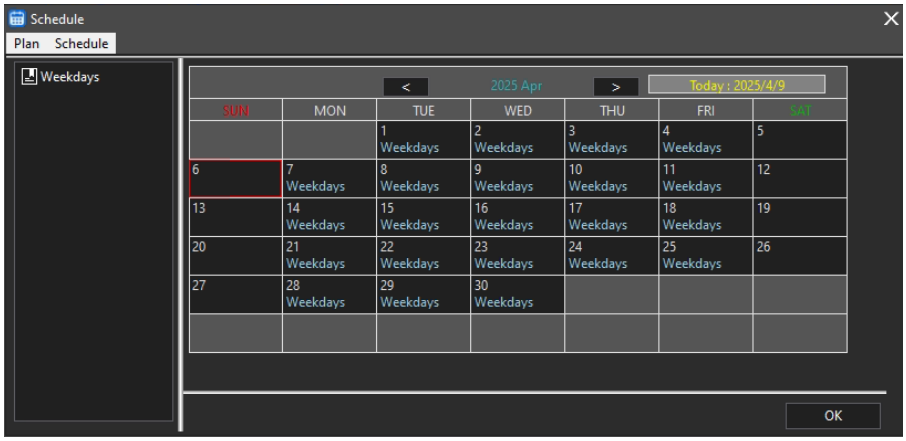
■ **AVP:** Enables video processing functions according to the defined monitoring schedule.

- **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.
- **IPC VA (Face Detection):** Enables Face Detection within the highlighted time periods. For details, see *Local Face Recognition* in Chapter 3.
- **IPC AI:** Enables the reception of the camera's AI video analysis events within the highlighted time periods. For details, see *Video Analysis by Camera* in Chapter 3.

Note: To enable scheduled monitoring for **IPC VA (Face Detection)** and **IPC AI**, make sure the **Record** option is enabled in the IP Cam Video Analysis dialog box. For details, see Step 5 in *Local Face Recognition* and Step 5 in *Video Analysis by Camera* in Chapter 3, respectively.

- **I/O Monitoring:** Enables I/O Monitoring within the highlighted time periods.
- **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:** Enables PTZ Object Tracking within the highlighted time periods.
- **IP Speaker:** Enables the speaker to play audio within the highlighted time periods. This function is available only when an IP speaker is connected.

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



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.

1.8.2 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 schedule plan to a specific date each year. Select a **Date** and a **Plan** and click the **Add** button.
   - **Edit Weekly:** Applies the schedule plan to the selected days each week.
   - **Edit Monthly:** Applies the schedule plan to a specific date each month. Select a **Day** of the month and a **Plan**, and click the **Add** button.
4. Double-click the Plan to edit the schedule timeline. For details, see the previous subsection *Creating a Schedule with Setup Wizard*.

1.8.3 Exporting and Importing Schedules

Schedule plans can be exported into an .xml file, and imported back later or to another GV-VMS.

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.**

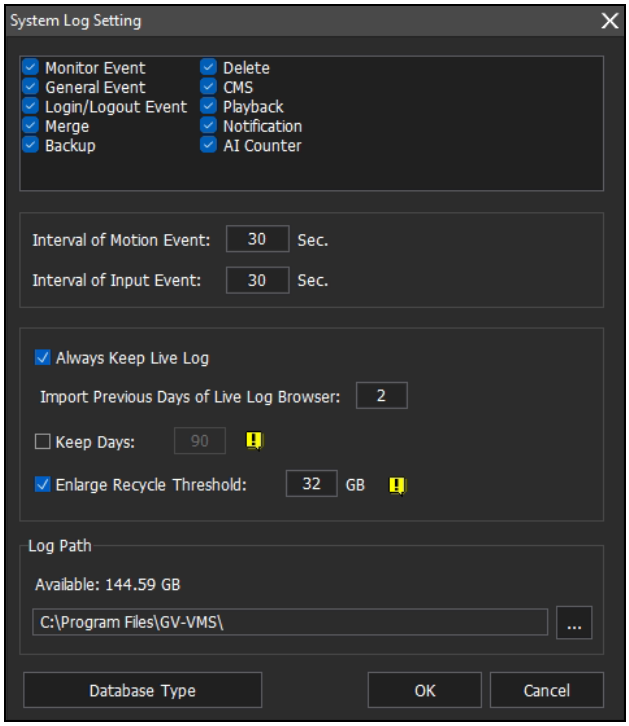
1.9 System Log

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.

1.9.1 Setting Up System Log

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



Select the type of event to 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 dialog box (see the dialog box in *Setting Up Motion Detection* earlier in this chapter) or **Register Input Event** in the I/O Application Setting dialog box (see the dialog box in *Setting Up Actions upon Input Trigger* in Chapter 6).

- **General Event:** Registers system startup/exit, network server start/stop, and monitoring start/stop.
- **Login/Logout Event:** Registers login or logout events of local users to the system and GV-WebCam Server.
- **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 Counter:** Registers counting results from the GV-3D People Count function in IPCVA (for GV-3D People Counter V2 or V3) and the Object Count function in IPCVA (for AI-capable GV-IP cameras).

The following settings are also available:

- **Interval of Motion Event:** Specify the log interval between motion-triggered events, which prevents the system from recording events too frequently when motion triggers are intensive.
- **Interval of Input Event:** Specify the log interval between input-triggered events, which prevents the system from recording 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 section). When the option is disabled, the logs of events 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 threshold (5 to 999 GB) for the system to start deleting old system logs when the available space in the assigned Log Path falls below this limit, in order to free up space for new files. The default threshold is set to 32 GB.
- **Log Path:** Specify the storage path for system logs. By default, the path is set to C:\Program Files\GV-VMS\. The available free space of the specified path will be displayed.
- **Database Type:** Select **Default Database** or **Advanced [Microsoft SQL Server]** as a database, and fill out the required connection information.

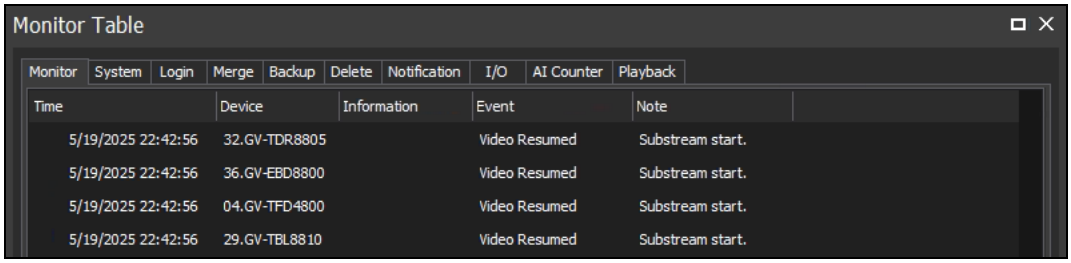
Note: If the designated storage space is not big enough to keep all video files for the defined days, the **Enlarge Recycle Threshold** setting will override the **Keep Days** setting.

1.9.2 Viewing System Log

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

Monitor Table

This table displays local events in the system.



[Monitor] Shows events related to camera connection and motion. Double-clicking an event can play back its recording if available.

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

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

[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 email notifications.

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

[AI Counter] Shows the counting results from the GV-3D People Count function in IPCVA (for GV-3D People Counter V2 or V3) and the Object Count function in IPCVA (for AI-capable GV-IP cameras).

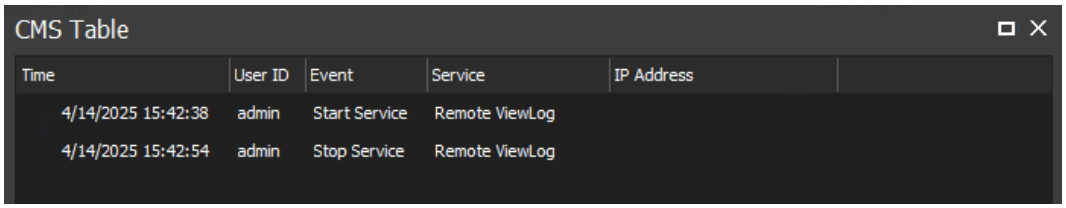
[Playback] Shows the playback events of recorded videos.

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 services (CMS).

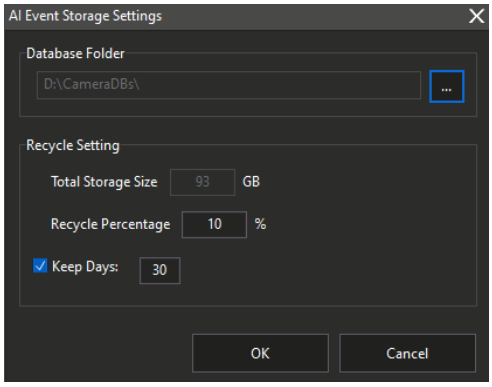


1.10 AI Event Storage

GV-VMS provides a wide range of functions that display images from AI, PVD, and face events, such as Event List and AI Query. You can configure the AI Event Storage Settings to manage the storage of related event images.

1.10.1 Setting Up AI Event Storage

In the AI Event Storage Settings, you can specify the database folder and the number of days to keep the images for. Click **ViewLog** > **Toolbar** > **Configure** > **AI Event Storage Settings**. This dialog box appears.



The following settings are available:

[Database Folder] Specify the storage path for AI event images, PVD motion images, and face images. By default, the path is set to D:\CameraDBs\.

[Recycle Setting]

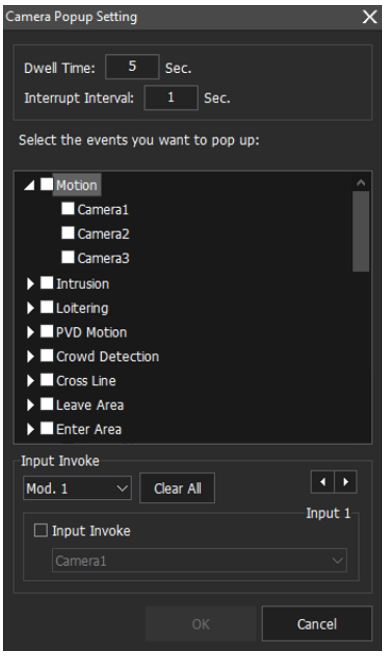
- **Total Storage Size:** Displays the maximum amount of disk space allocated for storing AI event images, PVD motion images, and face images. When the occupied space exceeds this limit, the system will start deleting the oldest files to free up space for new ones. The value is automatically calculated 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.

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.

1.11 Other Functions

1.11.1 Popping Up Live View

To set up a popup live view, which overlays the entire main screen, upon events, click **Home** > **Toolbar** > **Configure** > **Camera Popup Setting**. This dialog box appears.



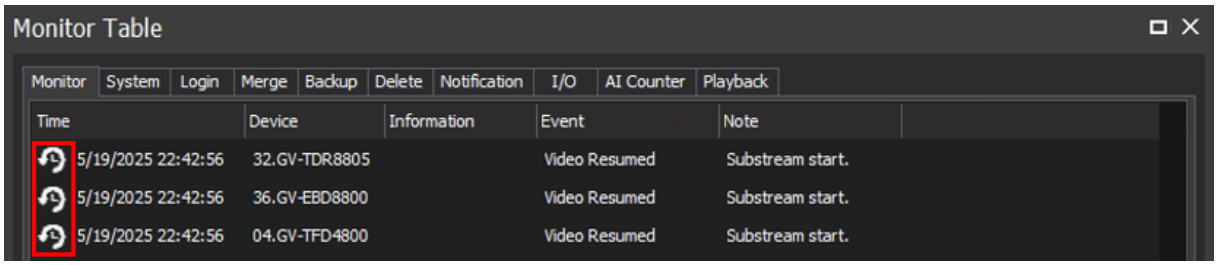
- **Dwell Time:** Specify the amount of time a popup view to remain in the foreground.
- **Interrupt Interval:** Specify the interval between popup views, which prevents frequent popup alerts when multiple cameras are activated at the same time.
- **Events:** Select the camera channel to pop up upon 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 will pop 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 dialog box (see the dialog box in *Setting Up Motion Detection* earlier in this chapter) to mask off certain areas on the camera image where motion will be ignored.

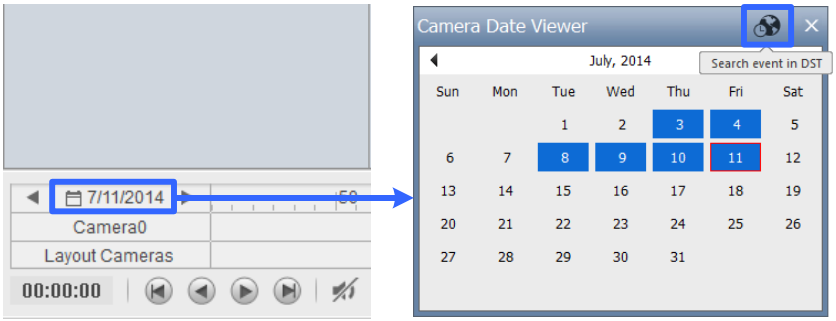
1.11.2 Adjusting to Daylight Saving Time

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

In the System Log, DST events are labeled with clock icons in the **Time** column.



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

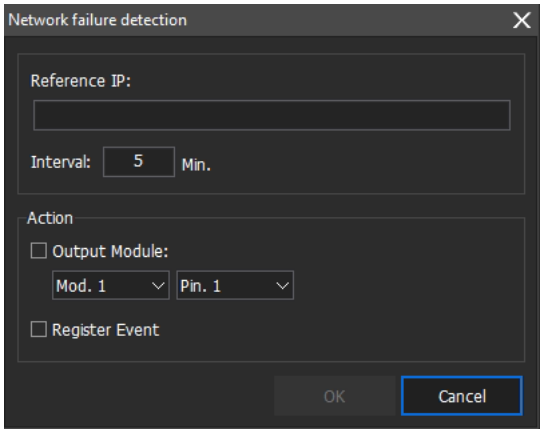


Note: Videos recorded during DST periods start with "GvDST", e.g., GvDST20140722.avi, to differentiate from regular video files that start with "Event", e.g., Event20081022.avi.

1.11.3 Setting Up Network Failure Detection

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

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



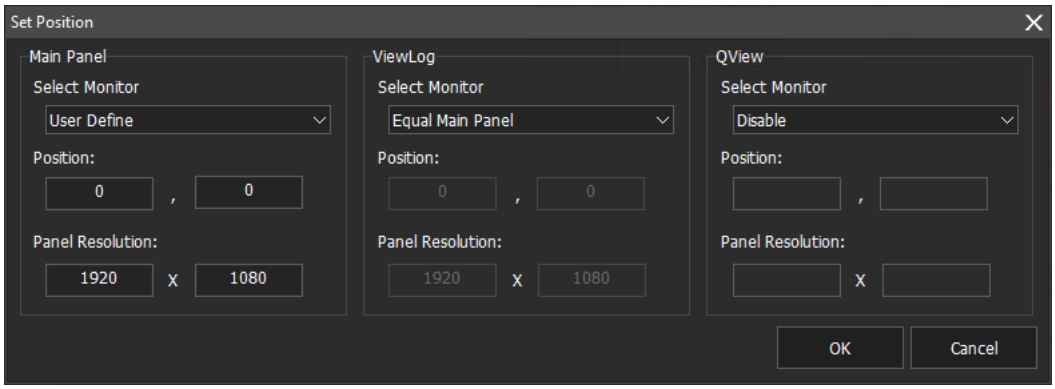
2. Under **IP Address**, type the IP address or domain name of the remote host.
3. Next to **Interval**, type the time interval between each ping in minutes ranging from 1 to 999. If the interval is 5 minutes, GV-VMS will ping the network host every 5 minutes to check if the connection is still active.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

1.12 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.

1.13 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.

1.13.1 Creating a Storyline in Live View

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

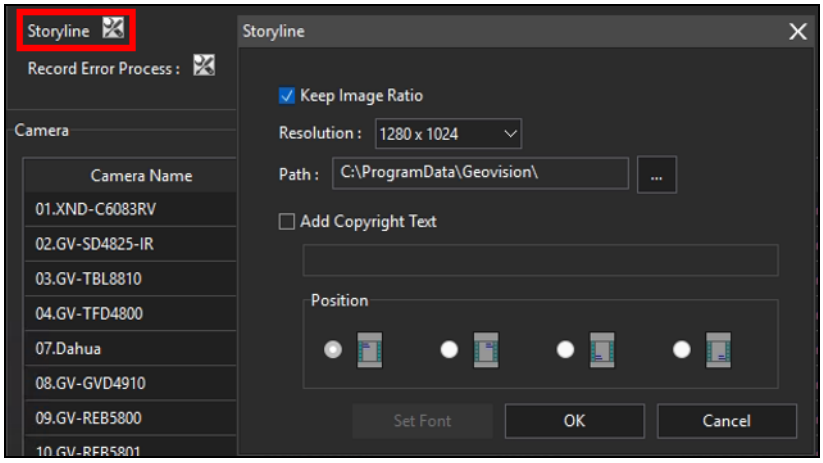
1. Select **Home** and set up the screen division.
2. In the Content List (No. 9 in *Main Screen* earlier in this chapter), click **Layout**, double-click **Windows**, and drag **Zoom Window** to a live view grid. Any camera views on the Zoom Window will be recorded as a storyline.
3. To display cameras 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 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 button next to *Storyline*.



1.13.2 Creating a Storyline in Video Playback

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

1. Select **ViewLog** .
2. In the Content List (No. 9 in *Main Screen* earlier in this chapter), click **Layout**, double-click **Windows**, and drag **Zoom Window** to a playback grid.
3. To display a video on the Zoom Window, click the **Zoom** button on the top right of a playback video.
4. On the Zoom Window, click the **Tools** icon > **Storyline** to start recording.
5. To record another video, click the **Zoom** button of that playback video.

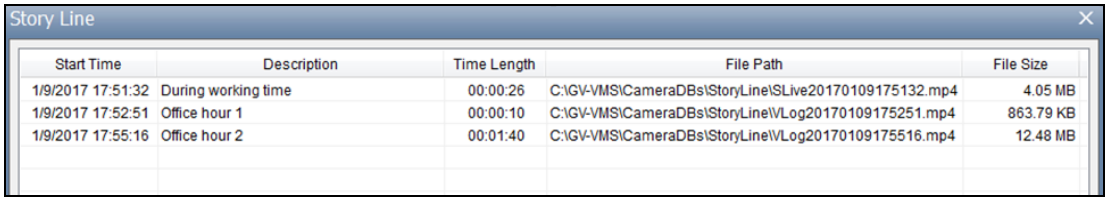
1.13.3 Creating a Storyline in QView

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 video from another camera, simply double-click another camera view.

1.13.4 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 on 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 95

2.1 Adding IP Cameras 95

2.1.1 Adding Cameras Manually 97

2.1.2 Scanning for Cameras 99

2.1.3 Mapping GV-IP Cameras Using GV-IP Device Utility 100

2.1.4 Adding Cameras of Mobile Devices using GV-Live Streaming 100

2.2 Configuring Individual IP Cameras 101

2.2.1 General Settings 102

2.2.2 Video Settings 103

2.2.3 Video Stream Settings 104

2.2.4 Audio Settings 106

2.2.5 Abnormality Settings 107

2.2.6 Recording Settings 107

2.2.7 Advanced Settings 109

2.2.8 POE Switch Settings 110

2.3 Connection Through RTSP, ONVIF & PSIA 111

2.4 On-Demand Display 113

2.5 Wide Angle Lens Dewarping 115

2.6 Fisheye View 117

2.6.1 Setting Up Fisheye View 118

2.6.2 Setting Up a Third-Party Fisheye Camera 121

2.6.3 Object Tracking 122

2.6.4 Virtual PTZ Tour 123

2.7 PTZ Camera 125

2.7.1 Accessing PTZ Control Panel and Auto Functions 126

2.7.2 Setting Up Idle Protection and Advanced Functions 128

2.8 PTZ Object Tracking 130

2.8.1 Dual Camera Tracking 130

2.8.2 Single Camera Tracking 133

2.9 Panoramic PTZ Object Tracking 135

2.9.1 Accessing the Live View 136

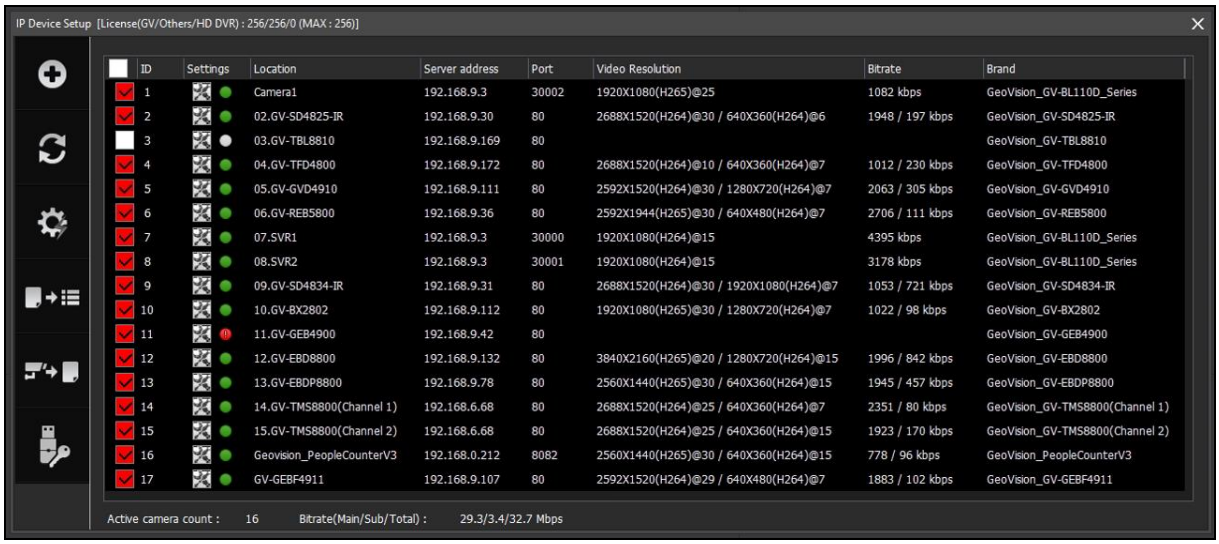
2.9.2 Automatic Object Tracking 137

CHAPTER 2

IP Camera Setup

2.1 Adding IP Cameras

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



IP Device Setup dialog box

- 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 GV-VMS Pro 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.

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

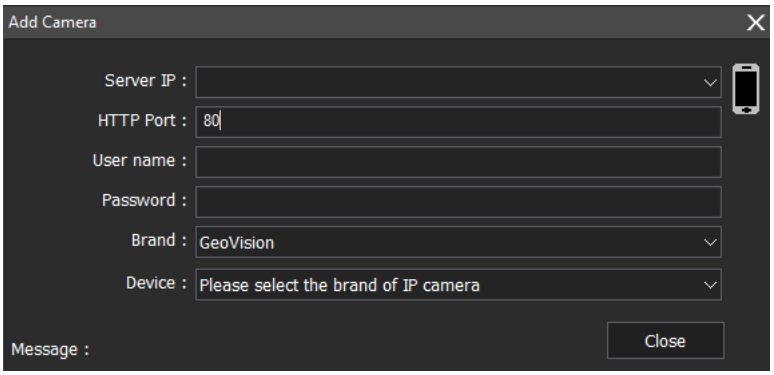
3rd-Party IP Devices

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

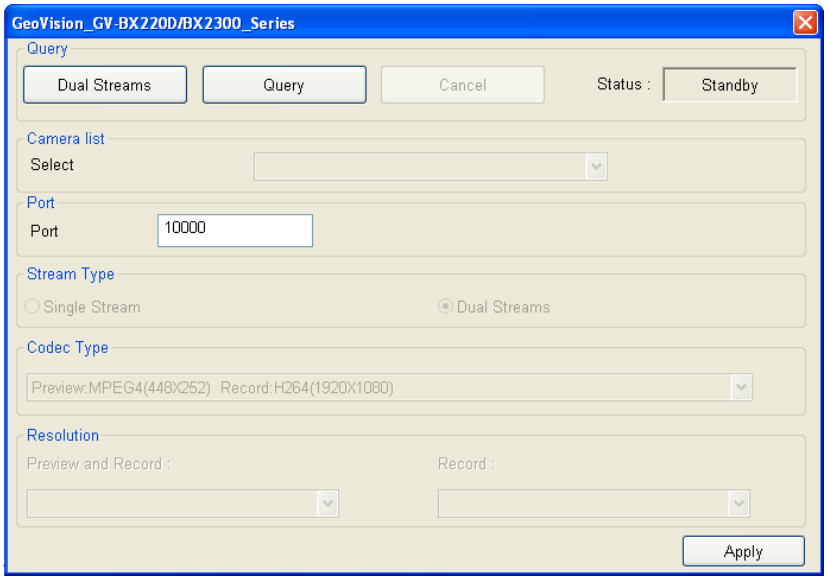
If a 3rd-party device cannot be detected using *Scan Camera* or *Automatic Setup*, you can add it manually using the **Add Camera** function. For details, see *Connection Through RTSP, ONVIF & PSIA* later in this chapter.

2.1.1 Adding Cameras Manually

1. To manually add IP devices, click **Add Camera** in the IP Device Setup dialog box (see the dialog box in *Adding IP Cameras* earlier in this chapter).
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.

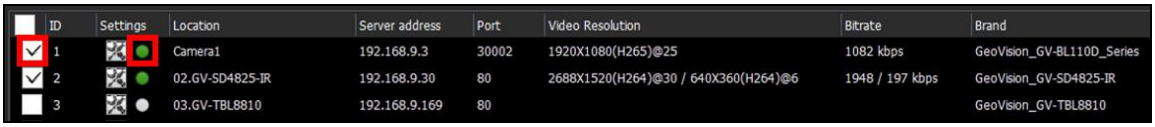


Camera Streaming Settings dialog box

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.



ID	Settings	Location	Server address	Port	Video Resolution	Bitrate	Brand
1		Camera1	192.168.9.3	30002	1920X1080(H265)@25	1082 kbps	GeoVision_GV-BL110D_Series
2		02.GV-SD4825-IR	192.168.9.30	80	2688X1520(H264)@30 / 640X360(H264)@6	1948 / 197 kbps	GeoVision_GV-SD4825-IR
3		03.GV-TBL8810	192.168.9.169	80			GeoVision_GV-TBL8810

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

Tips: You can access the camera's own configuration interface by right-clicking the camera in the IP Device Setup dialog box and selecting **Remote Camera Setting**.

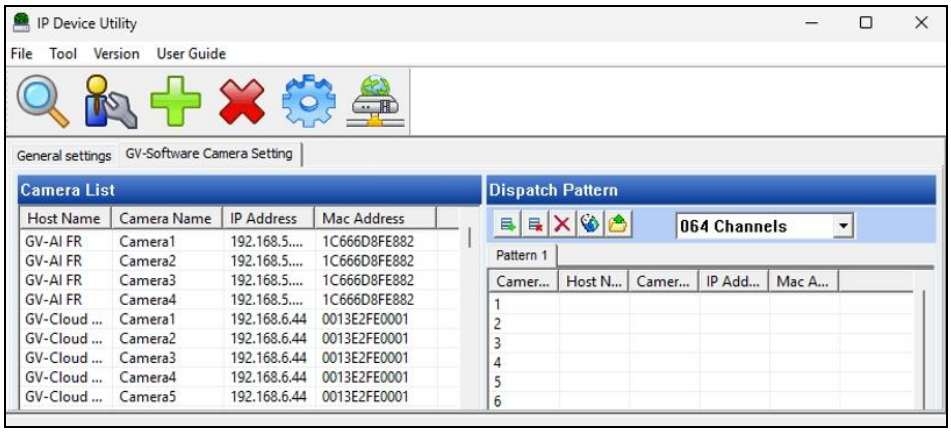
2.1.2 Scanning for Cameras

1. To detect IP devices on the LAN, click **Scan Camera**  in the IP Device Setup dialog box (see the dialog box in *Adding IP Cameras* earlier in this chapter). 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 (see the dialog box in *Adding Cameras Manually* earlier in this chapter).
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 GV-VMS. 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 dialog box (see the dialog box in *Adding IP Cameras* earlier in this chapter). All the available IP cameras on the LAN are detected and listed in the window.



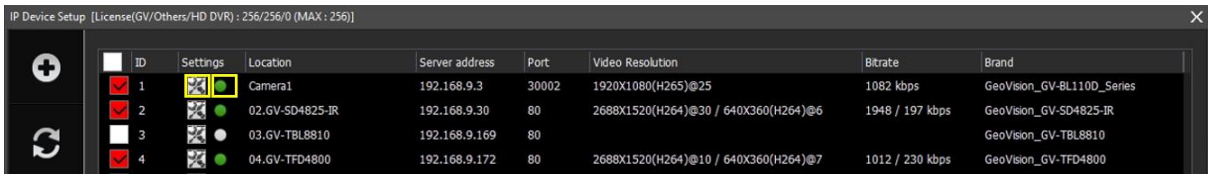
To map IP cameras to the channels of GV-VMS, see *Assigning Camera Channels for GV-DVR / NVR / VMS* in the *GV-IP Device Utility Guide*.

2.1.4 Adding Cameras of Mobile Devices using GV-Live Streaming

GV-Live Streaming is a paid mobile app that allows the camera of your Android / iOS mobile device to connect and stream live view to GV-VMS via GV-Relay. For details, see the *GV-Live Streaming Installation Guide*.

2.2 Configuring Individual IP Cameras

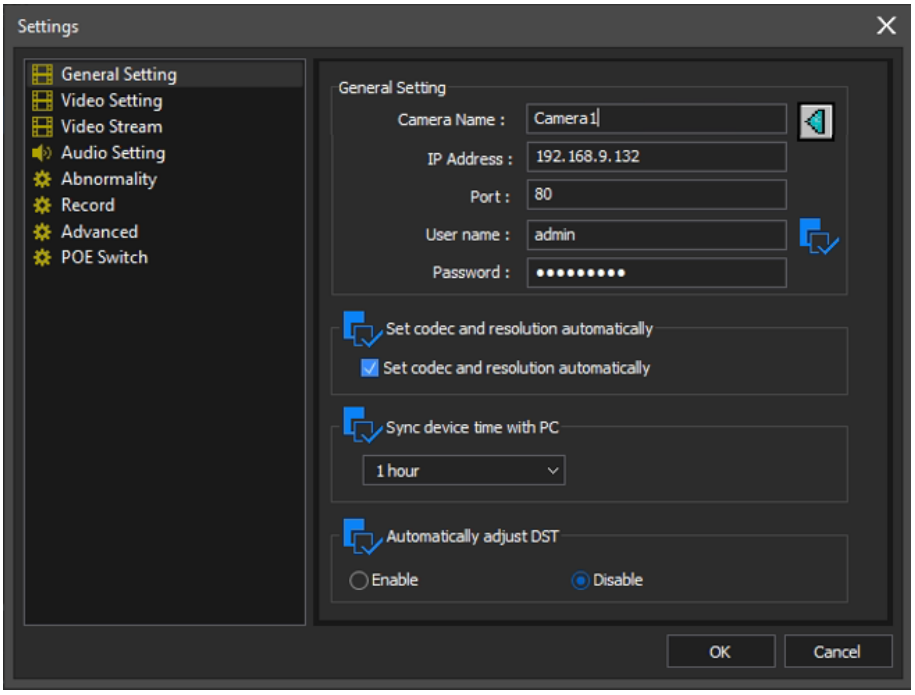
To configure IP camera settings, such as video, audio, and other general settings, click the **Setup** button  of the connected camera on the IP Device List.



Tip: To configure IP camera settings, you can also right-click a camera on the Content List (No. 9 in *Main Screen* in Chapter 1) and select **IP Device Setup**.

2.2.1 General Settings

In the General Settings dialog box, you can configure settings such as the camera name, auto-recovery of codec and resolution, time synchronization, and DST adjustment.



[General Settings] Type a name for the camera. Click  if you want to restore the default name. Modify the IP address, port, username, and password. Note that this function is only available for configuration when the camera is disconnected.

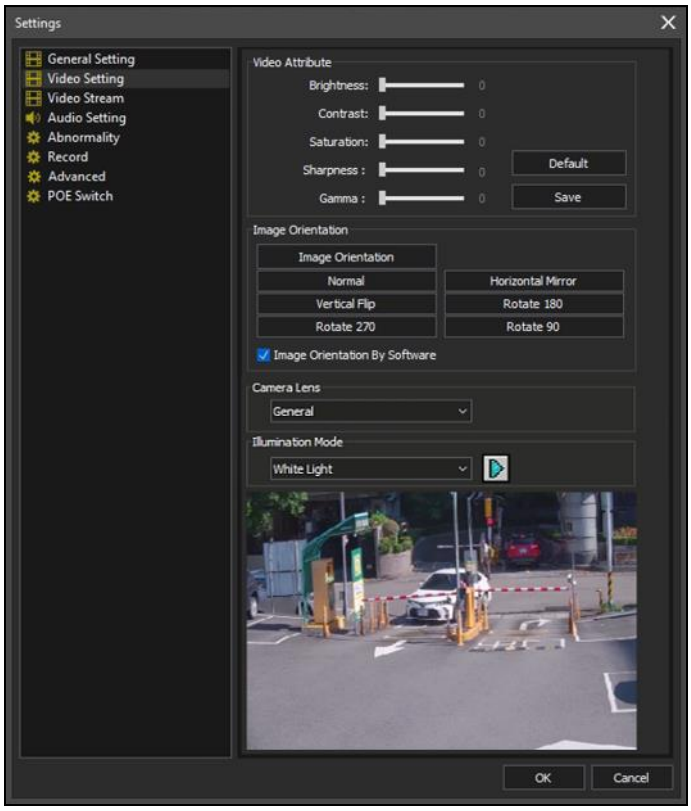
[Set Codec and Resolution Automatically] If enabled, GV-VMS will resume the configured codec and resolution when it detects the changes made by the camera.

[Sync Device Time with PC] This function is set to *NO* by default, meaning the camera time will not sync with the GV-VMS system time. When an interval of *1 – 24 hours* is selected, the camera time syncs with GV-VMS upon connection and re-syncs automatically at the specified interval.

[Automatically Adjust DST] If enabled, the time on GV-IP Device's Web interface will be synchronized with that on the system when the DST period starts or ends.

2.2.2 Video Settings

In the Video Settings dialog box, you can configure settings such as image attributes, orientation, and lens options.



[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°**. Selecting **Image Orientation by Software** allows GV-VMS to perform the rotation; otherwise, the function is processed directly by the IP camera. Note that the **Rotate 90°** and **Rotate 270°** (Corridor Format) options are supported only by certain GV-IP Cameras.

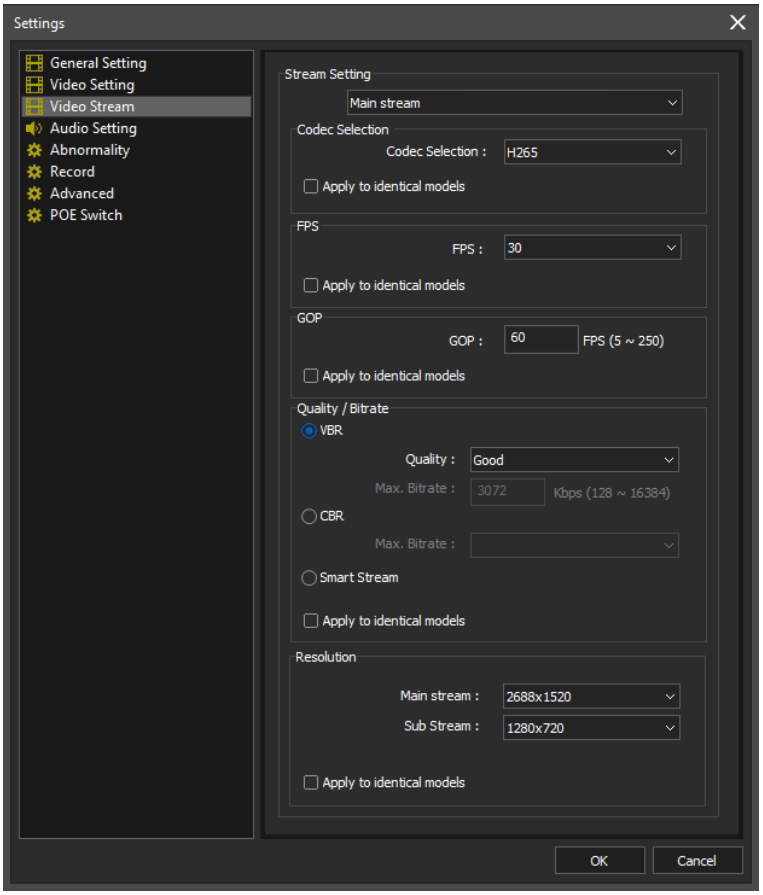
[Camera Lens] Select **Wide Angle** if you want to correct warping toward the edge of the camera image. For details, see *Wide Angle Lens Dewarping* later in this chapter. If you are using third-party fisheye cameras, select **IMV1 Panorama** for the camera installed with an ImmerVision IMV1 Panorama Lens, and select **Fisheye** for other third-party fisheye cameras. For details, see *Setting Up a Third-Party Fisheye Camera* later in this chapter.

[Illumination Mode] Adjust the illumination mode by selecting **Smart Supplement Light** (default), **White Light**, or **Infrared Light**. When Smart Supplement Light is selected, the IP camera automatically turns on the IR light or white light under low ambient light. It switches to white light when a person enters the detection area, and returns to IR light when no person is detected. This function is available only for certain GV-IP Cameras.

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

2.2.3 Video Stream Settings

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



Video Stream Settings dialog box

[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.

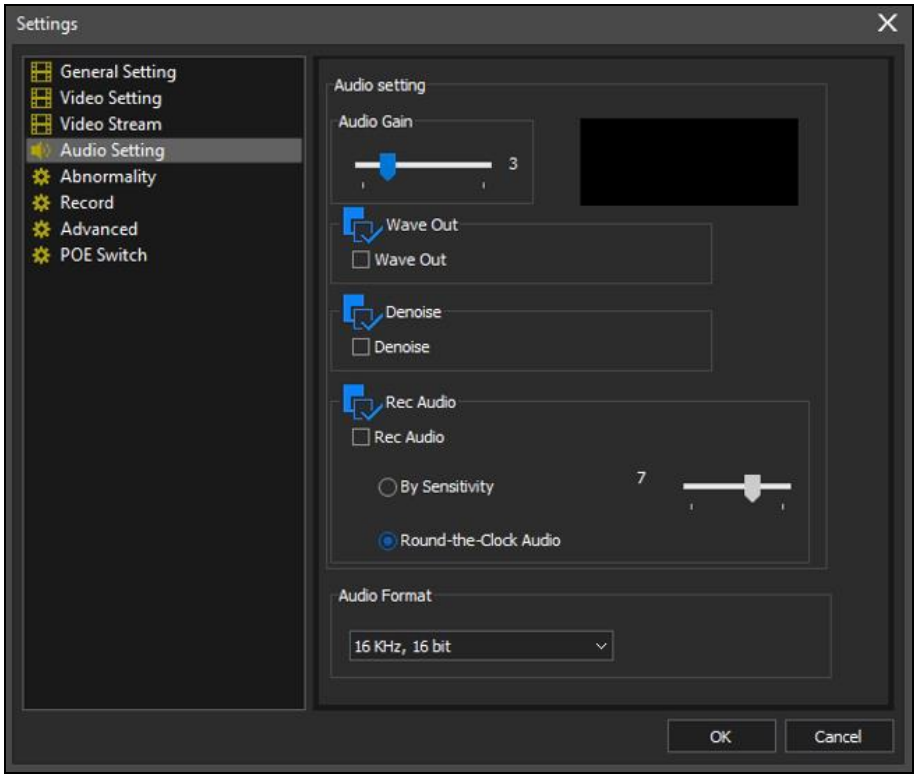
Note:

1. Changes made to the Video Stream page will change the settings on the IP camera.
2. The following default sub stream settings are applied during initial setup based on the number of connected channels:
   a. If 1 to 32 channels are connected, all sub streams are set to 15 fps with a GOP of 30.
   b. If more than 32 channels are connected, all sub streams are set to 7 fps with a GOP of 14.

   These values help define the minimum system requirements and can be adjusted afterward.
3. Select **Apply to identical models** to apply the settings to all identical models.

2.2.4 Audio Settings

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



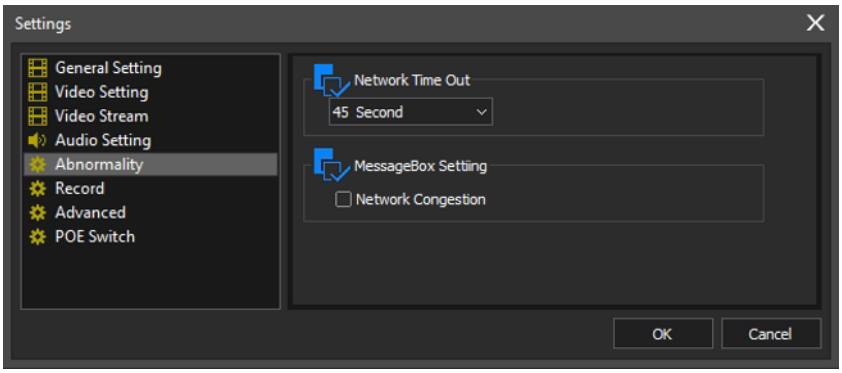
[Audio Settings]

- **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**.

2.2.5 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.

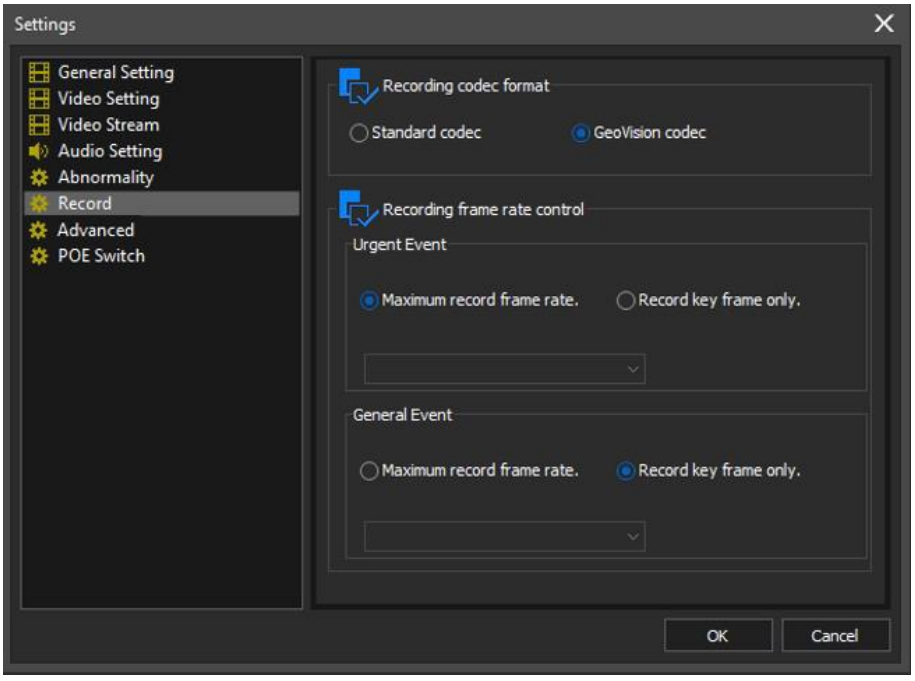


[Network Time Out] When network disconnection exceeds the specified time period, the status icon in the IP Device Setup dialog box (see the dialog box in *Adding IP Cameras* earlier in this chapter) becomes yellow.

[Message Box Setting] When enabled, the Network Congestion message will pop up under such a condition.

2.2.6 Recording Settings

In the Record dialog box, you can configure settings such as the recording codec format, recording frame rate for different event types, and key frame recording options.



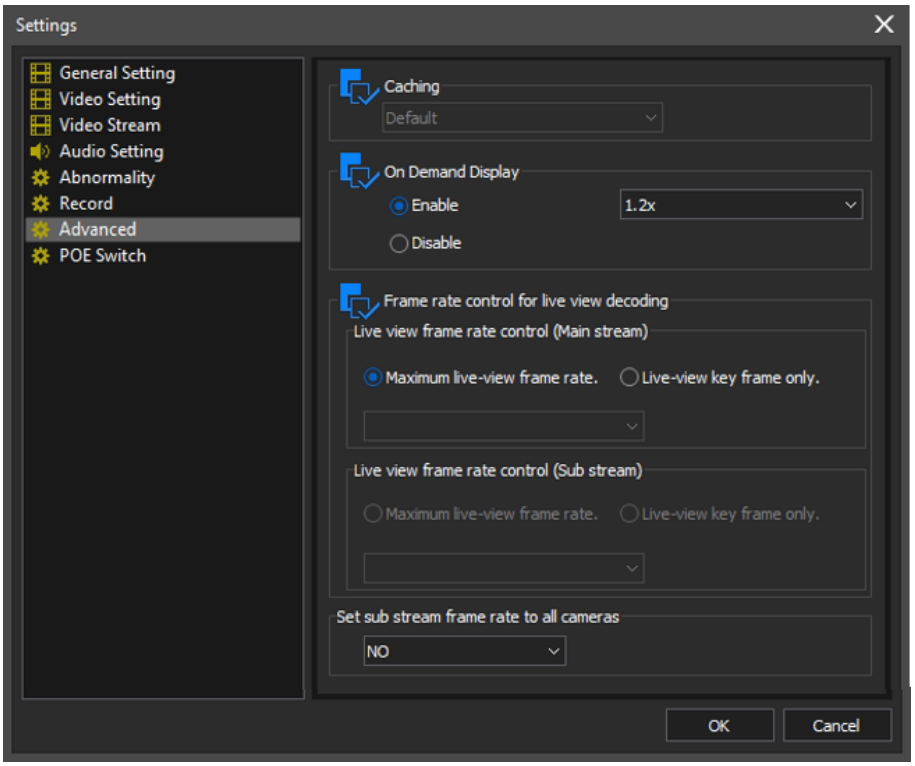
[Recording Codec Format] Specify whether to record in standard or GeoVision codec.

[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**.

2.2.7 Advanced Settings

In the Advanced dialog box, you can configure settings such as live view caching, on-demand resolution adjustment, live view frame rate control, and global sub stream frame rate settings.



[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.

[On Demand Display] Enable automatic adjustment of live view resolution. For details, see *On Demand Display* later in this chapter.

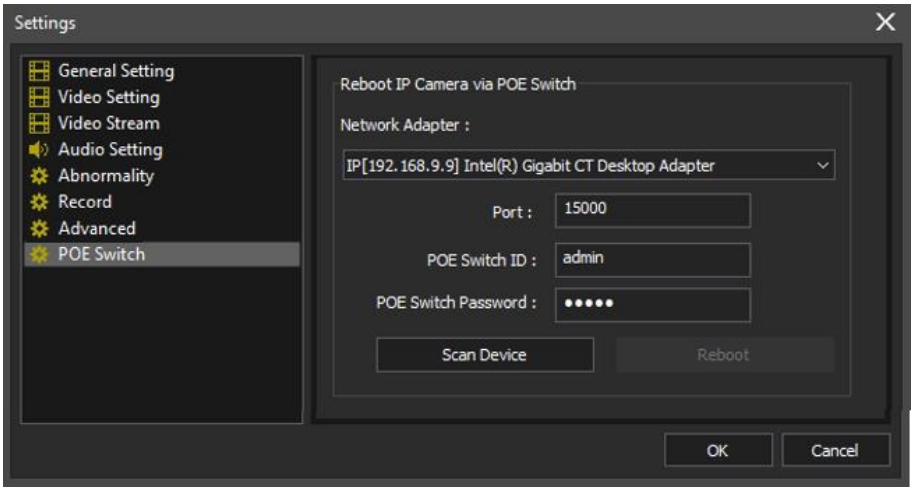
[Frame Rate Control for Live View Decoding]

- **Live View Frame Rate Control (Main / Sub Stream):** Set the live view frame rate for main stream and sub stream.
  - When using **MJPEG**, every frame is a key frame, so the options of **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.

[Set Sub Stream Frame Rate to All Cameras] By default, when 1 to 32 channels are connected, the sub stream frame rate is automatically set to 15 fps; when more than 32 channels are connected, it is set to 7 fps. Select from the dropdown list to manually adjust the sub stream frame rate for all cameras at once, from 1 fps to 15 fps.

2.2.8 POE Switch Settings

In the POE Switch dialog box, you can configure settings such as rebooting a specific IP camera through a connected GV-POE Switch with Web management.

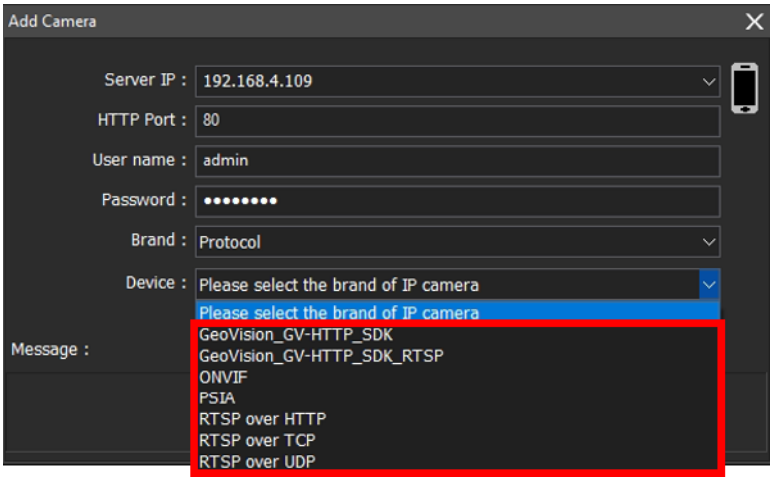


- **Reboot IP Camera via POE Switch:** Restart a specified camera via its connected GV-POE Switch with the Web management functionality. Type the ID and Password of the switch to start rebooting.

2.3 Connection Through RTSP, ONVIF & PSIA

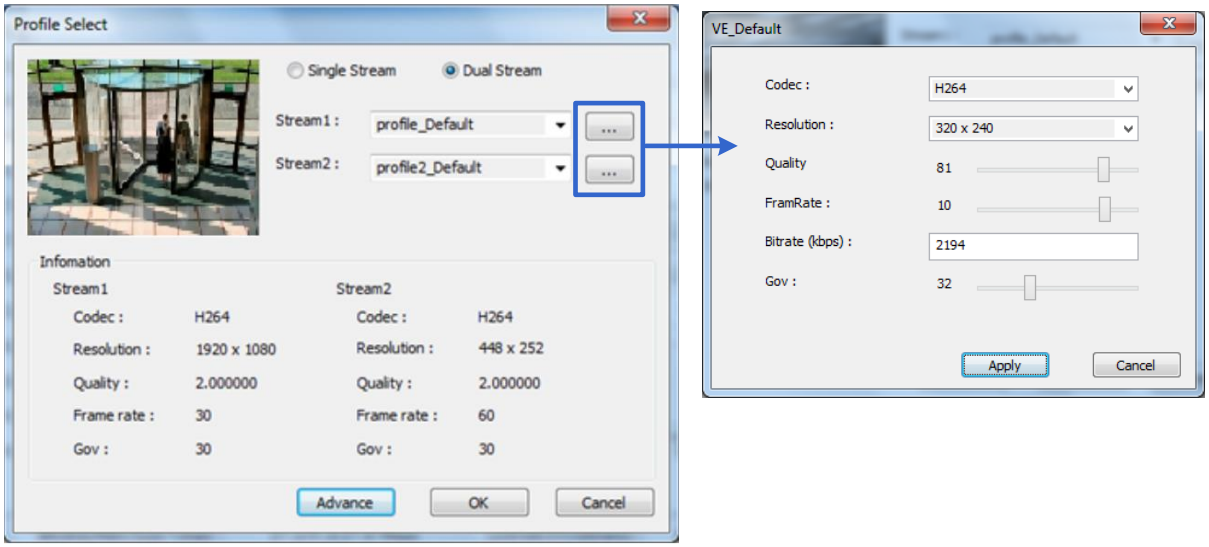
To add IP devices compliant with RTSP, ONVIF, or PSIA protocol to GV-VMS, follow the steps below.

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:

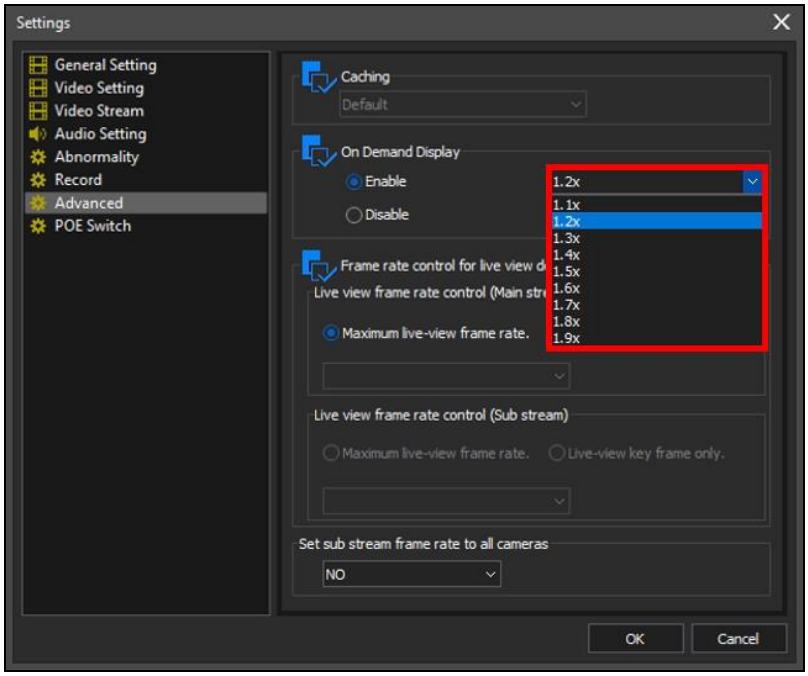
   - For an AXIS IP camera, type RTSP://<IP of the IP camera>/<codec>/media.amp
   - For a HIKVISION IP camera, type RTSP://username:password@<IP of the IP Camera>
9. Click **OK** to add the IP camera to the IP Device List.

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 GV-VMS and you have selected **Dual Stream** during setup. For details, see *Adding IP Cameras* earlier in this chapter.
2. In the IP Device Setup dialog box (see the dialog box in *Adding IP Cameras* earlier in this chapter), click the **Setup** button of the desired connected camera within the IP Device List, and select **Advanced**.
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.



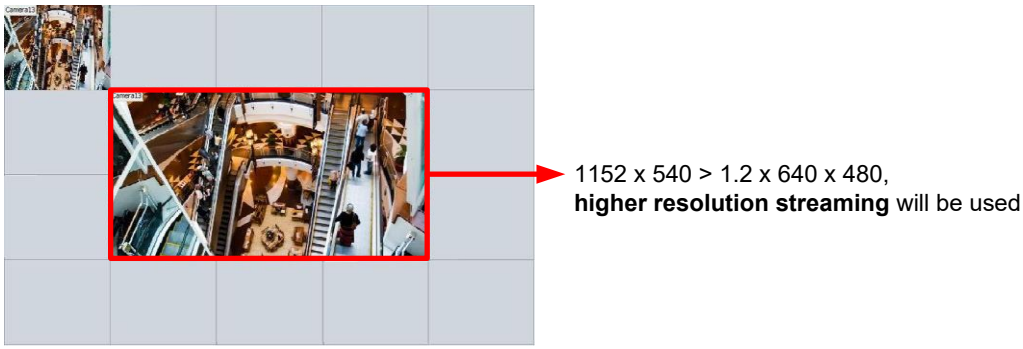
Note:

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

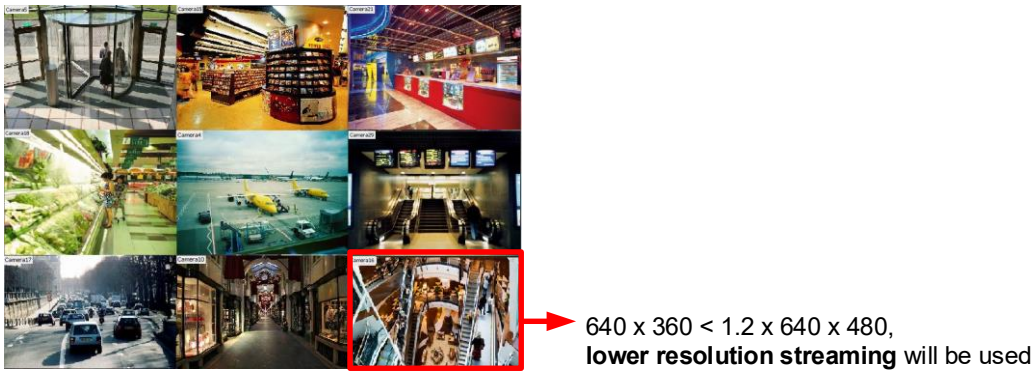
The resolution of sub stream is 640 x 480, and a value of **1.2 times the resolution of the sub stream** has been selected for the On Demand Display function.

- **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.

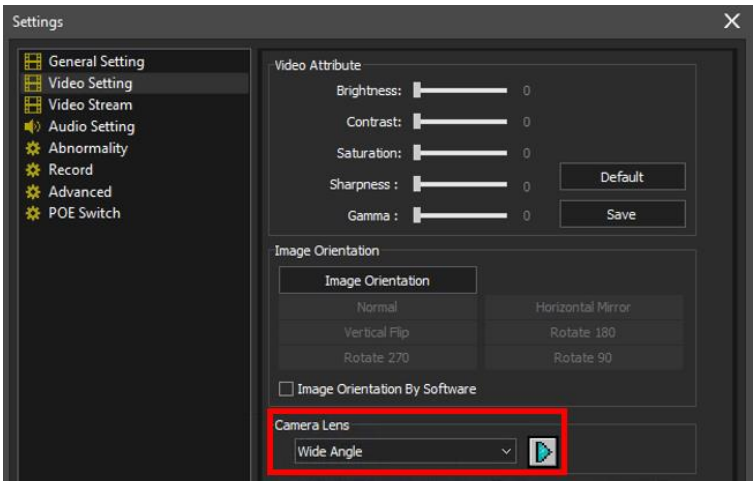
2.5 Wide Angle Lens Dewarping

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

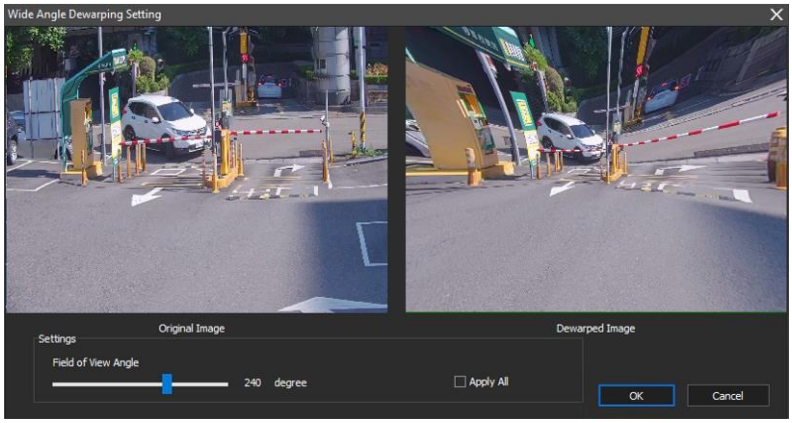
1. Click **Home** > **Toolbar** > **Configure** > **Camera Install**. The IP Device Setup dialog box appears.
2. Click **Settings** .



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 to 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, a graphics card supporting DirectX 10.1 or above is required.



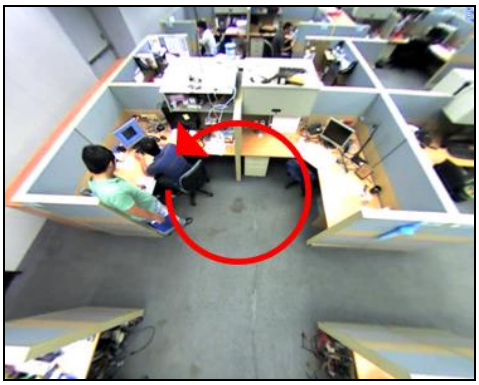
Quad view: 4 PTZ views



360 degree: 2 PTZ view & 1 360º view



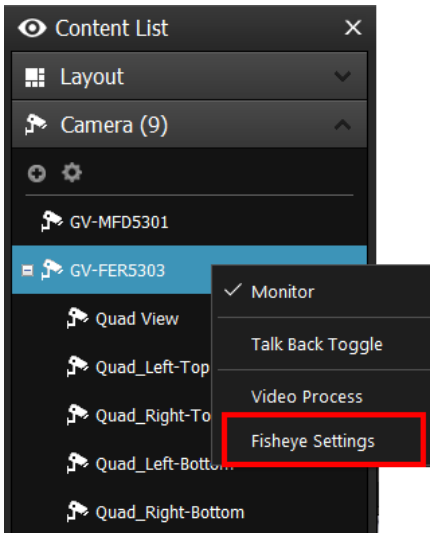
Dual 180 degree: 2 180º views



Single view: 1 PTZ view

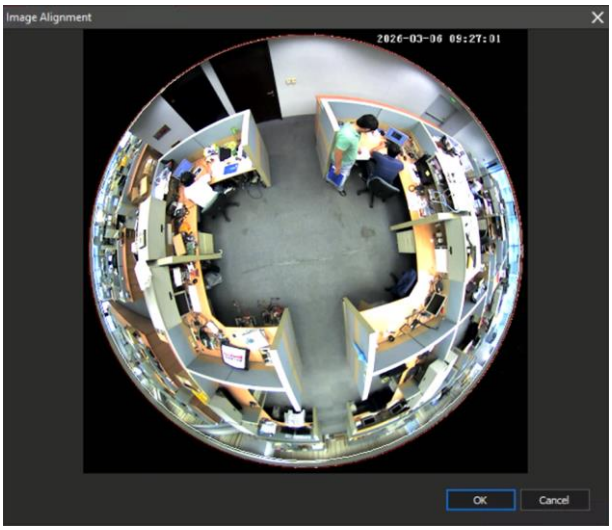
2.6.1 Setting Up Fisheye View

1. To display the dewarped view, from the Content List (No. 9 in *Main Screen* in Chapter 1), drag the fisheye camera (circular source image) or one of the dewarped fisheye images (e.g., Quad View) to the live view grid.
2. To change the fisheye settings, right-click the fisheye camera from the Content List, and then select **Fisheye Settings**. The Fisheye Settings dialog box appears.



3. Right-click within any view in the Fisheye Settings dialog box, and select **Fisheye Option** to access the following settings:

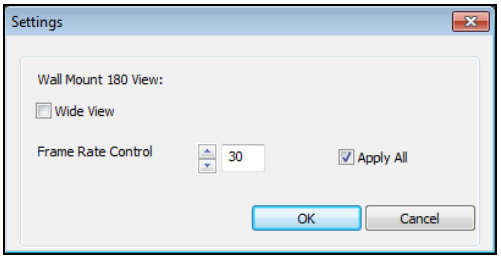
   - **Image Alignment:** Align the circle first with the outer edge of the fisheye image, then with the inner edge of the image frame to ensure correct dewarping.



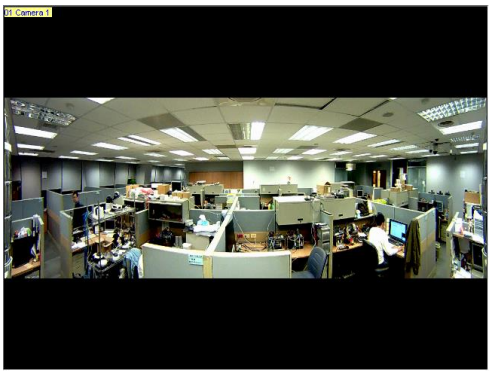
   - **Camera Mode:** You can choose among four view modes.
     - **Quad view:** Composed of four PTZ views.

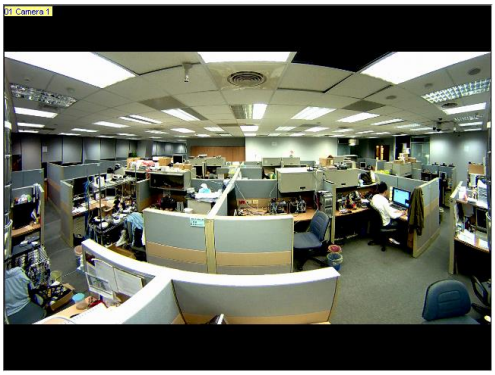
- ⊙ **360 degree:** Composed of two PTZ views and one 360º panoramic view.
- ⊙ **Dual 180 degree:** Composed of two 180º views.
- ⊙ **Single view:** Composed of one PTZ view. This view mode supports the advanced Picture-in-Picture (PIP) function, which allows you to have a close-up dewarped view without missing the entire view of the 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 the 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:** 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 section.
  - ⊙ **Disable automatic zoom adjustment during 360 Object Tracking:** Enabled by default. When disabled, the zoom ratio will be kept 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 section.
- **Settings:**



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





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

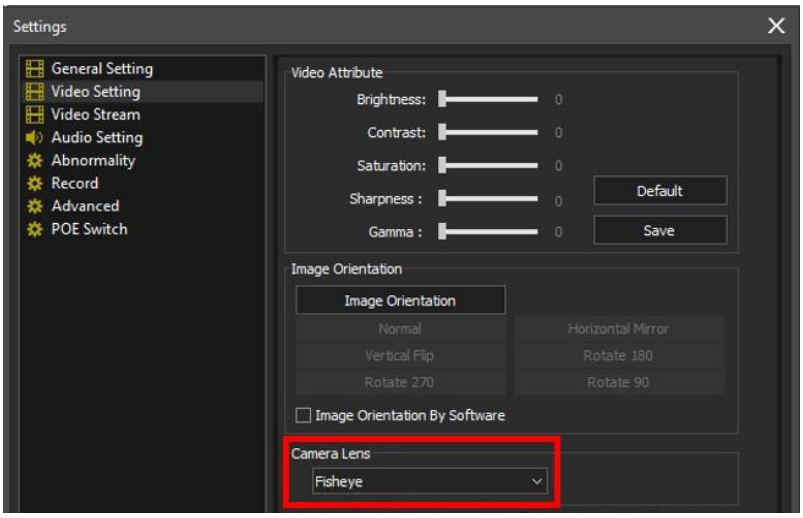
- **Frame Rate Control:** Limits the frame rate of the fisheye live view to a specified rate. Select **Apply All** to apply the frame rate to all fisheye views.

4. Drag the dewarped fisheye views from the Content List (No. 9 in *Main Screen* in Chapter 1) to live view grids for display. You can drag and drop the 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 GV-VMS. The camera should appear in the Content List (No. 9 in *Main Screen* in Chapter 1).
2. Select the camera lens type to dewarp the image.
   A. Click **Home** > **Toolbar** > **Configure** > **Camera Install**. The IP Device Setup dialog box appears. Then click the **Settings** button of the desired camera.
   B. For the camera installed with an ImmerVision IMV1 Panorama Lens, select **IMV1 Panomorph** using the Camera Lens dropdown list.
   C. For other third-party fisheye cameras, select **Fisheye** using the Camera Lens dropdown list.

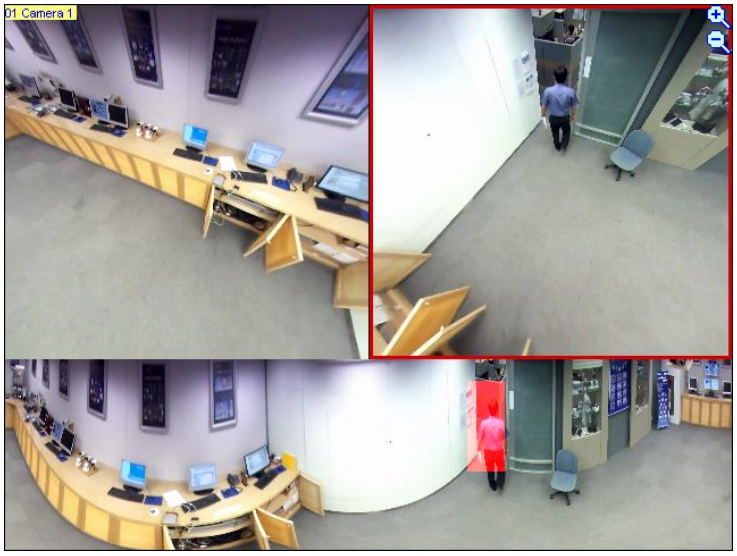


3. From the Content List, drag the fisheye camera (circular source image) or one of the dewarped fisheye images (e.g., Quad View) to the live view grid.
4. To access fisheye-related functions, follow Steps 2 to 4, *Setting up Fisheye View* earlier in this chapter.

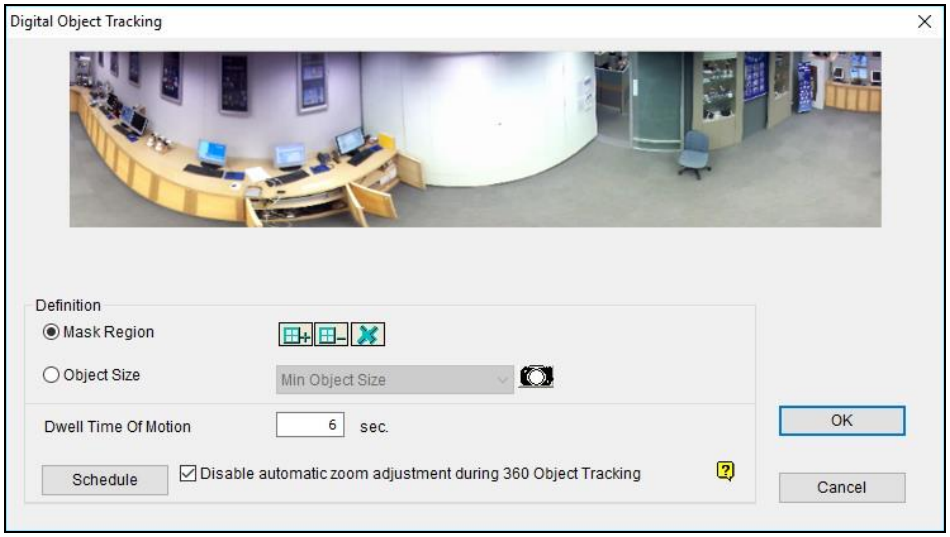
Note: Regardless of the view mode selected here, the hemispherical fisheye source image will be recorded. When playing back fisheye events in ViewLog, GV-VMS can convert the source image to different view modes according to your preference. To play back the events in fisheye view mode, select **ViewLog**, and in the Content List (No. 9 in *Main Screen* in Chapter 1), 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 Steps 1 to 3 in *Setting Up Fisheye View* earlier in this section 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.

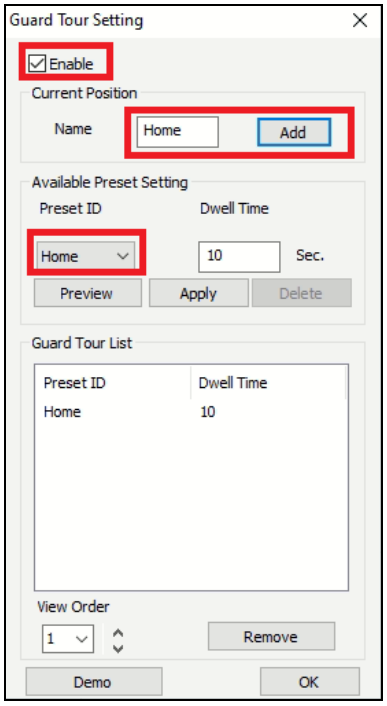
3. To enable object tracking, on the Fisheye Settings window, right-click the fisheye view, and then select **Fisheye** > **360 Object Tracking** > **Tracking**.

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 Step 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 (No. 9 in *Main Screen* in Chapter 1), and then select **Fisheye Settings**. The Fisheye Settings window appears.
3. Right-click the fisheye view on the window, and then select **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.

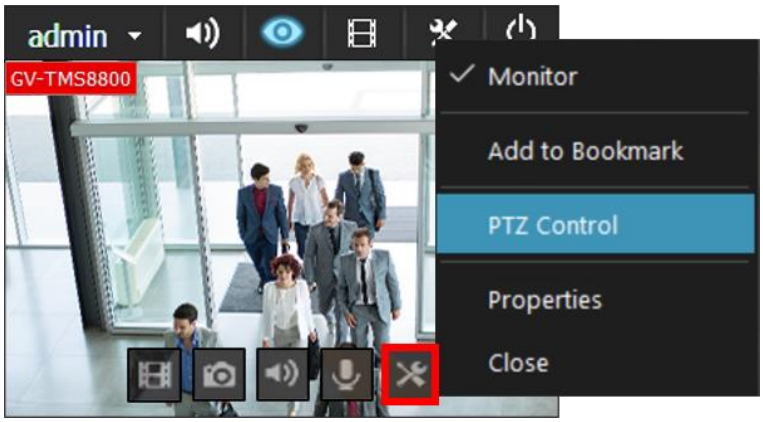


6. Specify the duration for the live view to stay on this preset point (dwell time). The default is **10** seconds.
7. Optionally click **Preview** to see a preview of the preset point.
8. Click **Apply**. This preset point is added to Guard Tour Setup.
9. To add more preset points, repeat the steps 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 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 the 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.

Tip: Alternatively, you can disable the PTZ functions of a PTZ camera by right-clicking it on the IP Device Setup page and selecting the **Disable PTZ Operation** option.



2.7.1 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 the 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 the amount of light in the environment.
- **Auto Go:** Allows you to enable Patrol, Auto Tracking, AutoPan, Sequence, and Cruise functions. Click **Stop Auto Function** to stop the currently running AutoPan, Sequence, or Cruise function.
- **Auto Set:** Allows you to set up AutoPan and Cruise functions. For details, see the following subsection *Auto Pan*.
- **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 to set a preset point, and then assign a preset point using a number or name.
- **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

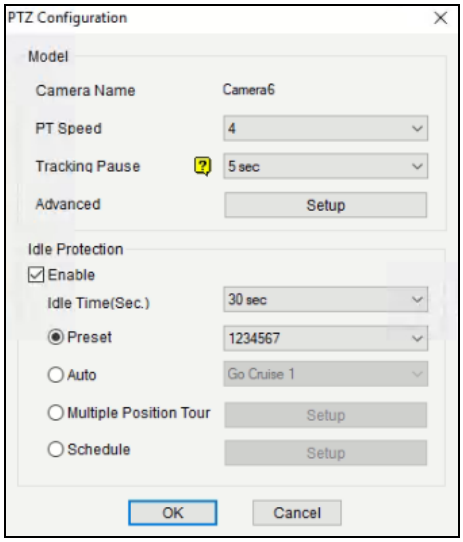
You can set up a route consisting of different directions, angles, and zooms for the PTZ camera to follow. Up to 4 Cruises can be created.

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**.

2.7.2 Setting Up Idle Protection and Advanced Functions

In the Content List under **Home** (No. 9 in *Main Screen* earlier in this chapter), right-click the PTZ camera and select **PTZ Setup**. This dialog box appears.



[Model]

- **PT Speed:** Adjust 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]

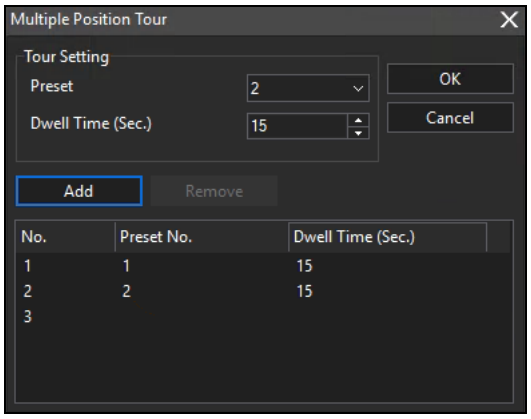
When the PTZ camera remains stationary for a certain period of time, the PTZ can automatically move to a Preset Point, enable an Auto function, begin a Multi Position Tour, or start a PTZ schedule.

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**, **Multiple Position Tour**, or **Schedule** as protection mode.
4. Click **OK**.

Setting Up 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.

2.8 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.

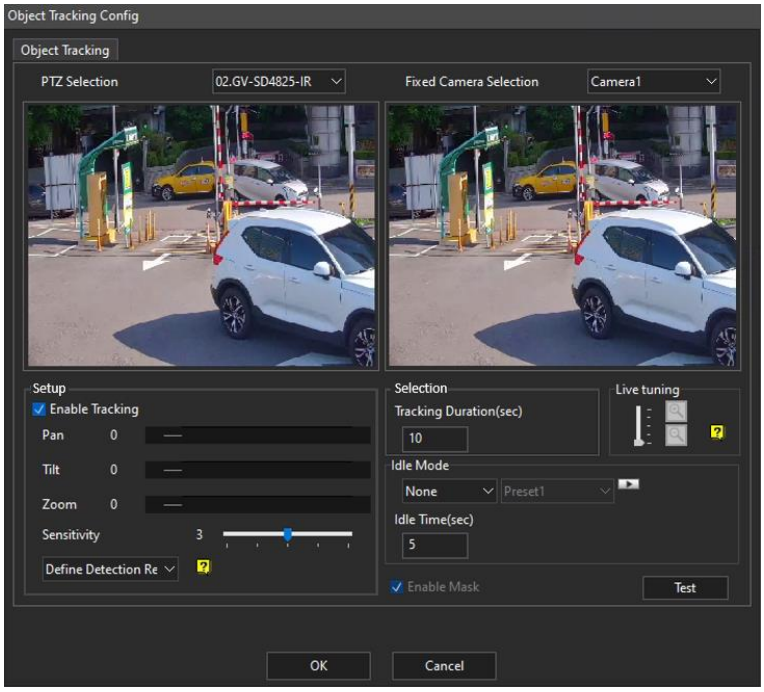
2.8.1 Dual Camera Tracking

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.

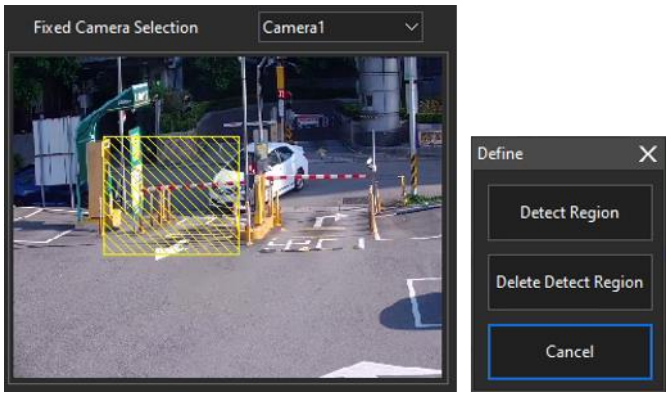
Note: The Dual Camera Tracking function is only supported by GV-PTZ010D, GV-QSD5730-Indoor / QSD5730-Outdoor / QSD5731-IR, GV-SD220 Series, GV-SD2722-IR / SD2723-IR / SD2733-IR / SD2300 / SD2301 / SD2411 / SD4825-IR / SD4834-IR.

---

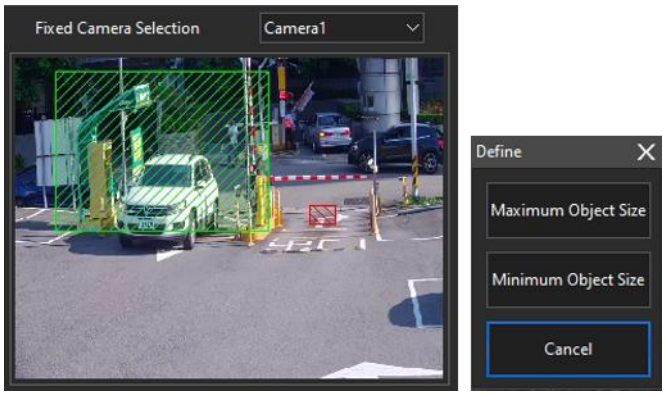
1. Click **Home** > **Toolbar** > **Configure** > **Object Tracking Setup**. The Object Tracking Config dialog box appears.
2. Select a **PTZ Camera** from the left dropdown list and a **Fixed Camera** from the right dropdown list.
3. Select **Enable Tracking** and start the settings.



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 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.

2.8.2 Single Camera Tracking

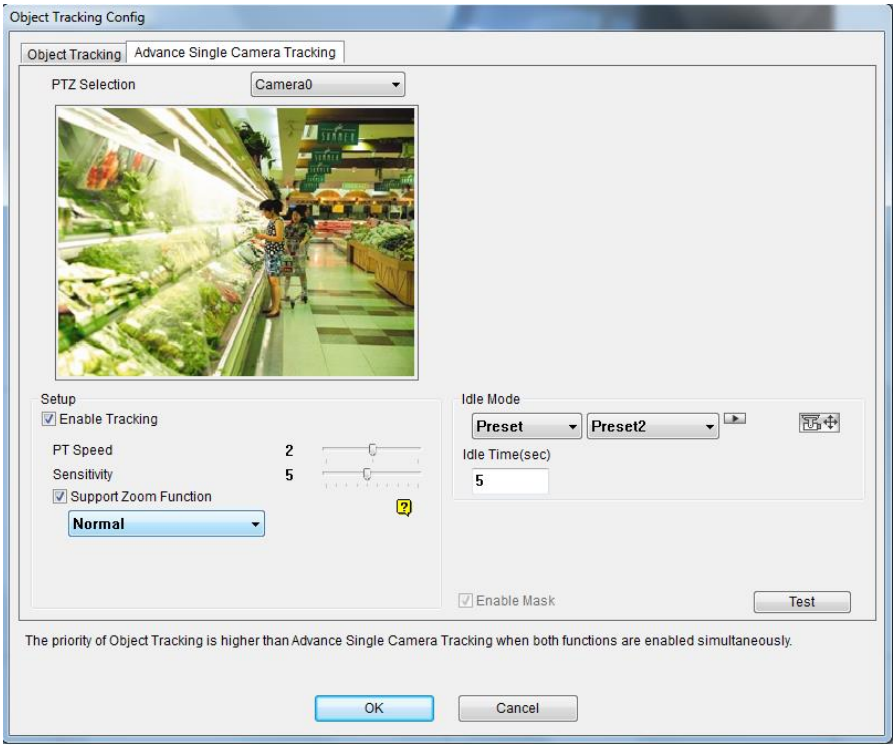
The Advanced Single Camera Tracking can track a moving object using only one PTZ camera. When an object moves within the view of the camera, the PTZ camera will follow its movement. When the object is out of view, the PTZ camera can be set to return to a designated position.

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* earlier in this chapter.

---

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**.

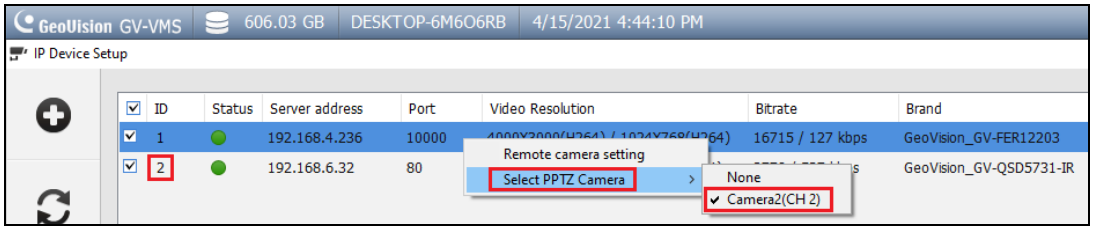
Tip: You can interrupt the PTZ camera tracking and take over the camera control by using PTZ Control Panel, PC's keyboard, and GV accessories such as GV-Keyboard, GV-IR Remote Control, and GV-Joystick. When the controlling device or panel is inactive for over 5 seconds, the PTZ camera will go back to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

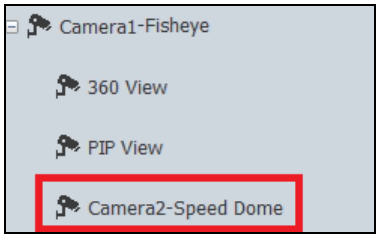
Note: When multiple objects are moving at the same time, the camera will track the object with the largest area.

2.9 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 (see the dialog box in *Adding IP Cameras* earlier in this chapter), 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 (No. 9 in *Main Screen* in Chapter 1).



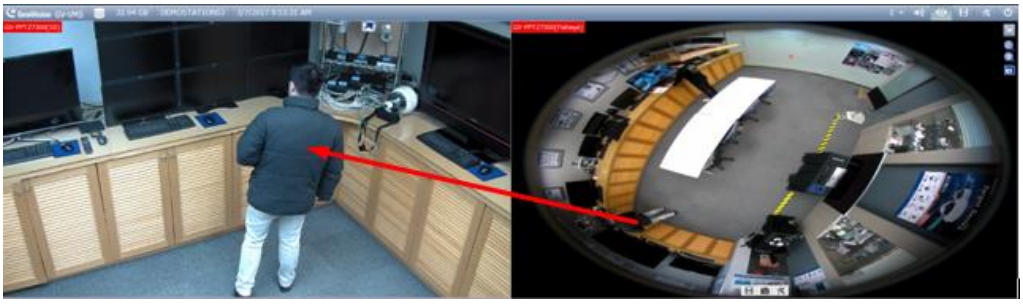


Note:

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.

2.9.1 Accessing the Live View

To access the live view of GV-Panoramic PTZ Camera, drag both the fisheye camera channel and speed dome channel in the Content List (No. 9 in *Main Screen* in Chapter 1) to the live view grid. Click on the fisheye live view, and the camera will turn toward the selected location.

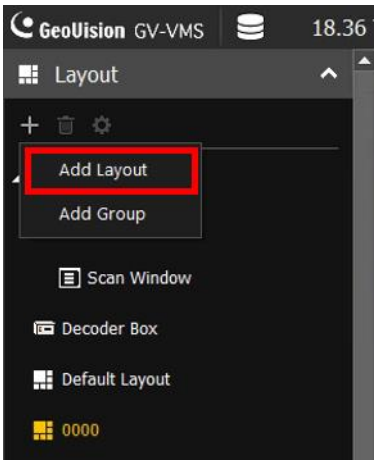


2.9.2 Automatic Object Tracking

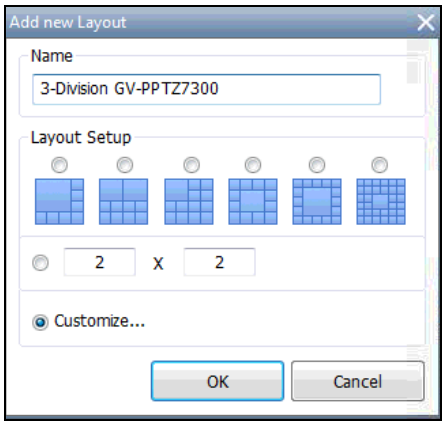
The PPTZ Automatic Object Tracking function only works in a 3-division live view. Follow the steps to create the 3-division live view and to enable the PPTZ Object Tracking in the 360 View.



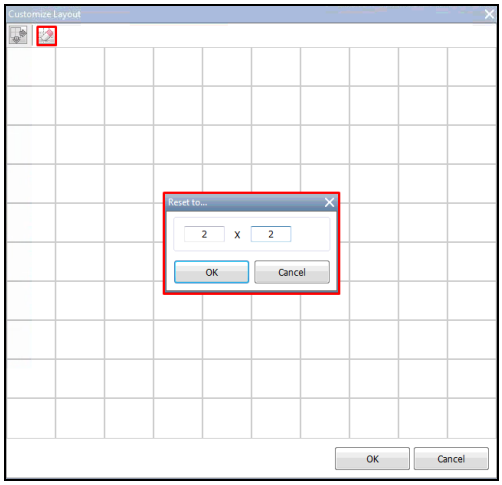
1. In the Content List (No. 9 in *Main Screen* in Chapter 1), click **Layout**.
2. Under **Layout**, click **Add** , and select **Add Layout**.



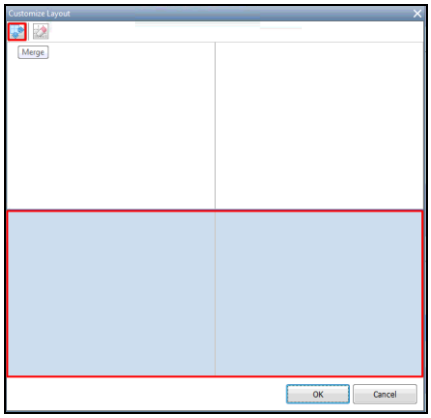
3. Type the name of the layout under **Name**, select **Customize**, and click **OK**.



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

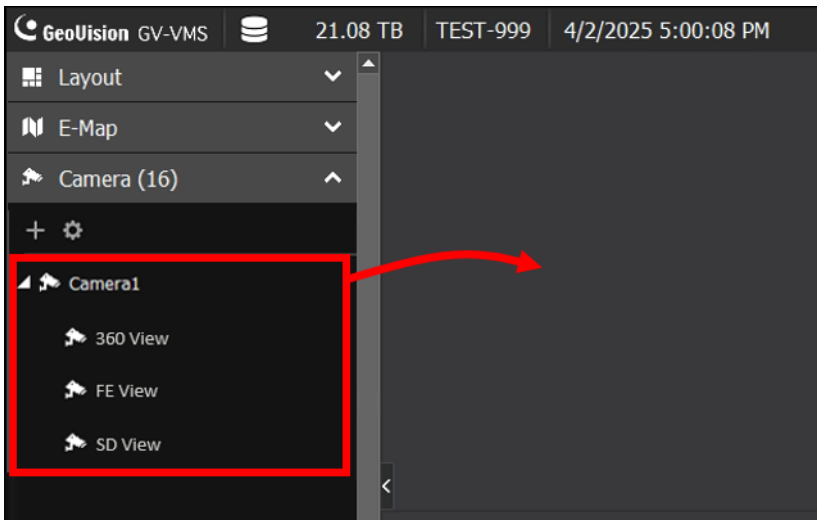


5. Select the 2 grids at the bottom, click **Merge** , and click **OK** to merge the grids.



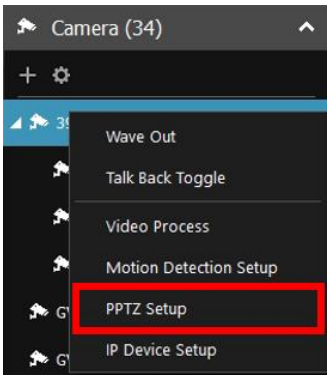
6. When the message “Do you want to assign the cameras to this layout automatically” appears, click **No** to assign the camera channels manually instead.

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.

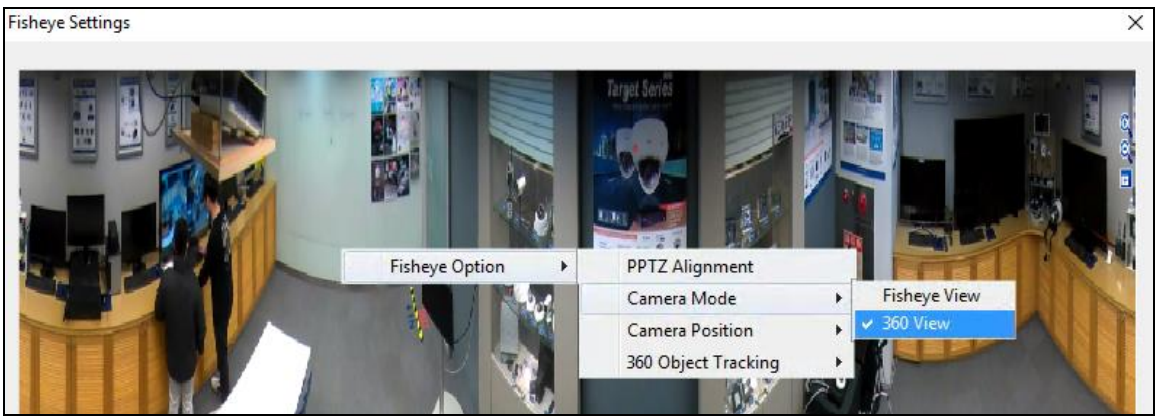


After creating the 3-division live view, go through the steps below to enable the object tracking options.

8. In the Content List, right-click the GV-PPTZ camera or the paired fisheye camera, and select **PPTZ Setup**. The Fisheye Settings dialog box appears.

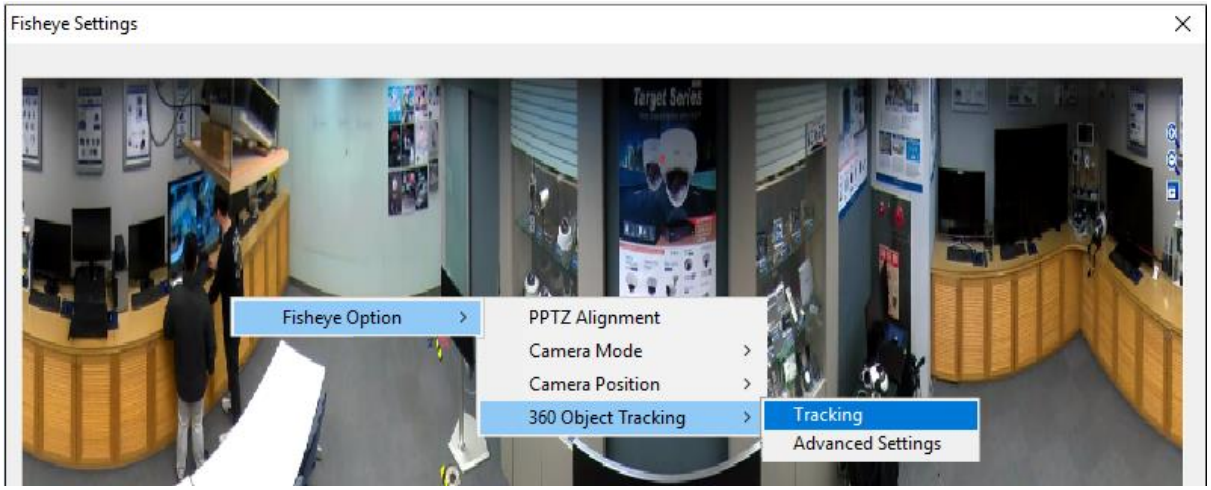


9. Right-click on the Fisheye Settings dialog box, and select **Fisheye Option** > **Camera Mode** > **360 View**.



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

11. Select **360 Object Tracking** > **Tracking** to enable the object tracking.



Chapter 3

Video Analysis..... 142

3.1 Privacy Mask Protection 142

3.1.1 Setting Up a Privacy Mask 142

3.1.2 Granting Access Privileges to Recoverable Areas 144

3.2 Advanced Scene Change Detection 145

3.3 Text Overlay 147

3.4 Face Recognition 149

3.4.1 Enrolling Face Data 150

3.4.2 Setting Up Face Groups 153

3.4.3 Synchronizing Face Databases 154

3.4.4 Defining Access Schedule 155

3.4.5 Setting Up Recognition Alerts 158

3.4.6 Backing Up Face Database 159

3.4.7 Face ID – Live Recognition Profiles 160

3.4.8 Viewing and Searching for Face Recognition Events 160

3.4.9 Tracking Recognized Faces 161

3.4.10 Integrating Face Recognition to Access Control 164

3.4.11 Batch Enrolling Faces and Access Cards 168

3.5 Local Face Recognition 172

3.6 Video Analysis by Camera 175

3.6.1 Setting Up Video Analysis by Camera 175

3.6.2 Setting Up Custom Keywords for 3rd-Party Events 178

CHAPTER

3

Video Analysis

3.1 Privacy Mask Protection

The Privacy Mask can conceal sensitive areas from view, including both live view and recorded videos. This feature is ideal for locations with displays, keyboard sequences (e.g., passwords), and other areas where sensitive information should not be visible.

You can also retrieve the blocked-out areas during playback. Passwords will be used to access the retrievable areas.

3.1.1 Setting Up a Privacy Mask

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**. The Setup dialog box appears.
2. From the Video Analysis dropdown list, select **Privacy Mask Setup**, select the desired cameras, and click **Setting**. This dialog box appears.



3. Select a camera.
4. Select Unrecoverable or Recoverable.
   - **Unrecoverable:** The blocked-out areas cannot be retrieved in recorded videos.
   - **Recoverable:** The blocked-out areas can be retrieved with password protection.
5. To add a mosaic privacy mask of Unrecoverable or Recoverable selected, click the **+** button, and drag it to the desired position on the camera view, and resize the mask area. The Unrecoverable mask is marked in black, while the recoverable mask is shown in brown.
6. To adjust the blur intensity, select **ROI Apply Mosaic** and move the slider. The higher the level, the less the mosaic blur.



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

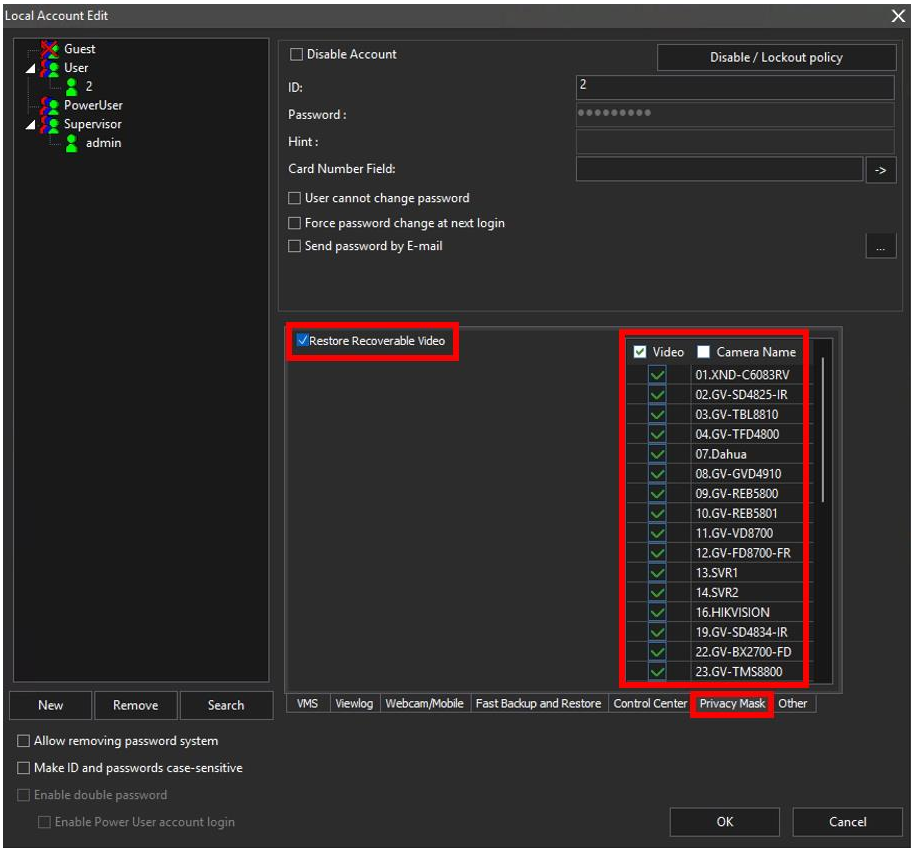
Note:

1. Up to 10 Privacy Mask areas can be configured for a camera channel, and each area can be set as a polygon with up to 50 edges.
2. Optionally create a schedule for Privacy Mask to be enabled only at the time periods specified. For details, see *Creating a Schedule with Setup Wizard* in Chapter 1.

3.1.2 Granting Access Privileges to Recoverable Areas

By default, only a Supervisor account has access to 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 a Power User or User account, click the **Privacy Mask** tab, select **Restore Recoverable Video**, and select the camera to grant the privilege to the Power User or User.

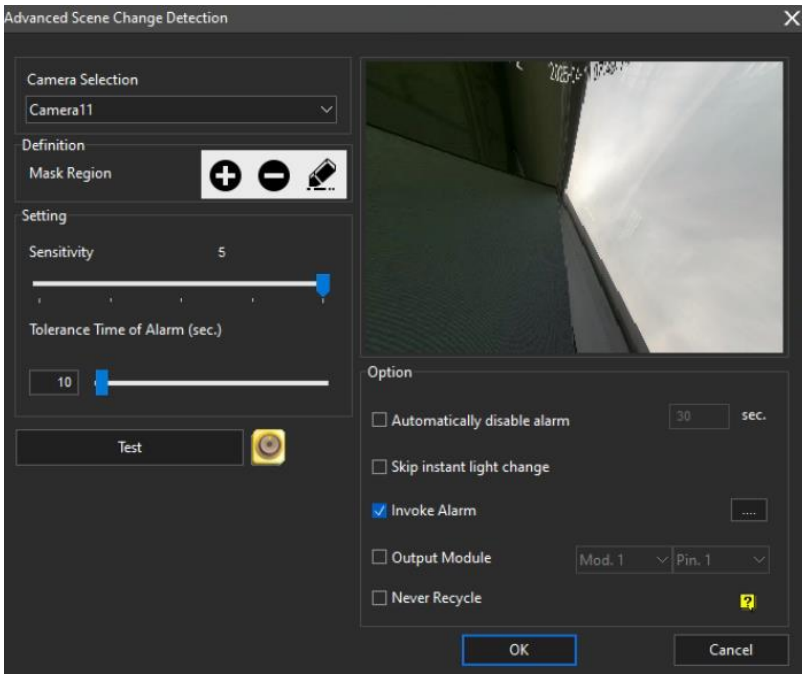


Note: If you open the event files (*.avi) directly from local drives, the valid ID and password are also required to access the blocked-out areas. For details on retrieving the blocked-out areas in the exported files, see *Merging and Exporting Video* in Chapter 4.

3.2 Advanced Scene Change Detection

The Advanced Scene Change Detection detects malicious changes to the scene, viewing angle, or focus clearness in both indoor and outdoor contexts.

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**. The Setup dialog box appears.
2. From the Video Analysis dropdown list, select **Advanced Scene Change Detection**, select the desired cameras, and click **Setting**. This dialog box appears.



3. Select a camera from the Camera Selection dropdown list, and configure these settings:
   - **Mask Region:** Masks off the area of the camera view where scene change detection will not be applied.
   - **Sensitivity:** Adjusts detection sensitivity. The higher the value, the more sensitive the system is to 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 the sound alarm, and the output module after a given duration. Note that disabling alerts does not disable alert settings or ongoing detection.

- **Skip Instant Light Change:** Ignores sudden illumination changes to minimize false alarms. For example, light switches can create rapid shifts in illumination. With this option enabled, the system will ignore significant illumination changes without generating an alarm and continue to monitor. See the **Note** below for potential risk.
- **Invoke Alarm:** Enables the computer alarm when a scene change is detected. Click the **[…]** button next to the option to assign a .wav sound file.
- **Output Module:** Activates the output device when a scene change is detected. Select this option and assign an installed output module and a pin number.
- **Never Recycle:** Prevents the system from recycling scene change event files once the recycle threshold is reached.

4. Click **Test** to verify your settings. If no scene change is detected, increase the **Sensitivity** value to make the system more sensitive 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 is highlighted in live view, the selected alarm or output is activated, and the event is 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, the system will not generate an alarm if the camera's lens is covered by malice.
   - This option is not recommended for infrared cameras.
2. To create schedules for Advanced Scene Change, see *Creating a Schedule with Setup Wizard* in Chapter 1.

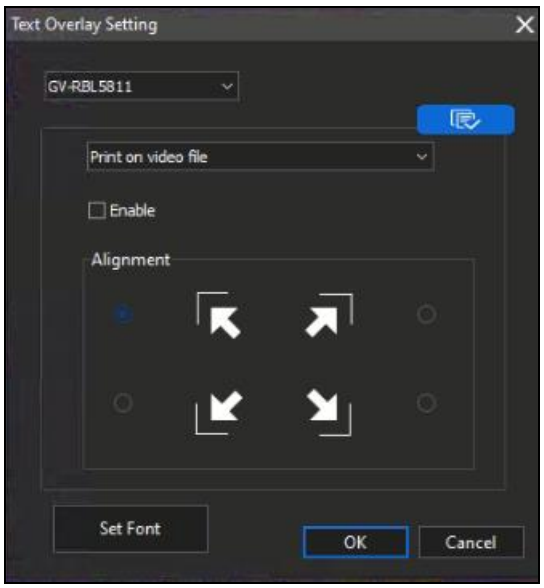
To manually stop all triggered alerts, click the **Tools** button  on the triggered channel, select **Reset Alert** > **Advanced Scene Change Detection**.

- **Reset Alert:** Disables and resets the triggered alarm. If the scene change remains over the preset tolerance time, the system will continue to identify it as a scene change and generate an alarm.

3.3 Text Overlay

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

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**. The Setup dialog box appears.
2. From the Video Analysis dropdown list, select **Text Overlay Setting**, select the desired cameras, and click **Setting**. This dialog box appears.



3. Select a camera.
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* in Chapter 5 in the *GV-ASManager User's Manual*.

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 > **Record**, and locate the Recording codec format.

- **Alignment:** Customize where camera information appears on a camera view.
- **Set Font:** Customize the font, font size, font style, and other settings.

3.4 Face Recognition

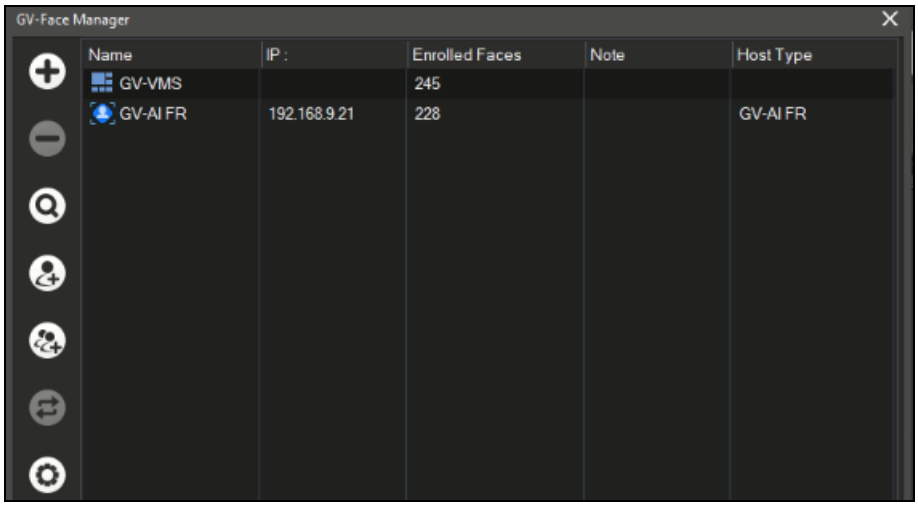
Face Recognition integrates the facial recognition capabilities of the following cameras and software, enabling the GV-VMS system to identify detected human faces:

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

These recognition events can be configured to trigger actions, such as running the desired applications, based on the recognition of designated face groups or unidentified individuals.

Note: For a detailed introduction to GV-VMS's local face recognition, see *Local Face Recognition* later in this chapter.

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



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

3.4.1 Enrolling Face Data

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

1. **GV-Face Recognition Camera**: GV-VD8700 and GV-FD8700-FR
2. **GV-AI FR software**
3. **GV-AI Server software**
4. **Local GV-VMS**

There are two methods to enroll faces:

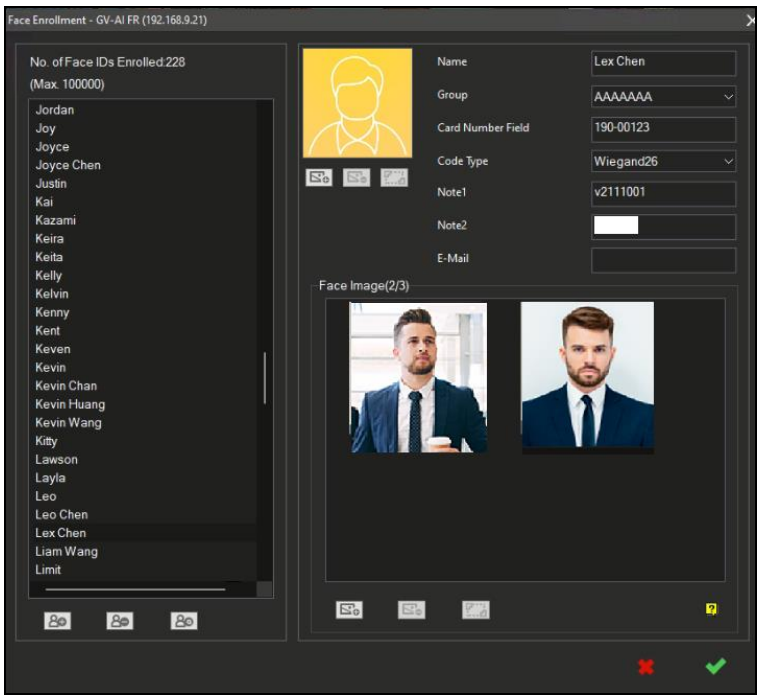
1. Enroll faces by adding portrait photos directly into the database of the connected cameras, GV-AI FR, GV-AI Server, or local GV-VMS. See the steps below.
2. Synchronize face data from other connected cameras, GV-AI FR, or GV-AI Server. See *Synchronizing Face Databases* later in this section.

IMPORTANT:

1. GV-VMS directly accesses and manages the face databases of GV-Face Recognition Camera, GV-AI FR, and GV-AI Server, meaning all changes are being made 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, follow the steps below:

1. Select a host 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 or snapshots for the Face ID selected from your local PC. Optionally crop the image added by selecting it and click **Crop Image** .
4. Configure the following options for the selected Face ID. The available options differ based on the selected host at Step 1:
   - **Name:** Name the Face ID.
   - **Group:** Select a group to categorize the Face ID. This setting can be used to trigger an alert response, such as running the desired applications, when persons from a specified group are recognized. See *Setting Up Face Groups* later in this section.
   - **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 section.
   - **Access Schedule:** Select a predefined schedule during 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 section.
5. Click **OK**.

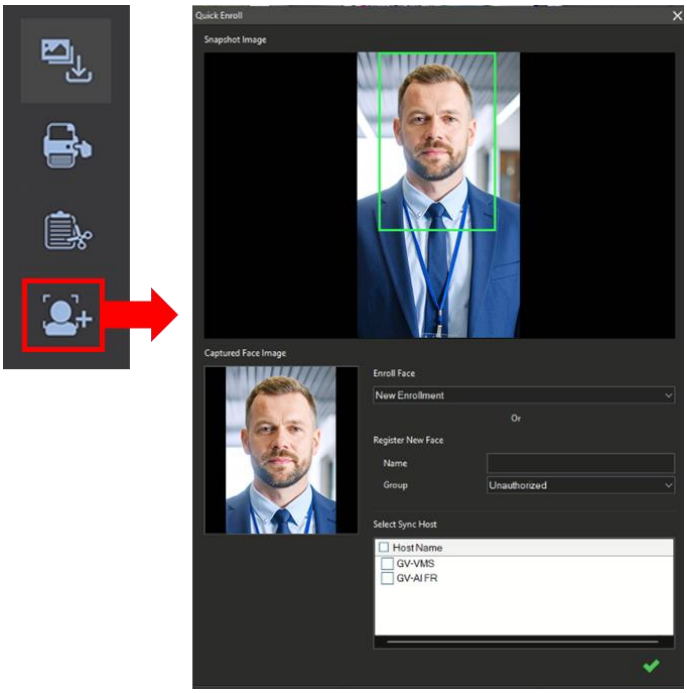
Note:

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

Enrolling Faces from Live View / ViewLog

Alternative to enrolling face data with photos, you can enroll with face images captured by any cameras connected to GV-VMS.

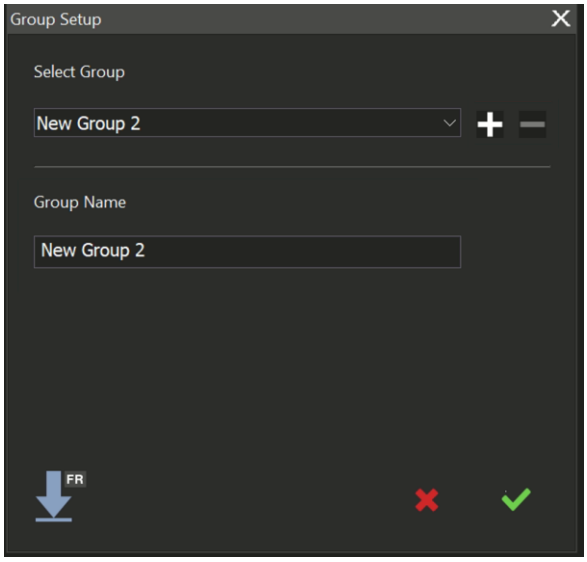
1. In Live View / ViewLog, click **Snapshot** at the bottom of a channel and select **Face Enroll** and click to confirm the image. The Quick Enroll window appears.



2. Click and drag on the image to highlight the face you want to enroll as a **snapshot**.
3. Select **New Enrollment**, type a name under **Register New Face** to create a new Face ID, and select a **Face Group** to add it to. Otherwise, select an existing one to add the face image to.
4. Select a host for the face enrollment under **Select Sync Host**.
5. Click to save the settings.

3.4.2 Setting Up Face Groups

To add or edit the face groups of a host (GV-Face Recognition Camera / GV-AI FR / GV-AI Server / local GV-VMS) , select a host on Face Manager and click **Group Setup** .



1. Click **Add Group** .
2. To edit the name of a face group, select the group from the Select Group dropdown list and modify its name under Group Name.
3. To import face groups from a connected GV-Face Recognition Camera / GV-AI FR / GV-AI Server, click **Import Group Settings** and select the desired host.

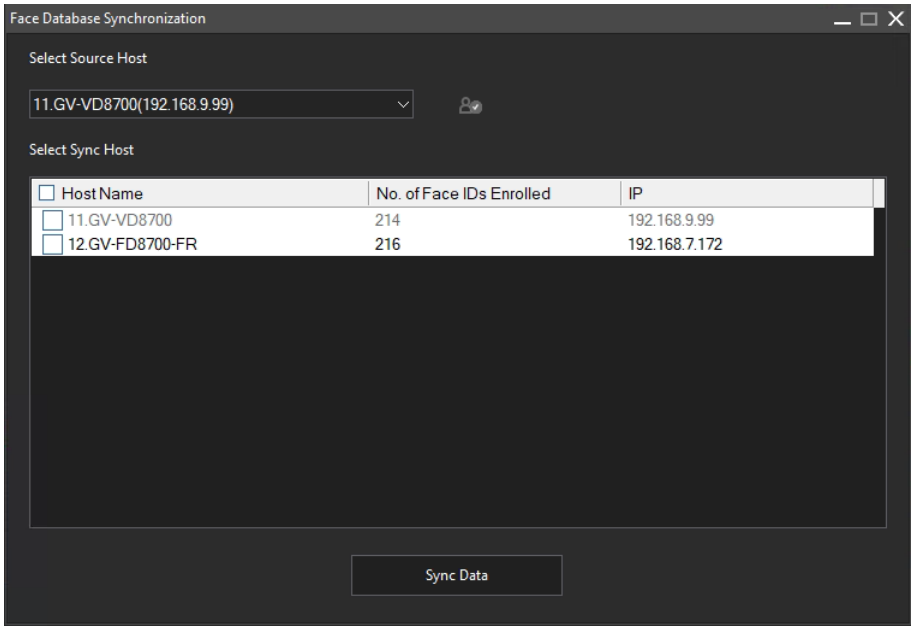
Note: The **Delete Group** function is not supported if Face Manager contains any GV-VD8700 (GV-Face Recognition Camera).

3.4.3 Synchronizing Face Databases

To synchronize the face databases across multiple GV-Face Recognition Cameras, GV-AI FRs, or GV-AI Servers, click **Face Database Synchronization** on **Face Manager**.

Note:

1. The database synchronization is not supported by GV-VMS's local face recognition.
2. GV-Face Recognition Cameras, GV-AI FRs, and GV-AI Servers each utilize an independent database. You cannot synchronize face databases between different types of systems (e.g., synchronizing a GV-Face Recognition Camera database with a GV-AI FR database).



- **Select Source Host:** Select the host you want to synchronize from.
- **Select Sync Faces** : Click the button to select Face IDs that you want to synchronize with.
- **Select Sync Host:** Select the hosts that you want to be synchronized with.
- **Sync Data:** Click to start synchronizing.

3.4.4 Defining Access Schedule

Access Schedules are used to specify the time periods in which specific persons (Face ID) are allowed or denied access from Monday to Sunday. Whenever a person is recognized outside of their allowed schedule, a schedule alert is recorded, which can be used to run the desired applications.

Note: The Access Schedule is not supported by GV-VMS's local facial recognition.

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**

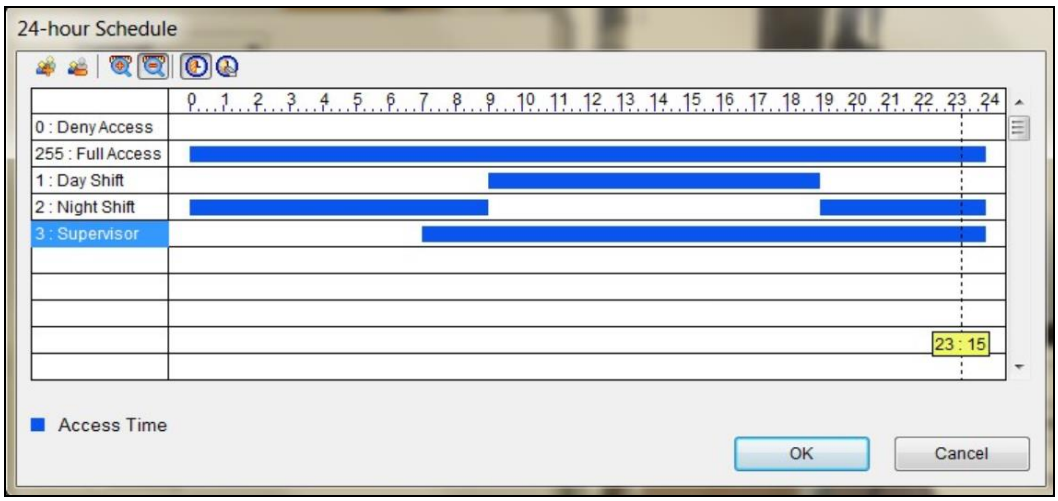
  Define the days a person is allowed / denied access of in a week.

- **Step 3 Assigning Weekly Schedules**

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

Step 1: Setting 24-Hour Schedules

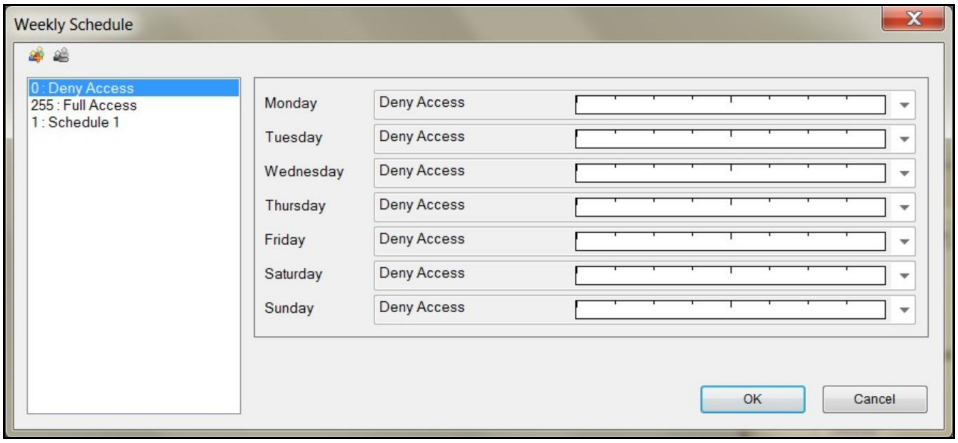
Before creating weekly schedules, you need to first define a number of desired 24-hour schedules that can be used to prepare the weekly schedules. On **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Settings** and select **24-hour Schedule**. In this window, up to 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.

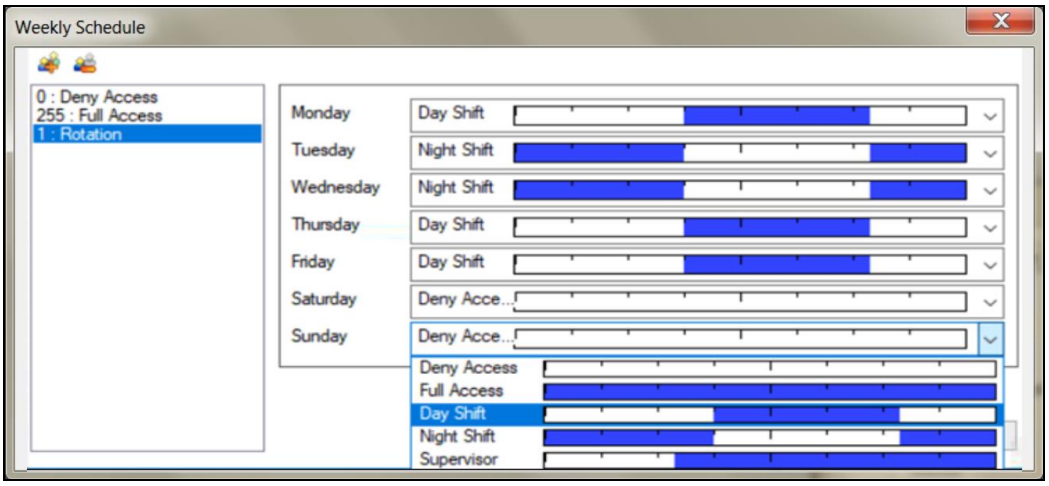
Step 2: Setting Weekly Schedules

Once the desired 24-hour schedules are set, click **Settings** 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**.

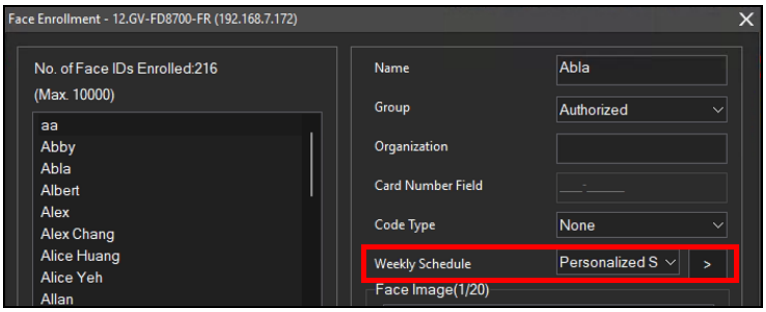
2. Select the desired schedules for **Monday** to **Sunday**, predefined from *Step 1* earlier in this section, in each of the respective dropdown lists, as exemplified below.



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.

Step 3: Assigning Weekly Schedules

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



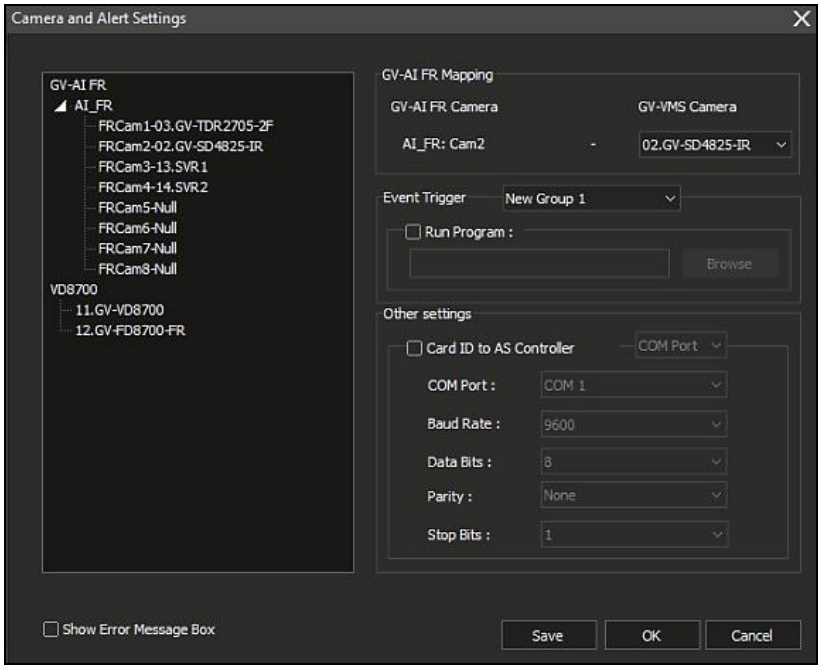
Once the Weekly Schedules are assigned, turn on monitoring of the camera channel to start access monitoring based on the schedules.

3.4.5 Setting Up Recognition Alerts

In this section, you can use Schedule Alerts, Unknown Alerts, or the Recognition Events of a specified group, e.g., Unauthorized, to run the desired applications.

Note: The recognition alerts feature is not supported by GV-VMS's local face recognition. For a detailed introduction to GV-VMS's local facial recognition, see *Local Face Recognition* later in this chapter.

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



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

- **Event Trigger:** Select Schedule Alert, Unknown Alert, or the Group of Face ID that the alerts or alarms set should be triggered for. For details on using Schedule Alerts, see *Defining Access Schedule* earlier in this section.
  - ⊙ **Run Program:** Click **Browse** to select a desired program to be executed upon trigger.

3.4.6 Backing Up Face Database

To back up the face database of a GV-Face Recognition Camera, GV-AI FR, GV-AI Server, or local GV-VMS:

1. Click **Settings** on **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**)
2. Select **Export Backup Data From…** and select the desired host. The database is saved on your local PC as a **.fdb* file.

To import a face database into a GV-Face Recognition Camera, GV-AI FR, GV-AI Server, or local GV-VMS:

1. Click **Settings** on **Face Manager**.
2. Select **Import Backup Data To…** and select the desired host.

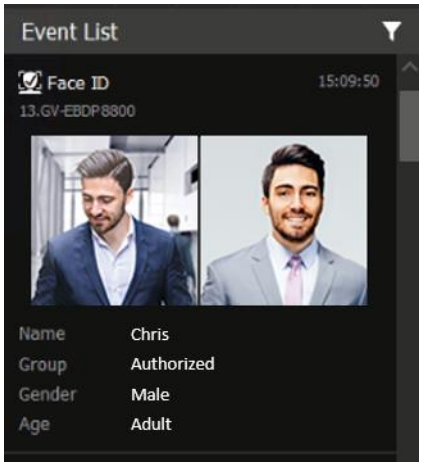
IMPORTANT: When a face database is imported into a host, it replaces all the original face data it contains.

3.4.7 Face ID – Live Recognition Profiles

The Event List allows users to view the simplified info of live face recognition events

Note: This feature is available only when at least one Face Recognition (FR) channel is actively recording.

To access Face ID data, click the **Filter** icon at the top of the Event List, select **Face ID**, and optionally select a specific **Face Group** or select **Show All** to view all entries.

	When a face recognition event occurs, you can view live recognition details including the person's captured and enrolled faces, name, face group, gender, age group, camera channel, and the time of recognition.

3.4.8 Viewing and Searching for Face Recognition Events

You can search for recognition events using a face image from recorded footage or by uploading an image from your PC. For details, see *Searching by Face Data* in *Performing an AI Query* in Chapter 4.

3.4.9 Tracking Recognized Faces

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

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

To display Face Tracking, complete the following settings:

- **Step 1 Synchronize Face Databases**

  To synchronize face databases, see *Synchronizing Face Databases* earlier in this section.

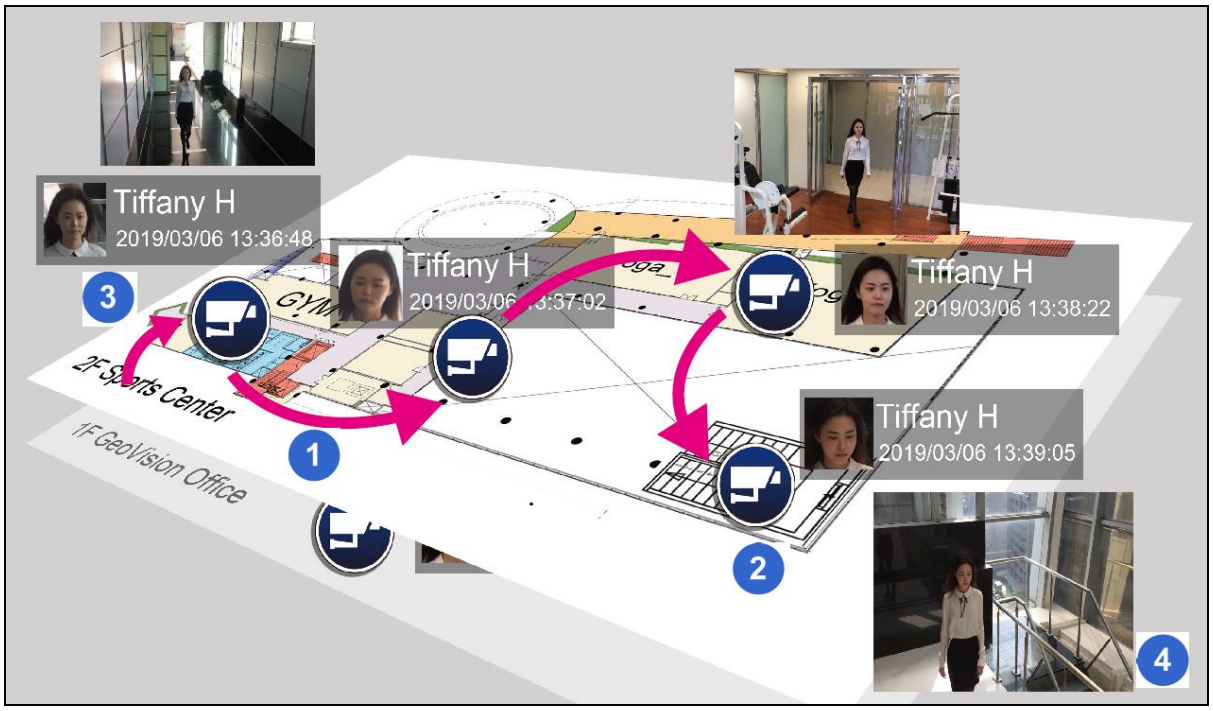
- **Step 2 Create an E-Map**

  To create an E-Map and add cameras, see *Creating E-Map* in Chapter 8.

- **Step 3 Enable Monitoring and Viewing**

  Enable monitoring for all GV-Face Recognition Camera, GV-AI FR, GV-AI Server, or Local FR channels where faces may be tracked. Then, drag the E-map from the Content List to the live view screen.

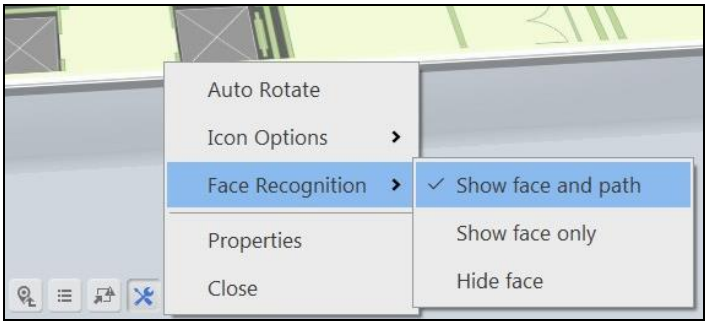
Once all the settings are properly configured, arrows will appear on the E-Map to indicate the movement paths of recognized individuals.



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

Adjusting the Display Mode on the E-Map

To adjust how recognition events and tracking paths are displayed on the E-Map, click **Tools** and select **Face Recognition** to access the following options:

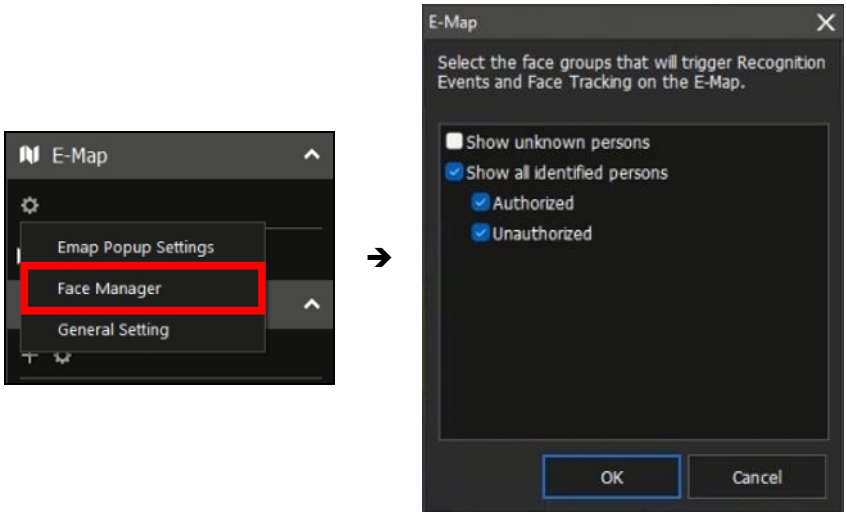


- **Show face and path:** Selected by default, displays both Recognition Events and Face Tracking on the E-Map.
- **Show face only:** Displays only Recognition Events on the E-Map.
- **Hide face:** Hides all Recognition Events and Face Tracking from the E-Map.

Selecting Face Groups for E-Map Events

To specify which Face Groups will trigger Recognition Events and Face Tracking on the E-Map, follow the steps below.

1. In the Content List of Live view, click **E-Map** > **Configure** > **Face Manager**. This window appears.

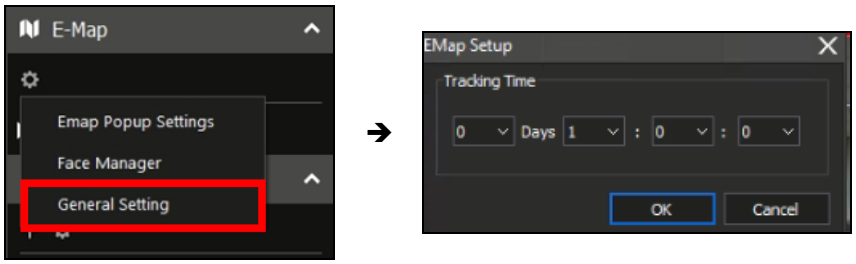


2. Select the face groups that will trigger Recognition Events and Face Tracking on the E-Map. For details on configuring Face Groups, see *Setting Up Face Groups* earlier in this chapter.
3. Click **OK** to save the settings.

Configuring Face Tracking

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

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



2. Under **Tracking Time**, set the duration for which Face Tracking remains effective by selecting days (0~31), hours (0~23), minutes (0~59), and seconds (0~59). Face Tracking will not be displayed for any subsequent Recognition Events occurring beyond the set Tracking Time.
3. Click **OK** to save the settings.

3.4.10 Integrating Face Recognition to Access Control

GV-VMS extends the face recognition feature of connected cameras by converting recognized faces into access card data for access control management. Before the integration, ensure the required controllers 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*.

Note: The access control integration is not supported by GV-VMS's local face recognition.

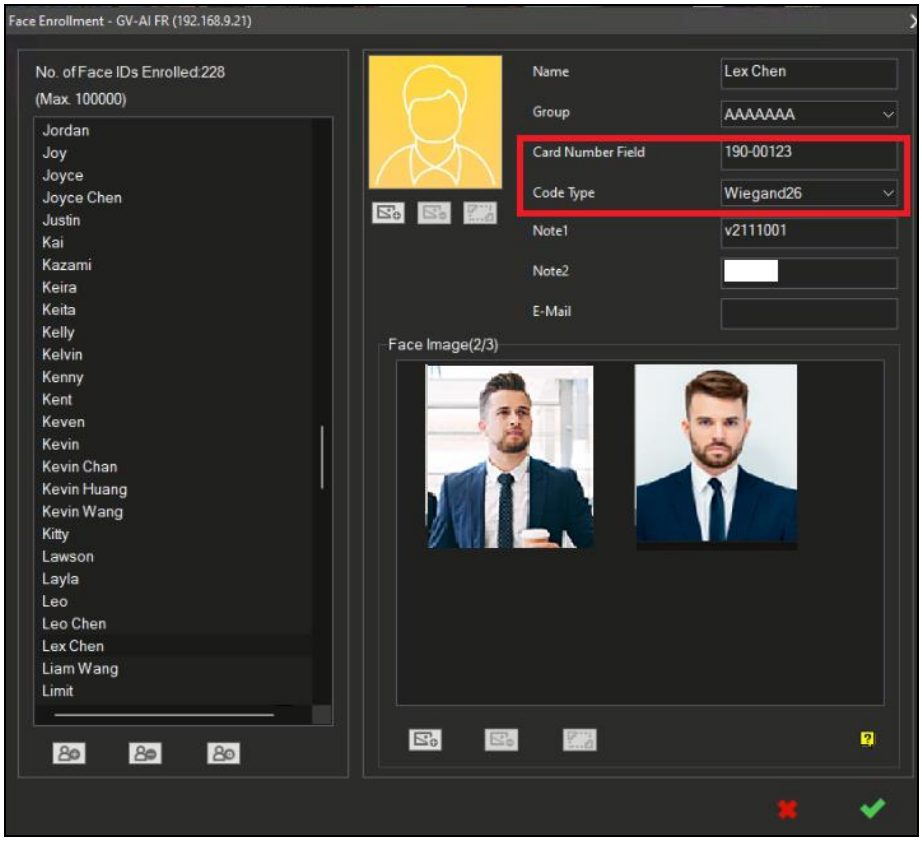
Pairing Face IDs with Access Cards

Face IDs of GV-Face Recognition Cameras / GV-AI FRs / GV-AI Servers can be paired with GeoVision access cards, key fobs, or 3rd-party smart cards for access control management through 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.



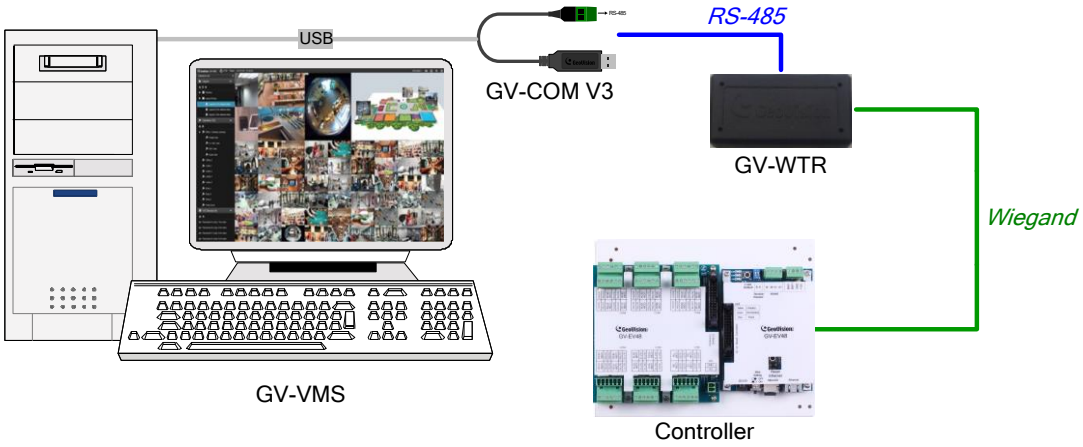
3. Click ✔ to save.

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

Connecting Controller

For GV-VMS to send the paired card number to the controller upon face recognition, the controller must be properly connected using one of the following two methods:

- **COM Port**



1. Connect GV-COM V3 to a USB port of the PC running GV-VMS.
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**

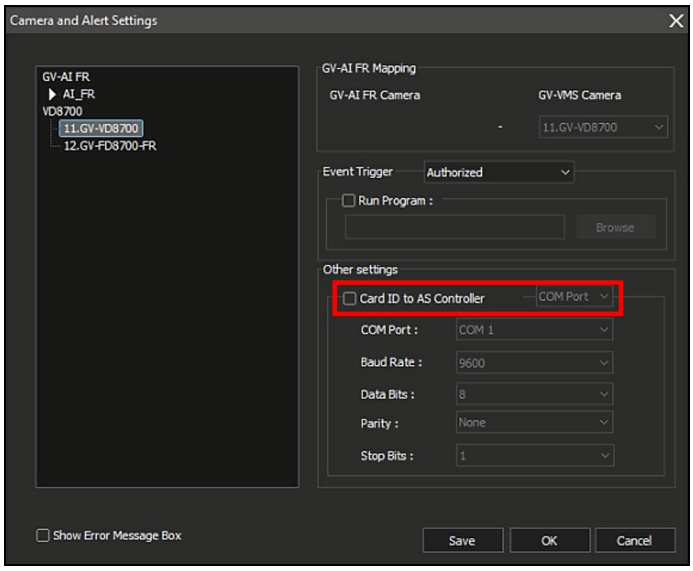
Connect the controller to the same network as your GV-VMS.

Sending Card Number to Controller by Face ID

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

1. In **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), click **Settings** and select **Camera and Alert Settings**.

2. Select the desired camera and enable **Card ID to AS Controller**. Then configure the necessary settings based on the type of connection used.



[COM Port]

- **COM Port:** Verify the COM port number of GV-COM V3 connected to the GV-VMS in **Windows Device Manager** and select the corresponding port. 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 on the same LAN as GV-VMS.

3.4.11 Batch Enrolling Faces and Access Cards

The batch enrolling feature of **GV-Face Manager** allows users to import large quantities of face photos and access card data to a connected host at all once.

Supported hosts include: GV-Face Recognition Camera, GV-AI FR, GV-AI Servers, Local GV-VMS.

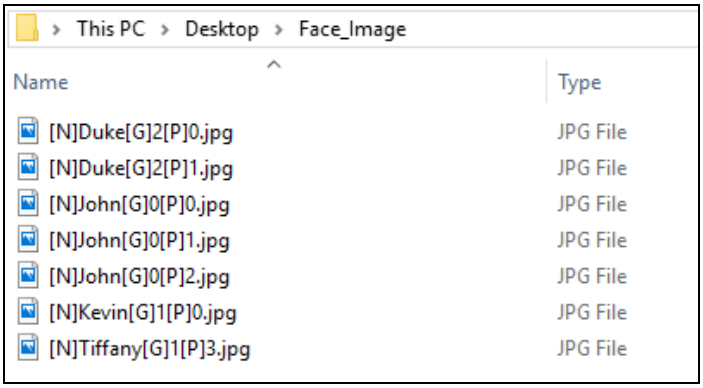
Batch Enrolling Faces Only

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

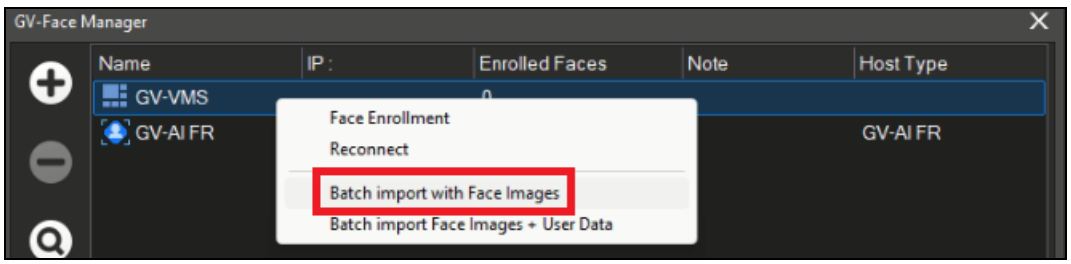
[N]<Face ID Name>[G]<Group No. – 1>[P]<Image No. – 1>.jpg

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 face images are properly named and saved in the same folder, right-click the target host in **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**) and select **Batch import from Face Images** to locate and choose 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

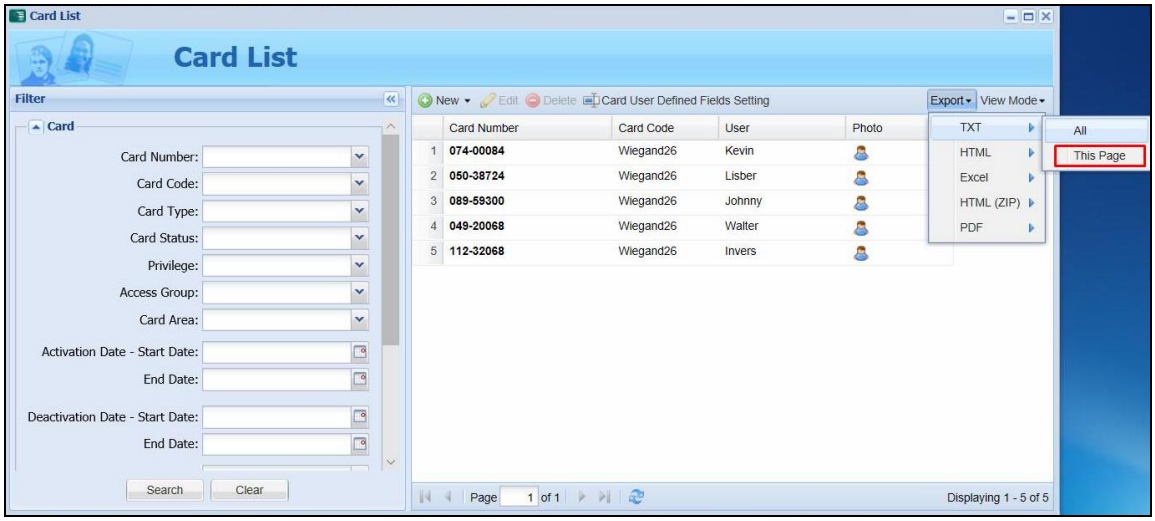
To enroll access card data along with multiple face photos from GV-ASManager to a connected host, follow the steps below:

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

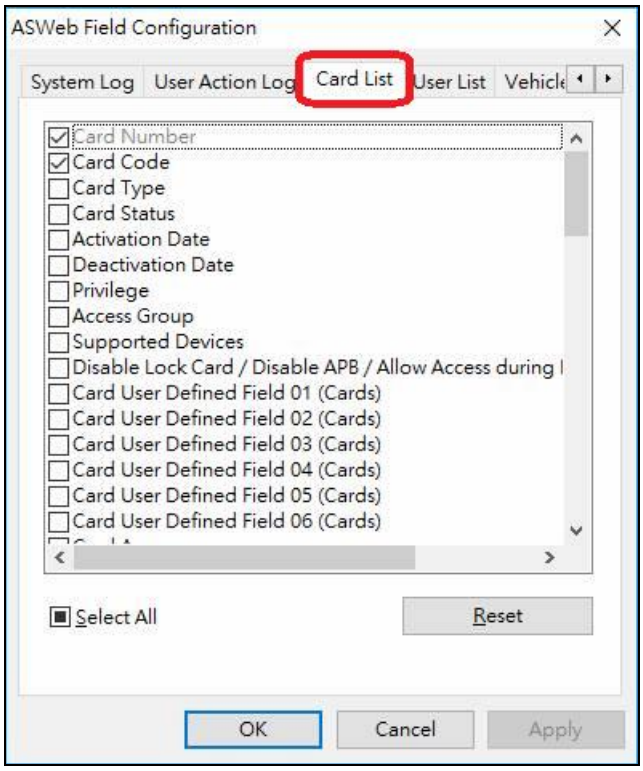
A. The **Display Names** of users on GV-ASManager, which are used as **Face ID names**, must not contain any spaces.

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

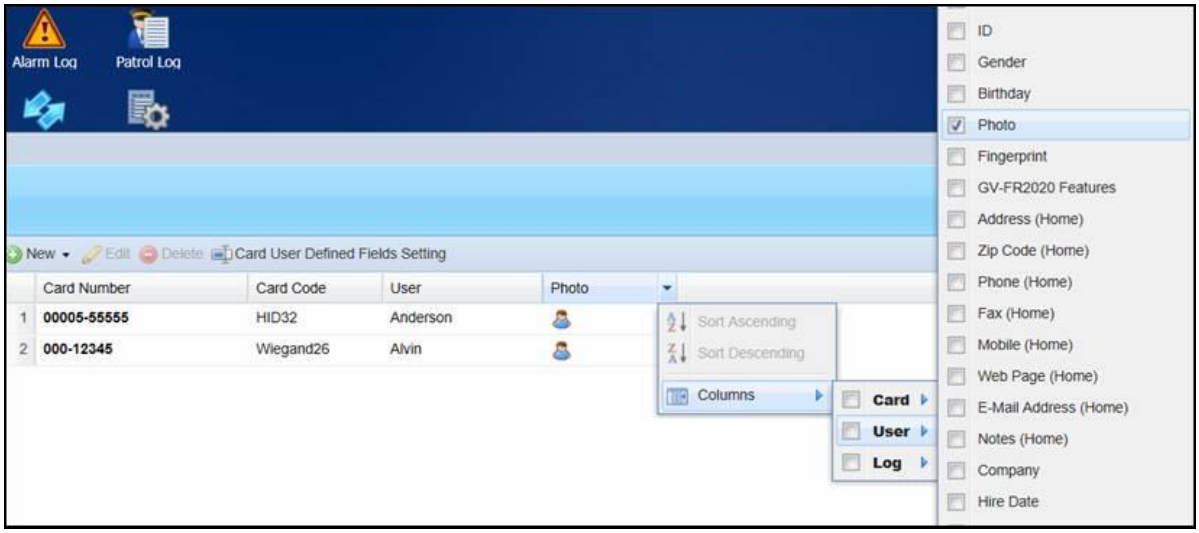
1. From the **Card List**  of GV-ASWeb, ensure the required card data are presented—**Card Number**, **Card Code**, **User**, and **Photo**. Then, click **Export** and select **TXT** > **This Page**.



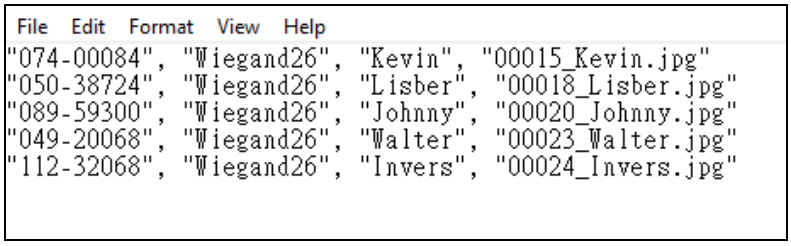
A. For the Card List to contain the required data, open **ASWeb Field Configuration** (under **Tools** in GV-ASManager), click the **Card List** tab, and select **Card Number**, **Card Code**, **User** and **Photo**.



B. In the **Card List**, configure the display to show the fields **Card Number**, **Card Code**, **User**, and **Photo**. To do this, click a column's arrow button and deselect all other fields.

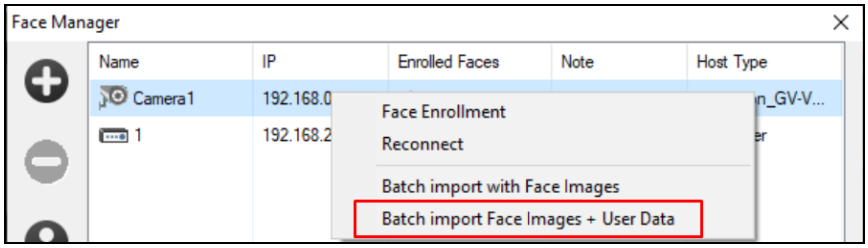


2. Save the exported TXT file (as exemplified below) in a specific folder.



3. Copy the user photos to be enrolled from the GV-ASManager directory (default:\\ASManager\Photo), and save them in the same folder as the TXT file.

4. Once all face photos are saved in the same folder as the TXT file, right-click the target host in **Face Manager** (**Home** > **Toolbar** > **Configure** > **Face Manager**), and click **Batch import Faces Images + User Data** to locate and choose the folder.



3.5 Local Face Recognition

In conjunction with the **face detection** function of AI-capable GV-IP cameras, GV-VMS has face recognition capabilities using its built-in face recognition engine and database.

The GV-VMS can process up to **10 face snapshots per second** for recognition, whether from multiple cameras or multiple frames from the same camera. While there's no limit on the number of open channels, excess snapshots are queued and processed at this fixed rate.

Recognition events of a specified group, such as Unauthorized, can be used to run the desired applications. To trigger alarms, send e-mail notifications, or initiate other alert actions, see *Setting Up Event Notifications* in Chapter 1. To learn which AI-capable GV-IP cameras support face detection, see *Camera's AI Events Supported by GV-VMS* in *Camera Features Supported by GV-VMS V20*.

To use the local face recognition feature in GV-VMS, complete the three steps outlined below. To begin, enable the face detection function on the connected camera, and then create a local face database. This will allow GV-VMS to convert the face detection events into face recognition.

To enable face detection on the connected camera

Refer to the camera's user's manual.

To create a local face database

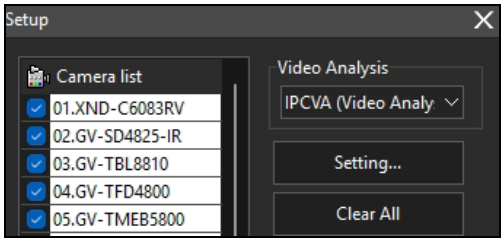
1. Enroll faces by adding portrait photos into the local face database. see *Enrolling Face Data* earlier in this chapter.
2. Enroll captured faces from live view or playback. See *Enrolling Faces from Live View / ViewLog* in *Enrolling Face Data* earlier in this chapter.

Note:

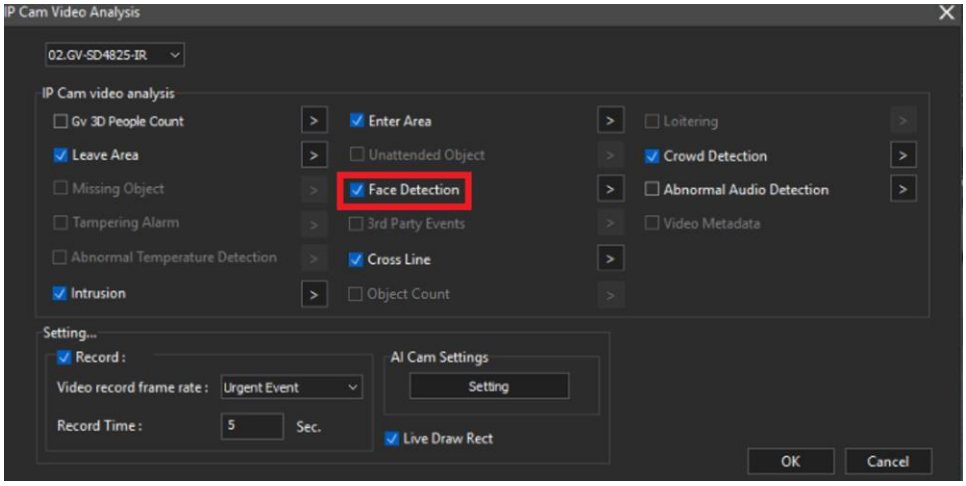
1. For the hardware specifications required for built-in face recognition (Local FR), see *Minimum System Requirements* in Chapter 1.
2. The local face database supports up to 100,000 face images in total, with up to 1 face image per face profile.
3. The size of the face within the photo should be greater than 150 pixels. For details on photo requirements, see *Photo Requirements* in Chapter 3 of the *GV-AI FR User's Manual*.

To enable face detection

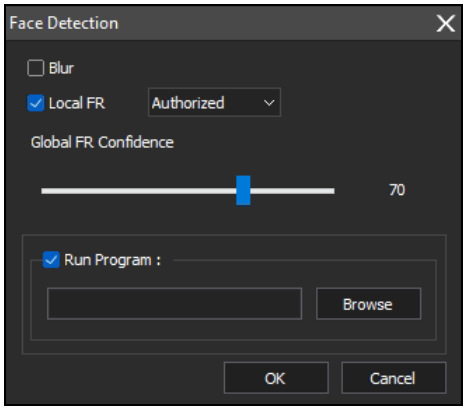
1. Click **Home** > **Toolbar** > **Configure** > **Video Process**.
2. In the Setup dialog box, select **IPCVA**, select the camera from which you want to enable face detection, and click **Setting**.



3. Select the camera from the dropdown list at the top, and enable **Face Detection**.



4. Click the arrow button > next to **Face Detection** to configure the following settings.



- **Blur:** Applies a blur effect to censor all detected faces.
- **Local FR:**

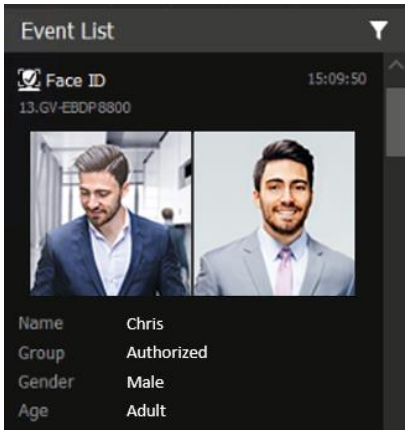
  Enable GV-VMS's local face recognition. Select either Unknown Alert or the face group for which alerts should be triggered. Note that local facial recognition does not support Schedule Alert.

- ⊙ **Global FR Confidence:** Adjust the Confidence level, from 0 to 99. The higher the level, the more definitive and stricter the camera is toward distinguishing between similar faces upon face recognition.

- ■ **Run Program:** Click **Browse** to select a desired program to be executed upon trigger.

5. Enable **Record**, set recording frame rate, and define the recording duration in seconds.
6. Enable **Live Draw Rect** under **Setting** to highlight detected faces on the live view upon face detection.
7. Click **OK**.

In the Event List, use the **Filter** function to select **Face ID**. When a face recognition event occurs, you can view live recognition details including the person's enrolled and captured faces, name, face group, gender, age group, camera channel, and the time of recognition. Double-clicking on an event can play back the video.



Note:

1. GV-VD8700 and GV-FD8700-FR are face recognition cameras that do not support the Face Detection function.
2. In the Event Filter, to search for Local FR (GV-VMS's local recognition) events, select **Face ID** under AI Event; to search for Face Detection events, select **Face** under Object Attributes.

3.6 Video Analysis by Camera

You can enable the reception of camera's video analysis events (also known as AI events), define recording parameters, configure remote AI event adjustments, and set the popup view duration to be triggered upon these AI events. To learn which camera's AI events are supported by GV-VMS, see *Camera Features Supported by GV-VMS V20*.

Note:

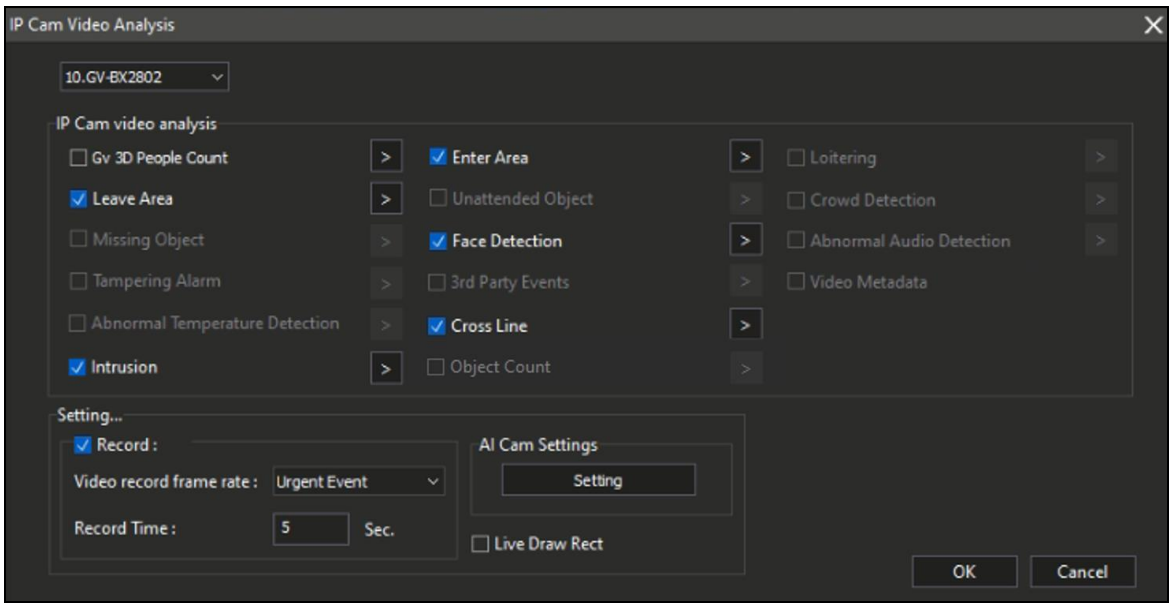
1. You can only choose either the camera or the GV-VMS system to process video analysis.
2. To receive AI events from cameras, enable **Sync device time with PC** in advance; see *General Settings* in Chapter 2.

3.6.1 Setting Up Video Analysis by Camera

This section describes the general settings for video analysis by camera in GV-VMS, applicable to all AI functions.

To access this feature, follow the steps below:

1. Click **Home** > **Toolbar** > **Configure** > **Video Process**.
2. In the Setup dialog box, select **IPCVA**, select the cameras, and select **Setting**. This dialog box appears.



IP Camera Video Analysis Functions

The enabled AI functions differ based on the camera selected, and the relevant AI functions must be configured on the camera first.

3. Select a camera.
4. Select the desired AI functions to configure:
5. To configure alert methods upon AI events, select the desired AI functions, and click the **arrow** > button next to each function:

   A. For **GV-3D People Count:** Establish a connection with GV-3D People Counter V2 or V3 to receive counting data.

   B. For **Intrusion, Cross Line, Leave Area, Enter Area**, **Loitering**, **Abnormal Audio Detection**, **3rd-Party Events**: Configure the popup view duration to be triggered upon these AI events. For details on 3rd-party events, see the following subsection *Setting Up Custom Keywords for 3rd-Party Events*.

   C. For **Object Count:** Configure the detection region and alarm reset interval or time to be triggered upon Target Counting events. Optionally, select **Web-report** > **Setting** to connect to GV-Web Report for real-time data monitoring. For details, see the *GV-Web Report User's Manual*.

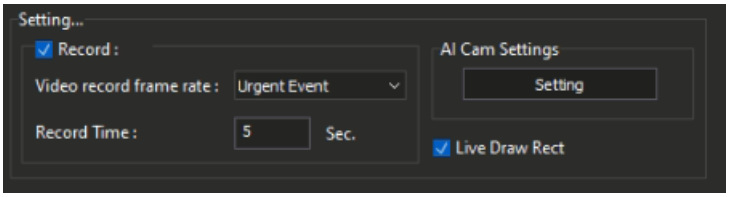
   D. For **Crowd Detection:** Configure the detection region, object number threshold, alert interval, or the popup view duration to be triggered upon Crowd Detection events.

   E. For **Abnormal Temperature Detection:** Only for GV-TMEB5800 (Thermal). Configure the detection region, trigger interval, or the popup view duration to be triggered when the temperature threshold set on the camera is reached. For details on configuring temperature measurement events on the camera, see *Displaying Temperature Readings* in Chapter 7 of the *GV-TMEB5800 Quick Start Guide*.

   F. For **Face Detection:** Select **Blur** to apply a blur effect to censor all detected faces, or run the desired applications to be triggered upon Face Detection events. To enable GV-VMS's local face recognition (Local FR), see *Local Face Recognition* earlier in this chapter.

   G. 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*.

Recording Settings

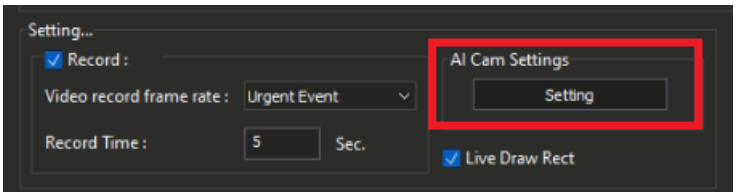


6. To record the AI events, select **Record**.
7. Set **Record Frame Rate** to Urgent Event (e.g., full frame) or General Event (e.g., key frame), and define the recording duration in seconds.
8. To display detection rectangles on the live view, select **Live Draw Rect**.

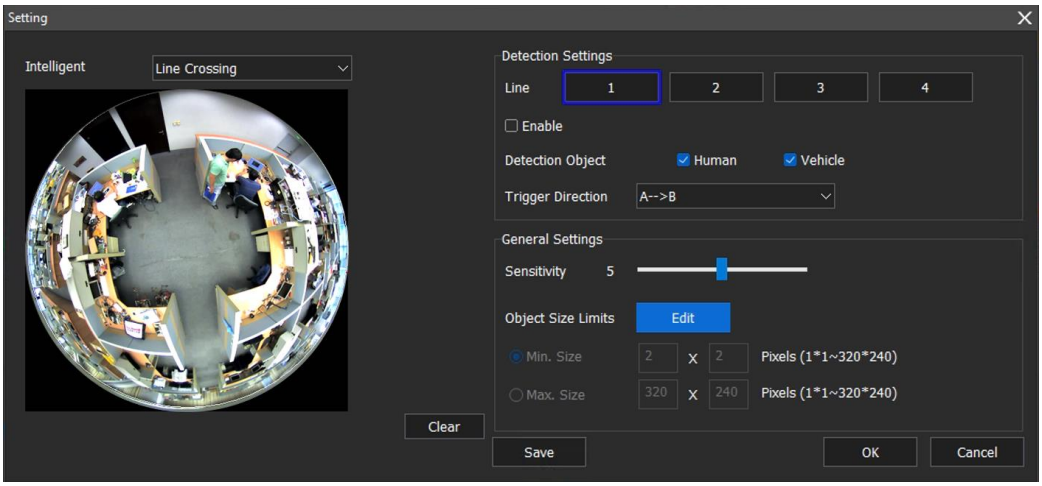
Note: Among the AI functions listed above, recording settings are unavailable for **GV-3D People Count** and **Video Metadata**. These functions are dedicated to connecting with the GV-3D People Counter and receiving camera metadata, respectively.

Remote AI Event Adjustments

You can directly configure the AI camera's alarm areas and PVD parameters from the GV-VMS system. Note that the function is only available for AI-capable GV-IP cameras.



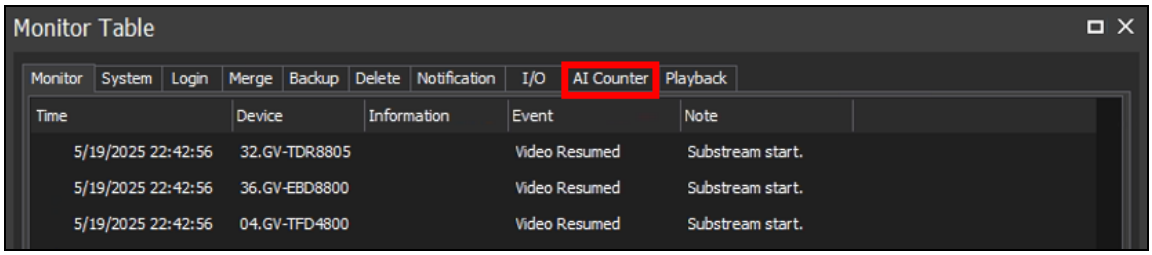
9. Click **Setting** of **AI Cam Settings**.
10. In the following example of Cross Line, configure detection rules, detection objects, sensitivity, size, and more. Once you click **OK**, the settings are applied to the remote AI camera immediately.



11. After the above settings, start monitoring.

The camera's object counting 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 the counting results from the GV-3D People Count function in IPCVA (for GV-3D People Counter V2 or V3) and the Object Count function in IPCVA (for AI-capable GV-IP cameras).



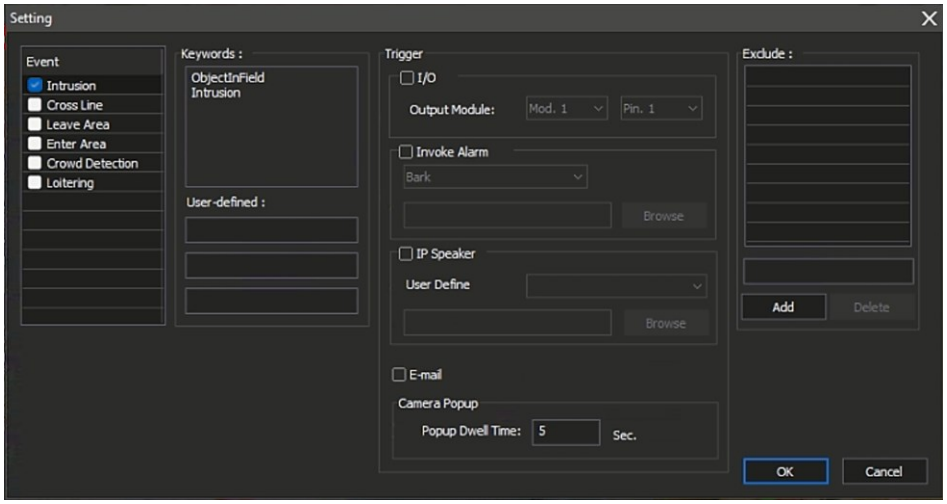
3.6.2 Setting Up Custom Keywords for 3rd-Party Events

This section describes how to configure custom keywords for 3rd-party events in GV-VMS, including keyword mapping to AI events and keyword-based event exclusion.

Note: Third-party cameras require ONVIF Profile M support.

To access this feature, follow the steps below:

1. Connect a 3rd-party camera to GV-VMS, then go to **Home** > **Toolbar** > **Configure** > **Video Process**.
2. Select the 3rd-party camera, choose **IPCVA**, and click **Setting**.
3. Enable **3rd Party Events**, then click the **arrow** button next to it. The Settings dialog box appears.



Configuring Keyword Mapping for Events

Keyword mapping allows the system to recognize specific keywords from the **Topic** field in 3rd-party events and map them to AI events supported by GV-VMS. After mapping, the event is displayed as a GV-VMS-supported AI event instead of a 3rd-party event. The supported AI events are listed in the left pane of the dialog box.

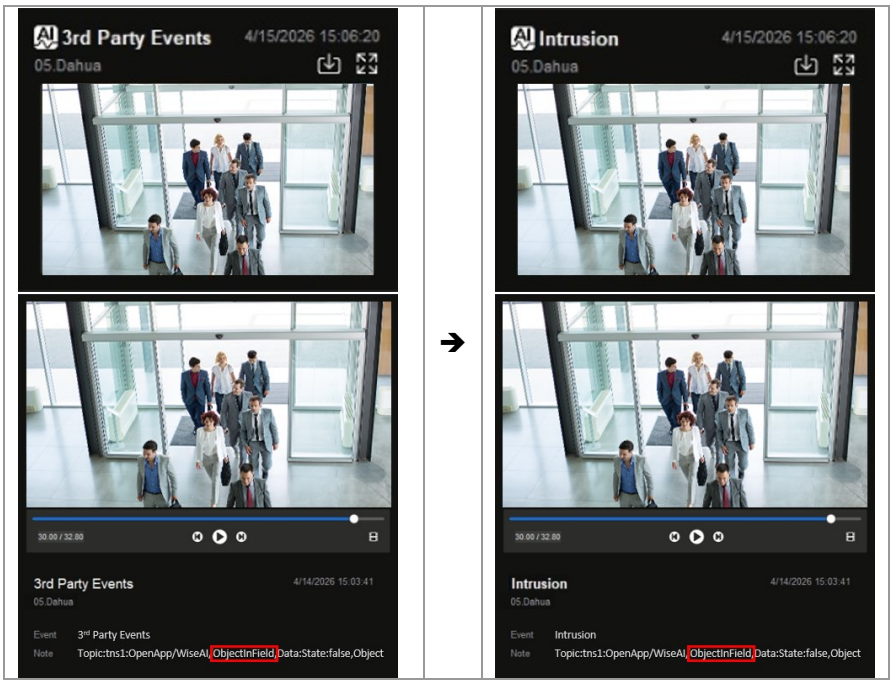
4. For events from the selected 3rd-party camera, select the **target AI event** from the list to enable keyword mapping.
5. In the Keywords box, predefined keywords are used to automatically map matching 3rd-party events to the selected AI event. You can also define up to **3 custom keywords or keyword phrases** in the User Defined input fields.

Configuring Keyword Exclusion

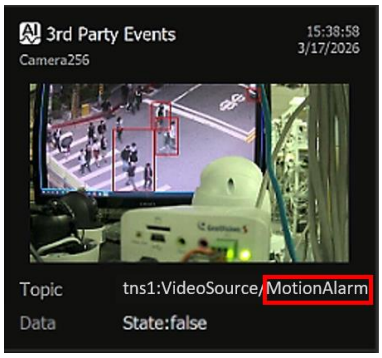
Keyword exclusion allows the system to filter out specific 3rd-party events based on keywords, e.g., filtering out non-AI events using keywords such as “Motion”. Events containing excluded keywords will not be displayed in the Event List or AI Query.

6. To filter out certain keywords from all events of the selected 3rd-party camera, type the keyword in the input field below the Exclude list.
7. Click **Add**. The keyword is added to the Exclude list.
8. Click **OK** to save settings.

In Event List or AI Query, events previously categorized as 3rd-party events are now categorized as GV-VMS-supported AI events (e.g., Intrusion). These events contain the specified keywords in their Topics. In the example below, **ObjectInField** is one of the predefined keywords for the Intrusion event.



Additionally, 3rd-party events with keywords added to the Exclude list are not displayed. In the example below, **MotionAlarm** is one of the excluded keywords.

	➔		➔	The event is no longer displayed in Event List / AI Query.

Chapter 4

Video Playback..... 182

4.1 Playing Back on ViewLog 183

4.1.1 ViewLog Window 184

4.1.2 ViewLog Control Panel 186

4.1.3 Adjusting the Camera View 189

4.1.4 Bookmarking Video Events in ViewLog 190

4.1.5 Searching Video Events with Record List 191

4.1.6 Merging and Exporting Video 192

4.1.7 Saving, Printing & Copying Images 197

4.1.8 Adjusting Distorted Views 198

4.2 Object Search 199

4.3 AI Query 201

4.3.1 Performing an AI Query 202

4.4 Advanced Log Browser 207

4.4.1 Controls on the Advanced Log Browser 207

4.4.2 Filter Settings 209

4.5 Single Player 210

4.5.1 The Single Player Window 210

4.6 Specifications 211

CHAPTER

4

Video Playback

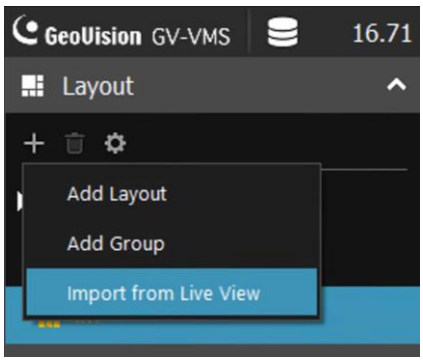
Recorded videos can be played back using the following software applications offered by GV-VMS. The summary below outlines their main characteristics to help you decide which application to use in a given situation.

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* later in this chapter.
Object Search	A more convenient tool to search video files recorded on motion or alarm. See *Object Search* later in this chapter.
Single Player	A player that plays back the backup recorded files with simple and easy playback functions. See *Single Player* later in this chapter.
GV-WebCam Server	A server that remotely accesses live view and plays back recordings on your Web browser without installing additional software. See *Chapter 7 Remote Viewing*.

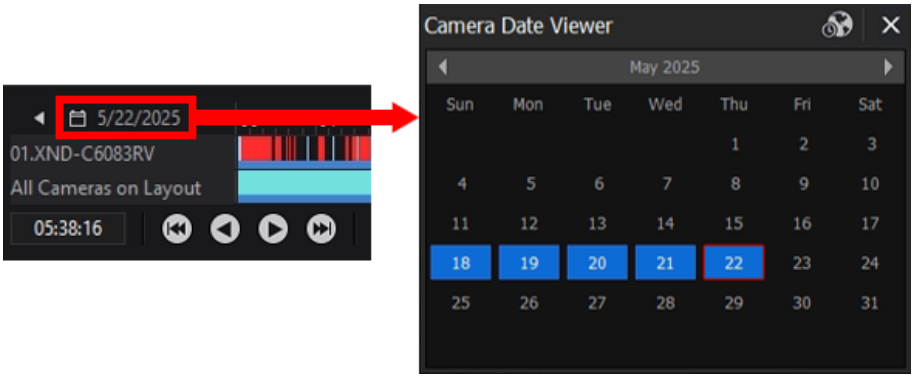
4.1 Playing Back on ViewLog

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

1. Select **ViewLog** .
2. In the Content List (No. 4 in *ViewLog Window* in Chapter 4), click **Layout** > **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.

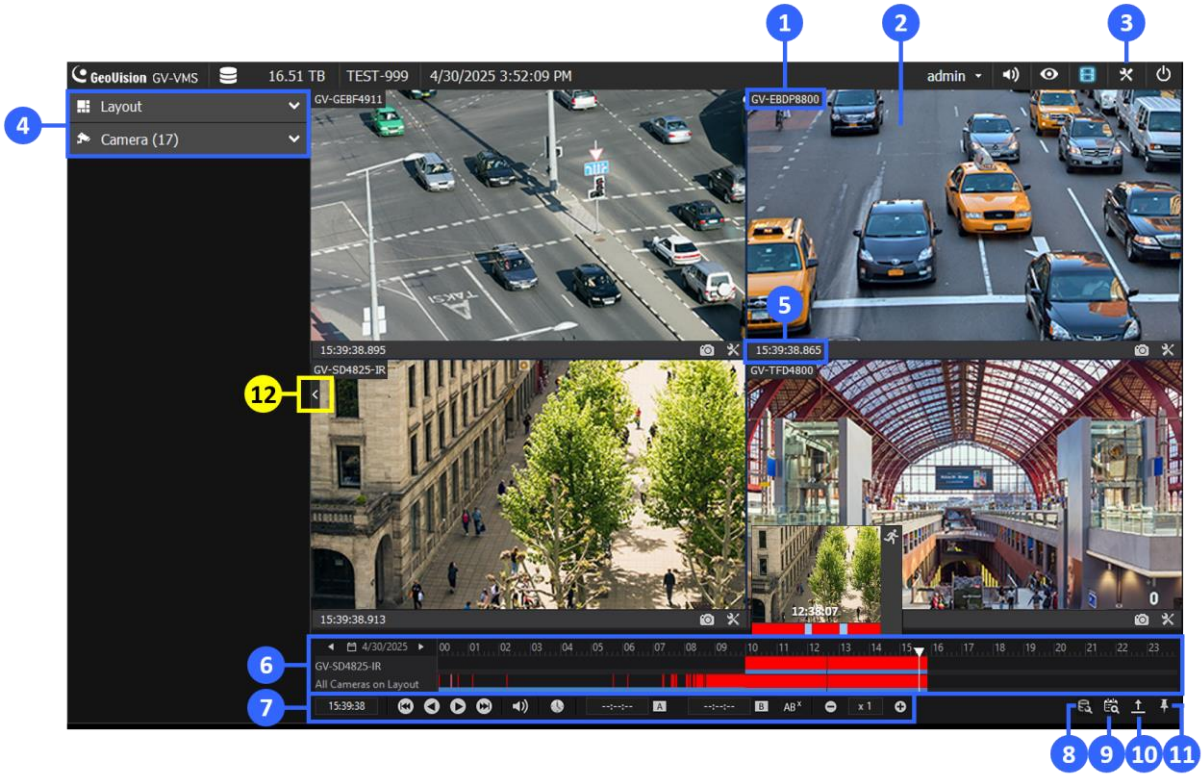


3. Optionally drag and drop more cameras from the Content List to the playback screen.
4. On the timeline, click the arrows or the date to select a date from a popup calendar.



5. Click **Play** to start playback. For details, see *ViewLog Control Panel* later in this section.

4.1.1 ViewLog Window



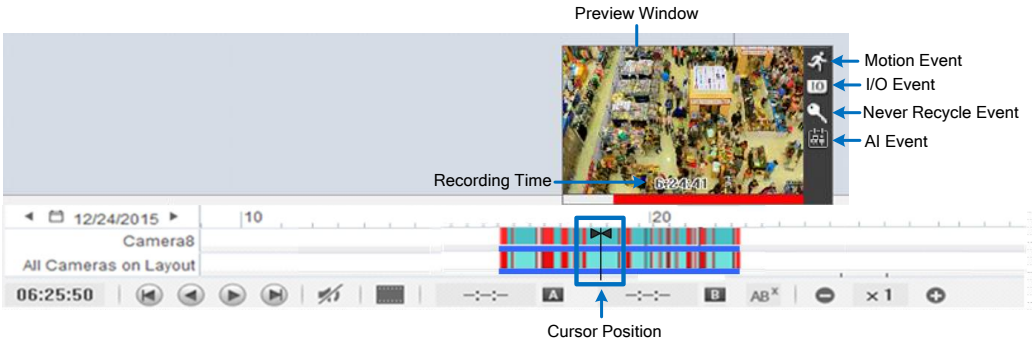
No.	Name	Description
1	Camera Name	Indicates the camera name.
2	Camera View	Displays the playback video.
3	Toolbar	Brings up these options when **ViewLog** is selected: • **Display Play Panel** : Display or hide the ViewLog timeline. This function is grayed out when the **Pinned** button is selected in the bottom-right corner. • **Tools** : Open record list, bookmark, storyline, object search, AI event search, advanced system log, event backup, and event export. • **Configure** : Preview video effects on sample images, and set up text overlay and object detection rectangles for playback. 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 section).

No.	Name	Description
4	Content List	When **ViewLog** is selected: Access playback layouts and the camera list.
5	Recorded Time	Indicates the time of recording.
6	ViewLog Timeline	Indicates the recording date and reflects video recordings. See *ViewLog Control Panel* later in this section.
7	Playback Panel	Contains typical playback control buttons. See *ViewLog Control Panel* later in this section.
8	Repair Database	Displays the background repair progress. See *Repairing Damaged File Paths* in Chapter 5.
9	Timeline Filter	Displays a popup window where you can select event types to show in different colors on the timeline. To change an event type's color, click its color box in the window.
10	Display All Database	Displays the recording timelines of all camera channels.
11	Pinned / Unpinned	Indicates whether the ViewLog Timeline is fixed in place. When set to **Pinned** , the timeline remains visible and cannot be hidden. Select to unpin the timeline, allowing it to be hidden using the **Display Play Panel** option in the Toolbar (see No. 3 above).
12	Collapse / Expand	Click the  and  buttons on the side of the Content List to collapse them.

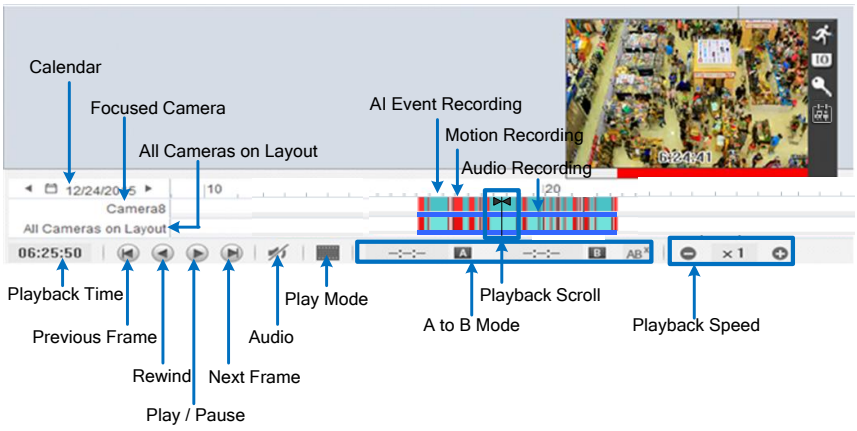
4.1.2 ViewLog Control Panel

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



Default 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

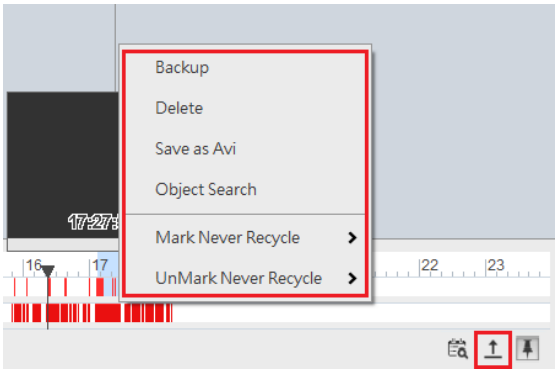
To change the default colors, click the **Timeline Filter** button at the bottom right of the ViewLog window, and click the color box of the desired event type.

Note:

1. Round-the-Clock events are shown as blue, except the following conditions:
   - If **Register Motion Event** or **Intrusion** is enabled, the timeline interval of the triggered event becomes red.
   - If **Webcam Service** is enabled, the timeline interval becomes red when users log onto GV-VMS remotely (such as using mobile applications).
   - If **Control Center Service / ERM Service** is enabled, the timeline interval becomes red when the connected GV-Software receives events from GV-VMS.
2. When several events occur concurrently, the timeline colors will overlap with one another based on the following sequence: AI events > Urgent (Motion / IO) > Never Recycle > Recordings retrieved from the SD cards of cameras.

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.



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

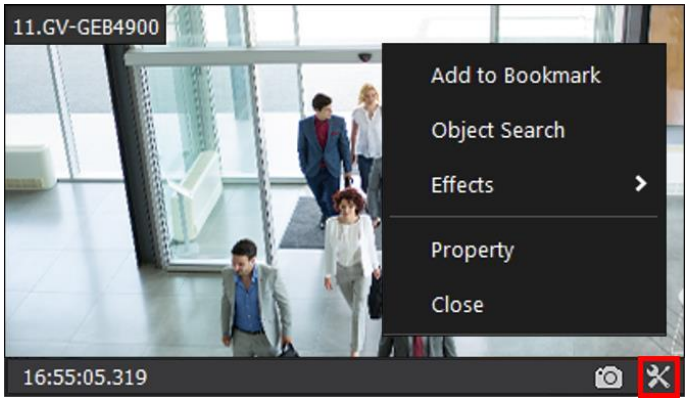
You can directly drag the timeline to search and view recordings of a previous or next day with recorded events.

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:



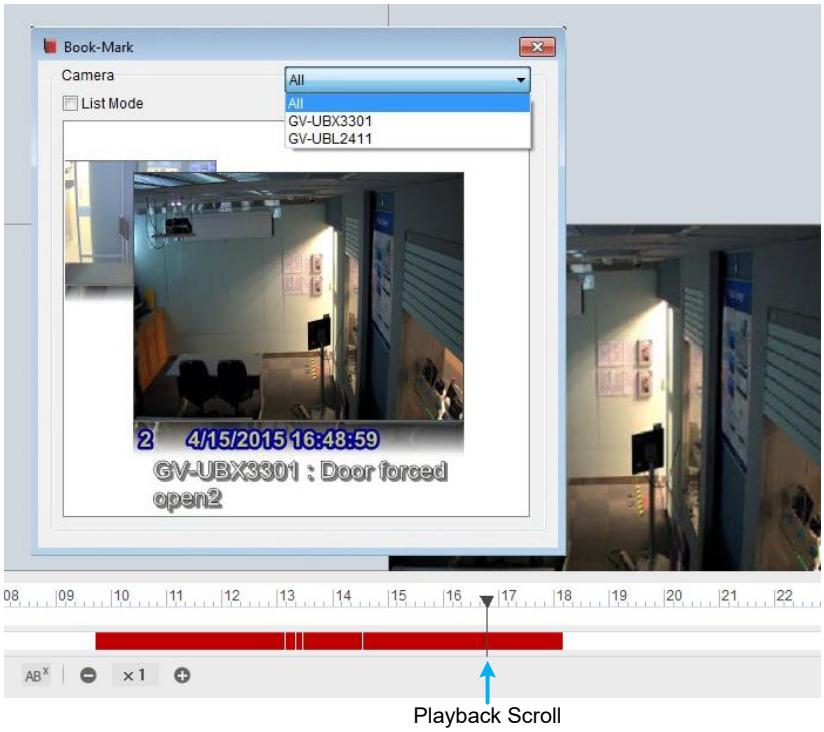
- **Add to Bookmark:** See the following subsection *Bookmarking Video Events in ViewLog*.
- **Object Search:** See *Object Search* later in this chapter.
- **Effects:** Click to apply image effects. After applying effects:
  - To take a snapshot of the current playback image, select **Copy** and then 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.



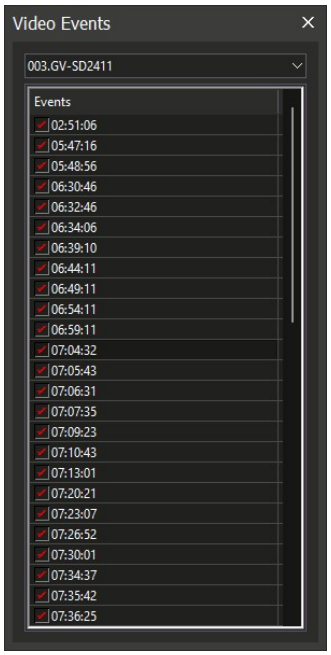
3. You can select **List Mode** to present all the bookmarks in a list.
4. To filter the bookmarks, you can select a camera from the dropdown list, or click **Filter** to narrow results by **Time Range** or **Search Description**. The Search Description option allows you to enter keywords or partial 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 Searching Video Events with Record List

The Record List allows users to search for video events by exact time and filter them by camera. Events are displayed in chronological order.

1. Click **ViewLog** > **Toolbar** > **Tools** > **Record List**. This dialog box appears.



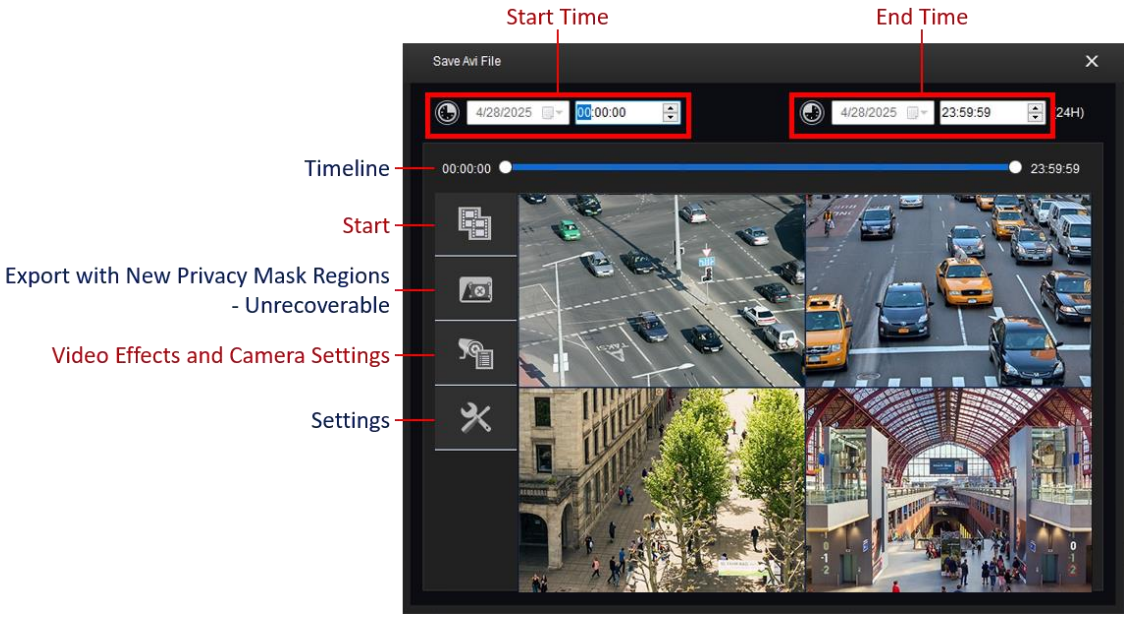
2. Select a camera from the dropdown list. You can also select a camera view in the **Playback** window to automatically switch the Record List to that camera.
3. Select an event to jump the Timeline in the **ViewLog Control Panel** to its corresponding position for playback.

4.1.6 Merging and Exporting Video

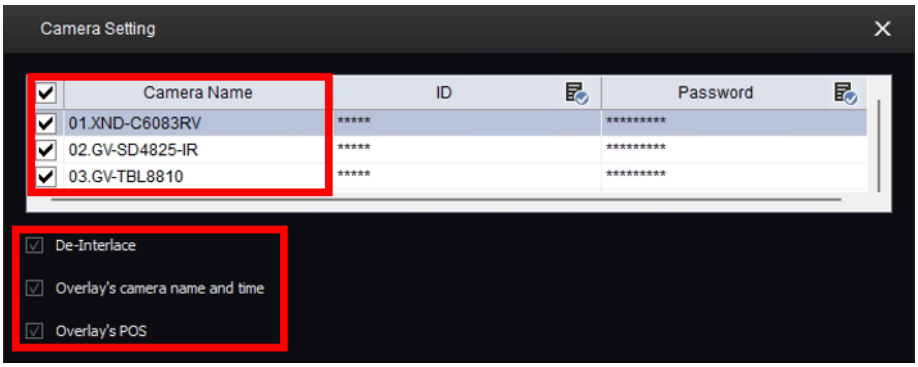
You can merge several videos into a single .avi or .exe file and export it to the local computer.

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.

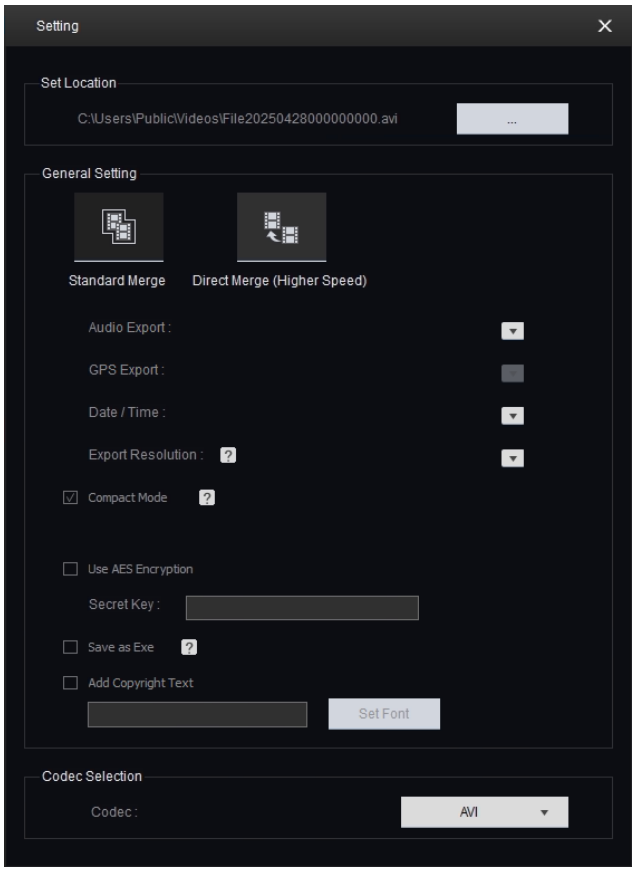


2. Click **Video Effects and Camera Settings** to select the camera channels you wish to export. Optionally enable additional camera settings.



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 **Settings** . 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: *Date / Time*, *Export Resolution*, *Use AES Encryption*, *Save as Exe*, *Codec Selection*, and *Export with New Privacy Masks Regions*.

- **Audio Export:** Select **Denoise** to remove audio noises from the video, or select **Channels** for audio exporting.
- **Date / Time:** Select whether to show the 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.
- **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 3rd-party player. Enable this feature to play back video on 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 that provides better image quality, higher frame rates, and smaller file sizes 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 on any computer.
- **AVI** 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.

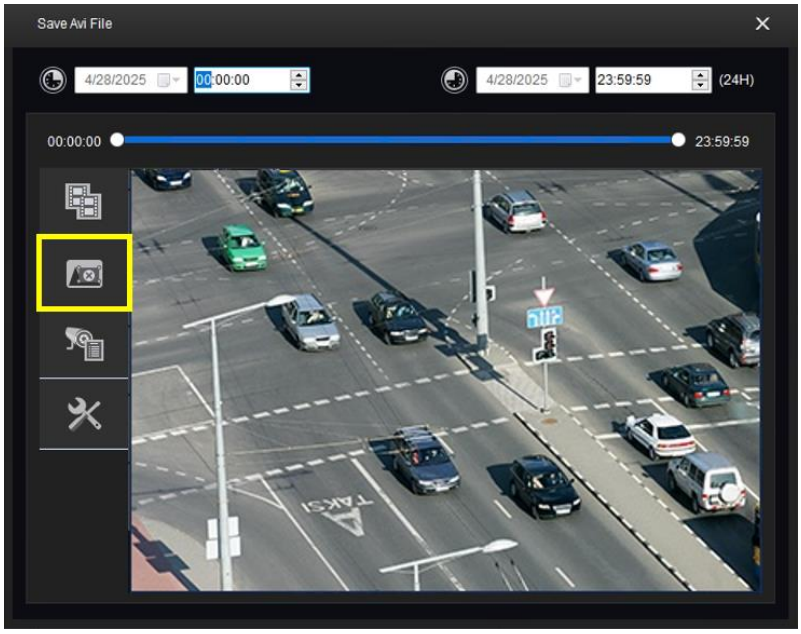


Note: Audio is not supported for videos exported in MPEG4 codec.

To optionally include other features in the exported video, refer to the following:

Configuring Privacy Mask

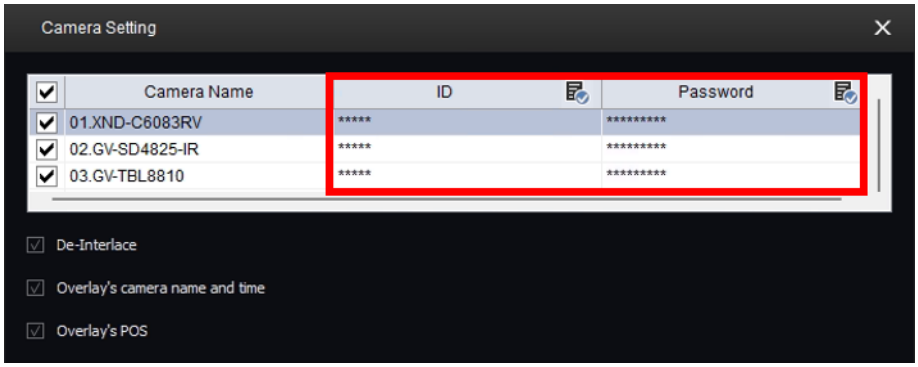
To configure the Privacy Mask settings for the exported files:



- **Unrecoverable Privacy Mask**: The masked areas cannot be retrieved in the exported files. To set up the masked areas, click and drag on the image, and select **Add** or **Delete**.

Retaining Recoverable Masked Areas

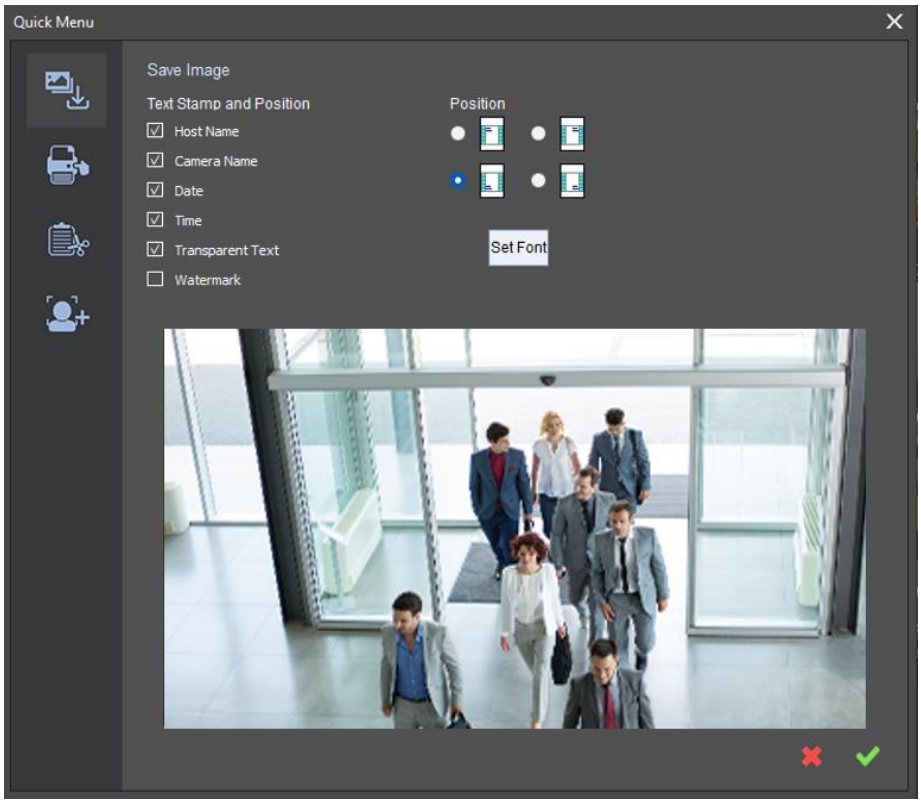
For recorded videos with Privacy Mask settings, by default, you can see the recoverable masked area created in the Main System when logging in with the administrator account. To retain the masked area before exporting recorded videos, type a random ID and password in the fields or leave the fields blank. 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 masked areas. To grant access rights to Power Users and Users, see *Granting Access Privileges to Recoverable Areas* in Chapter 3.

4.1.7 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.

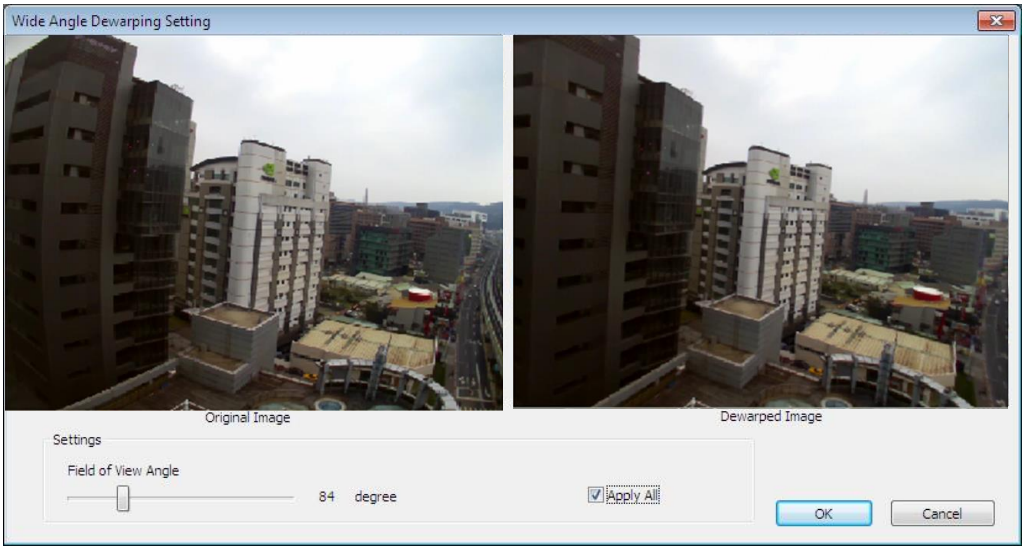
   [Position] Select a desired position, upper-left, upper-right, bottom-left, or bottom-right, where the texts will be added to the image saved.

   [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.

4.1.8 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 camera is immediately dewarped.

4.2 Object Search

Object Search allows you to search for alarm or PVD events in the recorded videos of a selected channel by specifying regions of interest. Two event types are available: Alarm and Smart Motion Search.

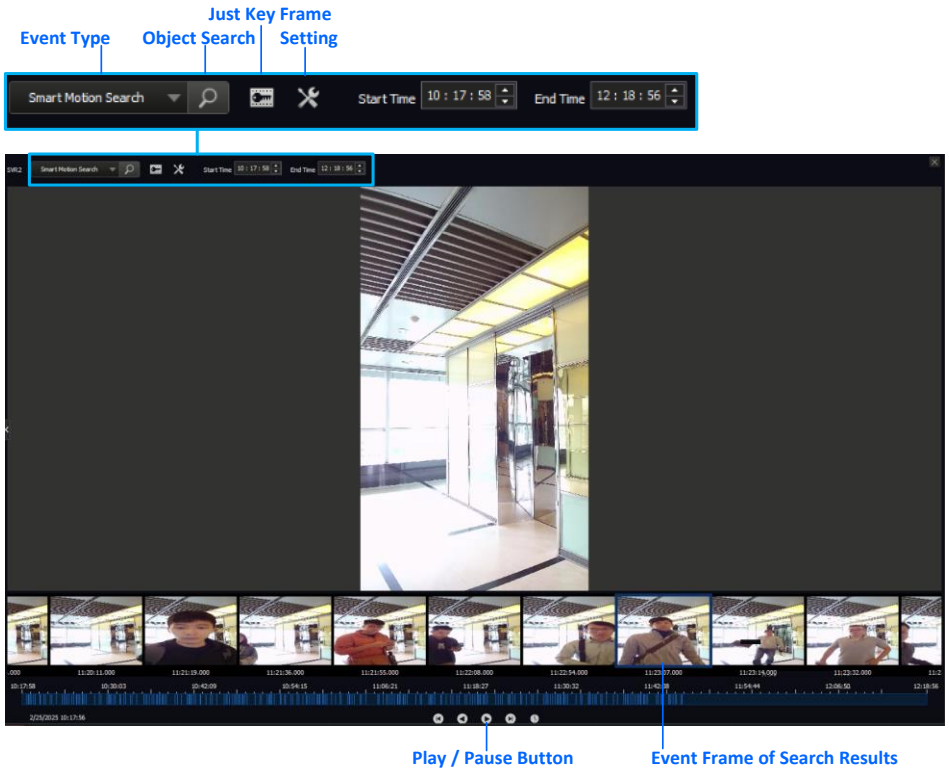
- **Alarm:** Performs motion analysis on recorded videos, allowing you to search for motion in designated regions of interest after recording. No pre-marked motion data is required.
- **Smart Motion Search:** Marks motion data during recording, allowing you to search for motion in designated regions of interest after recording, specifically for people or vehicle activity if PVD is enabled.

This function is ideal for when you know an incident occurred in a specific area but are unsure of the exact time. By drawing a region of interest (ROI) on the camera's field of view, the system will automatically search for any video clips containing person or vehicle activity within that area.

Note: To mark PVD motion while recording, enable both **PVD** and **Smart Motion Search** on cameras before recording. For details on the two options, 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: **Alarm** or **Smart Motion Search**.
4. Click **Setting** .
5. For **Alarm**: Set different detection sensitivities for different areas of the camera image. By default, a rectangular detection region is created at the top left.
   - To create new detection regions: Click the **+** button to create a new region. Up to 10 regions can be created, including the default region.
   - To modify existing regions: Select a region, then adjust its sensitivity level using the slider (default: level 3, range: 1–5), drag the region to reposition it, or double-click on the image to add a vertex. You can drag a vertex to adjust the shape, or right-click a vertex and select **Delete** to remove it.
   - To remove regions: Click the **-** button to switch to Remove mode, then drag across a region to remove it.
   - To restore default settings: Click **Default** to reset to a single rectangular region at the top left.

   Note: Regions can only be modified in the Add mode. Click the **+** button to switch to Add mode when needed.

   For **Smart Motion Detection**: The image is divided into grids.
   - To create new detection regions: Click the **+** button to switch to Add mode (enabled by default). Drag across the image to select grids and define detection regions. The system will search for any clips triggered by alarm or PVD events within the selected regions.
   - To remove regions: Click the **-** button to switch to Remove mode, then drag across the image to deselect grids.
   - To clear all regions: Click **Erase**.
6. Click **OK** to save settings.
7. Click **Just Key Frame** to search only key frames, if necessary.
8. Click **Search** . The events found to have alarm or PVD motion are highlighted in blue on the timeline.
9. Double-click an event frame or click the **Play** button to view the event.

4.3 AI Query

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

If you want to perform advanced filtering of general, system, or people / vehicle counting events, see *Advanced Log Browser* later in this chapter.

Note:

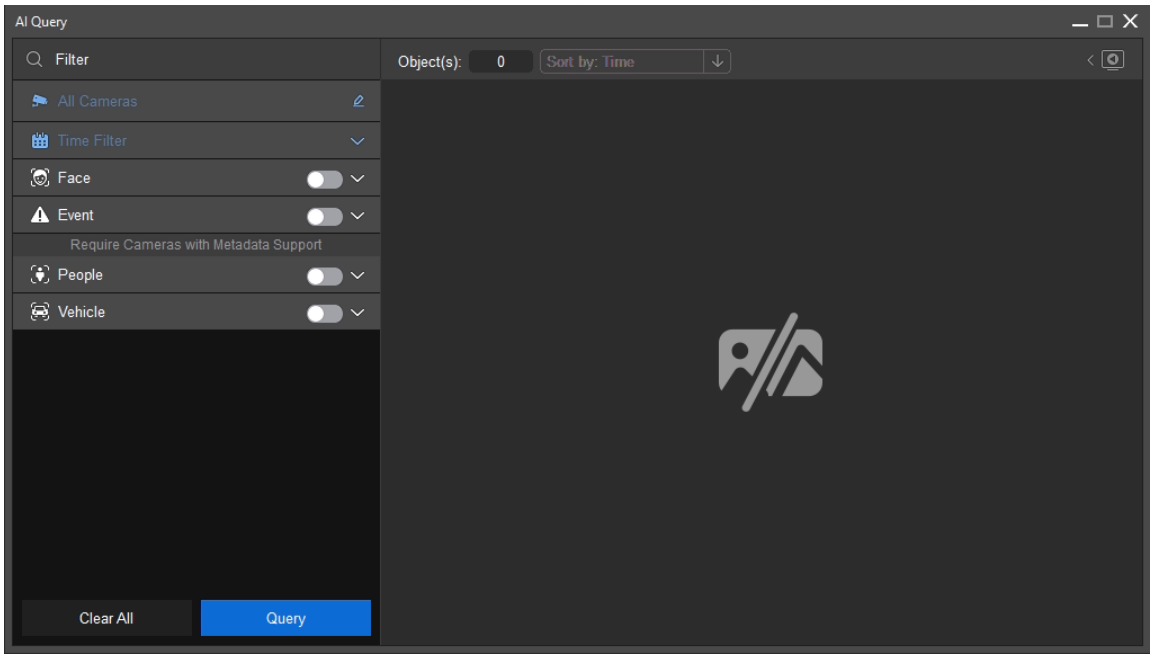
1. Filtering by people and vehicle attributes is supported only on cameras that provide video metadata. For the list of supported GV-IP cameras, see *Camera's Video Metadata Supported by GV-VMS V20* in *Camera Features Supported by GV-VMS V20*.
2. Before AI and PVD events can appear in AI Query, ensure they are configured before recording, in the IP Cam Video Analysis and Advanced Motion Detection Setup dialog boxes, respectively. Querying can only be done after recording, once these settings are in place.
   - For AI event setup, including face, people, and vehicle attribute detection, see *Video Analysis by Camera* in Chapter 3. For face attributes, see **Face Detection**. For people and vehicle attributes, see **Video Metadata**, both under *Video Analysis by Camera*.
   - For PVD event setup, see *Setting Up Motion Detection* in Chapter 1.
3. The AI Query function is used to search for detection or recognition results. To enhance detection accuracy, refer to the camera's user manual for various AI event settings. For **face searches**, you can adjust the Confidence parameter in the AI Query filter to refine the similarity of search results.
4. Supervisors can restrict user access to AI Query by disabling **Browse System Log** in the ViewLog tab of the Local Account Edit dialog box (accessed by clicking the **account ID** at the top right of the main window > **Password Setup** > **Local Account Edit**).

4.3.1 Performing an AI Query

You can search using face data or by filtering event types, people attributes, or vehicle attributes.

To begin the AI query, follow the steps below.

1. Click **ViewLog** > **Toolbar** > **Tools** > **AI Query**. The AI Query dialog box 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*, *People*, 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.

After completing the preliminary steps above, continue with the specific search method that applies, described in the following subsections.

Searching by Face Data

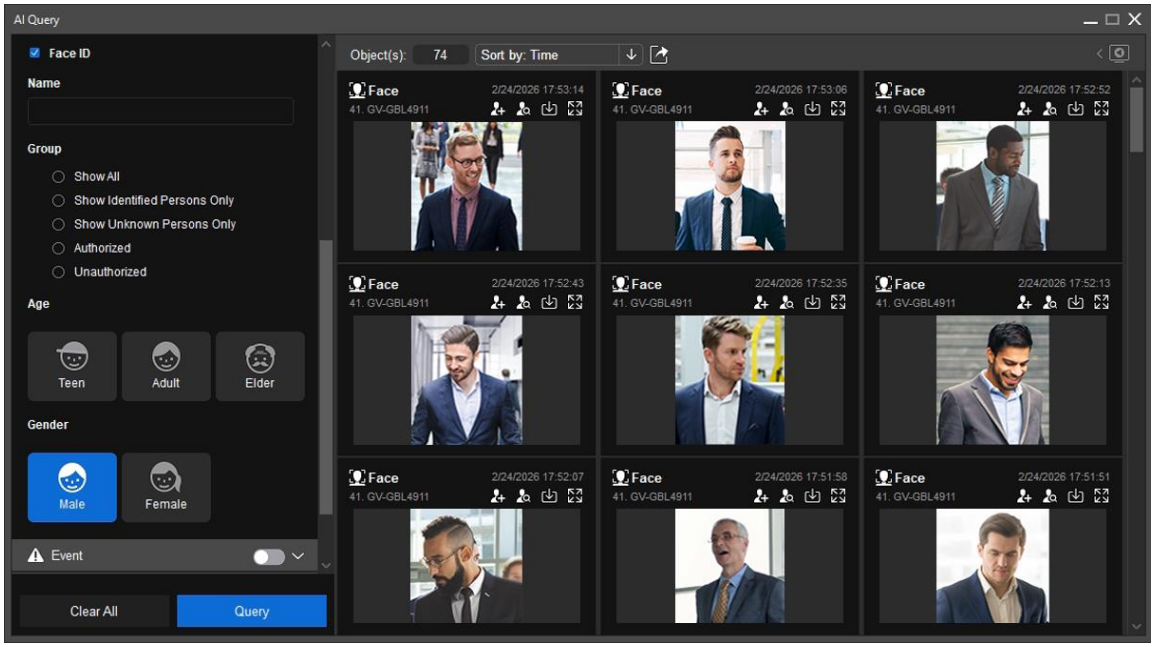
1. Enable the **Face** filter. You can search recorded recognition events for both identified and unknown individuals by uploading a reference face image (*Face Matching*), or by name or group (*Face ID*), provided the name is first enrolled in the face database. You can also filter by face attributes such as age group and gender.

   - **Face Matching:** Click the  button to upload a reference face image from your PC and search for similar recognition events. Optionally, adjust the **Confidence** parameter to set the minimum similarity threshold for search results compared to the uploaded face image.
   - **Face ID:** To search recognition events by name or group, first enable **Face ID**, then enter a person's *Name* (if enrolled in the face database) or select their *Group*. Available groups include *Show All*, *Show Identified Persons Only* (those successfully recognized from the face database), *Show Unknown Persons Only*, and other custom groups.
   - **Age Group / Gender:** Filter recognition events by face attributes such as *Age Group* and *Gender*, which are automatically estimated during detection. The search returns results that match all selected attributes simultaneously. For example, selecting **Male** and **Adult** shows only adult males. You can also select multiple values within one attribute to broaden results – for instance, **Male** with **Teen + Adult + Elder** returns all male age groups.

Note: When Face Matching is enabled, only face recognition results appear in the log, while other event search filters are ignored.

---

2. Click **Query**. The matching face events are displayed. You can sort the results by time in ascending or descending order.



If you are using **Face Matching**, a blue number in parentheses appears at the top of each event, indicating the similarity level between the search results and the uploaded reference image. The similarity percentage ranges from the set Confidence parameter up to 100%. In addition to time, you can also sort the results by confidence in ascending or descending order.



3. Click the icon on an event snapshot to enroll faces. See *Enrolling Faces from Live View / ViewLog* in *Enrolling Face Data* in Chapter 3.
4. Click the icon on an event snapshot to use it as a reference for searching other similar recognition events. This function allows you to find past occurrences of the same person based on facial similarity.
5. Click the icon on an event snapshot to save the image.
6. By clicking an event snapshot, you can view its playback and event details.

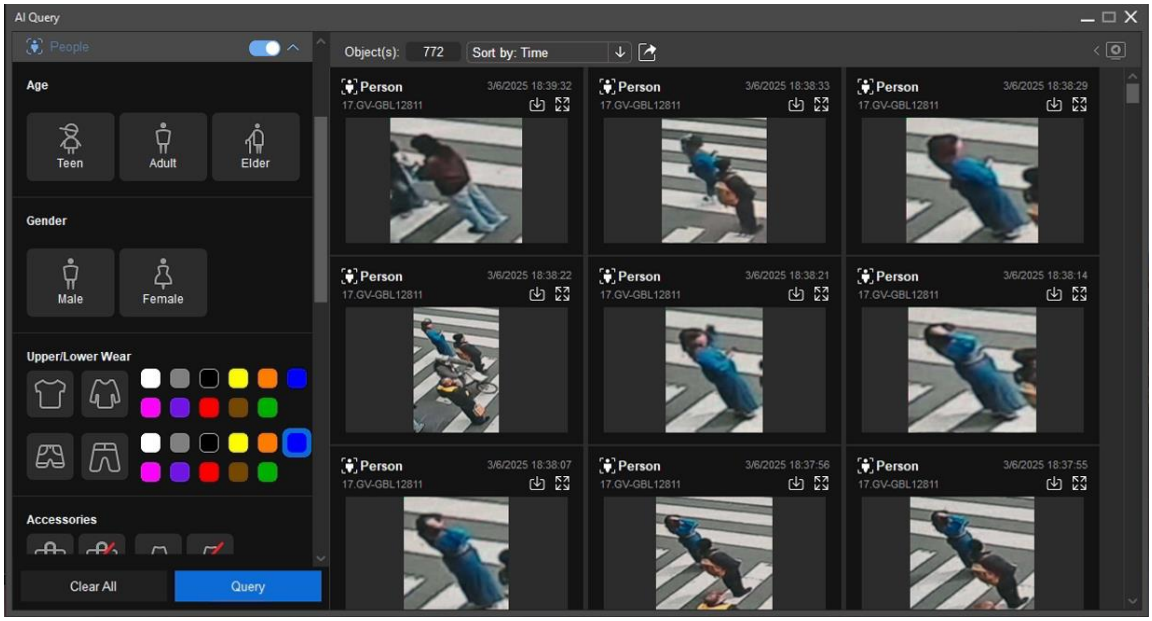
Searching by Event Types, People Attributes, or Vehicle Attributes

1. 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 **People** or **Vehicle** and filter by their respective attributes. The search returns results that match all selected attributes simultaneously. For example, selecting **Male** and **Adult** shows only adult males. You can also select multiple values within one attribute to broaden results – for instance, **Male** with **Teen + Adult + Elder** returns all male age groups. Available attributes include:

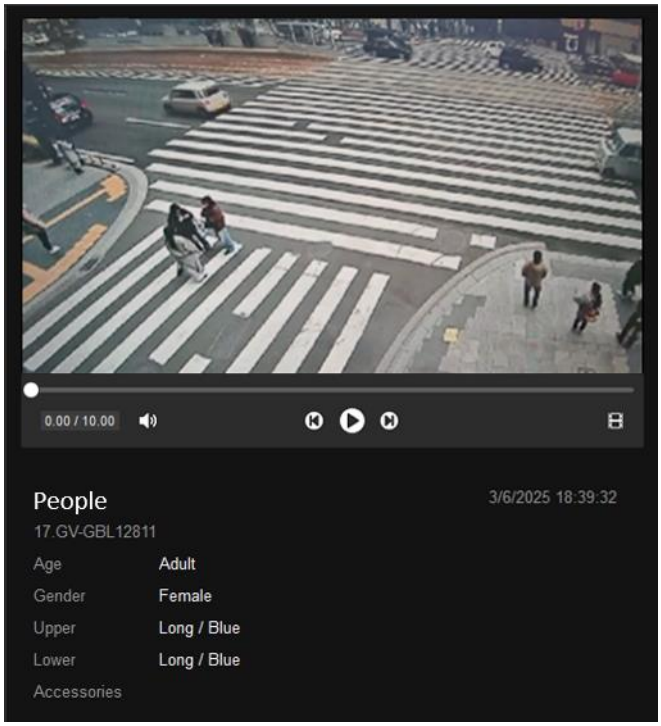
   - **People:** *Age*, *Gender*, *Upper/Lower Wear*, and *Accessories*.
   - **Vehicle:** *Type*, *Color*, and *Brand*.

2. Click **Query**. The matching events are displayed. In the example below, the people attributes are filtered by blue upper wear. You can sort the results by time in ascending or descending order.



3. Click the  icon on an event snapshot to save the image.

4. By clicking an event snapshot, you can view its playback and event details.



Tip:

1. In the Event Playback panel, 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 screen 

.
2. To export query results, click the icon beside the object count.
   - **CSV:** Saves as an Excel file and an image folder.
   - **PDF:** Saves as a PDF file.

Note: The maximum number of query results is 10,000.

4.4 Advanced Log Browser

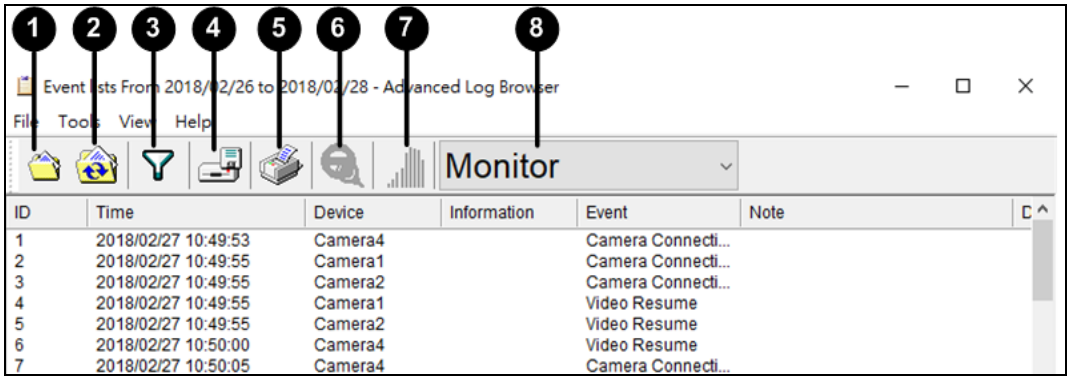
With the Advanced Log Browser, you can perform post-event review and filtering of general events, system activities, or people / vehicle counting events using advanced criteria such as device, time range, and event subtype. It provides more comprehensive and detailed log data than the System Log, making 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* earlier in this chapter.

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.

4.4.1 Controls on the Advanced Log Browser



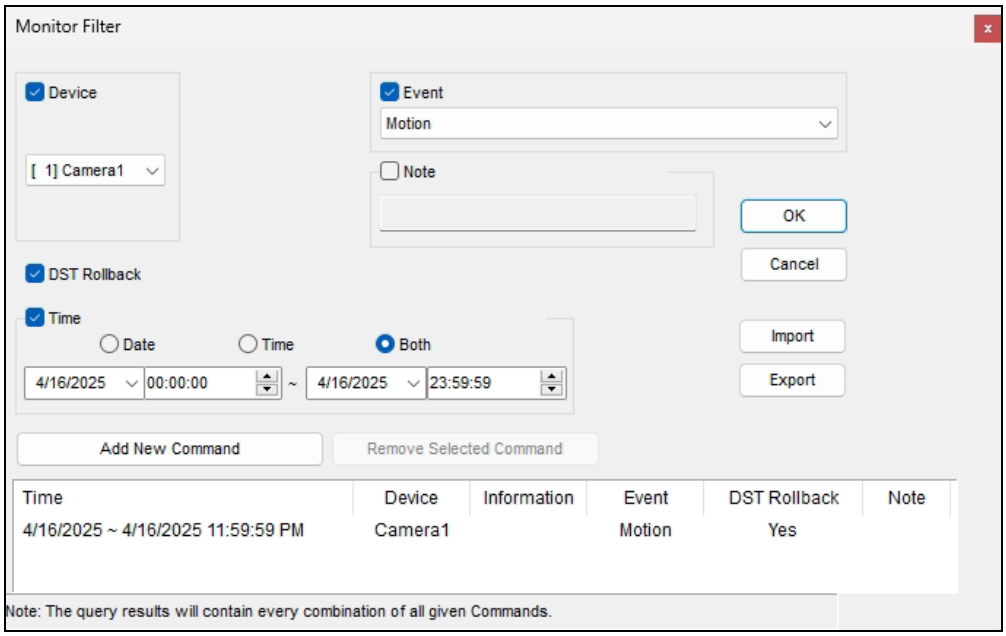
No.	Name	Description
1	Open	Opens an event log.
2	Reload	Select **Reload All Table** or **Reload Current Table** to refresh loaded data.
3	Filter	Defines the search criteria. See the following subsection *Filter Settings*.
4	Backup	Select **All Tables** to back up all logs, or select **Current Table** 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 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 V2 or V3) and the Object 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, and AI Counter.

4.4.2 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 (No. 3 in *Controls on the Advanced Log Browser* earlier in this section) > **Default Filter**. This dialog box appears.



2. Define the filter criteria, such as a specific camera, an event, 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.

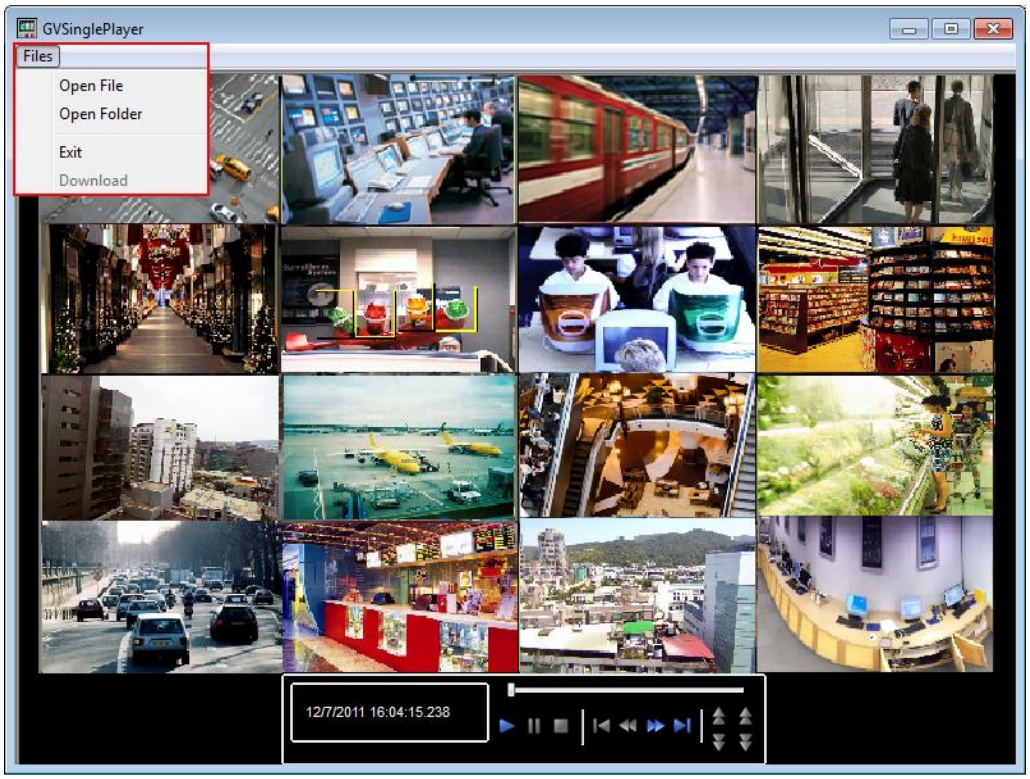
Note: The default Export path is **C:\ProgramData\Geovision\Syslog_Favorites**. If you change this path, the exported file will not appear under the **Favorites** option.

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 The 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..... 213

5.1 Backing Up Log Data..... 213

5.2 Backing Up Recorded Files..... 214

5.3 Deleting Recorded Files..... 217

5.4 Repairing Damaged File Paths..... 218

5.5 Repairing Damaged Video Files..... 220

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 cloud storage services.

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.

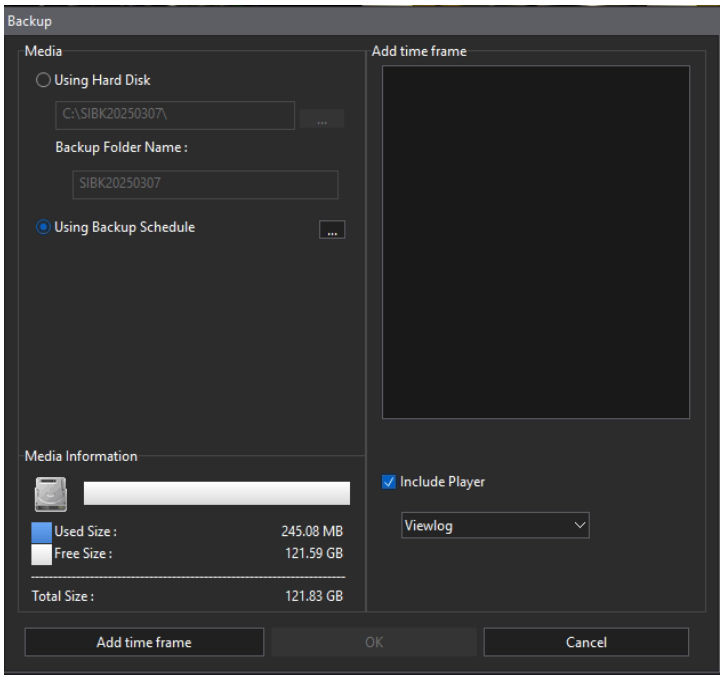
   [Export with Video/Audio data] Backs up video/audio attachments with log data.
4. Click **OK**. The Backup dialog box appears (see the dialog box in *Backing Up Recorded Files* later in this chapter).
5. In the Media section, select the method and destination to back up the log files and click **OK** to back up.

Note:

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

5.2 Backing Up Recorded Files

1. Click **ViewLog** > **Toolbar** > **Tools** > **Backup**. The Backup dialog box appears.

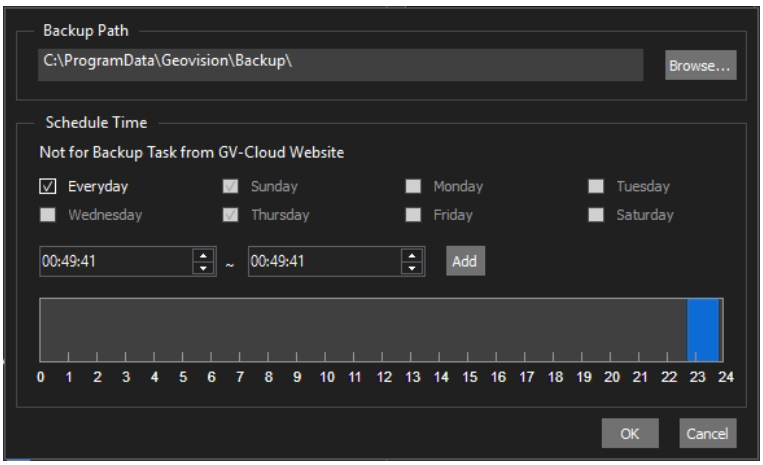


Backup dialog box

2. Select the destination media to back up files.

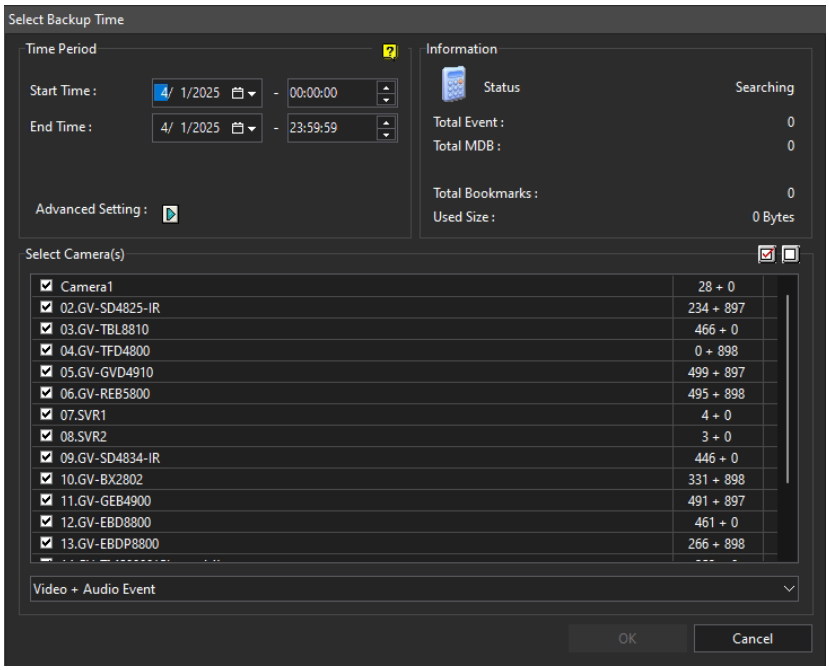
[Media]

- **Using Hard Disk:** Click the **[…]** button to select the desired hard disk.
  - **Backup Folder Name:** Type a desired name for the backup folder.
- **Using Backup Schedule:** Allows users to schedule backups to the local disk. Click the **[…]** button. This dialog box appears. Choose a destination path for storing recorded videos and specify when the backup should run, including the days and time periods.



[Media Information] Indicates free and used space on 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.
- **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.

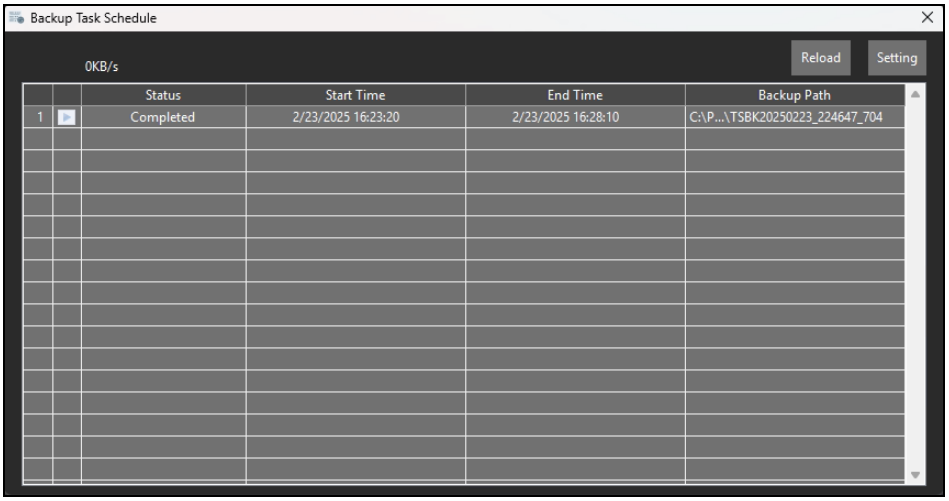
- **Video + Audio dropdown list:** Select the types of video events for backup.

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.

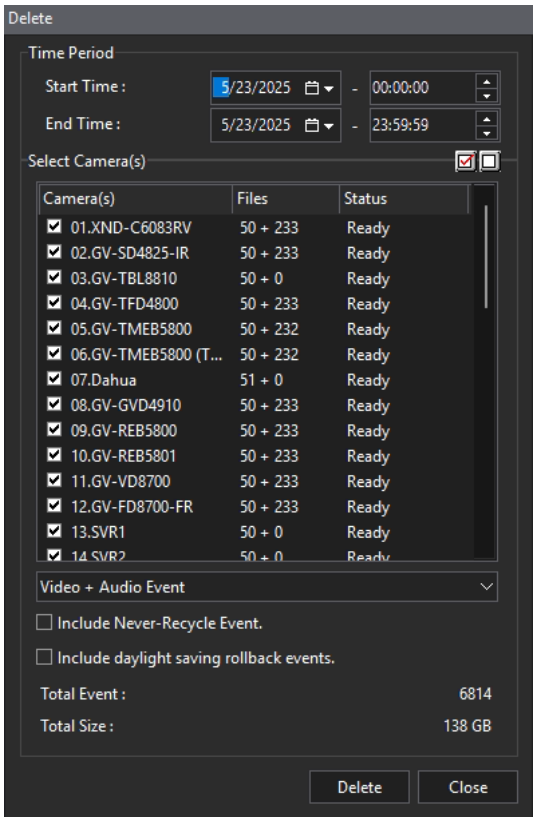
Note: For details on the ViewLog player and Single Player, see *Chapter 4 Video Playback*.

Tip: If you select **Using Backup Schedule** and a schedule is created, click the **Show Backup Task Schedule** icon  from the Windows system tray to view the backup status.



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.

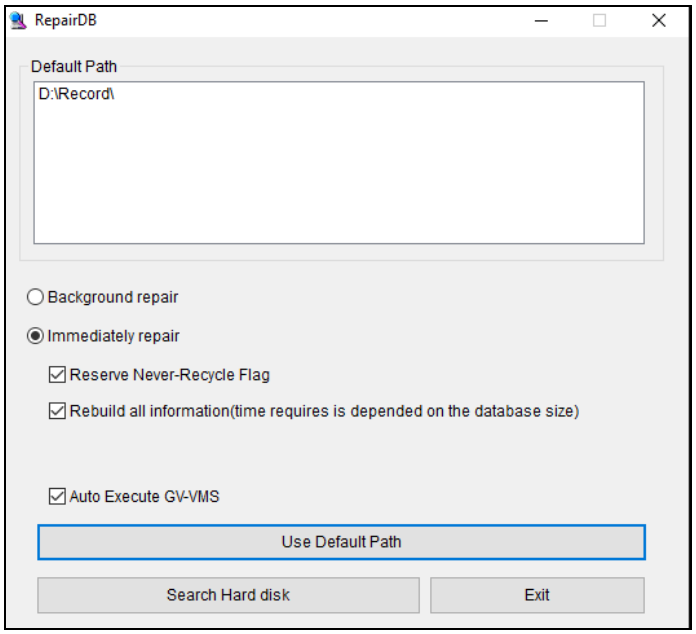
5.4 Repairing Damaged File Paths

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, GV-VMS 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 **Windows Start** > **All apps** > **GV-VMS 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 GV-VMS continues its operation. Select **Immediately repair** to thoroughly repair your recorded files while GV-VMS 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 GV-VMS. You can optionally enable **Auto Execute GV-VMS** to allow GV-VMS to automatically restart after Immediately Repair is completed.
6. Click **OK**.

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 occur 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)**.**

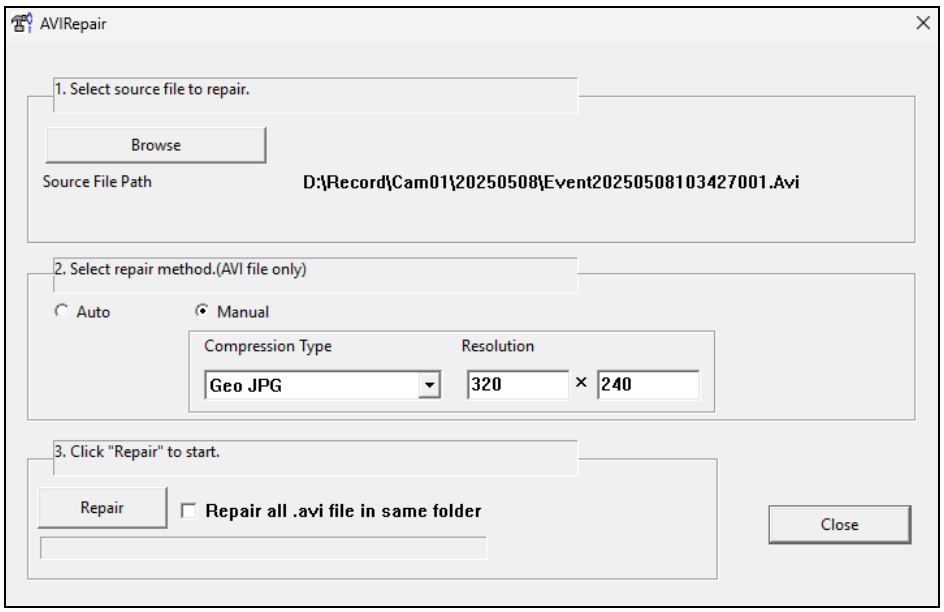
5.5 Repairing Damaged Video Files

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

Tip: If the computer was not shut down properly, the first thing you should do before starting GV-VMS 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 the 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** **Complete 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 223

6.1 Setting Up I/O Devices 223

6.1.1 Adding I/O Devices 224

6.1.2 Setting Up Input and Output Devices 225

6.1.3 Latch Trigger 227

6.1.4 Keeping Last Toggle Status 229

6.1.5 Setting Up PLC I/O devices 231

6.2 Advanced I/O Applications 233

6.2.1 Setting Up Actions upon Input or Output Trigger 234

6.2.2 Moving PTZ Camera to Preset Points upon Input Trigger 235

6.2.3 Setting Up Momentary and Maintained Modes 236

6.2.4 Deactivating Alarm and Alert upon Input Trigger 237

6.2.5 Other I/O Application Functions 238

6.3 I/O Devices in Content List 239

6.4 Visual Automation 240

CHAPTER

6

I/O Applications

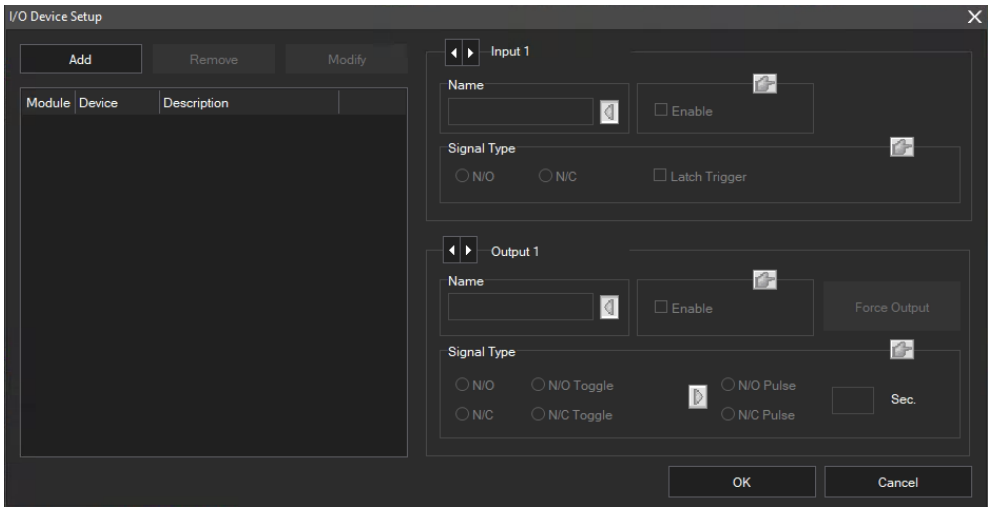
This chapter describes how to configure and control GV-VMS's I/O devices. I/O applications include the following features:

- Record videos, send e-mail notifications, and trigger output devices 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 GV-VMS, 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 GV-VMS, click **Home** > **Toolbar** > **Configure** > **Accessories** > **I/O Device** (if available) > **I/O Device Setup**. This dialog box appears.



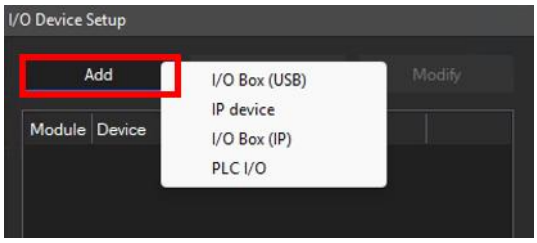
I/O Device Setup dialog box

Note: The **I/O Device** option only appears 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 (No. 9 in *Main Screen* in Chapter 1) and select **Configure** > **I/O Device Setup**.

6.1.1 Adding I/O Devices

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



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

- **I/O Box (USB):** Select if GV-VMS 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:** GV-VMS can remotely control the I/O devices connected to GV-IP Devices through network connection. Select the GV-IP Device with I/O devices installed and click the >> button.

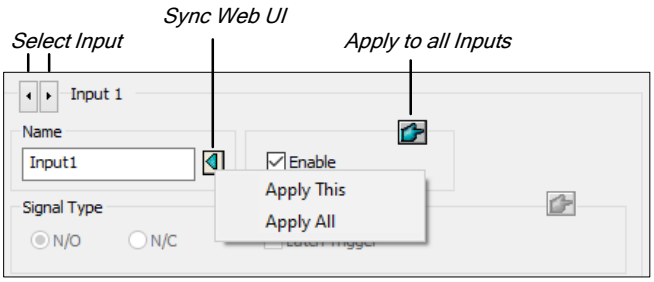
- **I/O Box (IP):** GV-VMS can remotely control the I/O devices connected to GV-I/O Box through network connection.
  1. Click the **Search** button to search for available devices under LAN or click the **Add** button to manually type the connection information of the device.
  2. Select the device 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 Input and Output Devices

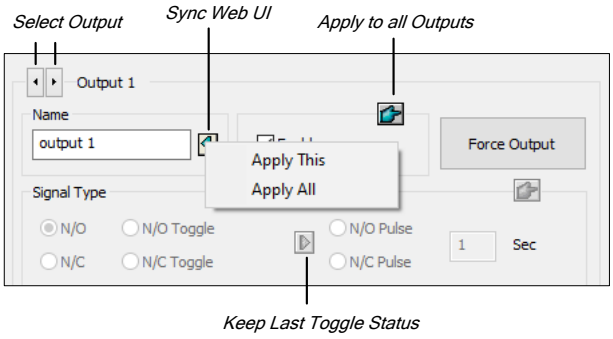
After adding the I/O device, enable the input and output devices. For GV-I/O Boxes connected through USB, you can configure the signal type on GV-VMS. For GV-IP Devices and GV-I/O Boxes connected through TCP/IP, you will have to configure the signal type on the device's Web interface.

[Input X] Click the **Arrow** buttons to select the input device 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: NO (normally open), NC (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**.

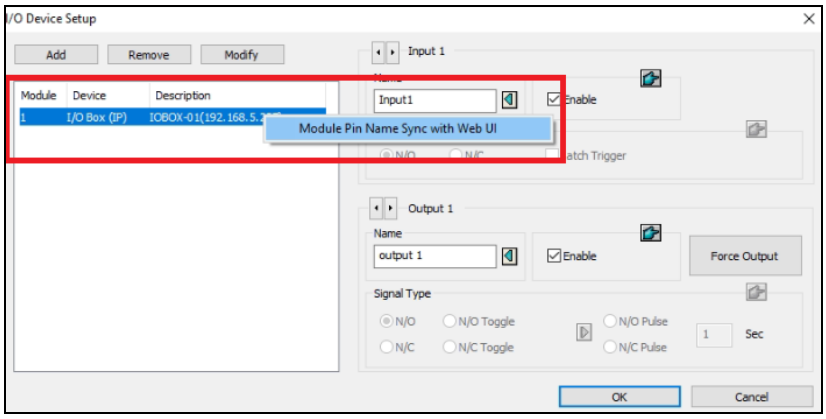


- **Name:** Name each output pin. Click the left Arrow button and select **Apply This** to sync the name of the specified output pin with that on the I/O device's Web interface. Optionally select **Apply All** to sync all names of the output pins with the ones on the I/O device's Web interface.
- **Force 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**.

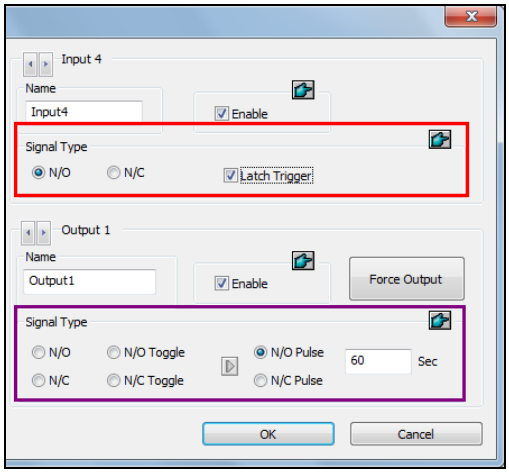


6.1.3 Latch Trigger

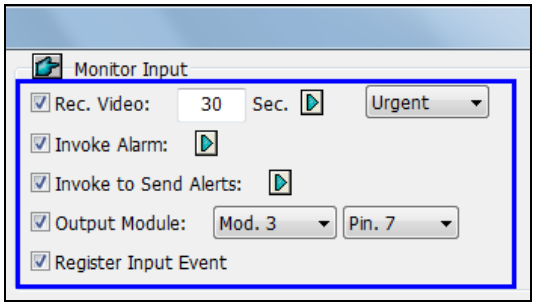
Instead of constant output alarm in N/O and N/C during the input trigger, the Latch Trigger option provides a momentary output trigger.

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

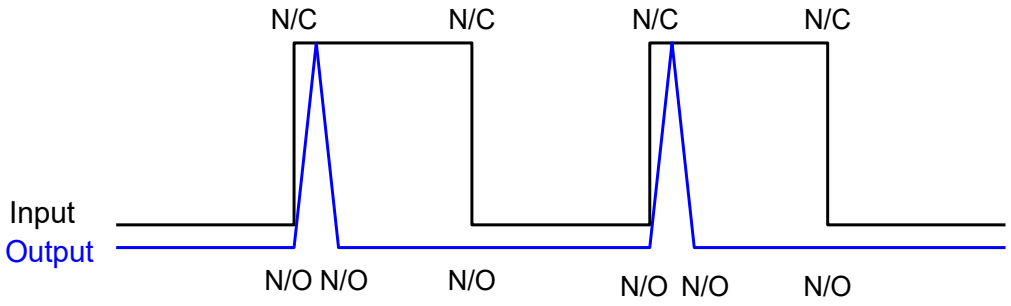
In the above scenario, Input 4 is set to N/O and Latch Trigger. When Input 4 is triggered:

- The camera starts recording for 30 seconds using the frame rate settings for Urgent Event and stops itself when the next input triggers (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.

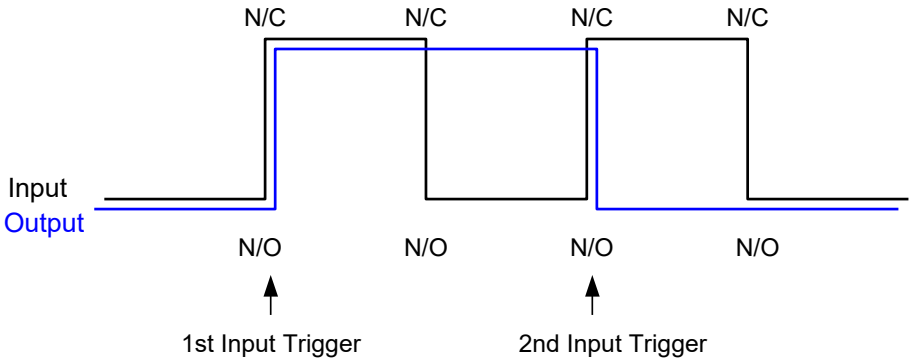
1. N/O (Normal Open) + Latch Trigger

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



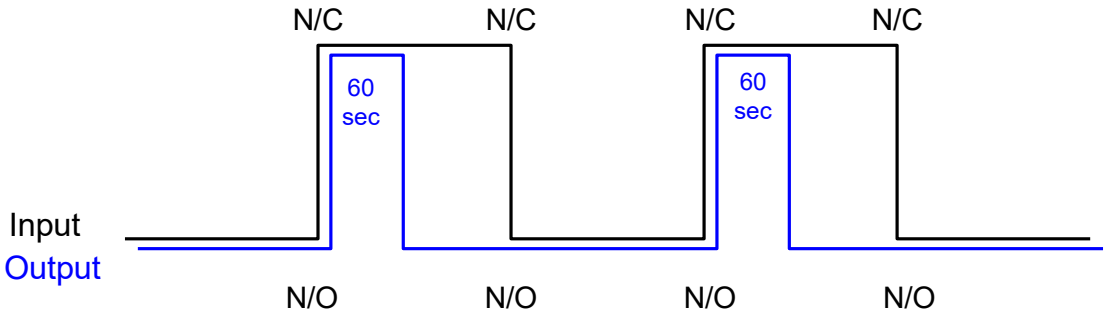
2. N/O Toggle + Latch Trigger

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.

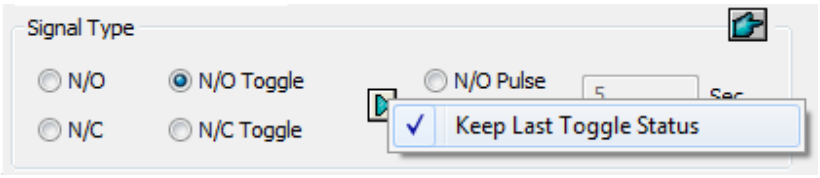


6.1.4 Keeping Last Toggle Status

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**.

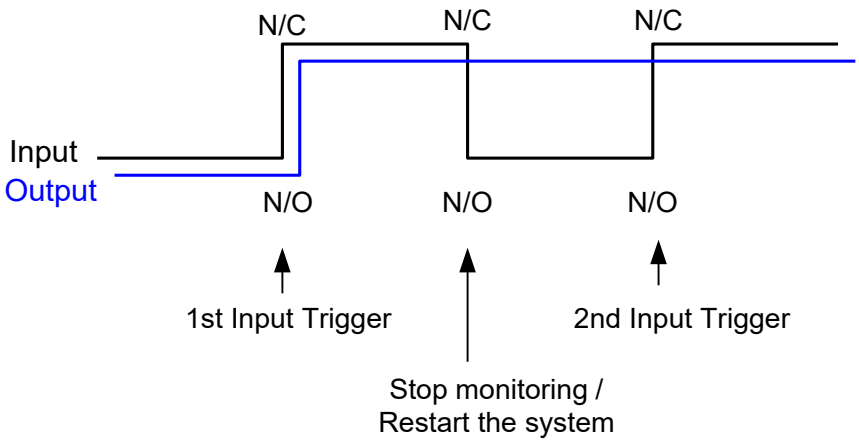


Application Example

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

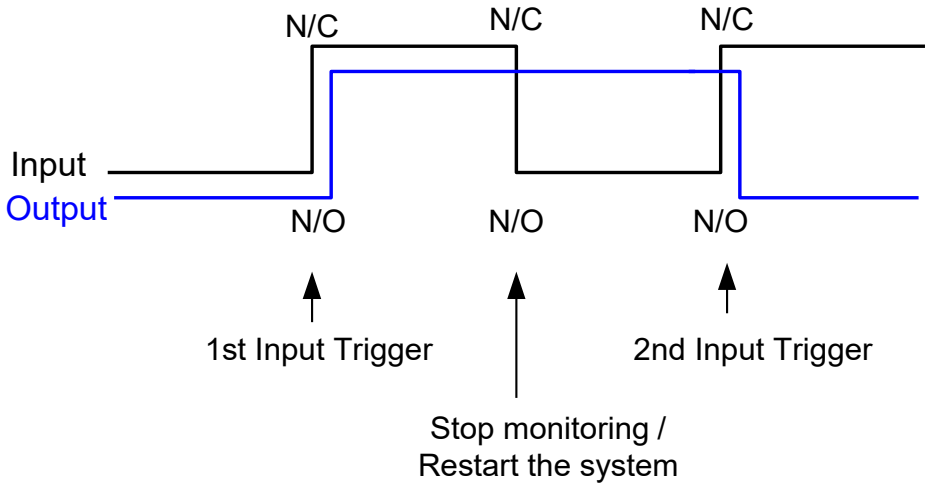
1. Input (N/O) + Output (N/O Toggle + Keep Last Toggle Status)

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



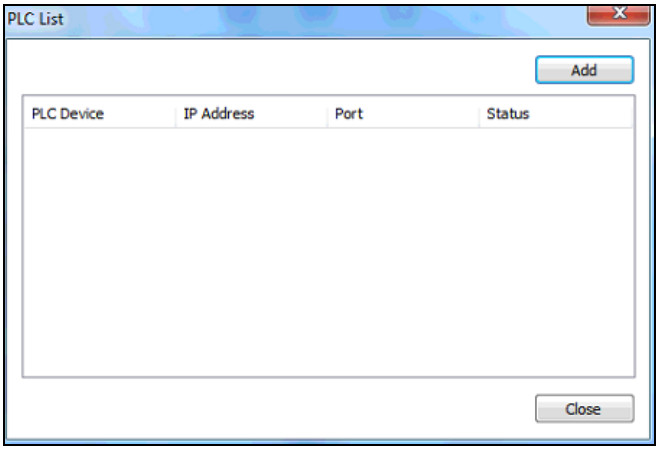
2. Input (N/O + Latch Trigger) + Output (N/O Toggle + Keep Last Toggle Status)

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.



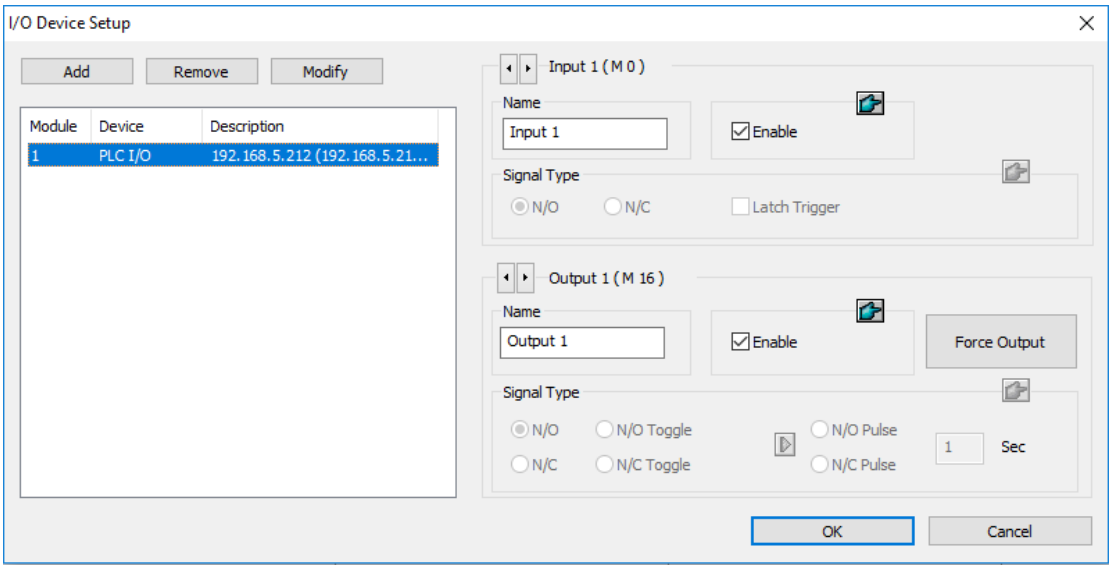
6.1.5 Setting Up PLC I/O devices

1. To connect a PLC I/O device to GV-VMS, click **Home** > **Toolbar** > **Configure** > **Accessories** > **PLC Device Setup**. This window appears.



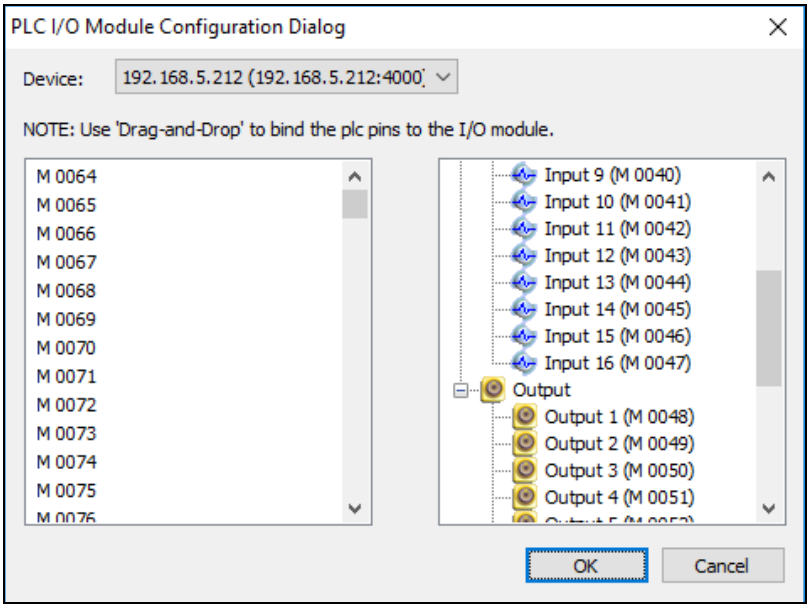
2. To add a PLC device, click the **Add** button, enter the following information: **Name**, **IP Address**, **Port**, **Password**, **M-Pin Range**, and **Connection Type**. The M-Pin Range supports up to 999,999 pins

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**.



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.

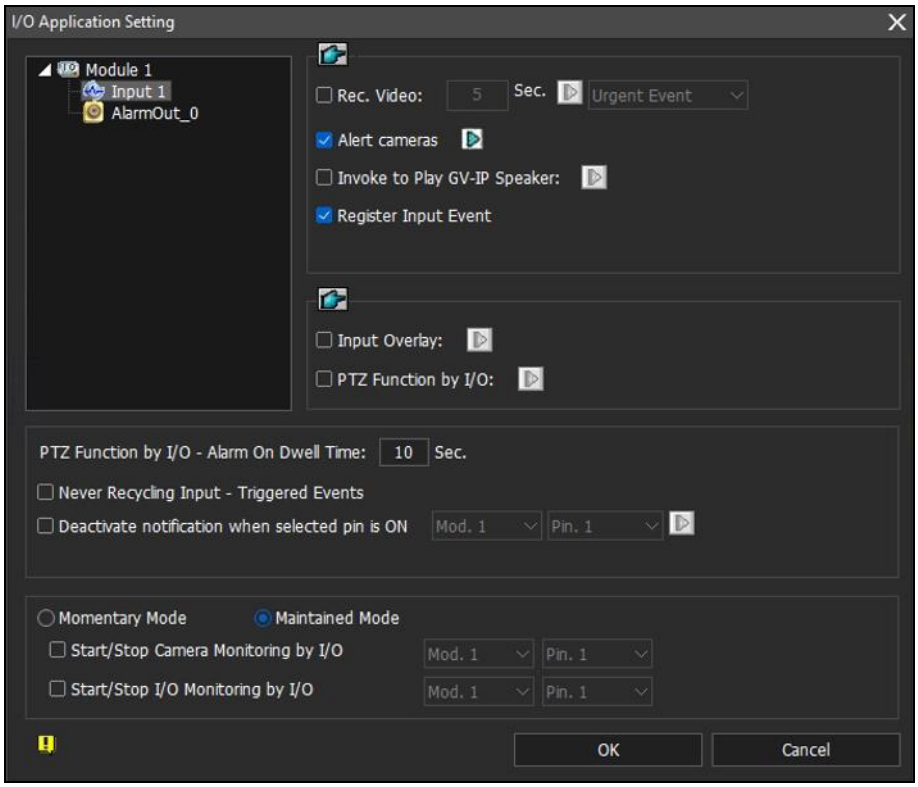
Note: Every Input/Output module can only support up to 16 pins. To use other pins, add more I/O modules.



6.2 Advanced I/O Applications

After adding I/O devices to GV-VMS, 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.



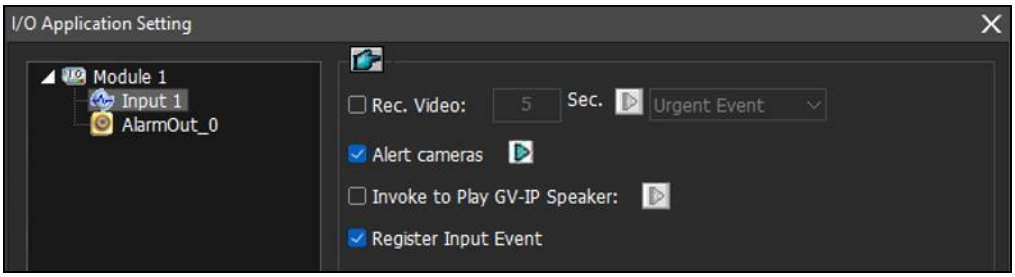
Note:

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 (No. 9 in *Main Screen* in Chapter 1) and select **Configure** > **I/O Application Setting**.

6.2.1 Setting Up Actions upon Input or Output 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 *Recording Settings* in Chapter 2.

- **Alert Cameras:** Sends e-mail notifications when triggered by an I/O device. Click the Arrow button to select the associated camera channels for video snapshots to be sent.

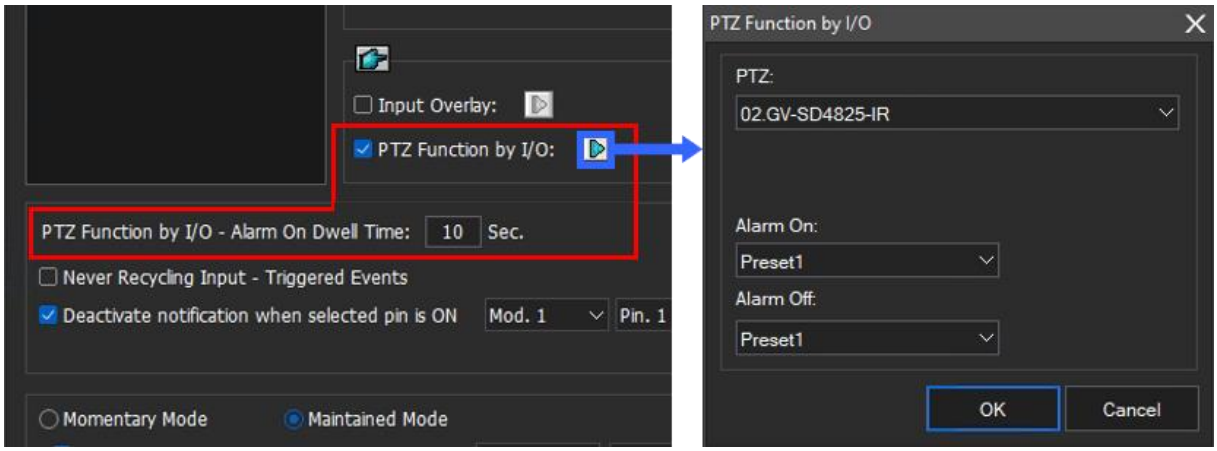
  To specify the recipient's e-mail address, you must enable **Send E-Mail** for an I/O Trigger event, and then complete the e-mail setup in **Send Alerts Approach Setup** (**Home** > **Toolbar** > **Configure** > **System Configure**). See *Setting Up E-Mail Notifications* in Chapter 1.

- **Invoke to Play GV-IP Speaker:** Activates the connected GV-IP Speaker to play audio files when triggered by an I/O device. Click the **Arrow** button to assign a different audio file and play mode for each GV-IP Speaker.

- **Register Input Event:** Registers the input trigger events into the System Log. Each event is labeled with ID, time, device name (camera or input), 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

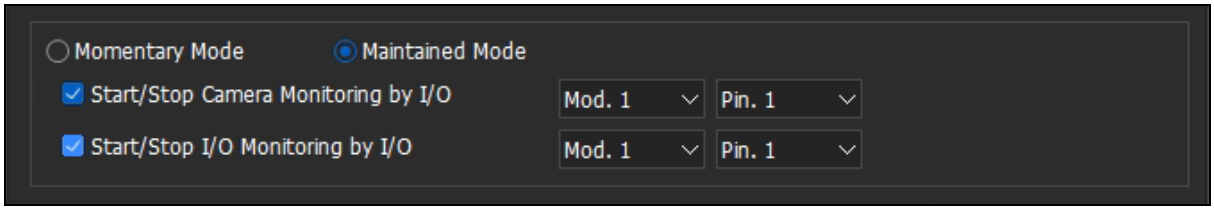
This feature allows you to move the PTZ camera to preset points when an input is triggered. Select an input number to be set up.



- **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



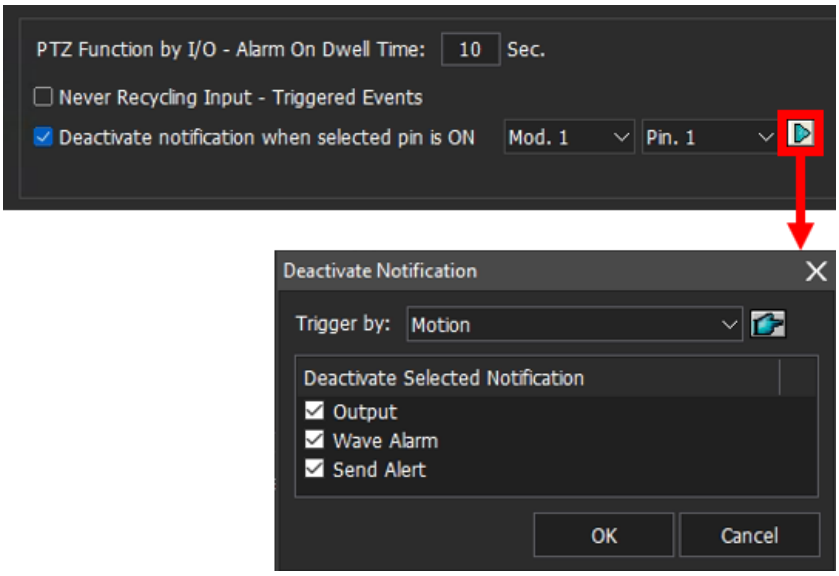
[Momentary Mode] Push button switches that are normally open and stay closed as long as the button is pressed. Momentary switches allow turn-on or turn-off from multiple locations.

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



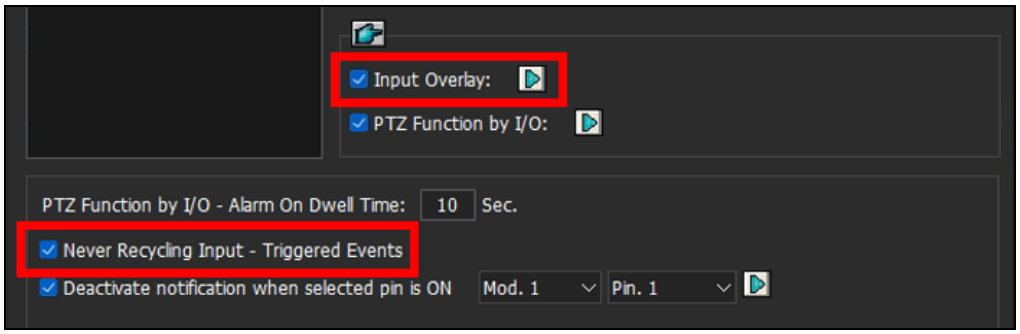
[Deactivate notification when selected pin is ON] When an assigned input module is activated, all designated alarms and alerts will be disabled. Assign an installed input module and a pin number for the application.

[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 and whether to recycle input-triggered events. Select an Input number to configure.



[Input Overlay] Overlays the name of an input device on live video for alert or to save the name to video files upon input trigger. To map cameras with the input device, click the **Arrow** button to select the camera.

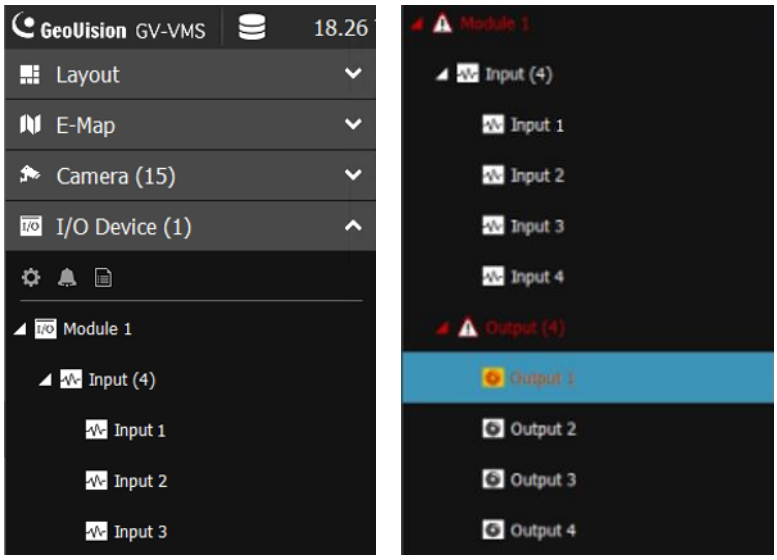
To overlay the name of a triggered input on live video, click **Home** > **Toolbar** > **Configure** > **Video Process**. In the dialog box that appears, select **Text Overlay Setting** in the Video Analysis dropdown list, select the camera, and click **Setting**. Select **Print on screen (Only for I/O 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.

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. In the Content List under **Home** (No. 9 in *Main Screen* in Chapter 1), click **I/O Device** to see the I/O devices added to GV-VMS. When an input or output is triggered, its icon will light up in the I/O Device list.

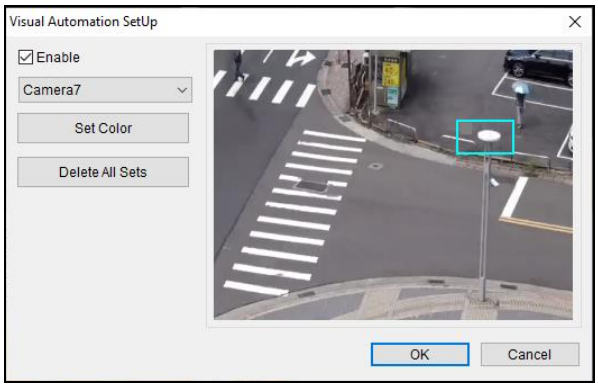


2. You can force the output device to be triggered by clicking its icon . Another way to trigger an output is to select an output and click the **Force Output** button .
3. To manually turn off a triggered output, right-click the triggered output in the list and click **Reset**.

6.4 Visual Automation

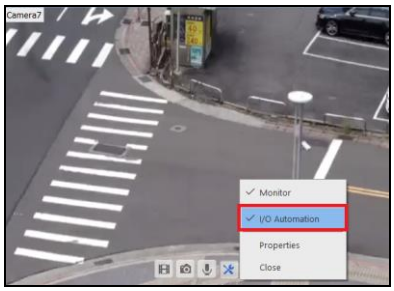
The Visual Automation helps you automate any electronic device by triggering the connected output. You can then intuitively click on the image of the electronic device, a light for example, to change its current state, e.g., turning the light on.

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 (No. 9 in *Main Screen* in Chapter 1) and select **Configure** > **Visual Automation Setting**.

Chapter 7

Remote Viewing 242

7.1 Remote Viewing Using a Web Browser 243

7.2 WebCam Server Settings 245

7.2.1 General Settings 245

7.2.2 Server Settings 247

7.2.3 JPG Settings 248

7.2.4 SDK Settings 249

7.2.5 UPnP Settings 251

7.2.6 Network Port Information 252

7.3 Mobile Service Settings 253

7.3.1 Basic Settings 254

7.3.2 QR Code Settings 255

7.3.3 RTSP Setting 256

7.4 Live View in Web Browsers 258

7.4.1 Functions on Live View 260

7.4.2 Picture-in-Picture View 261

7.4.3 Recording Video to File 262

7.4.4 Fisheye View 263

7.5 Remote Playback 264

7.6 Event List Query 265

7.7 Configure 267

7.7.1 Camera List 267

7.7.2 Server Information 268

7.7.3 Download Center 268

7.7.4 Connect to GV-Cloud 269

7.8 GV-Edge Recording Manager 271

7.9 Mobile Phone Applications 272

CHAPTER

7

Remote Viewing

With a Web browser, you can remotely view live video, and download and play back video files through GV-WebCam Server.

Remote Computer Requirements

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

OS	64-bit Windows 10 / 11 / Server 2016 / Server 2019 / Server 2022
CPU	6th Generation i5-6400, 3.3 GHz
Memory	8 GB RAM
OS HDD	80 GB
Network	TCP/IP
Web Browser	Chrome V137.0.7151.68 or later Microsoft Edge V137.0.3296.62 or later Mozilla Firefox V139.0.1 or later

Note: Some remote functions may not be supported by Web browsers without the plugin. To access the full functionality of GV-WebCam Server, please download the Web Plugin.

Internet Access Requirements

1. To connect to the Internet, GV-VMS must have an IP address or domain name provided by your Internet Service Provider (ISP). If the IP address is dynamic, you can use a DDNS service to automatically update the IP address for GV-VMS. For the service, see *Dynamic DNS* in Chapter 9.
2. If GV-VMS is behind a router or firewall, ensure the following ports are open to use GV-WebCam Server: HTTP Port (80), Command Port (4550), Data Port (5550), and Audio Port (6550).

7.1 Remote Viewing Using a Web Browser

GV-VMS includes a built-in GV-WebCam Server that allows you to remotely view and manage camera streams from GV-VMS using a Web browser. To access this feature, follow the steps below.

1. To enable GV-WebCam Server on GV-VMS, 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 GV-VMS system. The Webcam Login dialog box appears.
3. Type the User ID and password for a GV-VMS account.
4. Click **Login**.
5. To access the full functionality of the GV-WebCam Server, download the Web Plugin by clicking the link above the live view window.



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**.

To configure settings for GV-WebCam Server and other mobile services, see the following sections.

7.2 WebCam Server Settings

7.3 Mobile Service Settings

For details on the GV-WebCam Server user interface in Web browsers, see the following sections.

7.4 Live View in Web Browsers

7.5 Remote Playback

7.6 Event List Query

7.7 Configure

For details on other remote viewing applications, see the following sections.

7.8 GV-Edge Recording Manager

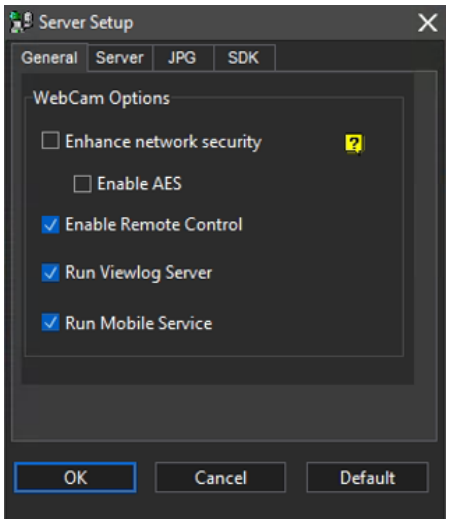
7.9 Mobile Phone Applications

7.2 WebCam Server Settings

To enable and configure the built-in WebCam Server, click **Home** > **Toolbar** > **Network** > **WebCam Server**.

7.2.1 General Settings

The General settings of GV-WebCam Server allow you to configure security features, remote access, and playback services for GV-WebCam Server.



WebCam Server Setup – General

- **Enhance Network Security:** If enabled, a word verification step is required for each GV-WebCam Server's login.
  - ⊙ **Enable AES:** Enable AES encryption to secure video transmission (for SDK integration only). To enable AES encryption for GV-WebCam Server, see Note 1 below.
- **Enable Remote Control:** Select to remotely configure the I/O devices through GV-WebCam Server.
- **Run Viewlog Server:** Enable remote playback of video files through GV-WebCam Server.
- **Run Mobile Service:** Enable the mobile function for connecting to GV-Eye and GV-Edge Recording Manager (Mac Version). Also, to remotely play back video files through GV-WebCam Server on Web browsers. For details, see *Mobile Service Settings* later in this chapter.

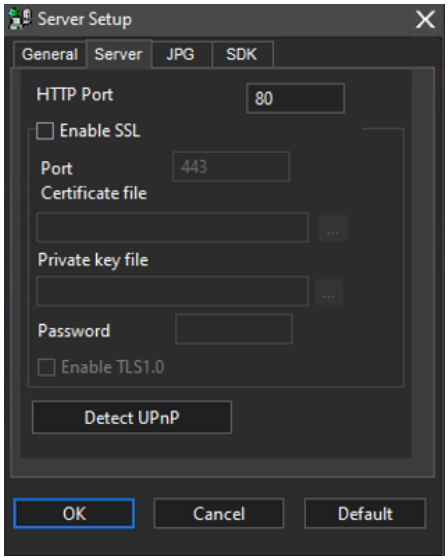
IMPORTANT: To remotely play back video files through GV-WebCam Server on Web browsers, both **Run ViewLog Server** and **Run Mobile Service** must be selected.

Note:

1. If you're opening GV-WebCam Server in a Web browser and want to secure the live stream between GV-VMS and GV-WebCam Server, you must enable AES Encryption in the Mobile Service settings. For details, see *Basic Settings* later in this chapter.
2. To limit the time a user can use GV-WebCam Server, go to the main page, click the **account ID** > **Password Setup** > **Local Account Edit.** Select a guest, user or power user, select the **Limit Connection Time** option in the WebCam/Mobile tab, and set the time limit. The time range is from 10 to 3600 seconds.

7.2.2 Server Settings

The Server settings allow you to configure GV-WebCam Server's network access, security protocols, and device discovery options.



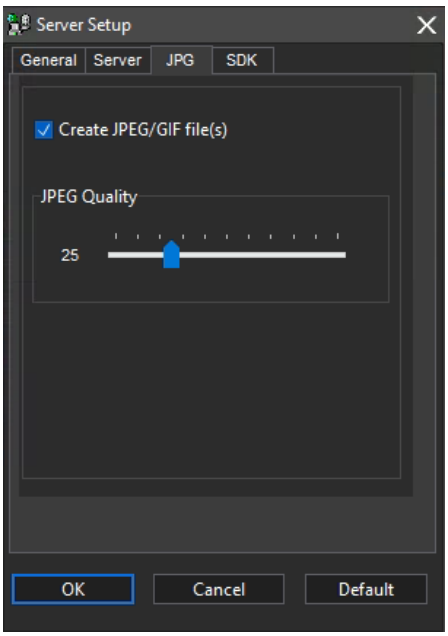
WebCam Server Setup – Server

- **HTTP Port:** Used to access the Internet. By default, it is 80.
- **Enable SSL:** Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of the 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 on 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 section.

7.2.3 JPG Settings

The JPG settings allow you to send JPEG or GIF files over the Internet.

Note: The JPG settings are used for SDK integration. For details on SDK integration, see the following subsection *SDK Settings*.



- **Create JPEG/GIF file(s):** Allows SDK-integrated applications to retrieve JPEG images. You can set the image quality – higher values improve image clarity but increase file size.

7.2.4 SDK Settings

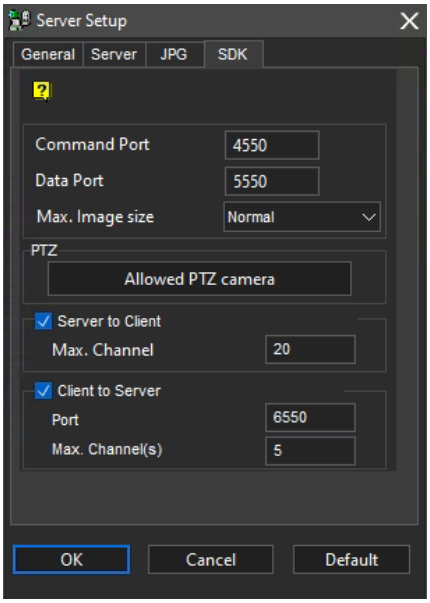
This section introduces settings specifically for SDK integration. These settings are not used by GV-WebCam Server and will not affect how GV-WebCam Server operates. Instead, they are used exclusively by 3rd-party applications developed using the GV-VMS SDK to access live video and audio streams and interact with GV-VMS remotely.

Connecting Audio Devices

Through the SDK, 3rd-party systems can access live audio at a remote site and transmit audio back to the GV-VMS server site when necessary. Before enabling these functions, ensure all the necessary hardware is in place:

1. To record audio, check that the connected IP camera has either a built-in audio function or an external microphone connected.
2. Make sure the sound card is already installed in the computer. Connect a multimedia speaker to the audio output of the computer's sound card to receive audio from the remote site.
3. Connect a desktop microphone to the input of the audio extension card (or cable) to send audio to the remote site.

Video and Audio Setup



- **Command Port:** Used by 3rd-party systems to access GV-VMS via SDK. By default, it is 4550.
- **Data Port:** Used to transfer video/audio data over the Internet through SDK integration. By default, it is 5550.

- **Max. Image size:** Select a maximum resolution allowed for SDK-based remote access. The default resolution 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:** Grants SDK control of specific PTZ cameras. Click the button and select which PTZ cameras are available for SDK-based remote control.

[Server to Client] Allows SDK-integrated clients to receive live audio from GV-VMS.

- **Max. Channel(s):** Specify the maximum number of channels allowed, with the upper limit of 40 channels.

[Client to Server] Allows SDK-integrated clients to transmit audio back to GV-VMS.

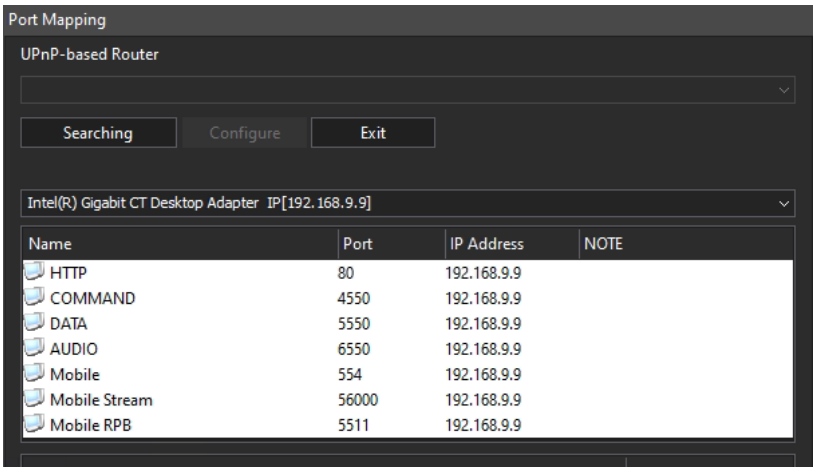
- **Port:** The default audio port is 6550.
- **Max. Channel(s):** Specify the maximum number of channels allowed for audio input, with the upper limit of 20 channels.

7.2.5 UPnP Settings

GV-WebCam Server supports UPnP (Universal Plug and Play) technology to automatically configure ports on the router connected to the GV-VMS computer's network. To use this feature, UPnP must be enabled both on the GV-VMS computer's operating system and on that local router.

To enable UPnP:

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



3. Click **Searching** to scan for UPnP-enabled routers on the local network.
4. If your server is connected to multiple routers, select one from the UPnP-based Router dropdown list.
5. If your server is connected to multiple network adapters, select one from the dropdown list under the Searching button.
6. Click **Configure** to automatically configure the communication ports on the selected router.

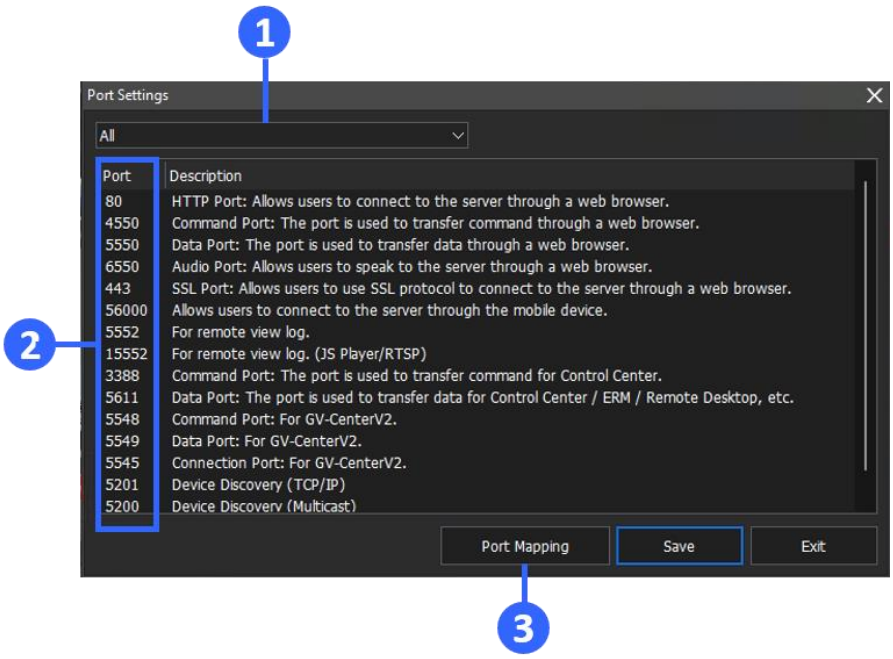
Note: If you are not using the default ports, modify the related ports in the Server and SDK tabs of the WebCam Server Setup dialog box (see the *Server Settings* subsection above and the *SDK Settings* subsection later in this section, respectively) and then click **OK**. Re-open the dialog box and follow the above steps to configure the router.

Tip: To enable UPnP, you can also click **Home** > **Toolbar** > **Network** > **Network Port Information**, and then select **Port Mapping**.

7.2.6 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*.

7.3 Mobile Service Settings

The Mobile Service enables remote video streaming from GV-VMS to other GV-Applications, including:

- GV-Eye
- GV-Edge Recording Manager (Mac Version)
- Multicast streaming via GV-Control Center

To access Mobile Service, click **Home** > **Toolbar** > **Network** > **Mobile Service**.

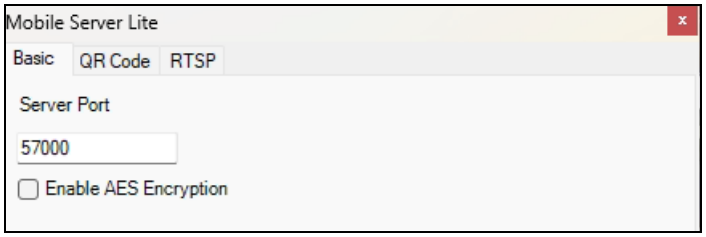
For details on connecting GV-Eye to GV-VMS, see *Connecting via GV-Relay QR Code* in Chapter 4 of the *GV-Eye Installation Guide*.

For details on connecting GV-Edge Recording Manager (Mac Version) to GV-VMS, see *Adding Hosts* in Chapter 6 of the *GV-Edge Recording Manager Quick Start Guide*.

For details on configuring multicast on GV-Control Center, see *Multicast Settings* in Chapter 9 of the *GV-Control Center User's Manual V4*.

7.3.1 Basic Settings

The Basic settings allow you to alter the server port and enable AES encryption.



- **Server Port:** Keep Mobile Server port 56000 as default until a modification is required to correlate with a change in the connected application.
- **Enable AES Encryption:** Enable AES encryption to secure video transmission. Additionally, if you're opening GV-WebCam Server in a Web browser and want to secure the live stream between GV-VMS and GV-WebCam Server, you must enable AES Encryption in the Mobile Service settings.

Note: The AES Encryption function is compatible with GV-Edge Recording Manager (V1.3.0.0 or later), GV-Control Center (V3.5.0.0 or later), and GV-Eye (V2.5 or later).

7.3.2 QR Code Settings

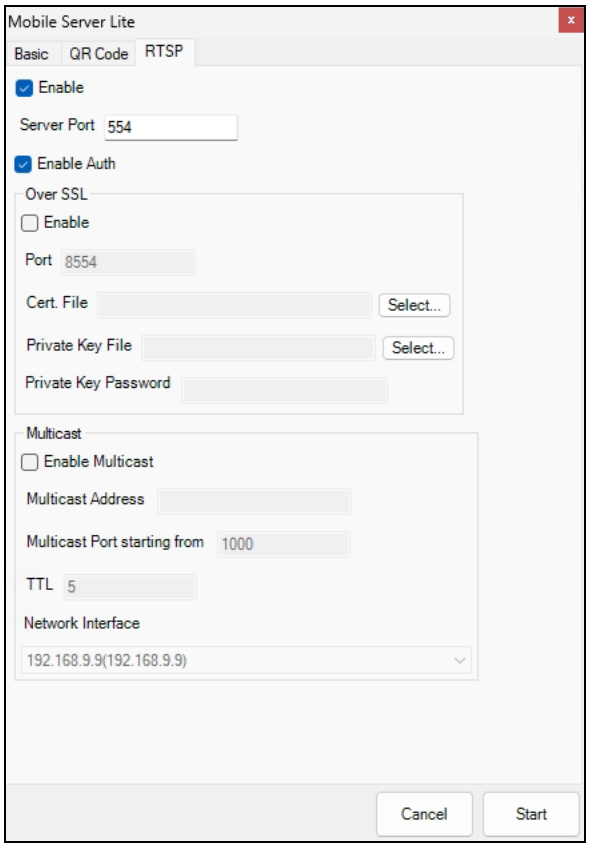
The QR Code settings enable connection to the GV-Eye mobile app. For details, see *Connecting via GV-Relay QR Code* in Chapter 4 of the *GV-Eye Installation Guide*.



7.3.3 RTSP Setting

To allow 3rd-party software to connect to GV-VMS through the RTSP protocol for accessing live video streams, follow the steps below.

Note: RTSP over SSL can currently only be played using FFmpeg. VLC does not support RTSP over SSL.



1. Select **Enable** to activate the RTSP service.
2. If necessary, modify the default **Server Port** (554), which is the port used for RTSP communication.
3. To enhance security, select **Enable Authentication**. Users will then be required to type the GV-VMS username and password when accessing the RTSP stream.
4. For an additional layer of security, select **Enable SSL** to encrypt the RTSP connection using the Secure Sockets Layer (SSL) protocol.
   - **Port:** If necessary, modify the default **SSL Port** (8554) used for RTSP over SSL.
   - **Cert. File:** Click **Select** to upload your own SSL certificate, either self-generated or issued by a certificate authority.
   - **Private Key File:** Click **Select** to upload the corresponding private key file.

- **Private Key Password:** Type the password if the private key file is encrypted.

5. Click **Start**. GV-VMS will begin broadcasting live video streams to 3rd-party software via RTSP.

When playing RTSP over SSL with FFmpeg, use the RTSP commands below to connect:

No ID and password required:

rtsp://<IP of GV-VMS>:<SSL Port>/<CamNo_StreamNo>

For example, **rtsp:// 192.168.3.111:8554/cam1_stream2**

ID and password required:

rtsp://<ID>:<Password>@<IP of GV-VMS>:<SSL Port>/<CamNo_StreamNo>

For example, **rtsp://admin:1234@192.168.3.111:8554/cam1_stream2**

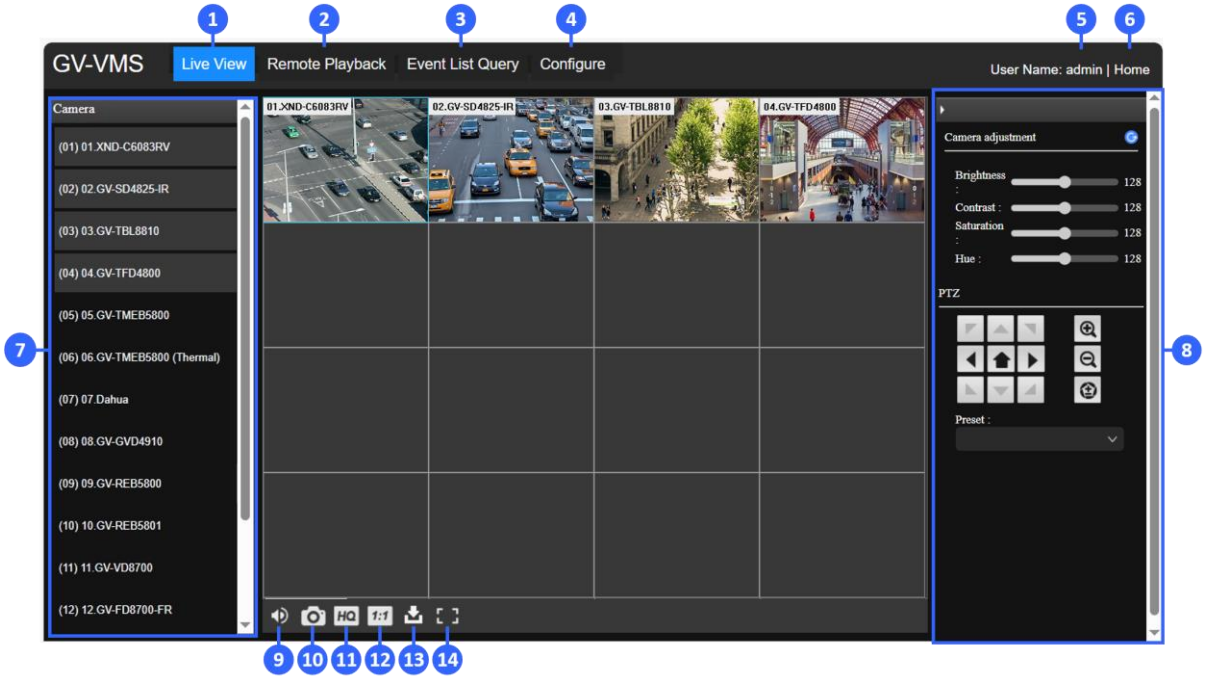
7.4 Live View in Web Browsers

After logging in to GV-WebCam Server from a Web browser, you can see the live view from GV-VMS, displaying up to 16 channels at a time and supporting up to 256 channels in total.

To display the cameras on the live view, follow the steps below.

1. Optionally, select an empty camera channel. A blue border appears, indicating the selection.
2. Select a camera from the camera list.
   - If a channel is selected, the camera's live view appears on that designated channel.
   - If no channel is selected, the camera's live view appears in the next available channel based on the layout sequence (left to right, top to bottom).

Note: To close a camera channel, click the corresponding camera in the camera list again.



No.	Name	Description
1	Live View	Shows the live view of cameras connected to GV-VMS. See the following subsections.
2	Remote Playback	Shows a timeline of recorded events for playback. See *Remote Playback* later in this chapter.

3	Event List Query	Allows users to remotely search for an event by device, time range, or event subtype. See *Event List Query* later in this chapter.
4	Configure	Accesses the *Camera List*, *Server Information*, and *Download Center*, where users can download optional viewing programs to the local PC. Also allows users to connect to GV-Cloud. See *Configure* later in this chapter.
5	Login ID	Shows the account username for accessing GV-VMS.
6	Home	Logs out and returns to the Login Page.
7	Camera List	Allows users to select the desired camera for display.
8	Control Panel	Click the button on the right side of the live view to expand the Control Panel, which brings up these options: ● **Camera Adjustment:** Configure brightness, contrast, saturation, and hue. ● **PTZ:** Move the camera view in any direction by clicking on a desired direction. For details on the PTZ control panel, see *Accessing PTZ Control Panel and Auto Functions* in Chapter 1.
9	Audio	Click to access live audio from the surveillance site.
10	Snapshot	Takes a snapshot of the displayed live view.
11	Quality	Switches the video to high quality (HD).
12	Zoom In	Enables the Picture in Picture (PIP) view, allowing users to zoom in or out on the live view. See *Picture-in-Picture View* later in this section.
13	Record	Saves video to a local computer in .avi format. See *Recording Video to File* later in this section.
14	Full Screen	Switches the live view to full screen.

7.4.1 Functions on Live View

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	After clicking **Zoom In** on the toolbar below the live view, use the mouse scroll to zoom in or out.

Right-click the live view of the desired camera to access the following options, if they are enabled or supported.

Note: You must download and install the Web Plugin to access all available features.

- **Snapshot:** Takes a snapshot of the selected live view.
- **Microphone:** Enables two-way audio by allowing you to speak to the surveillance site.
- **Fisheye:** Switches into the fisheye view. See *Fisheye View* later in this section.
- **Object Detection:** Displays object detection rectangles on the live view.
- **Information:** Displays video details, including codec, resolution, bitrate, and frame rate (FPS).
- **Fisheye Options:** Appears when the Fisheye option is selected. See *Fisheye View* later in this section.
- **Mega Pixel Settings:** Appears when the **Zoom In**  option in the toolbar is enabled. See the following subsection *Picture-in-Picture View*.

7.4.2 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. To enable the PIP view, select the desired camera from the camera list, and then click **Zoom In** on the toolbar below the live view. An inset window of the camera view appears in the live view.



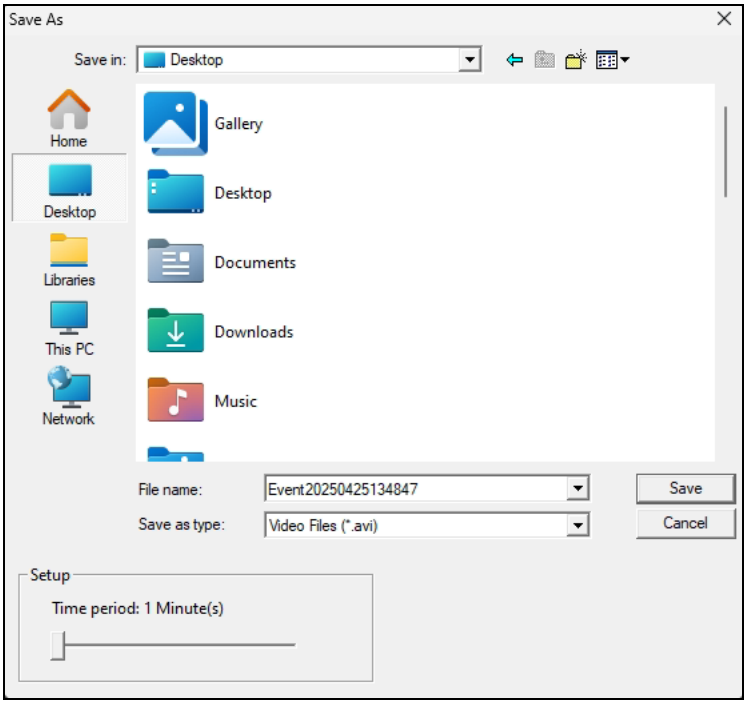
2. Move the navigation box around in the inset window to have a close-up view of the selected area. You can adjust the size of the navigation box if needed.
3. Drag the inset window to adjust its location on the live view if needed.
4. To change the color of the focus area, right-click the live view and select **Mega Pixel Settings** > **Set Color of Focus Area**.
5. To hide the PIP window, right-click the live view and select **Mega Pixel Settings** > **Hide PIP Window.**
6. To exit the PIP view, click **Zoom In** on the toolbar below the live view again.

7.4.3 Recording Video to File

You can manually record video and save it as an .avi file. To access this feature, follow the steps below.

Note: You must download and install the Web Plugin to access this feature.

1. Select the desired camera from the camera list, and then click **Record** on the toolbar below the live view. The file window appears.



2. Rename the video and choose the file destination.
3. The recording is automatically split into multiple files based on the selected duration. For example, with a 1-minute setting, a 3-minute recording will result in three separate files. To adjust the duration, drag the **Time Period** slider at the bottom left of the window and choose a duration between 1 and 5 minutes.
4. Click **Save** to begin the recording.
5. To stop the recording, click **Record** again on the toolbar below the live view. The video will be saved to your selected destination.

7.4.4 Fisheye View

With the Fisheye option enabled, a single camera can cover all angles of a location. The circular fisheye view can be dewarped into four view modes, and you can drag PTZ views to different angles. For details, see *Fisheye View* in Chapter 2.

To set up Fisheye View in GV-WebCam Server for Web browsers, follow the steps below.

1. To display the dewarped view, select the desired camera (circular source image) from the camera list, right-click its live view, and then select **Fisheye**.
2. To change the dewarped settings, right-click the camera live view, and then select **Fisheye Options** to access fisheye-related functions. For details, see Step 3 in *Setting Up Fisheye View* in Chapter 2.

7.5 Remote Playback

With the Remote Playback (RPB) function on GV-WebCam Server, you can play back the recorded files of the connected GV-VMS.

Note: To access the functions listed in this section, download the Web Plugin.

To allow remote access to GV-VMS:

- Ensure GV-WebCam Server is activated on GV-VMS, with **Run ViewLog Server** enabled in the General tab of the WebCam Server Setup dialog box (see "WebCam Server Setup – General" in *General Settings* earlier in this chapter).

To play back recordings, follow the steps below.

1. Select **Remote Playback** from the top menu (see No. 2 in *Live View in Web Browsers* earlier in this chapter). The Remote Playback page appears.
2. Select a camera from the camera list. The camera's live view appears in the next available channel based on the layout sequence (left to right, top to bottom).
3. Select a date and move the cursor to the color blocks on the timeline. Click the **Play** button to start. For details on the control panel, see *ViewLog Control Panel* in Chapter 4.
4. To access additional playback features, click **Tools** at the bottom right of the camera channel. You can enable / disable text overlay and object detection rectangles, and prioritize sub stream display during playback (see *Multi-Channel Playback* at the beginning of this manual).



Note: To close a camera channel, click the corresponding camera in the camera list again.

7.6 Event List Query

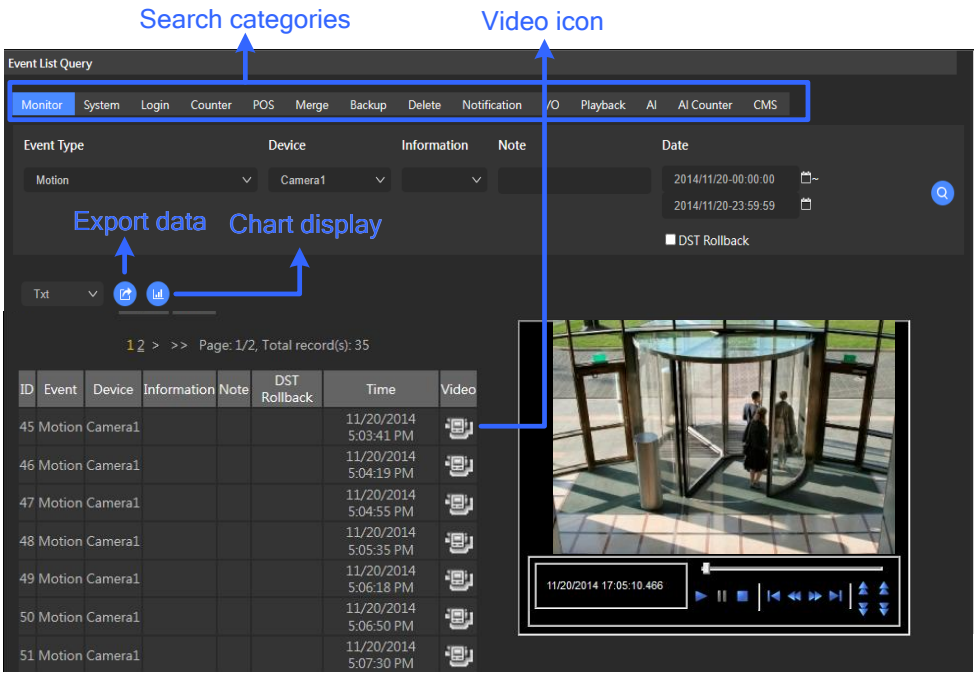
The Event List Query function on GV-WebCam Server allows you to remotely search for an event by defining event type and time. The search results can be displayed in text form or in a chart. You can also play back events instantly from the search results.

To allow remote access to GV-VMS:

- Ensure that GV-WebCam Server is activated on GV-VMS, with **Run ViewLog Server** enabled in the General tab of the WebCam Server Setup dialog box (see "WebCam Server Setup – General" in *General Settings* earlier in this chapter).

To remotely play back events, follow the steps below.

1. Select **Event List Query** from the top menu (see No. 3 in *Live View in Web Browsers* earlier in this chapter). The Event List Query page appears.
2. On the top, select one of the following search categories: **Monitor**, **System**, **Login**, **POS**, **Merge**, **Backup**, **Delete**, **Notification**, **I/O**, **Playback**, **AI Event**, **AI Counter**, and **CMS**. Note that these categories are based on those of System Log in the Main System, except for AI Event, which can only be viewed in Event List and AI Query 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 the **Query** button . The search results will be displayed in text form.



5. To play back the attached video, click the **Video** icon . For more playback features, right-click on the video image.

6. To export the search results, select one of the formats and click the **Export** icon.

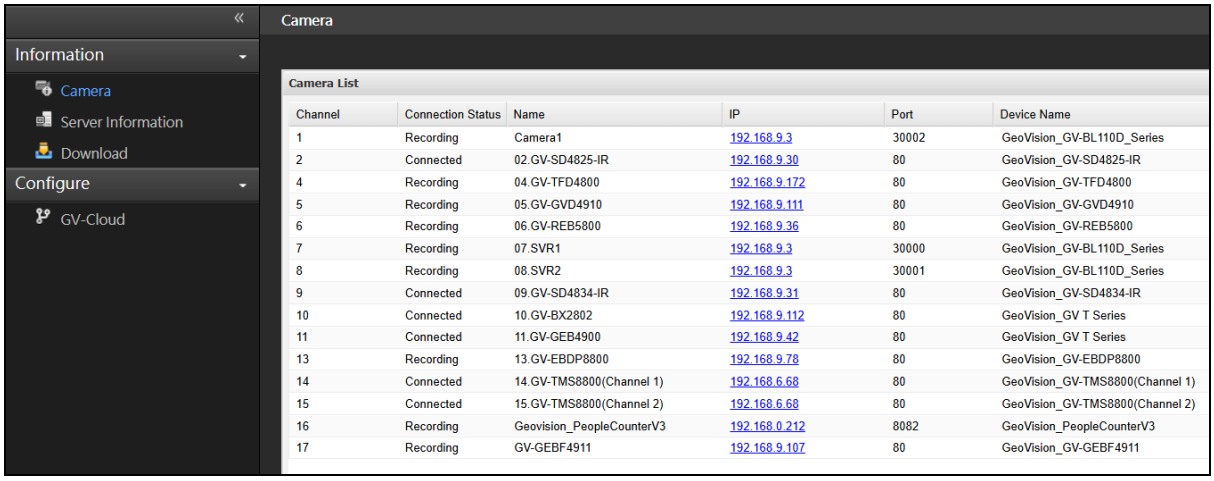
7. To graph the search results, click the **Chart** icon.

7.7 Configure

To access the configuration settings in the GV-WebCam Server, select **Configure** from the top menu (see No. 4 in *Live View in Web Browsers* earlier in this chapter). The Configure page appears.

7.7.1 Camera List

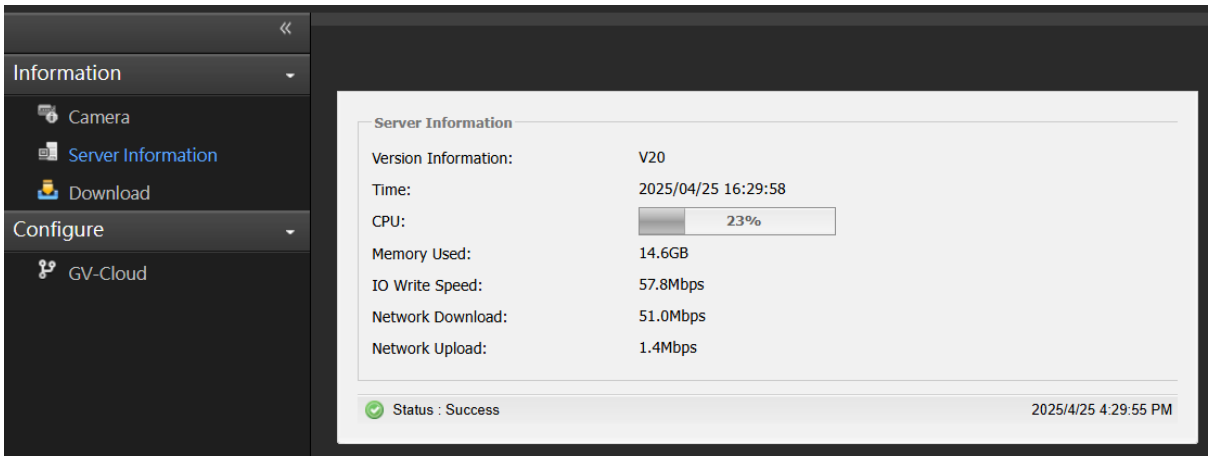
To view the camera connection status, name, IP, and port number, select **Information > Camera** from the left menu. The Camera page appears.



Channel	Connection Status	Name	IP	Port	Device Name
1	Recording	Camera1	192.168.9.3	30002	GeoVision_GV-BL110D_Series
2	Connected	02.GV-SD4825-IR	192.168.9.30	80	GeoVision_GV-SD4825-IR
4	Recording	04.GV-TFD4800	192.168.9.172	80	GeoVision_GV-TFD4800
5	Recording	05.GV-GVD4910	192.168.9.111	80	GeoVision_GV-GVD4910
6	Recording	06.GV-REB5800	192.168.9.36	80	GeoVision_GV-REB5800
7	Recording	07.SVR1	192.168.9.3	30000	GeoVision_GV-BL110D_Series
8	Recording	08.SVR2	192.168.9.3	30001	GeoVision_GV-BL110D_Series
9	Connected	09.GV-SD4834-IR	192.168.9.31	80	GeoVision_GV-SD4834-IR
10	Connected	10.GV-BX2802	192.168.9.112	80	GeoVision_GV T Series
11	Connected	11.GV-GEB4900	192.168.9.42	80	GeoVision_GV T Series
13	Recording	13.GV-EBDP8800	192.168.9.78	80	GeoVision_GV-EBDP8800
14	Connected	14.GV-TMS8800(Channel 1)	192.168.6.68	80	GeoVision_GV-TMS8800(Channel 1)
15	Connected	15.GV-TMS8800(Channel 2)	192.168.6.68	80	GeoVision_GV-TMS8800(Channel 2)
16	Recording	Geovision_PeopleCounterV3	192.168.0.212	8082	GeoVision_PeopleCounterV3
17	Recording	GV-GEBF4911	192.168.9.107	80	GeoVision_GV-GEBF4911

7.7.2 Server Information

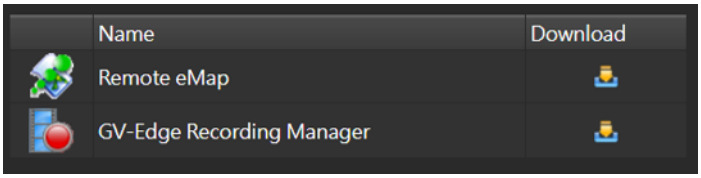
To view the server information, including version information, time, CPU usage, memory usage, I/O write speed, network download speed, and network upload speed, select **Information > Server Information** from the left menu. The Server Information page appears.



7.7.3 Download Center

The Download Center allows you to download GV-Remote E-Map and GV-Edge Recording Manager. To download the applications, follow the steps below.

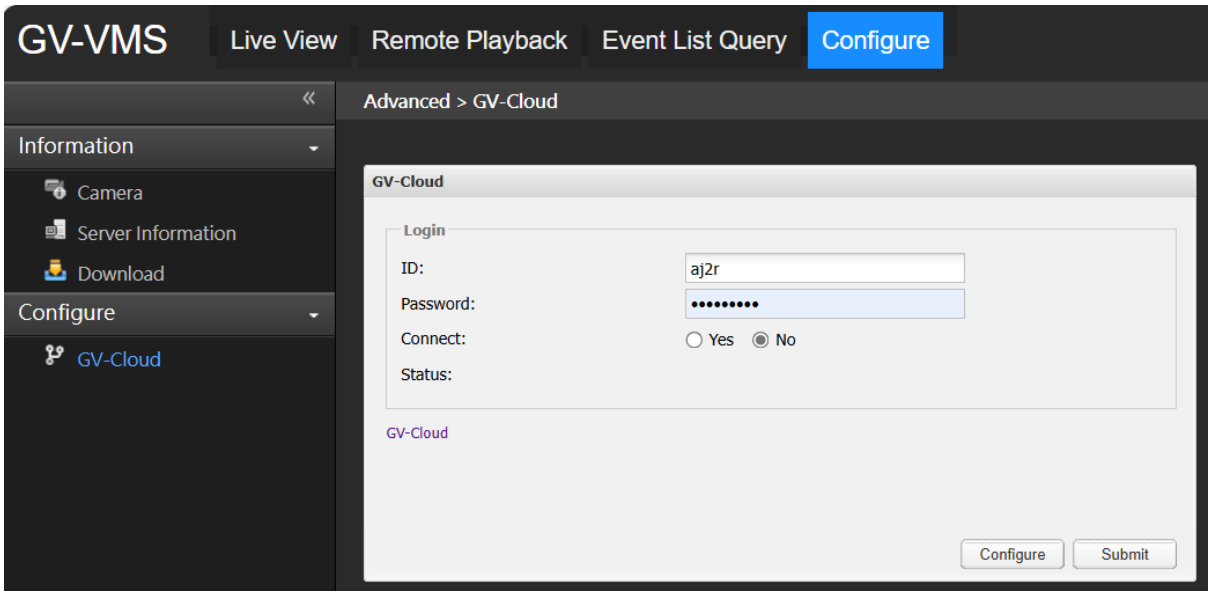
1. Select **Information > Download** from the left menu. The Download page appears.



2. Click **Download** next to your desired application.
3. Follow the on-screen instructions to install the programs. When the installation is complete, the message "*Install Complete*" will be displayed.

7.7.4 Connect to GV-Cloud

To connect GV-VMS to GV-Cloud via GV-WebCam Server, select **Configure > 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.

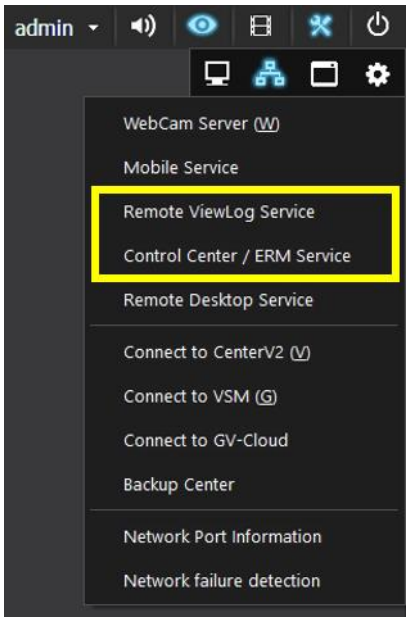
7.8 GV-Edge Recording Manager

GV-Edge Recording Manager combines live monitoring and remote control of GeoVision IP devices and software into a single management interface. For details on GV-Edge Recording Manager, visit the GeoVision Website:

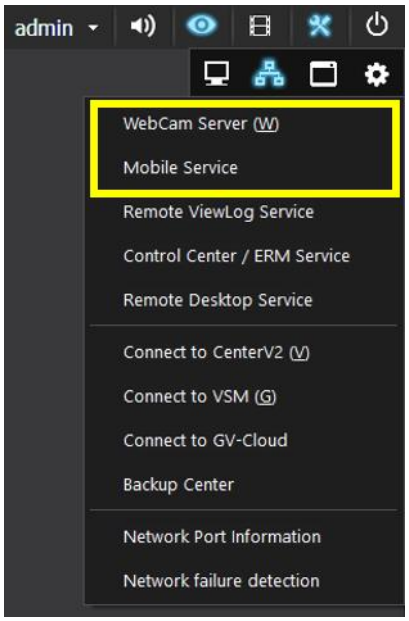
- GV-Edge Recording Manager (Windows Version)
- GV-Edge Recording Manager (Mac Version)

In GV-VMS, go to **Home** > **Toolbar** > **Network**, and ensure the following services are enabled:

- **GV-Edge Recording Manager (Windows Version):** Make sure that **Remote ViewLog Service** and **Control Center / ERM Service** are enabled.
- **GV-Edge Recording Manager (Mac Version):** Make sure that **WebCam Server** and **Mobile Service** are enabled.



For GV-ERM (Windows)



For GV-ERM (Mac)

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 GV-VMS and GV-Edge Recording Manager through AES encryption, see *Mobile Service Settings* earlier in this chapter.
3. The **Substream FIFO** function under CMS Service can reduce GV-VMS's CPU usage and improve streaming quality at the cost of increased bandwidth. The number of remote connections allowed from a single GV-VMS is determined on the amount of bandwidth available. To access CMS Service, first enable it by clicking **Network** > **Control Center / ERM Service**, and click the **CMS Service** icon from the Windows taskbar at the bottom. To locate the Substream FIFO function, click the **Configure** button

7.9 Mobile Phone Applications

With a smartphone, you can access live view and play back recordings from GV-VMS using the GV-Eye mobile app. GV-Eye can be downloaded from the App Store or the Android Market.

For details, see the *GV-Eye Installation Guide*.

Chapter 8

E-Map Application 274

8.1 The E-Map Editor 274

8.1.1 The E-Map Editor Window 275

8.1.2 Creating an E-Map 277

8.1.3 Creating an E-Map for a Remote Host 280

8.2 Starting E-Map 281

8.2.1 Setting Up Popup Map 282

8.3 3D E-Map Display 283

8.3.1 3D E-Map Display 283

8.3.2 Utilizing 3D E-Map Icons 284

8.4 Remotely Accessing E-Map 286

8.4.1 The Remote E-Map Window 287

8.4.2 Accessing E-Maps of Multiple Hosts 289

8.4.3 Configuring the Remote E-Map 290

8.4.4 Viewing Event List and Playing Back Videos 292

8.5 E-Map Server 293

8.5.1 Installing E-Map Server 293

8.5.2 The E-Map Server Window 294

8.5.3 Setting Up E-Map Server 295

8.5.4 Connecting to E-Map Server 295

CHAPTER 8

E-Map Application

The E-Map displays the monitoring area on an electronic map, by which the operator can easily locate the cameras, sensors, and alarms triggered by motion or I/O devices.

The application is available through two programs: **GV-E-Map Editor**, which is included with the installation of GV-VMS, and **GV-E-Map Server**, which is intended for use on a designated server.

Note: GV-VMS V20 does not currently support GV-E-Map Server.

8.1 The E-Map Editor

The E-Map Editor allows you to import a floor plan in .bmp, .gif, or .jpeg formats, and use the icons of cameras and I/O devices to customize a map.

8.1.1 The E-Map Editor Window

The E-Map Editor comes with the installation of GV-VMS. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **E-Map Editor**. The E-Map Editor window appears.



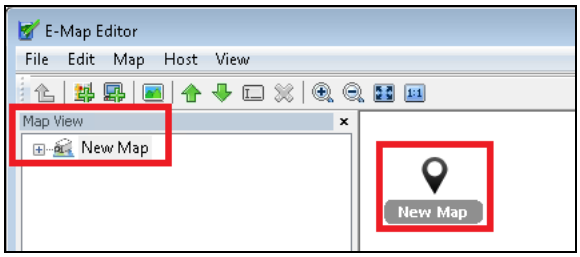
The controls in the E-Map Editor window:

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	Zoom In	Enlarges the Map View.
8	Zoom Out	Diminishes the Map View.
9	Fit to Screen	Adjusts the Map View to fit the current size of the window.
10	Actual Size	Displays the actual size of 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 an E-Map

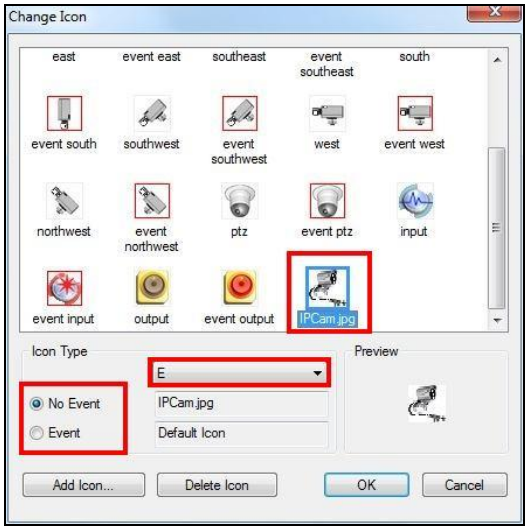
1. To create an E-Map, click **Add Map** on the toolbar. A New Map file is created in Map View and the Floor Plan window separately.



2. Click the **New Map** file in Map View, and click the **Load Map** button (No. 4 in *The E-Map Editor Window* earlier in this chapter) to import a graphic file. The file opens in the Floor Plan window.
3. Drag and drop the icons from Host View (No. 13 in *The E-Map Editor Window* earlier in this chapter) 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.

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 a 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.



6. Click **File** in the window menu and select **Save to VMS** to save the file to the GV-VMS folder, or select **Save to File** to save the file to the desired path.

Advanced Settings

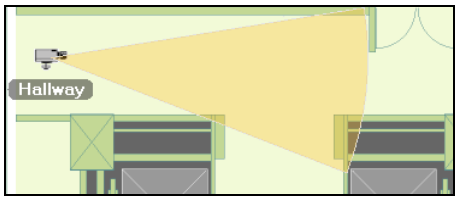
Optionally, you can have the following settings on your created E-Map.

Note: The changes in the orientation of camera icons will not be reflected on the 3D E-Map.

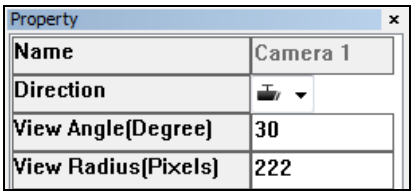
A. View Zone

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.



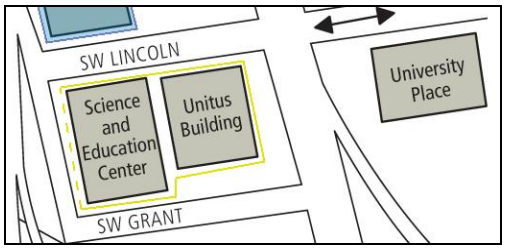
2. Move the mouse to adjust the size and direction of the view zone.
3. Right-click the map and select **Finish** to finalize the zone.
4. You can also adjust the property of the view zone from the Property menu.



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 then 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 highlighted 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 an E-Map for a Remote Host

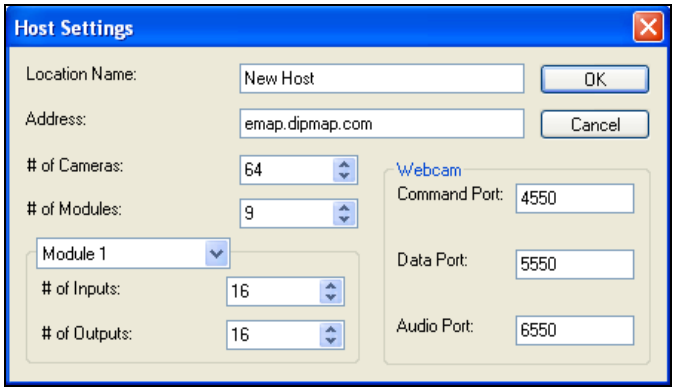
Aside from the local host (GV-VMS), E-Maps can also be created for remote hosts. Through the Remote E-Map function, these E-Maps can be accessed and monitored through a Web browser. For how to remotely access E-Maps, see *Accessing E-Maps of Multiple Hosts* later in this chapter.

Note:

1. The Remote E-Map supports up to 64 channels (channels 1~ 64). For additional channel support, use the Remote E-Map in **GV-Control Center V4**.
2. 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.

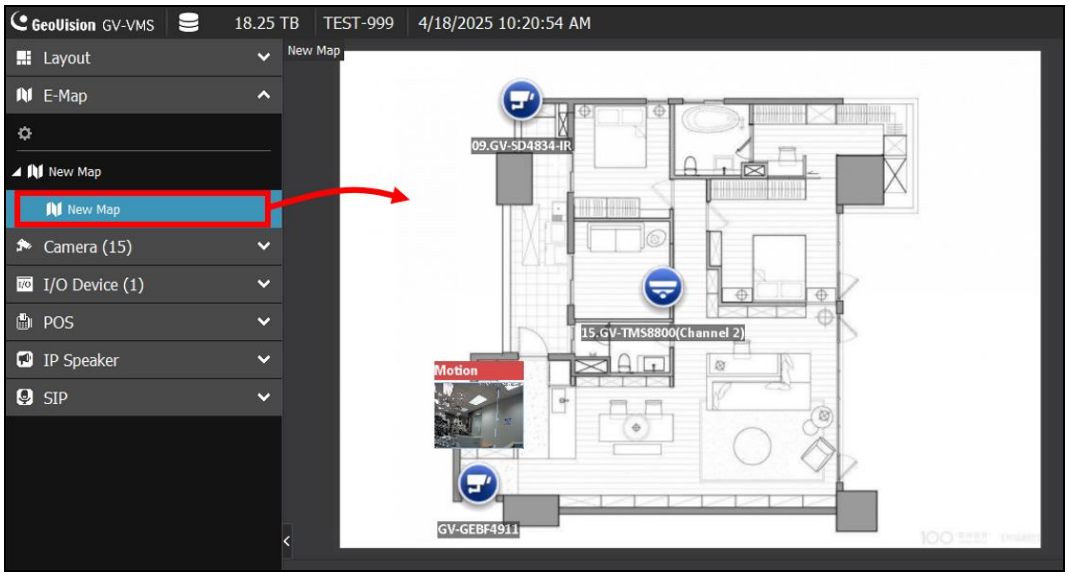


3. Type the necessary information, such as IP address and the number of cameras, and click **OK**.
4. Follow the instructions in *Creating an E-Map* earlier in this section to create an E-Map for the remote host.

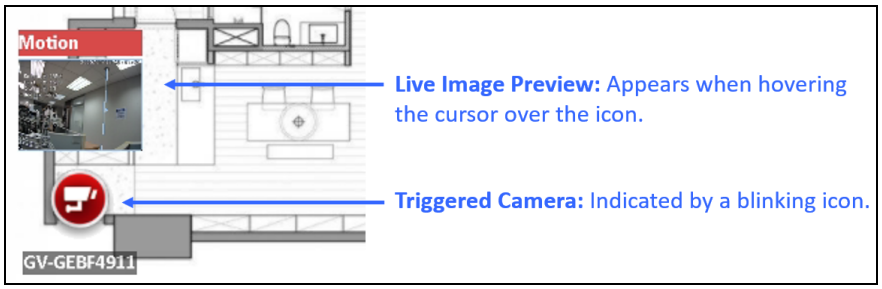
8.2 Starting E-Map

After an E-Map is created, you can start the E-Map on GV-VMS 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. In the Content List under **Home** (No. 9 in *Main Screen* in Chapter 1), click **E-Map**, 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.

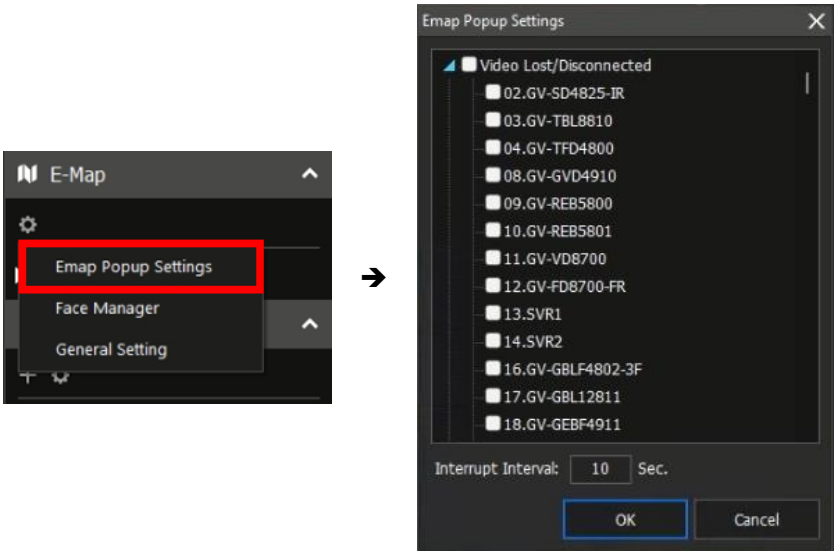


Note: If you have created the E-Maps for multiple hosts, you can see these map files in the Content List. However, these maps won't function on GV-VMS but only work on the Remote WebCam. See *Accessing E-Maps of Multiple Hosts* later in this chapter.

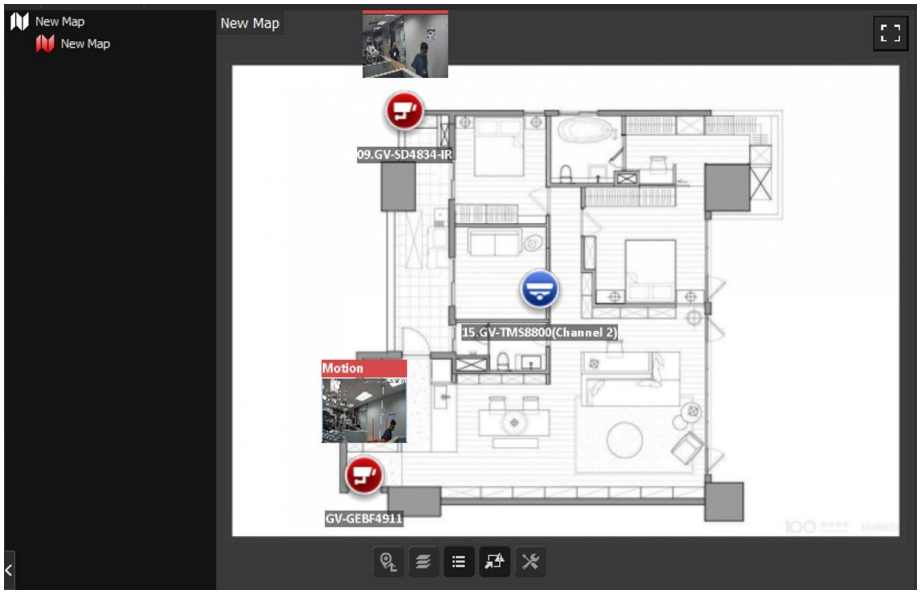
8.2.1 Setting Up Popup Map

When multiple E-Maps are being monitored simultaneously, the pop-up 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 (No. 9 in *Main Screen* in Chapter 1), click **E-Map** > **Configure** > **Emap Popup Settings**.



2. Select the desired cameras and input devices for the application, and specify **Interrupt Interval**. During this interval, any subsequent triggers will be ignored to prevent frequent map pop-ups.
3. At the bottom of the E-Map grid, click **E-Map Auto Pop-Up** to enable the function.



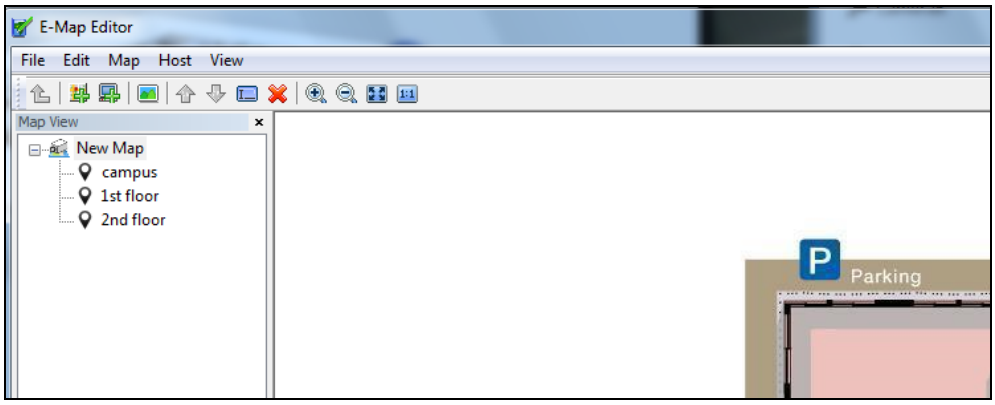
8.3 3D E-Map Display

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.

8.3.1 3D E-Map Display

To display the monitoring area in 3D view, follow the steps below.

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, go to GV-VMS and select **Home** .
3. In the Content List (No. 9 in *Main Screen* in Chapter 1), click **E-Map** and drag the created E-Map to the live view grid.
4. To zoom in / out of the monitoring area, 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 (No. 2 in *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 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. ■ **Face Recognition:** For details, see *Tracking Recognized Faces* in *Chapter 3*. ➢ **Show face and path** ➢ **Show face only** ➢ **Hide face** ■ **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 by first connecting through a Web browser and then installing the Remote E-Map program.

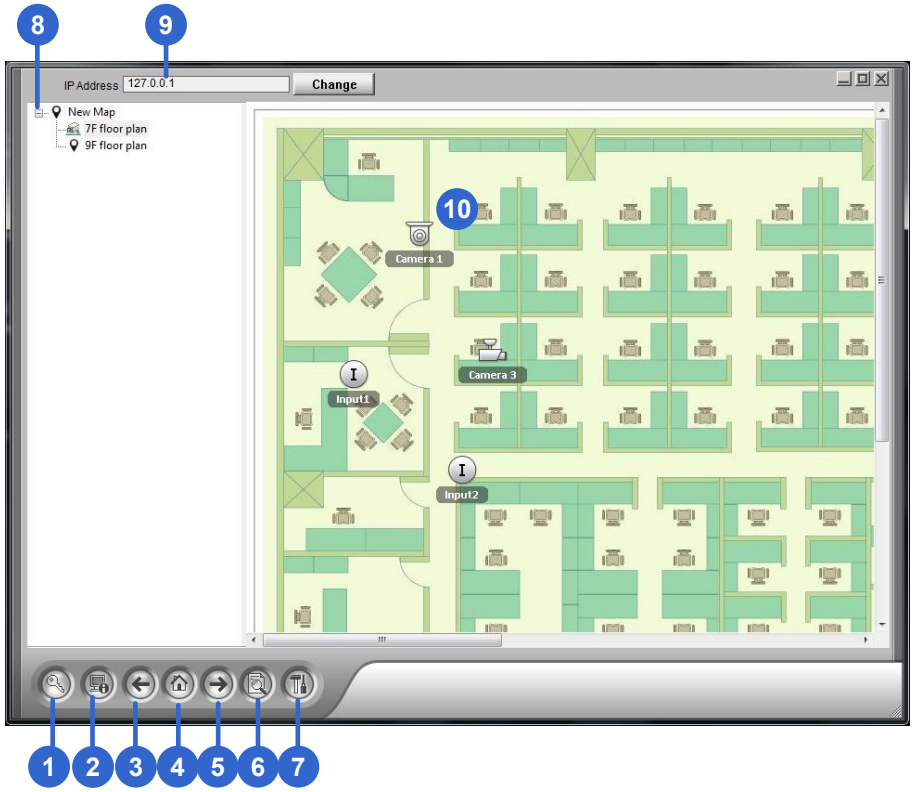
Note: The Remote E-Map supports up to 64 channels (channels 1 ~ 64). For additional channel support, use the Remote E-Map in **GV Control Center V4**.

---

1. To allow remote access to E-Maps, click **Home** > **Toolbar** > **Network** > **WebCam Server** on GV-VMS. The Server Setup dialog box appears.
2. Click **OK** to start GV-WebCam Server.
3. On your remote computer, open the Web browser and type the IP address of the GV-VMS host. Once the connection is established, the Live View page appears.
4. Select **Configure** from the top menu, and then select **Information** > **Download** from the left menu. The Download page appears.
5. Click **Download** next to Remote E-Map, and install the program on your remote computer.
6. After completing the installation, go to **Windows Start** > **All apps** > **Remote E-Map folder** > **Remote E-Map**. The Login dialog box appears.
7. Type the login credentials of the GV-VMS account you want to use, and click . The Remote E-Map window is displayed.

Tip: To download the Remote E-Map program, you can also visit the GeoVision Website, select **Utility** from the dropdown list, and click the **Download** icon of GV-Remote E-Map.

8.4.1 The Remote E-Map Window



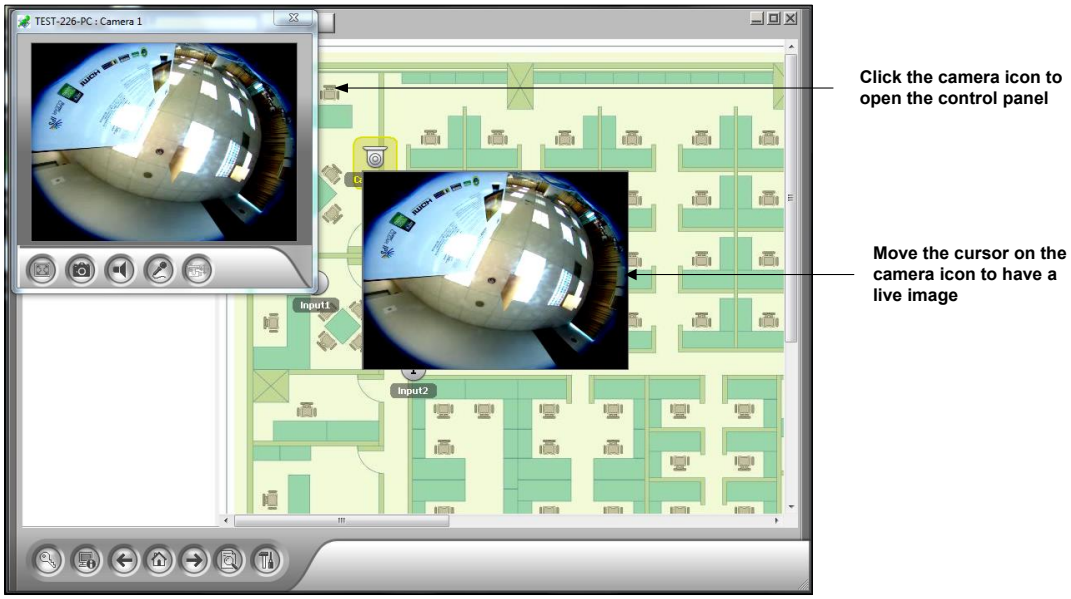
The controls in the window:

No.	Name	Description
1	Login	Logs up to 500 hosts.
2	Host Information	View 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.
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 (No. 7 above) and select **Disable 3D eMap**.

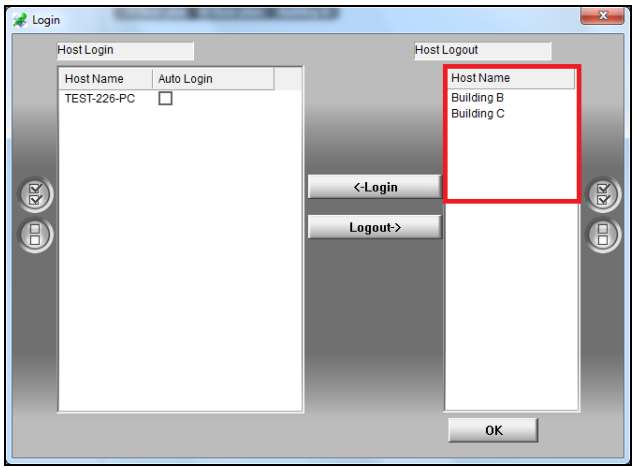
Controls in the Camera Icon



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 GV-Remote E-Map. Up to 500 hosts can be accessed at a time.

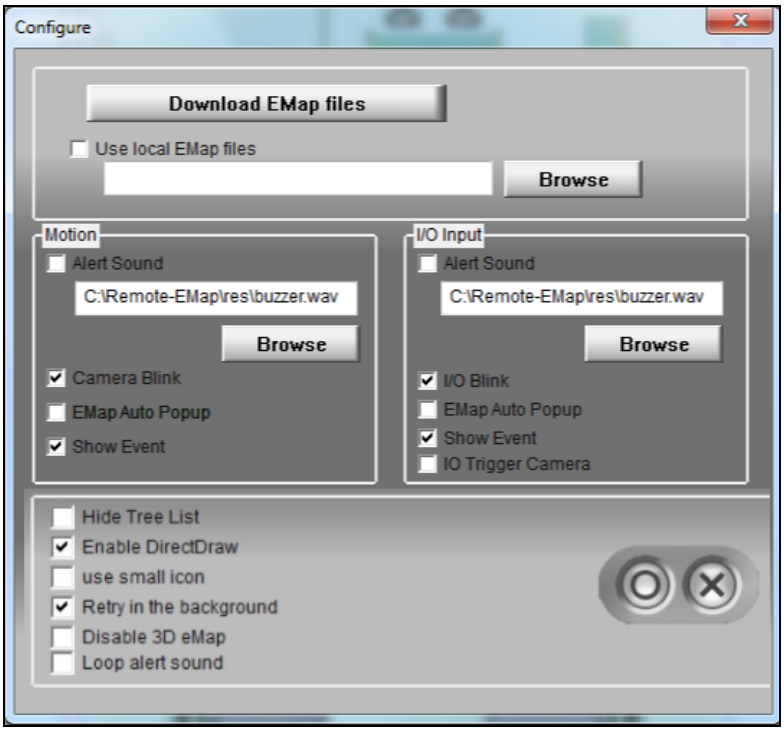
1. To start, click **Login**  on the Remote E-Map window. The Login window appears.
2. Select a host on the right panel and click **Login**. You are prompted for the required login info.



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]

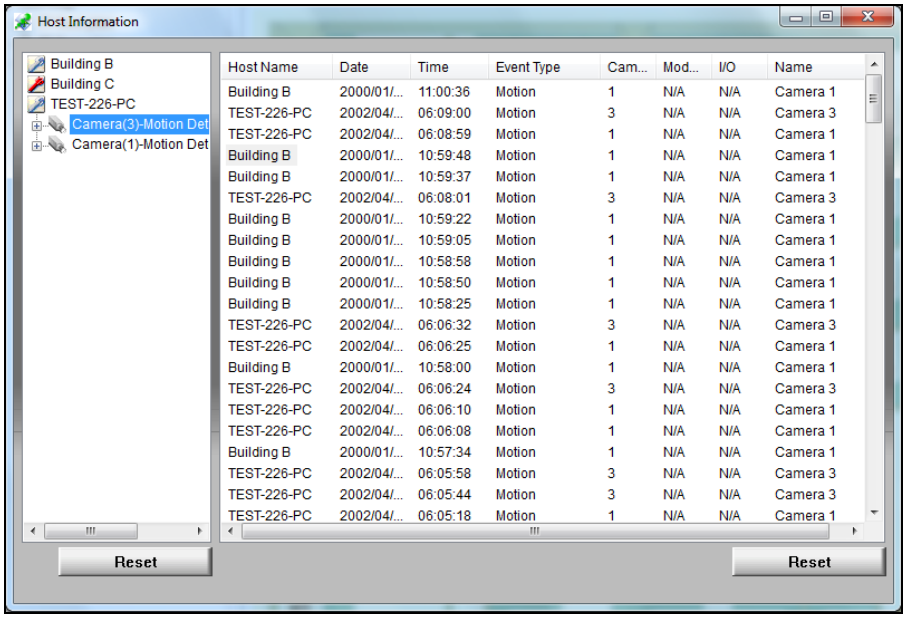
- **Alert Sound:** Assign a .wav file to alert the operator when cameras or I/O devices are triggered.
- **Camera Blink, I/O Blink:** When cameras or I/O devices are triggered, their icons on the E-Map flash.
- **E-Map Auto Popup:** When cameras or I/O devices are triggered, the related map will pop 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 related camera views will pop up. To enable this function, you must map input devices to cameras on the GV-VMS first. See *Popping Up 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:** Enable for devices to be displayed by smaller icons.
- **Retry in the Background:** When the Remote E-Map is disconnected from GV-VMS, a warning message will pop up every 30 seconds. Select to hide the message and retry the connection in the background.
- **Disable 3D E-Map:** 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 advanced 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 E-Map Server, you can monitor different sites on electronic maps through any computer accessible to the network.

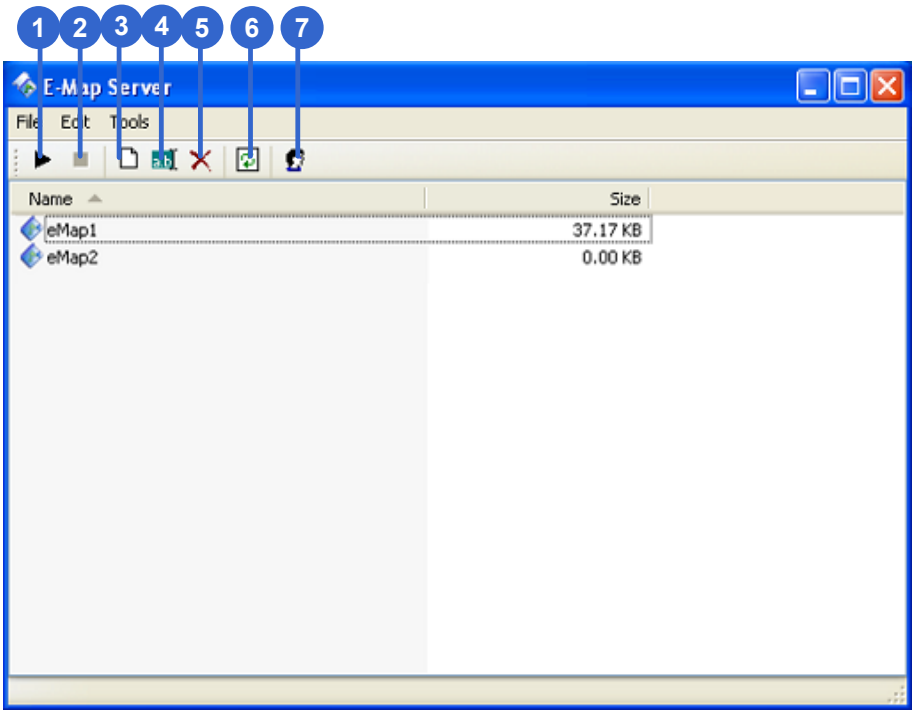
Note: GV-VMS V20 does not currently support GV-E-Map Server.

8.5.1 Installing E-Map Server

To download GV E-Map Server, you can visit the GeoVision Website, select **Utility** from the dropdown list, and click the **Download** icon of GV-E-Map Server.

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 for 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 (**No. 3 in *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** (No. 7 in *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 (see *The Remote E-Map Window* earlier in this chapter).
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 GV-VMS, make sure GV-WebCam Server is enabled. See *Remotely Accessing E-Map* earlier in this chapter.

Chapter 9

Useful Utilities 298

9.1 Dynamic DNS 298
9.1.1 Running Dynamic DNS 298
9.1.2 Registering and Starting Dynamic DNS 298
9.2 Watermark Viewer 299
9.2.1 Activating Watermark Protection 299
9.2.2 Running Watermark Proof 299
9.2.3 The Main Window 300
9.3 Windows Lockup 301
9.3.1 The GV-Desktop Screen 301
9.3.2 GV-Desktop Features 302
9.3.3 Token File for Safe Mode 305
9.4 GV-Authentication Server 306
9.4.1 Installing the Server 306
9.4.2 The Main Window 307
9.4.3 Creating Clients 308
9.4.4 Creating User Accounts 310
9.4.5 Importing Groups and Users from Active Directory 313
9.4.6 Starting GV-Authentication Server 316
9.4.7 Connecting to GV-Authentication Server 318
9.4.8 Remote Access from Other Video Management Software / Mobile Application 320
9.5 Fast Backup and Restore 323
9.5.1 Running the FBR Program 323
9.5.2 Plugin Component 324
9.5.3 Customizing the Features 325
9.5.4 Backing Up and Restoring Settings 326
9.6 Language Setting 329
9.6.1 Installing the MultiLang Tool 329
9.6.2 Revising the Translated Text 330
9.6.3 Setting the UI Language to English 333
9.7 Alert Notifications Through SNMP Protocol 334
9.8 Local and Remote Backup 335
9.8.1 Remote Backup 335

9.8.2 Local Backup 335
9.8.3 Advanced Settings 337
9.9 Report Generator 341
9.10 GV-Cloud VMS 341

CHAPTER 9

Useful Utilities

GV-VMS supports some advanced utilities to enhance the system performance in a security network.

9.1 Dynamic DNS

GV-Dynamic DNS maps your GV-VMS 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 GV-VMS. To access the service, go to **Windows Start** > **All apps** > **GV-VMS 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*:

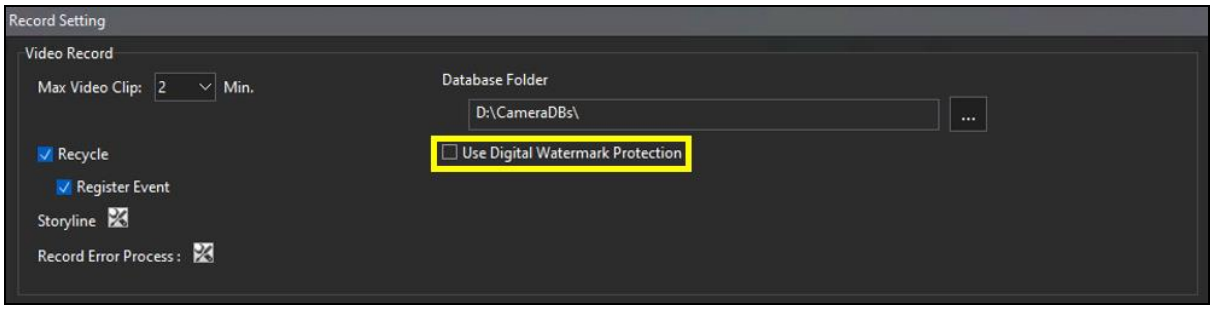
- Registering Domain Name with DDNS
- Starting Dynamic DNS

9.2 Watermark Viewer

GV-VMS 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 GV-VMS, to further verify the authenticity of the recording.

9.2.1 Activating Watermark Protection

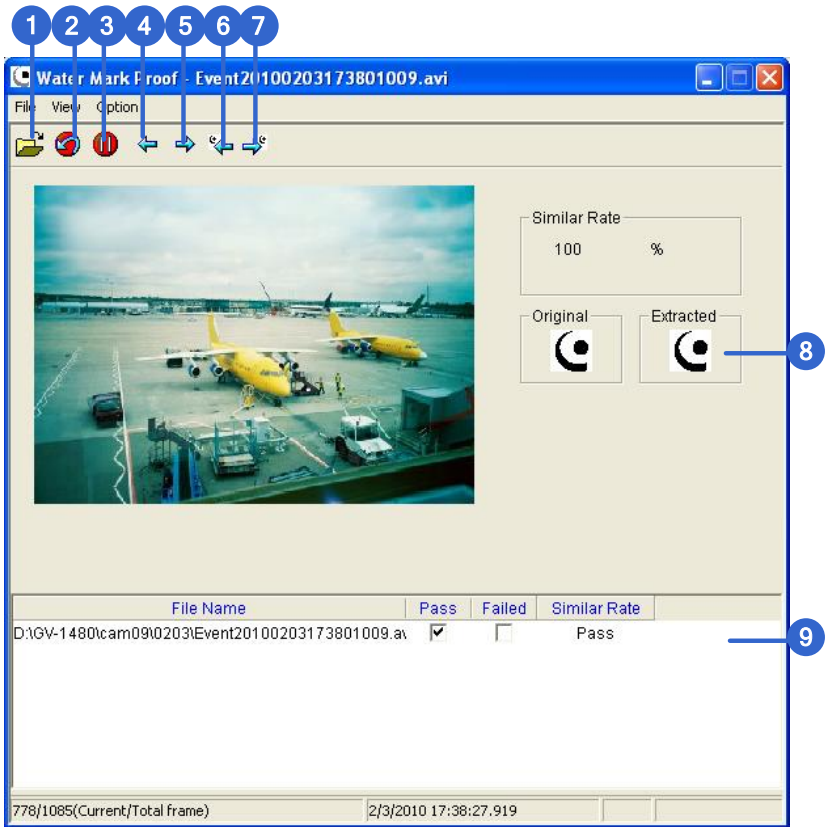
To enable the watermark protection, click **Home** > **Toolbar** > **Configure** > **System Configure** > **Record Setting**, and select **Use Digital Watermark Protection**. GV-VMS will digitally sign videos during recording.



9.2.2 Running Watermark Proof

1. Locate the GV-VMS folder and run **WMProof.exe**. The Watermark Proof window appears.
2. Click **File** from the menu bar, select **Open**, locate the recorded file (.avi), and click **Open**. The selected file is listed on the File List (No. 9 in 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 a watermark during recording, a check mark will appear in the **Failed** column.
3. To play the recording, double-click the listed file in the window.

9.2.3 The Main Window



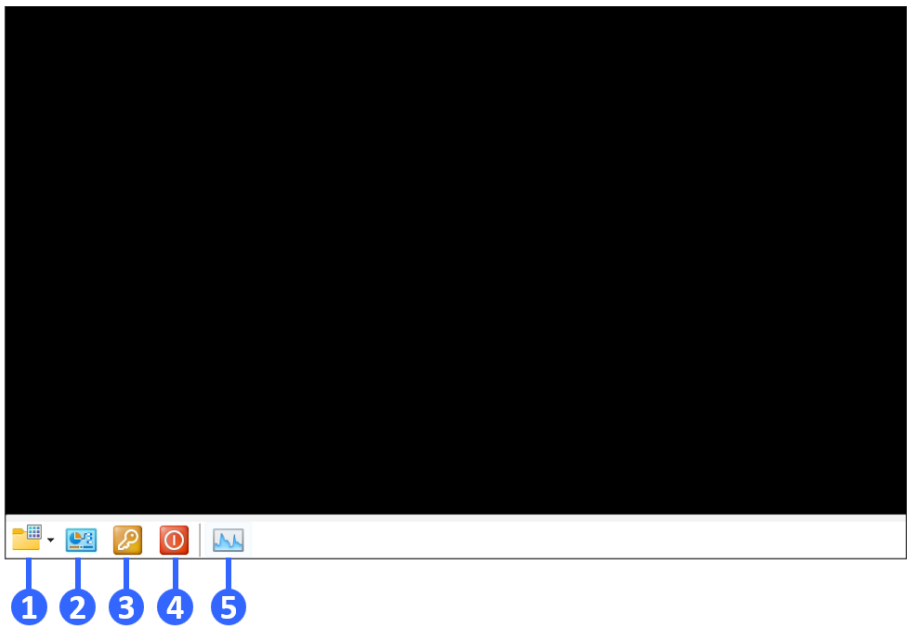
No.	Name	Description
1	Open File	Opens the recorded file.
2	First Frame	Goes to the first frame of the file.
3	Play	Plays the file.
4	Previous Frame	Goes to the previous frame of the file.
5	Next Frame	Goes to the next frame of the file.
6	Previous Watermark Frame	Goes to the previous frame that contains 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 may lock up the Windows desktop while launching a customized GV-Desktop. In GV-Desktop, users are limited to running GV-VMS and only selected programs.

9.3.1 The GV-Desktop Screen

GV-Desktop is included in the installation of GV-VMS. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **Key Lock Utility**. The GV-Desktop screen appears.

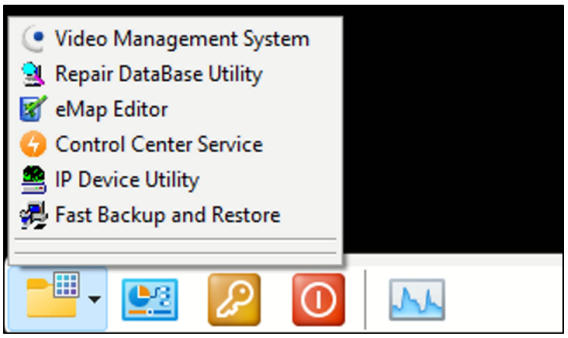


No.	Name	Description
1	Programs	Accesses programs.
2	Settings	Adds programs to the Programs menu.
3	Log Off	Logs off GV-Desktop.
4	Shut Down	Shuts down the computer.
5	Task Manager	Views the tasks currently running on your computer.

9.3.2 GV-Desktop Features

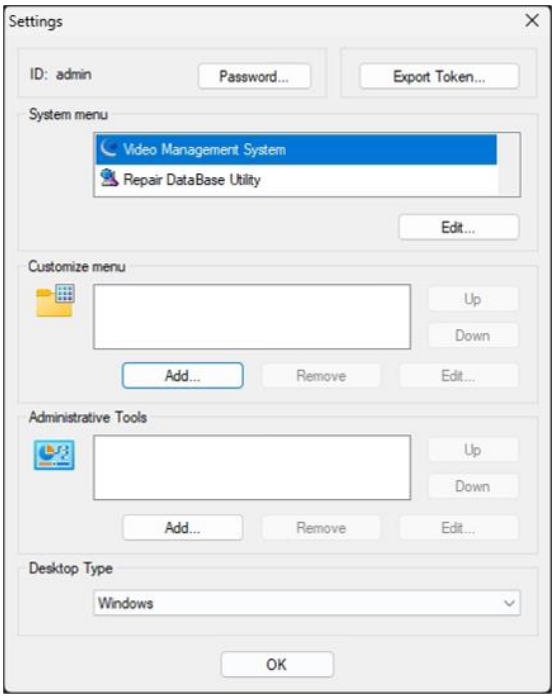
Programs

Click the **Programs** button (No. 1 in *The GV-Desktop Screen* earlier in this section) to see the Programs menu. The default programs are Video Management System (GV-VMS), 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 (No. 2 in *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 section.

[System Menu] Select a desired program and click the **Edit** button to change its name.

[Customize Menu] Set up the Programs menu as desired. To add a program, click the **Add** button. In the Shortcut dialog box, type the program name, click the button next to the field to assign a path, and click **OK**.

[Administrative Tools] Set up the Programs menu as instructed in *Customized Menu* option. To run the added programs configured in the Administrative Tools field, the administrative ID and Password are required.

[Desktop Type] Select Windows or GV-VMS from the dropdown list. The selected desktop will launch the next time you log into the computer.

Log Off

Click the **Log off** button (No. 3 in *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 (No. 4 in *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 (No. 5 in *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 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 in the GV-Desktop Settings dialog box (see the dialog box in *Settings* in *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 GV-Desktop Settings dialog box appears (see the dialog box in *Settings* in *GV-Desktop Features* earlier in this section), 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 GV-Authentication Server

GV-Authentication Server is a password and account management system for multiple GV-VMS systems. Through GV-Authentication Server, the administrator can create the accounts with different access rights to a group of GV-VMS systems. Once any GV-VMS is connected to GV-Authentication Server, the previous password settings in local GV-VMS will be invalid. Local GV-VMS will submit to the full control of GV-Authentication Server.

Note:

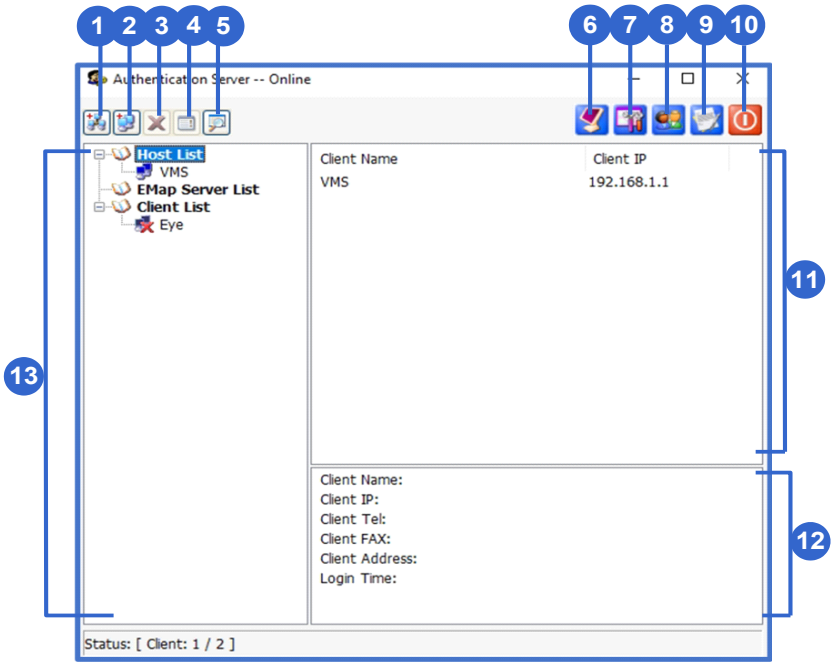
1. In GV-VMS V20 environments, GV-Authentication Server provides channel management for the first 64 channels per system. For channels beyond the first 64 (channels 65–256), use GV-Enterprise to manage user access permissions. See *Setup Flowchart* in Chapter 1 of the *GV-Enterprise User's Manual*.
2. In addition to GV-VMS / DVR / NVR, where GV-Authentication Server acts as a password and account management system, GV-Authentication Server also supports E-Map Server, GV-Control Center, GV-Edge Recording Manager, and the GV-Eye app to allow users access to a specified group of GV-VMS / DVR / NVR hosts through an Authentication user account.
3. 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** on the GeoVision Website.

9.4.2 The Main Window

Go to **Windows Start** > **All apps** > **AuthServer folder** > **AuthServer**. This window appears.

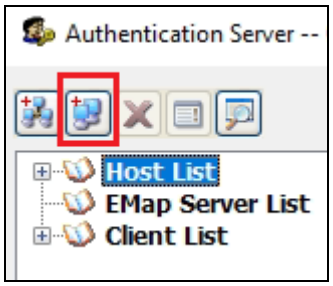


No.	Button	Description
1	Add An Area	Creates an Area group.
2	Add A Client	Creates a client account.
3	Delete An Area / Client	Deletes an existing group or client.
4	View / Edit A Client	Select a client from the Client List, and click to view / edit it.
5	Find A Client	Finds an existing client.
6	Start / Stop Service	Starts / Stops GV-Authentication Server.
7	Server Setup	Configures GV-Authentication Server.
8	Account Setup	Configures passwords and grants permissions to clients. Imports groups from Active Directory.
9	Log	Sets up GV-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: GV-VMS / NVR, E-Map Server, GV-Control Center, GV-Edge Recording Manager and GV-Eye.
12	Client Information	Lists the information of the selected client.
13	Client List	Lists the created clients.

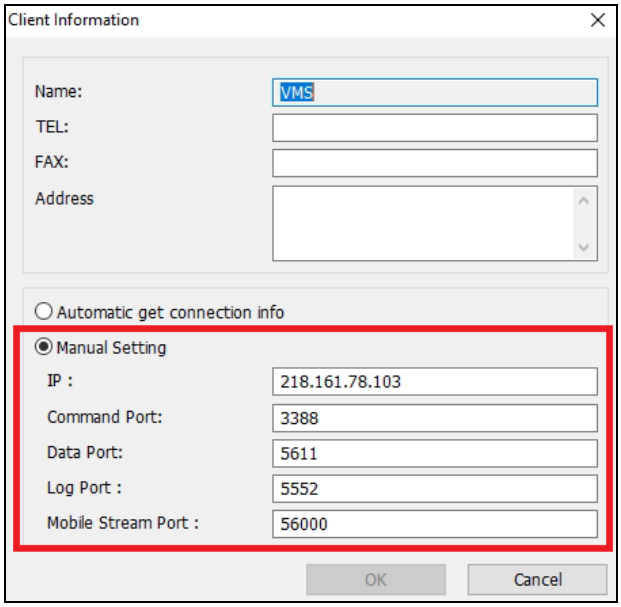
9.4.3 Creating Clients

You must first create and arrange the clients whose user credentials will be centrally managed by GV-Authentication Server. To create a list of GV-VMS clients, follow the steps below.

1. To create a GV-VMS client, highlight the **Host List** from the left pane and click the **Add A Client** button . The Client Information dialog box appears.

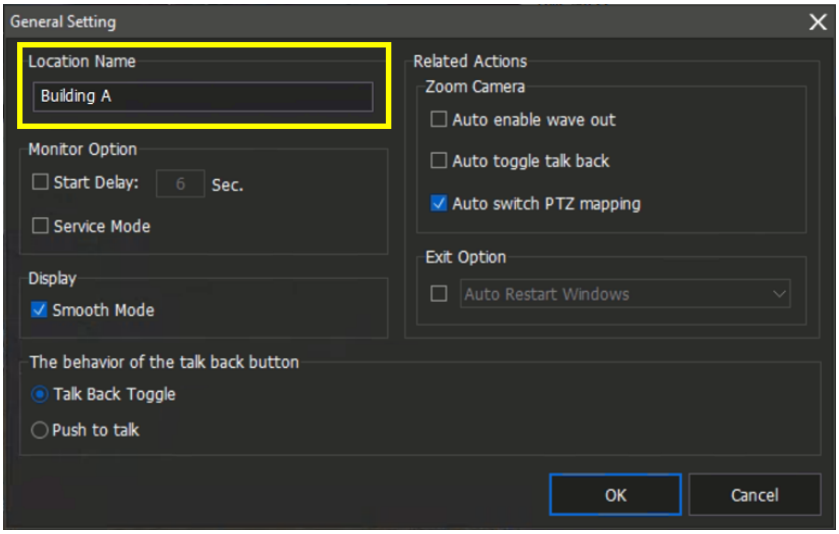


2. Type the client's information and select **Automatic get connection info**. The **Name** must match that of the local GV-VMS.
3. Optionally select **Manual Setting** and type the IP address of GV-Authentication Server. Keep the default ports or modify them if necessary.



4. Click **OK**.

Tip: To view the name of your GV-VMS system, select **Home** > **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 (No. 1 in *The Main Window* earlier in this section). The created group appears under the selected List.

9.4.4 Creating User Accounts

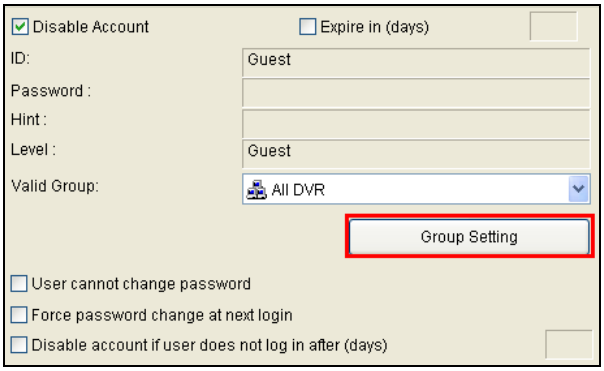
To create user accounts with different access rights and assign the user accounts to a group of GV-VMS clients, follow the steps below.

1. Click the **Account Setup** button (No. 8 in *The Main Window* earlier in this section) > **Password Setup**. The Password Setup dialog box appears.
2. Create a user account. Refer to *Account and Password* in Chapter 1.

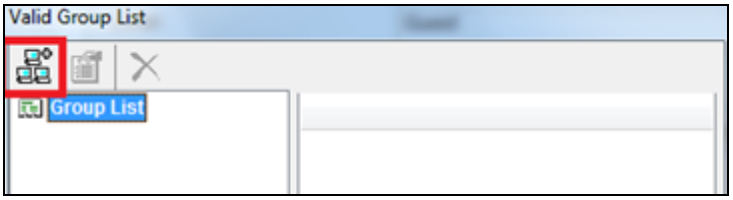
Note: The Administrator has the authority of changing the passwords of any accounts.

---

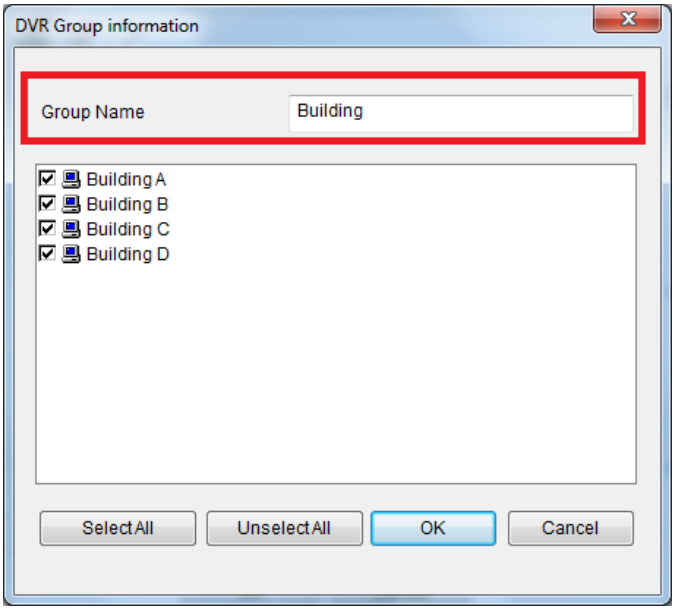
3. To assign the created user to a group of GV-VMS clients:
   A. Click the **Group Setting** button.



   B. In the Valid Group List window, click the **New Group** button.

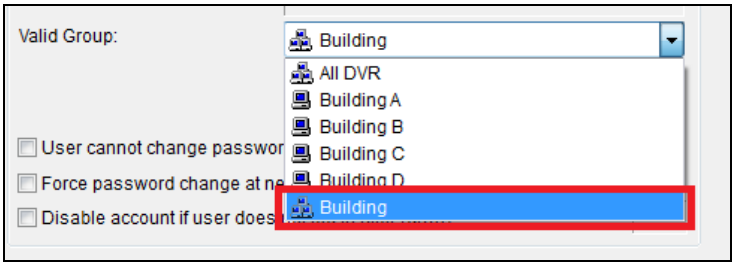


C. In the DVR Group Information window, name the group, select the GV-VMS clients to be added to the group. Click **OK**.



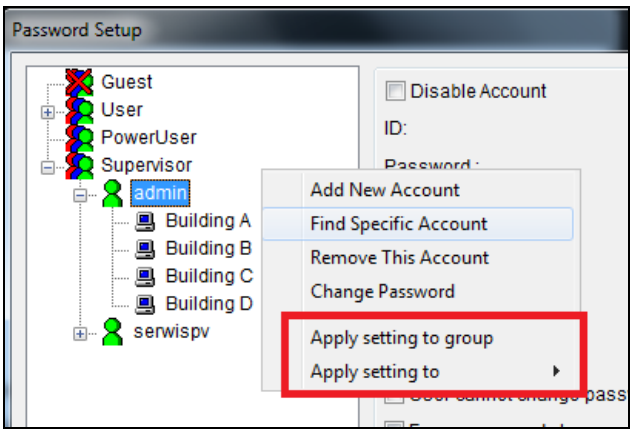
D. Click **OK** again to return to the Password Setup window.

E. Use the **Valid Group** dropdown list to select the created group. The user will be able to log in the assigned GV-VMS clients.

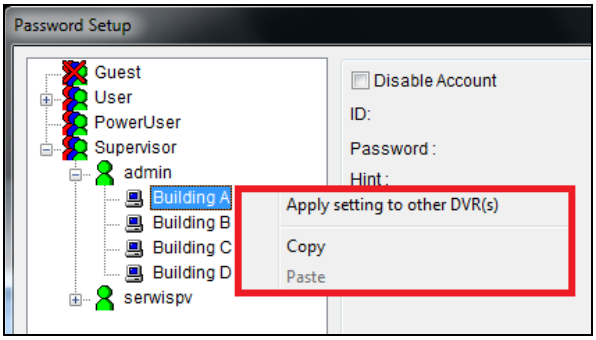


4. Optionally use the following functions to arrange the user and client accounts.

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.



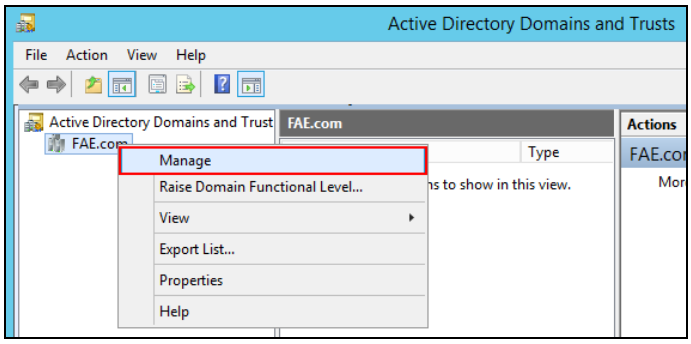
9.4.5 Importing Groups and Users from Active Directory

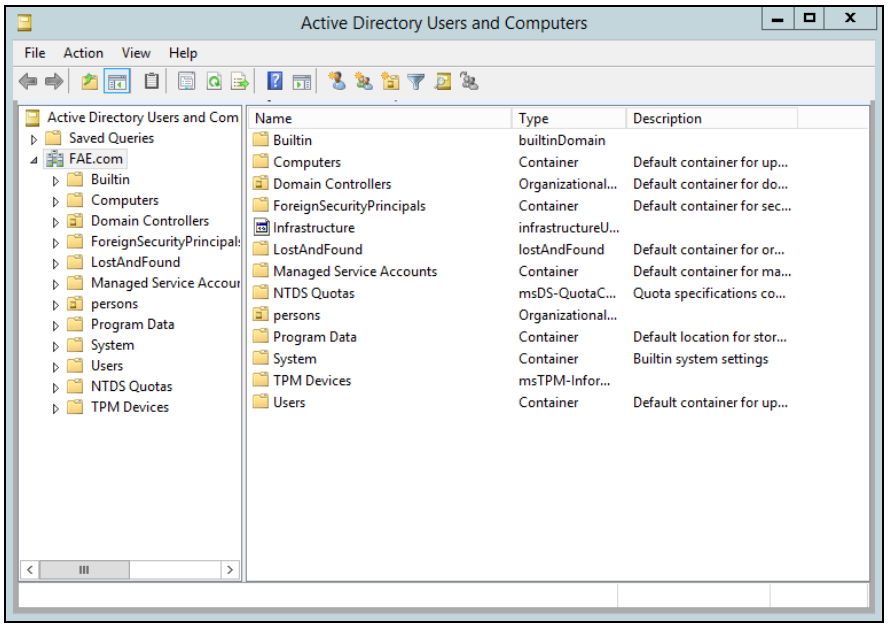
To create user accounts efficiently, you can import groups and users from Microsoft's Active Directory to GV-Authentication Server. You will need to install Active Directory on Windows Server and set up users into groups before following the steps below.

Note: User accounts in Active Directory need to be grouped into Groups settings first as only groups can be imported into GV-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.





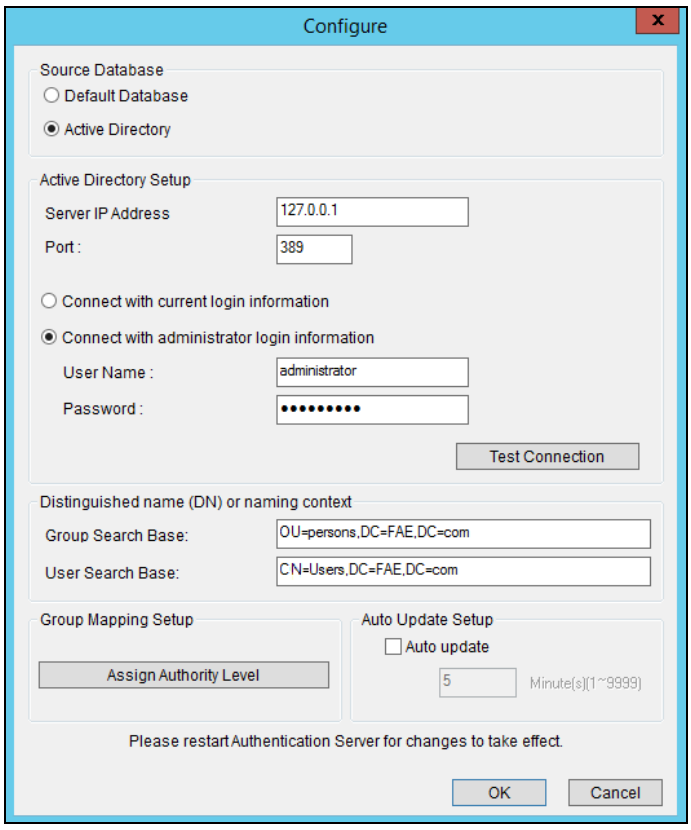
3. On the **View** menu, select **Advanced Features**.

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**.

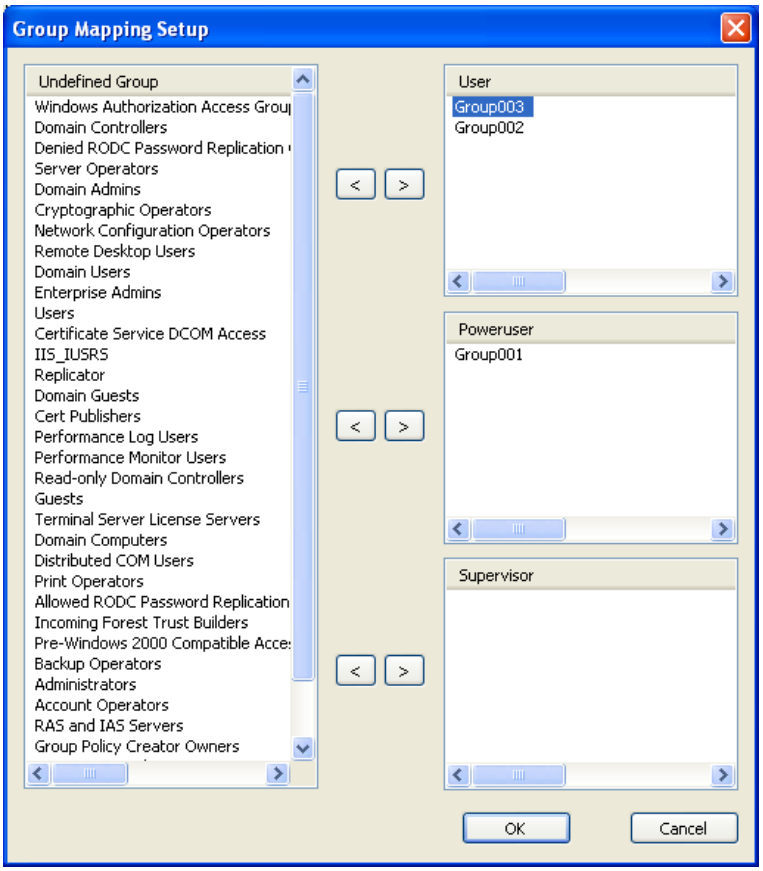
---

5. Select the **Attribute Editor** tab, double-click the attribute **distinguishedName** 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 GV-Authentication Server, click the **Account Setup** button (No. 8 in *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.

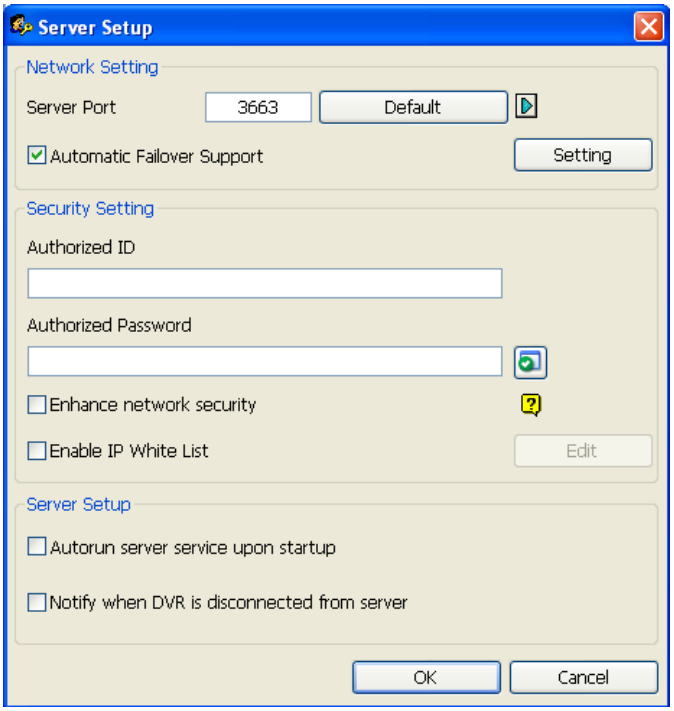


   B. Select the groups detected in Active Directory from the Undefined Group list and use the arrow buttons < > to assign the groups to User, Power User or Supervisor level.
   C. Click **OK** to import the user data into the Password Setup window.
10. To automatically update changes to user data in Active Directory, click **Auto Update** and specify the update frequency in minutes.
11. Click **OK** and restart GV-Authentication Server to apply the settings.

9.4.6 Starting GV-Authentication Server

To configure and start GV-Authentication Server, follow the steps below.

1. Click the **Server Setup** button (No. 7 in *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-VMS client to log into GV-Authentication Server.
3. Click **OK** to apply the settings.
4. Click the **Start / Stop Service** button (No. 6 in *The Main Window* earlier in this section) to start the services.

Optionally, you can configure the following settings before starting GV-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 GV-Authentication Servers in case the primary GV-Authentication Server fails. If it 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 GV-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 GV-Authentication Server is ready to resume the services, close the failover GV-Authentication Server so the connection from clients can move back to the primary.

[Security Setting]

- **Enhance network security:** Strengthen network security on GV-Authentication Server.
- **Enable IP White List:** Click **Edit** to create a list of IP addresses only which are allowed to establish connection with GV-Authentication Server.

[Server Setting]

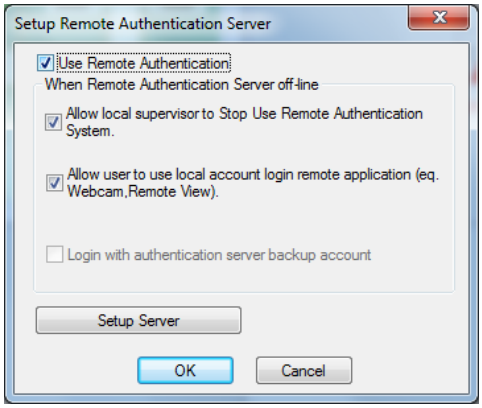
- **Auto run server service upon startup:** Starts the service automatically upon the startup of GV-Authentication Server.
- **Notify when DVR is disconnected from server:** Notify GV-Authentication Server with a pop-up window when GV-VMS is disconnected with GV-Authentication Server.

9.4.7 Connecting to GV-Authentication Server

To configure GV-VMS in order to access GV-Authentication Server remotely through a network connection, follow the steps below.

1. On the main screen of GV-VMS, click **User** > **Password Setup** > **Remote Authentication Setup**. The Setup Remote GV-Authentication Server dialog box appears.





2. Select **Use Remote Authentication** and optionally select:

   [When Remote GV-Authentication Server Off-line]

   - **Allow local supervisor to stop using Remote Authentication System:** Allow the local supervisor to stop the Authentication application when the connection fails with GV-Authentication Server. Note if the option is disabled and the connection fails with GV-Authentication Server, the local supervisor will not be able to log into GV-VMS, and the dialog box will not be accessible until the connection resumes.
   - **Allow user to use local account login remote application:** Allow local users to access remote applications with their previous password and ID settings when the connection with GV-Authentication Server fails.
   - **Login with GV-Authentication Server backup account:** Keep using password settings created on GV-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 GV-Authentication Server.
5. Type the **Authorized ID** and **Authorized Password** of GV-Authentication Server.
6. Click **OK** to start the connection. When the connection is established, the previous password settings in GV-VMS 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 GV-Authentication Server works, the Login dialog box will appear upon starting GV-VMS. Type the user account created on GV-Authentication Server to log into GV-VMS.

Note: The disconnection icon will appear in the Login dialog box (see the dialog box 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 GV-Authentication Server.
2. The client name does not match the location name of GV-VMS (see the General Setting dialog box in *Creating Clients* earlier in this section).
3. The network connection encounters traffic problems.

9.4.8 Remote Access from Other Video Management Software / Mobile Application

GV-Authentication Server supports E-Map Server, GV-Control Center, GV-Edge Recording Manager, and GV-Eye to allow users to access a specified group of GV-VMS hosts through an Authentication user account.

You must first set up remote authentication on E-Map Server, GV-Control Center, GV-Edge Recording Manager, or GV-Eye. After they are connected to GV-Authentication Server, the user will be prompted to log in with the user ID and password you created on GV-Authentication Server. Once the user logs in, a list of GV-VMS hosts authorized to the user account will be displayed, and the user will be able to view the assigned cameras.

Setting Up GV-Authentication Server

You need to create and arrange client accounts of E-Map Server, GV-Control Center, GV-Edge Recording Manager, or GV-Eye under their separate lists on the GV-Authentication Server window (see *The Main Window* earlier in this section).

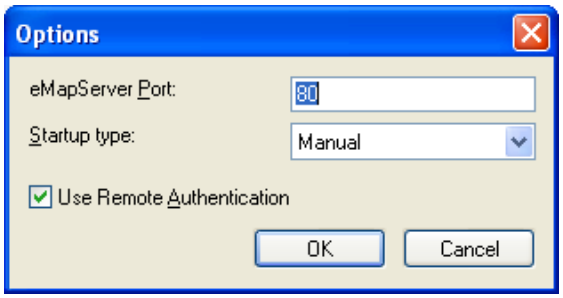
1. In the Client List field, click the **E-Map Server List** or **Client List**, and click the **Add A Client** button (No. 2 in *The Main Window* earlier in this section). The Client Information dialog box appears.
2. Type the name and information of the desired software or mobile app to be connected. The name does not need to match the location name of the software or mobile app.
3. Click **OK** to add the client.

Accessing from E-Map Server

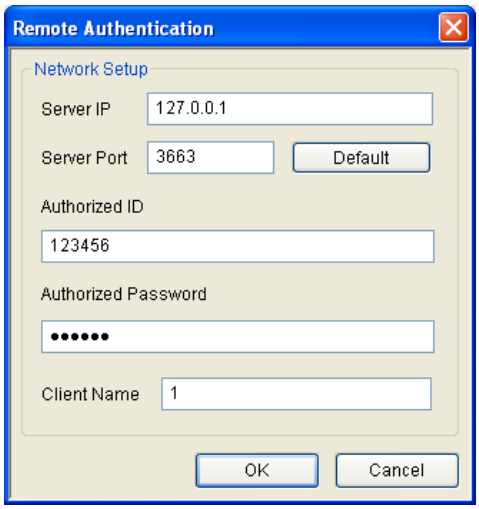
The E-Map Server can access the account setting of GV-Authentication Server.

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 GV-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 GV-Authentication Server, as well as the E-Map Server's client name created on GV-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 GV-Authentication Server. A list of assigned GV-VMS 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*.

Accessing from GV-Edge Recording Manager / GV-Eye

GV-Edge Recording Manager and GV-Eye can access account settings of GV-Authentication Server. For details, see *Chapter 11 Authentication Server* in the *GV-Edge Recording Manager User's Manual* or *Chapter 13 Connecting to Authentication Server* in the *GV-Eye Installation Guide*.

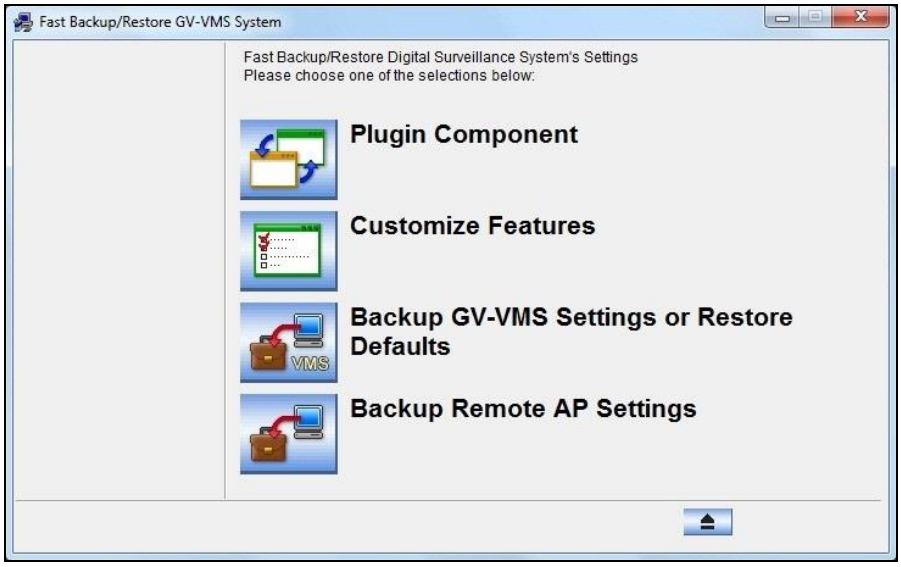
9.5 Fast Backup and Restore

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 GV-VMS.

9.5.1 Running the FBR Program

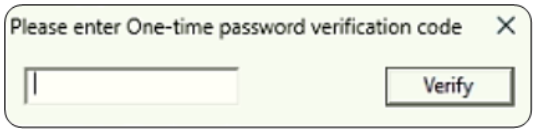
To run the FBR program, follow the steps below.

1. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **Fast Backup and Restore Main System**. This window appears.



Fast Backup and Restore window

2. The first time you click any button, type a valid GV-VMS ID and password when prompted. If **Multi-factor authentication** is enabled (see *Configuring Account Settings* in Chapter 1), you will also need to enter a verification code generated by your authentication app.

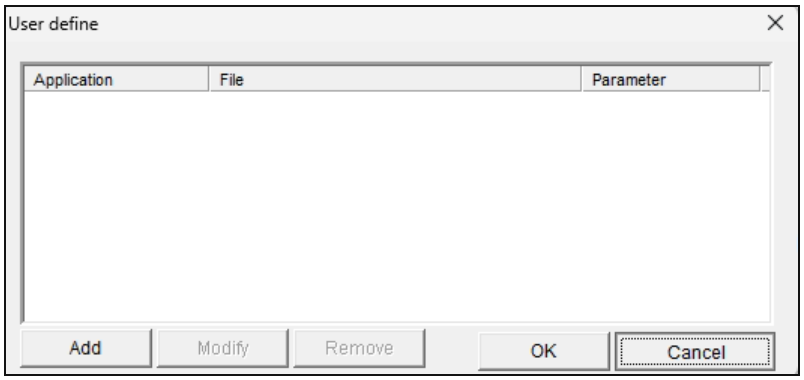


After this, you can start configuring the settings.

9.5.2 Plugin Component

You can add programs to your GV-VMS 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.

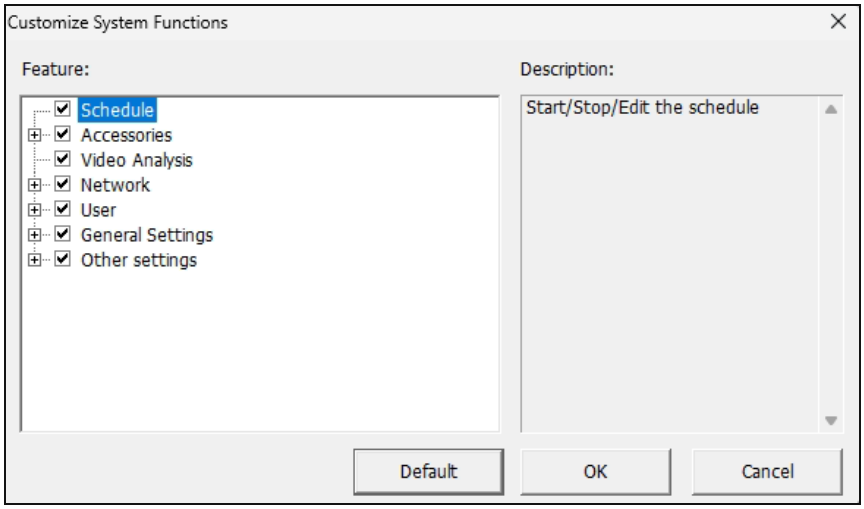
---

1. Type the name of the desired application, locate its path, and click **OK**.
2. To add more applications, repeat steps 1 to 3 and click **OK** in the User Define dialog box.
3. To access the added applications, run GV-VMS, 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 GV-VMS.
3. Click **OK** to save the settings.
4. Restart GV-VMS for the settings to take effect.

9.5.4 Backing Up and Restoring Settings

You can back up the configurations you made in GV-VMS, and restore the backup data to the current system or import it to another GV-VMS.

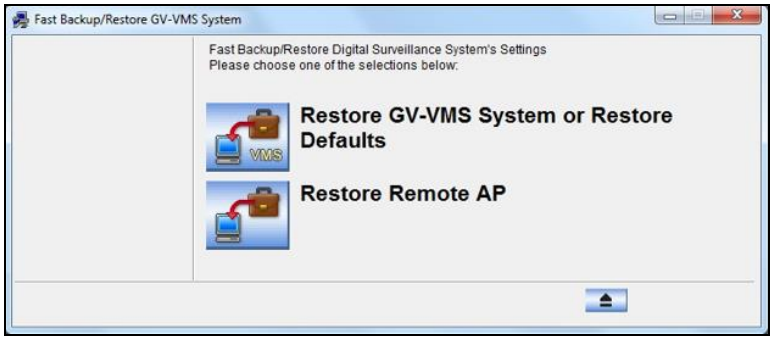
Backing Up the Settings

1. In the Fast Backup and Restore window (see the window in *Running the FBR Program* earlier in this section), click **Backup GV-VMS 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-VMS System Settings” message will appear.

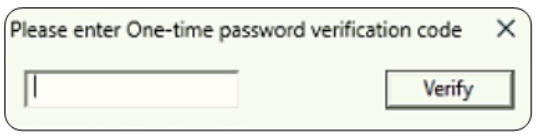
Restoring the System

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. This window appears.



2. The first time you click any button, type a valid GV-VMS ID and password when prompted. If **Multi-factor authentication** is enabled (see *Configuring Account Settings* in Chapter 1), you will also need to enter a verification code generated by your authentication app.

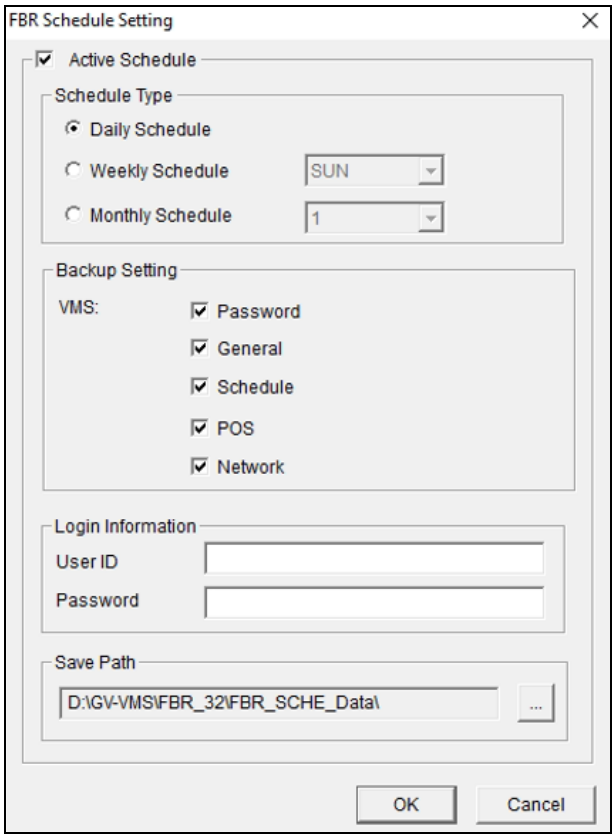


3. Click **Restore GV-VMS System or Restore Defaults** > **Restore Backup Settings**. and select which backup settings you want to restore.
4. Click the **Next Step** button to start restoring. When the restoration is complete, the “Successfully Restore GV-VMS System Settings” message will appear.

Scheduling Configuration Backup

You can now set up a regular schedule with password protection to back up the GV-VMS configurations you made.

1. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **Fast Backup and Restore Main System**.
2. Click **Backup GV-VMS Settings or Restore Defaults** > **Schedule Setting**. This dialog box appears.



3. Enable **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 GV-VMS.
   - **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 to those of a user account created in GV-VMS. 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 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 Too**l 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.

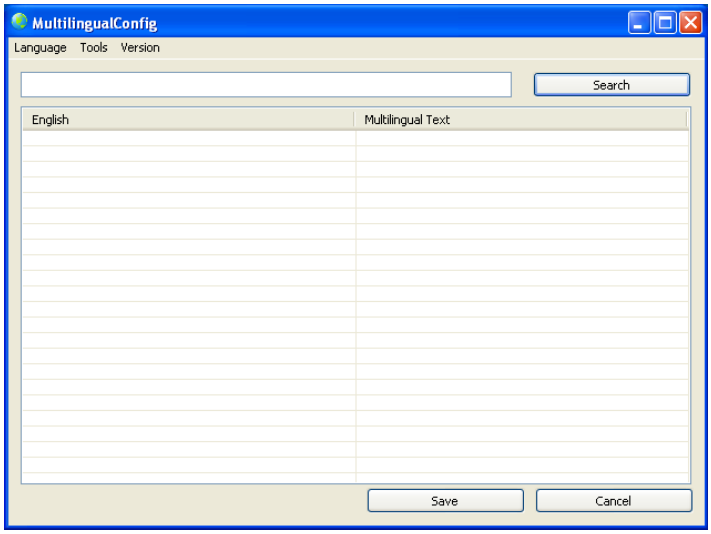
9.6.1 Installing the MultiLang Tool

You can install **GV-MultiLang Tool** from **Utility** on the GeoVision Website.

9.6.2 Revising the Translated Text

Revising the Translated Text

1. After completing the installation, close all GeoVision applications, and go to **Windows Start** > **All apps** > **MultilingualConfig folder** > **MultilingualConfig**. This dialog box appears.

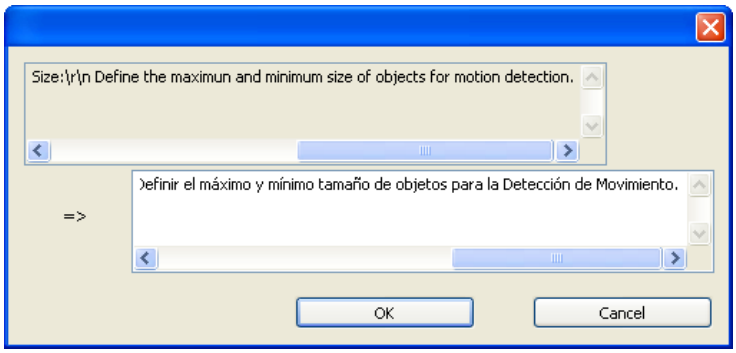


2. Click **Language** and select the language of the text you want to revise.
3. Click **Version** to select the version of GV-VMS that you want to revise.
4. In the **Search** field, type all or part of the text in English or the target language and click **Search**. The results are displayed.

Note: The search is case sensitive.

---

5. Double-click the text you want to revise. This dialog box appears.



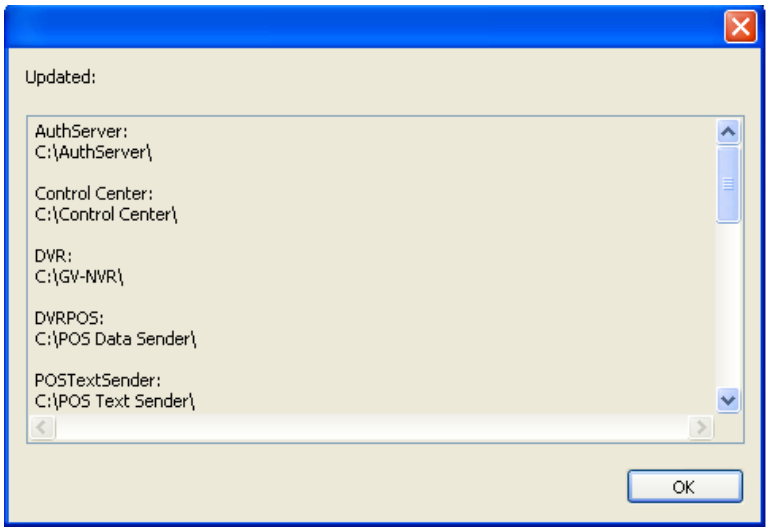
6. Revise the translated text and click **OK**.

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-VMS, GV-Authentication Server, GV-Center V2, GV-Dispatch Server, GV-Fast Backup and Restore (FBR), GV-IP Device Utility, GV-MCamCtrl Utility, and GV-Remote E-Map.

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.

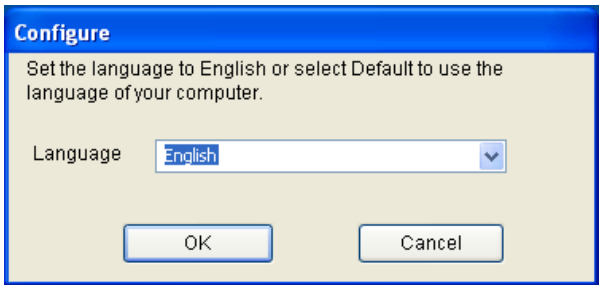
9.6.3 Setting the UI Language to English

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
- 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.

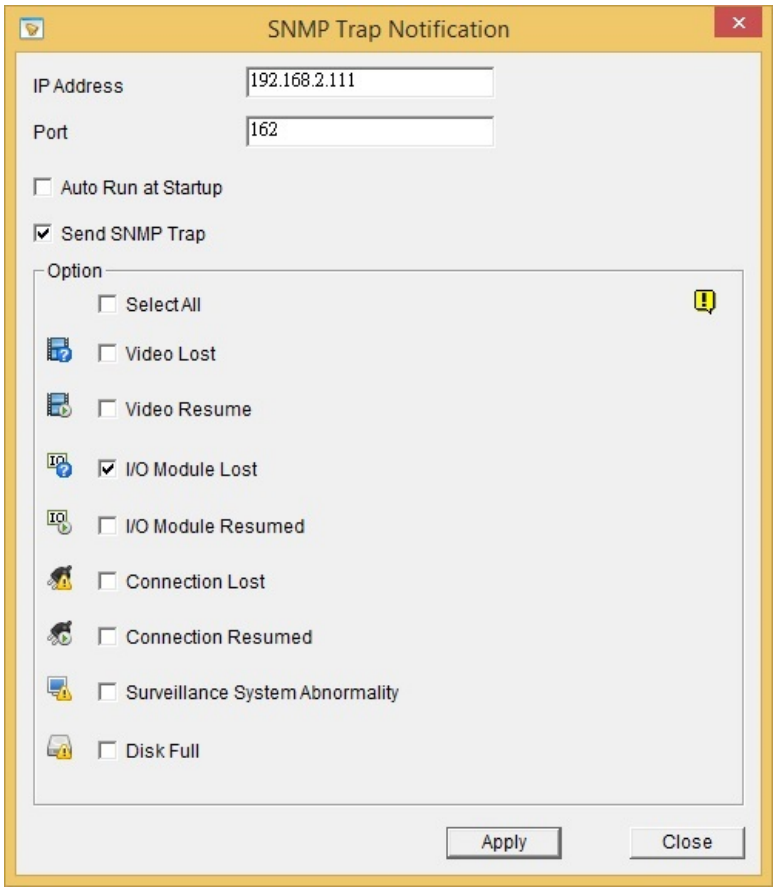


2. Click **OK** and restart your GeoVision software or application to enable the English UI.

9.7 Alert Notifications Through SNMP Protocol

You can send alert notifications to SNMP-compatible software by using the SNMP Trap Notification utility.

1. Go to **Windows Start** > **All apps** > **GV-VMS folder** > **SNMPTrapNotification**. 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**.

9.8 Local and Remote Backup

GV-VMS 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.

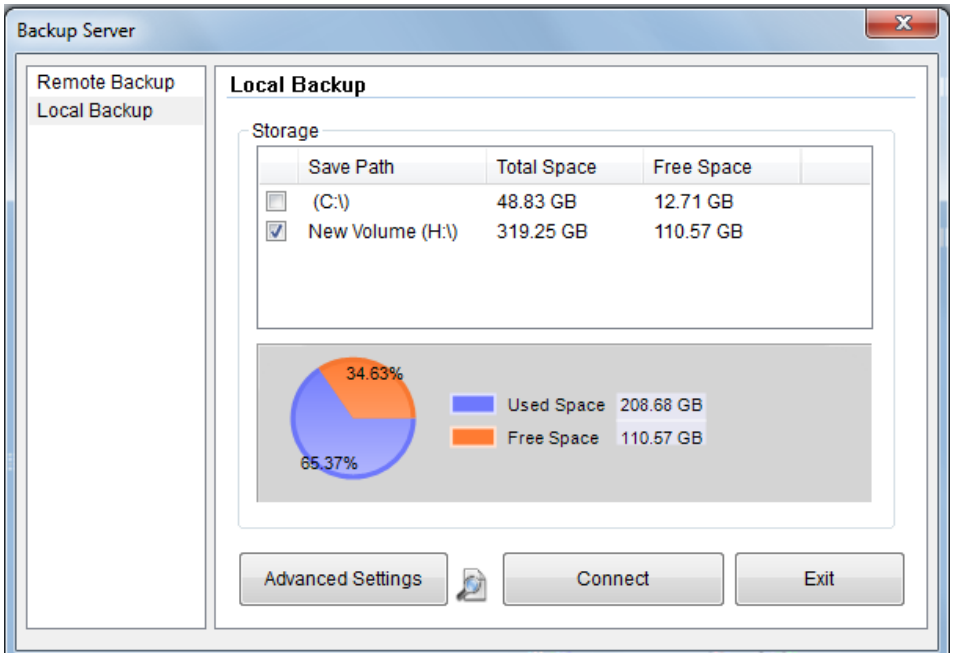
9.8.1 Remote Backup

To back up with GV-Backup Center, see *Connecting GV-VMS* in Chapter 3 in the *GV-Backup Center User's Manual*.

9.8.2 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.

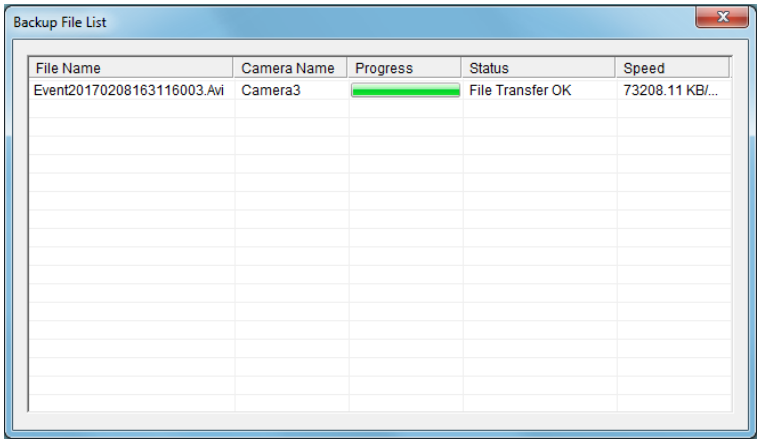


2. Select **Local Backup** in the left panel.

3. Specify which hard drive you want to back up your files to. 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 Settings for Local Backup* in *Advanced Settings* 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.



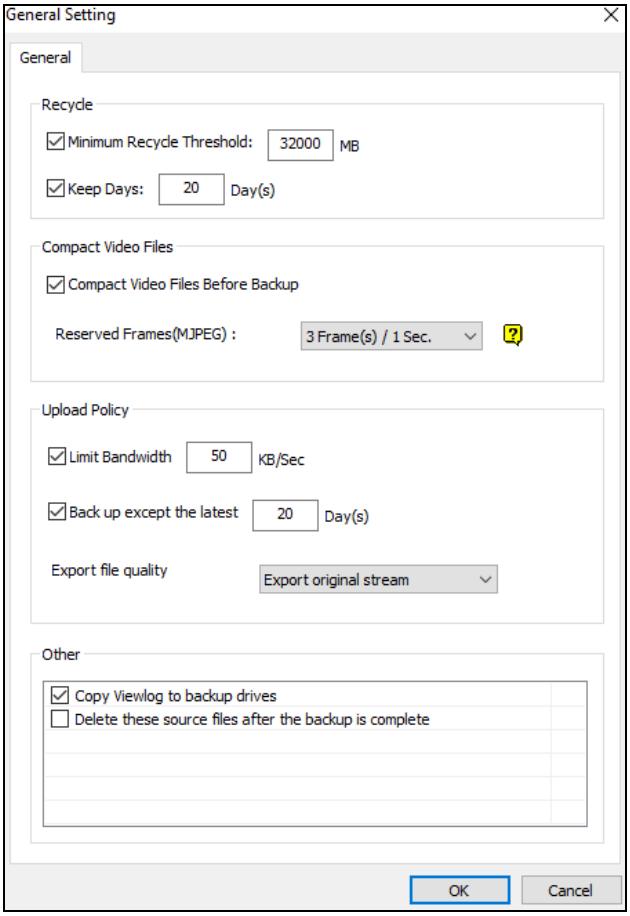
Note:

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-VMS.

9.8.3 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 on the local hard drive.

[Compact Video Files]

- **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 GV-VMS after the files are successfully backed up.

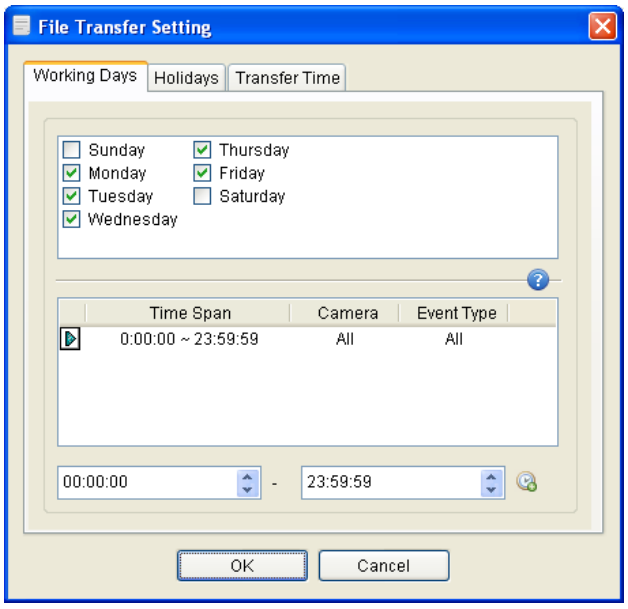
File Transfer Settings for Local Backup

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 the transfer time.

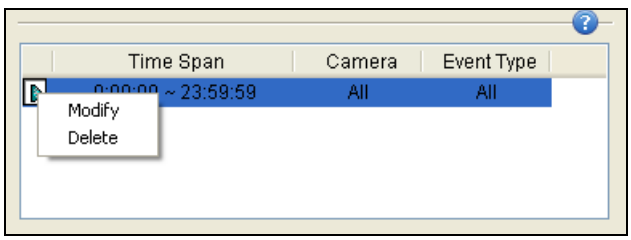
In this setting dialog box, you can define the following backup rules:

- The day of the recordings to be transferred.
- The time period of the recordings to be transferred.
- The type of the recordings to be transferred, including motion detection, I/O trigger, or all types of events.
- The time to back up the files.

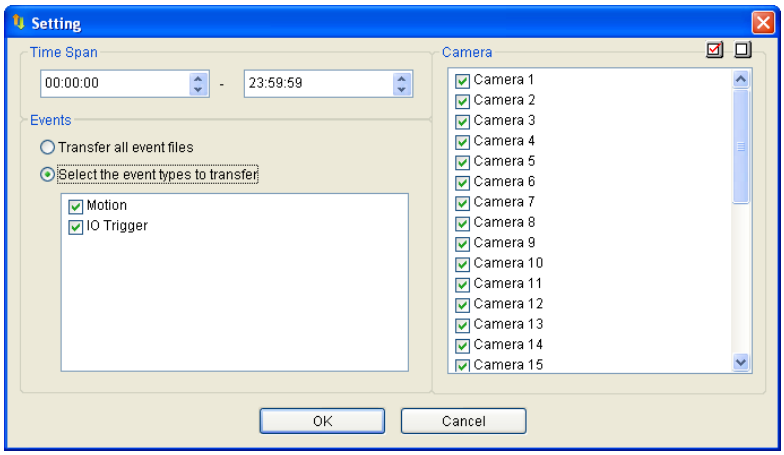


[Working Days] Define up to 10 backup rules to specify which recordings to be transferred to the assigned hard disk drive, including their type, time period, and the days of the week they were recorded.

1. Select a day from Monday to Sunday.
2. Click the arrow button before Time Span and select **Modify**.

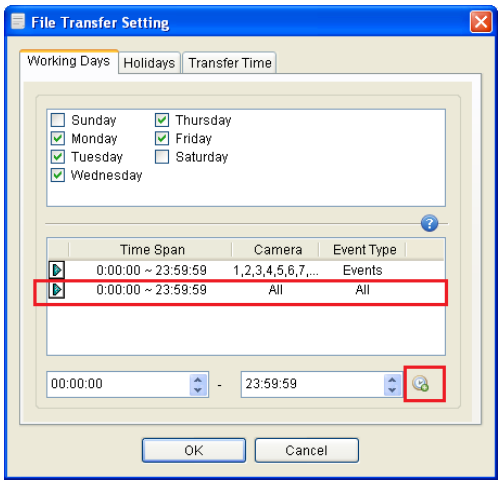


3. In this dialog box, select the **Camera** whose recordings you want to back up, specify the **Time Span** of the recordings to be backed up, and select the **Events** that you want to back up – All Events, Motion Events, or I/O Trigger Events.



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.

9.9 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-VMS without requiring additional installation.

For details, see the *Report Generator User's Guide*.

9.10 GV-Cloud VMS

To connect to GV-Cloud VMS, see *Connecting GV-VMS or GV-AI Guard* in Chapter 2 of the *GV-Cloud VMS User's Manual* for detailed instructions.

Chapter 10

Point-Of-Sale (POS) Application 343

10.1 Displaying Transactions on the Screen 344

10.2 Setting Up Text Overlay 345

10.3 Filtering Transactions for a Product Item 346

10.4 Triggering Transaction Alarms 348

10.5 Mapping Codepage 350

10.6 Coloring Transactions of a Product Item 351

10.7 Displaying Receipt Details of a Transaction 354

10.7.1 Setting Up Receipt Display Conditions 354

10.8 Filtering Transactions by a Keyword 360

10.9 Searching for POS Events 363

10.9.1 Advanced Search Panel 364

CHAPTER 10

Point-Of-Sale (POS) Application

A POS device can be integrated to GV-VMS 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

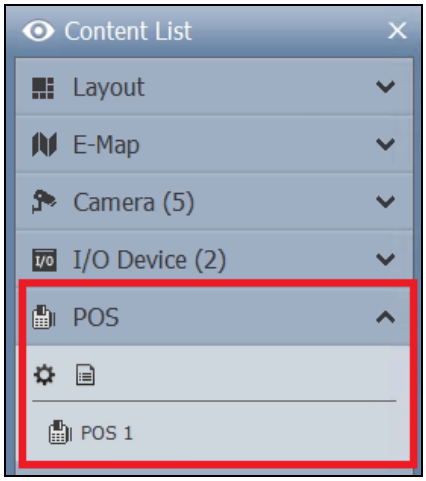
To find out which solution is suitable for you, please check the flowchart.

10.1 Displaying Transactions on the Screen

You can display transaction data on any of the 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 (No. 9 in *Main Screen* in Chapter 1). For details on setting up a POS device, check the flowchart.

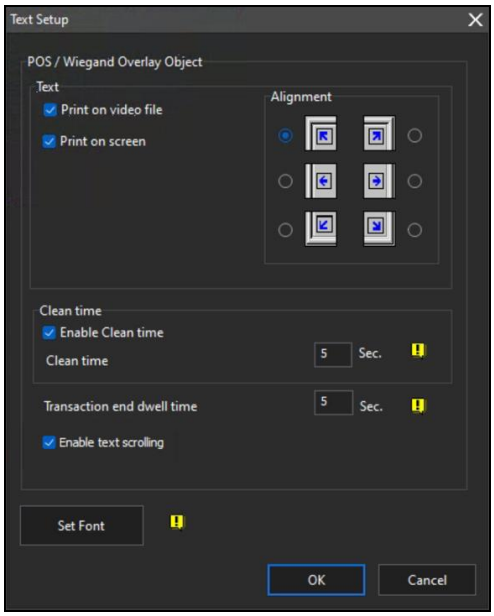
2. Drag and drop the created POS device to any of the screen divisions. Once the transaction on the POS starts, the data will be displayed on the screen.



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 adjust the text font and position of transaction data on live view and recorded files, click the **Text Setup** button on the POS Device dialog box (**Home** > **Toolbar** > **Configure** > **Accessories** > **POS Device Setup** > select a POS device from 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 (No. 9 in *Main Screen* in Chapter 1) 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]

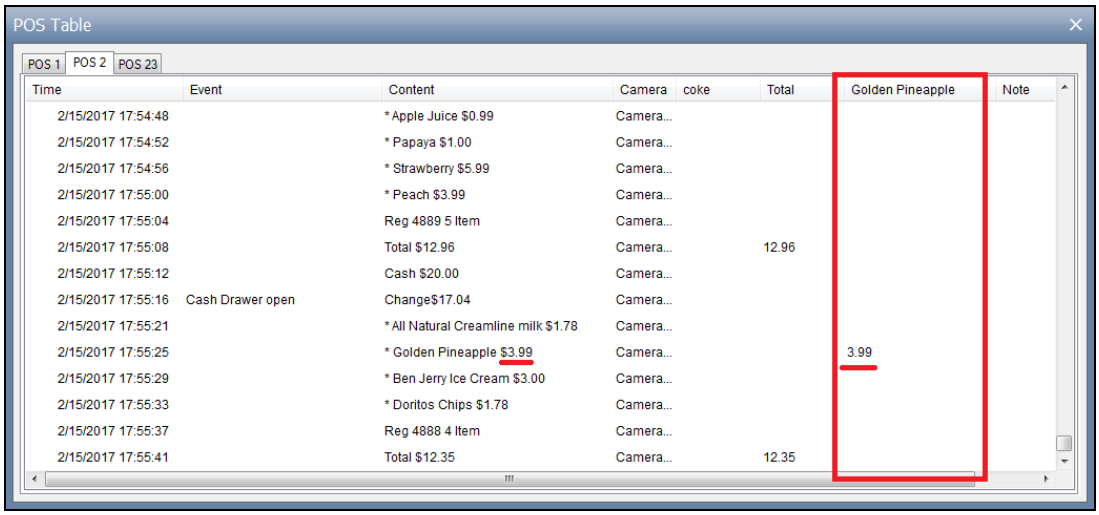
- **Clean time:** Specify the amount of time in seconds after which GV-VMS has not received the transaction data from the POS device, i.e., the cashier stops entering the transaction data. The already-displayed POS data will be hidden from live view.

- **Transaction end dwell time:** Specify the amount of time in seconds that POS data stays on the live view before the next transaction.
- **Enable text scrolling:** By default, this option is enabled, and POS text in the live view scrolls upward. When disabled, the text is cleared upon reaching a certain limit and restarts from the top.
- **Set Font:** Click the button to set up the font for POS data.

10.3 Filtering Transactions for a Product Item

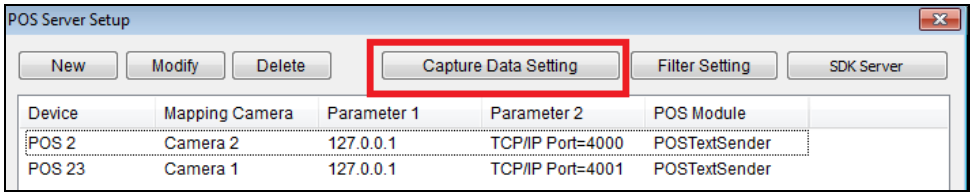
POS Field Filter allows you to create an independent column for a transaction item in the System Log. The feature filters the transactions, and highlights the price of the item under the created column.

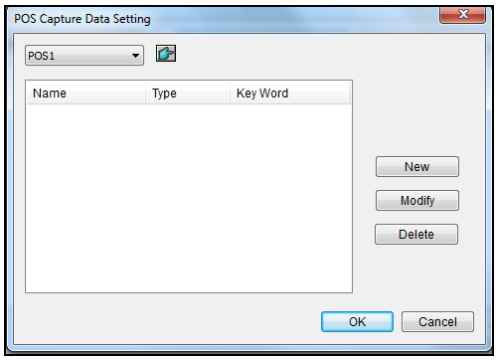
For this example, the transaction item is “Golden Pineapple” whose transaction data stands out in the System Log to attract your attention.



To set up the function, follow the steps below:

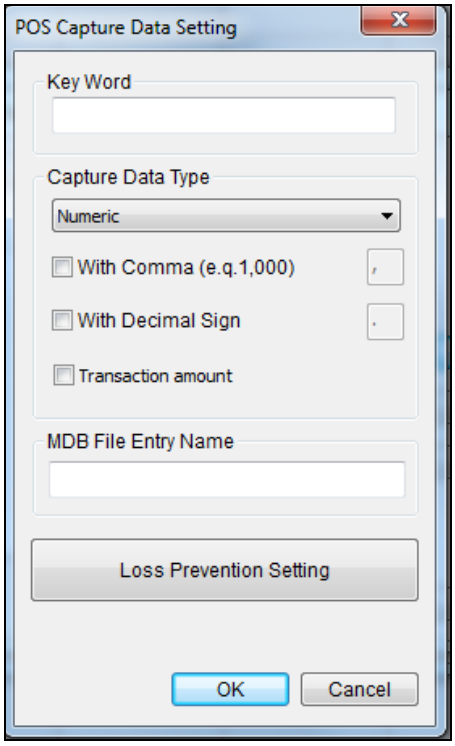
1. On the POS Server Setup dialog box, select a POS device, and select **Capture Data Setting**. The POS Capture Data Setting dialog box appears.





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 letters, 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.

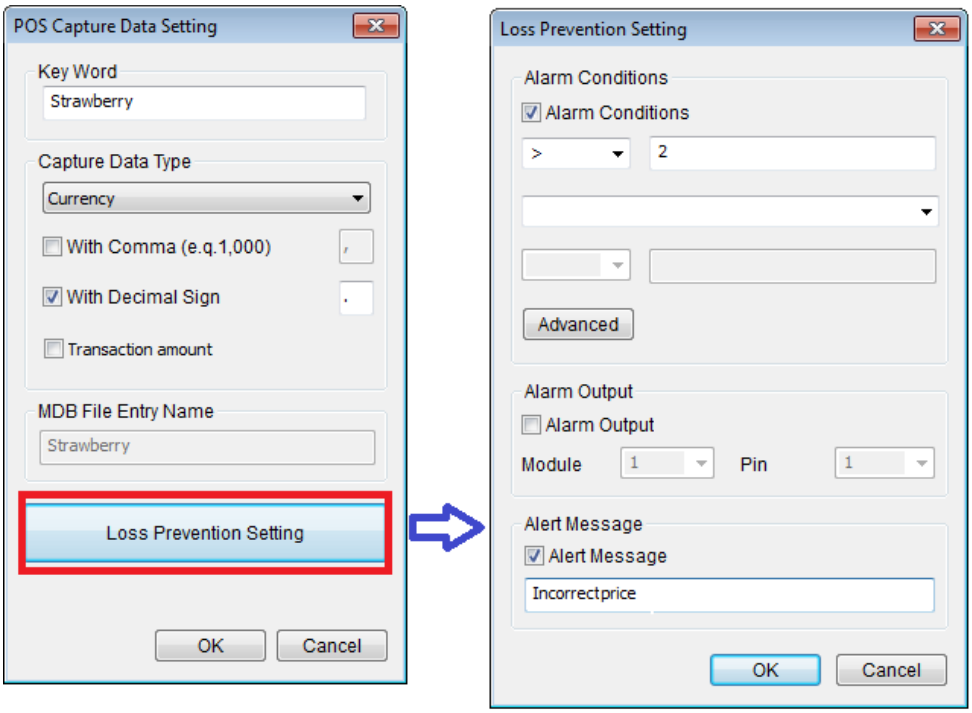
4. Click **OK**.
5. Open the POS Table (**Home** > **Toolbar** > **Tools** > **System Log** > **POS Table**) to see the filtering results.

Tip: To open the POS Table, you can also expand **POS** in the Content List (No. 9 in *Main Screen* in Chapter 1) and select **View Event Log**.

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.



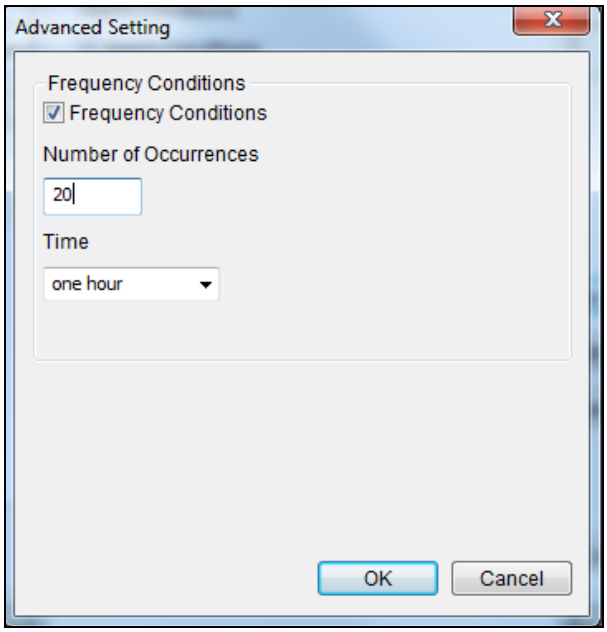
[Alarm Conditions] Define the price range for an alarm condition. For this example, when the price amount in a transaction is *great than* (>) than 2 dollars, the assigned alarm output and e-mail alert will be activated.

[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.

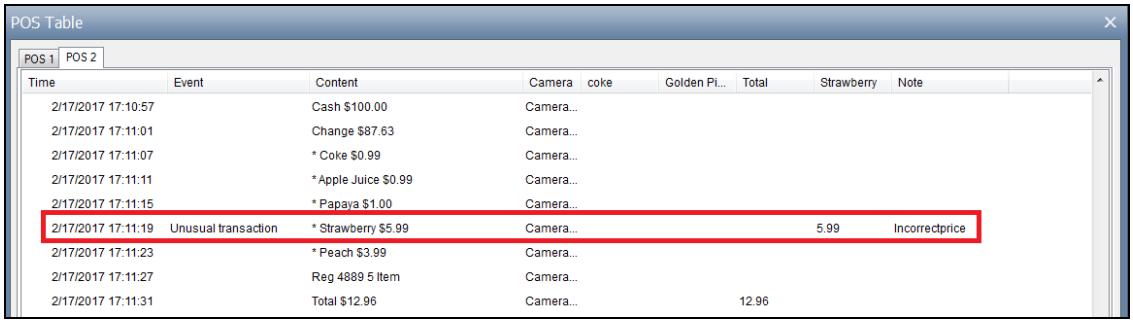
[Alert Message] Type an alert message (the space between letters is not allowed). When the defined alarm condition is met, e-mail notifications will be sent. To configure the e-mail server, see *Setting Up E-mail Notifications* in Chapter 1. In addition, the alert message will be recorded in the System 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.



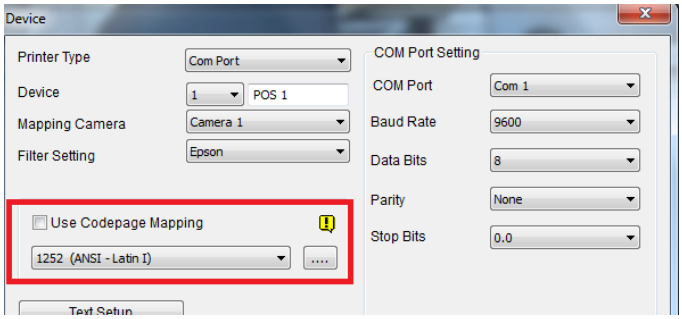
10.5 Mapping Codepage

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.

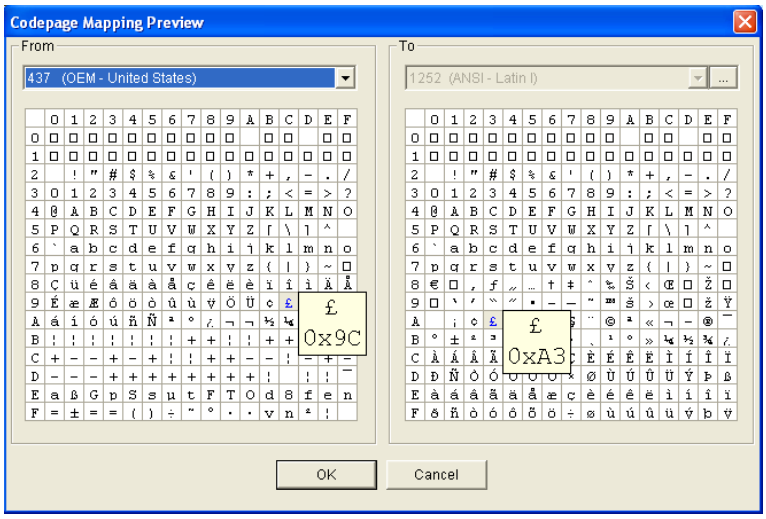
Note: When you cannot find a proper “Script” in the **Set Font** option in the POS Text Setup dialog box (see the dialog box in *Setting Up Text Overlay* earlier in this chapter), you may use the Codepage feature to fix the display issue of transaction text.

---

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.

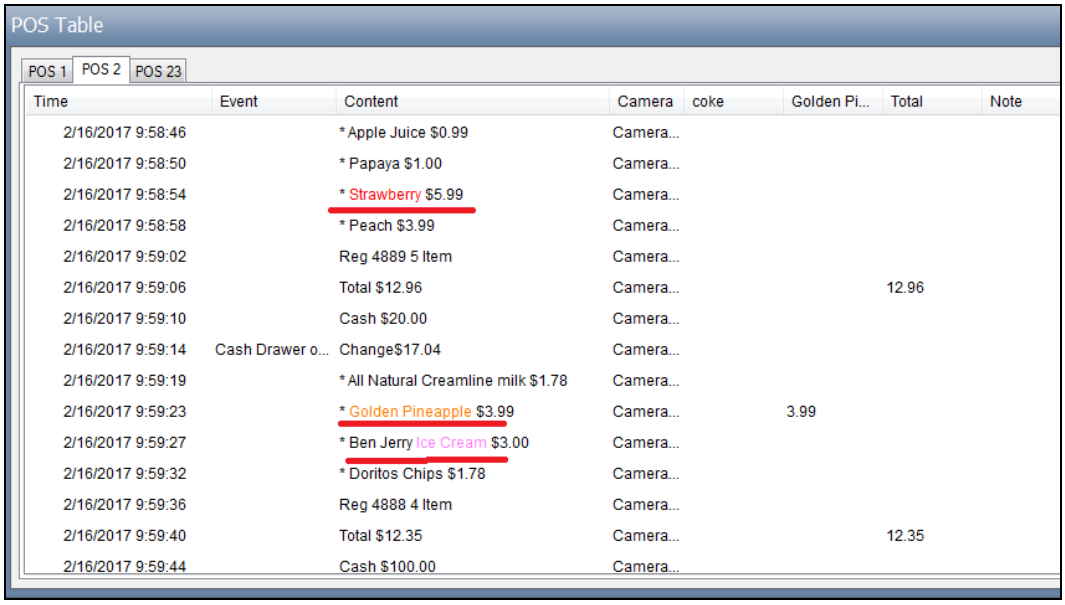


3. In the From field, select one symbol or character that are not displayed correctly. In this example, you can see its previous character code (From side: Ox9C) has been transferred to the default equivalent (To side: OxA3).

10.6 Coloring Transactions of a Product Item

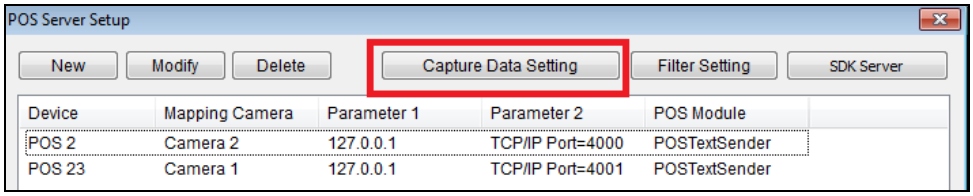
You can highlight a desired transaction item in any color. When the transaction item is identified, its text will have an outstanding color than others on the live view, and the alarm and e-mail alerts can be triggered at the same time. For example, if the liquor is prohibited for sale in the midnight, a seller can use this feature to prevent from any unintentional sale.

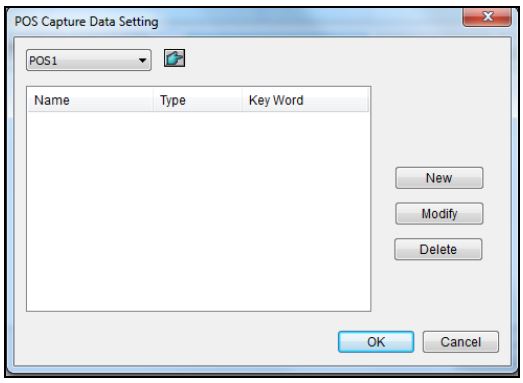
The identification will be recorded in the System Log for later retrieval as well. In this example, the transaction item “Strawberry” is colored red, “Golden Pineapple” is orange, and “Ice Cream” is pink whenever these transaction items appear.



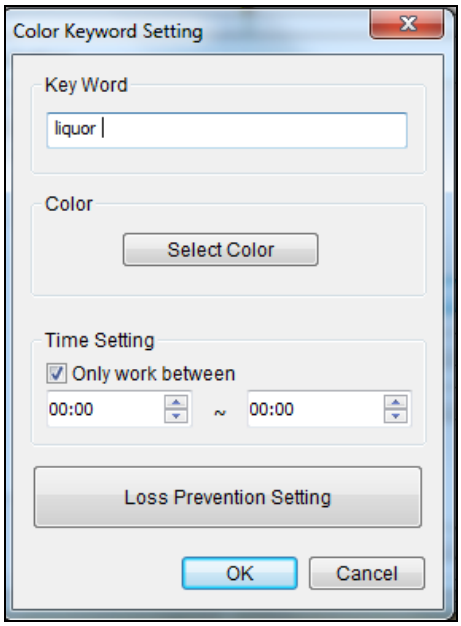
To configure the coloring feature, follow the steps below:

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.



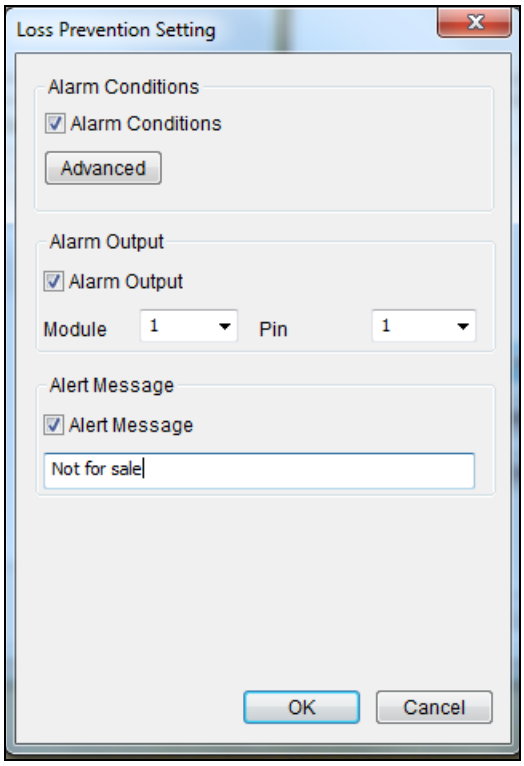
[Key Word] Type the keyword to be identified in the transactions. The field is case sensitive.

[Color] Select a color to show on the keyword.

[Only Work Between] Specify the time 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.



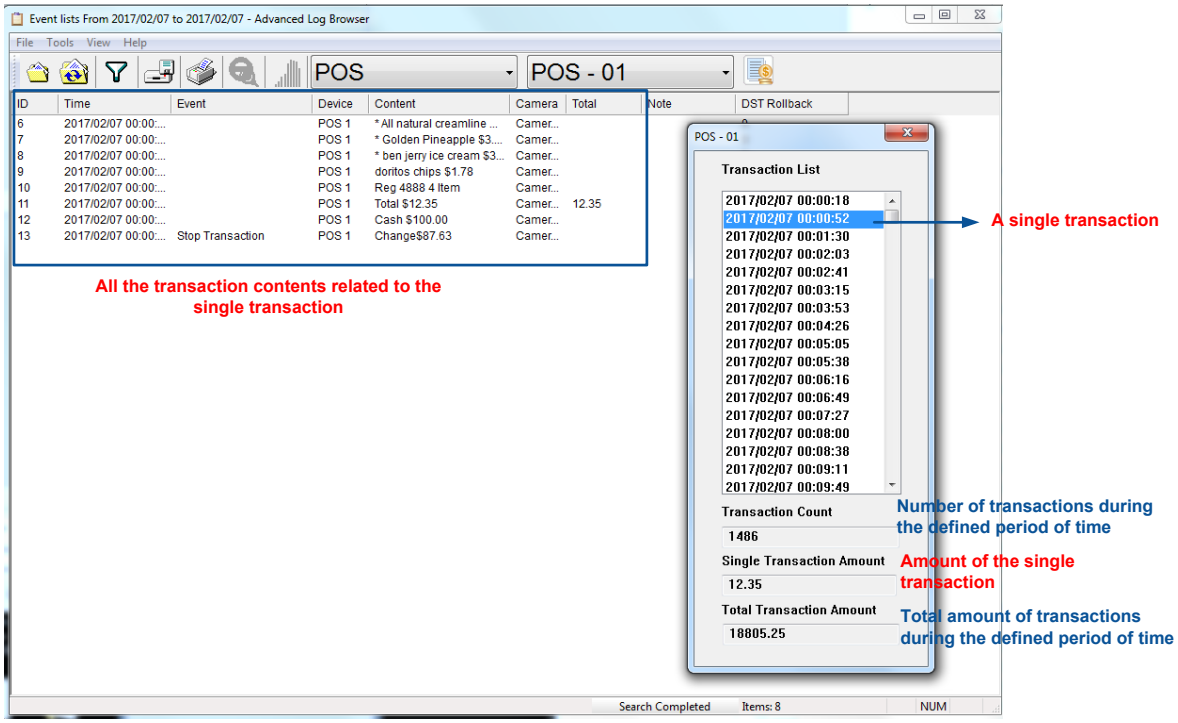
- **Alarm Conditions:** Enable the alarm when the defined text is detected. To configure alarm frequency, click the **Advanced** button. For details, see Step 3 in *Triggering Transaction Alarms* earlier in this chapter.
- **Alarm Output:** Assign an installed output module. When the defined alarm condition 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 appears not only 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.



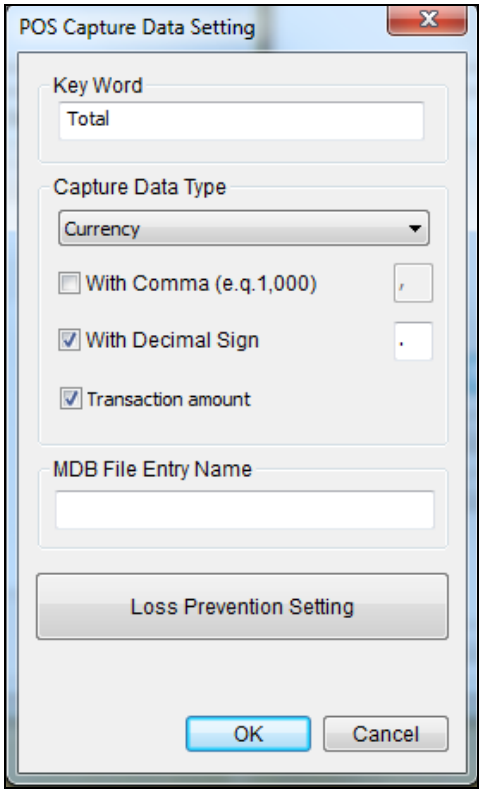
10.7.1 Setting Up Receipt Display Conditions

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:

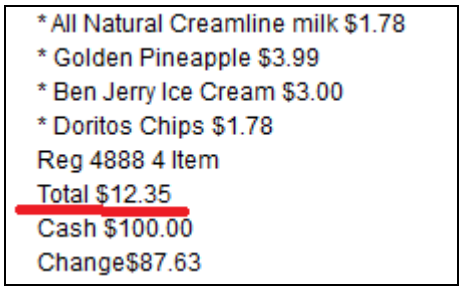
- *Step 1: Defining the Amount of a Transaction Shown on the Receipt*
- *Step 2: Define How a Transaction Ends on the Receipt*
- *Step 3: Displaying Receipt Details of a Transaction*

Step 1: 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.



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.

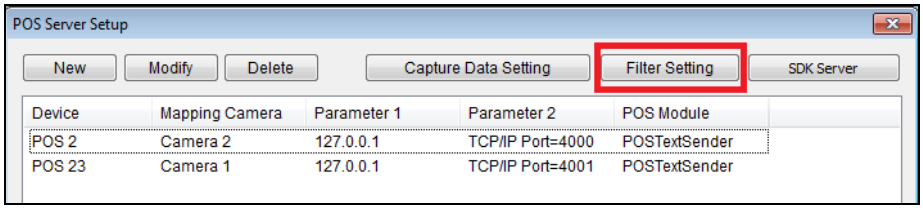
   a. Under Capture Data Type, define if the total amount is attached with a currency symbol. In this example, select **Currency** because the currency symbol $ is used.

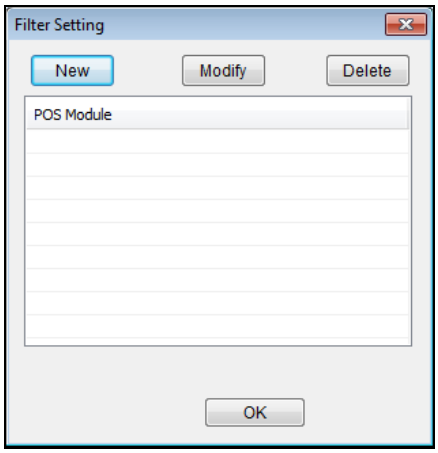
   b. Select **With Comma** if there are commas in the total amount. Select **With Decimal Sign** if there are decimal signs in the total amount. In this example of "Total $12.35", select **With Decimal Sign**.

4. Select **Transaction Amount**, and click **OK**.

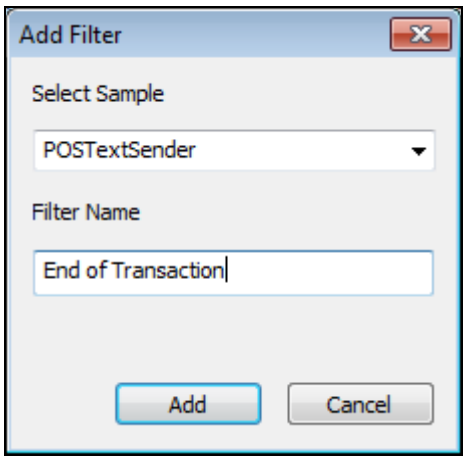
Step 2: Defining How a Transaction Ends on the Receipt

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.

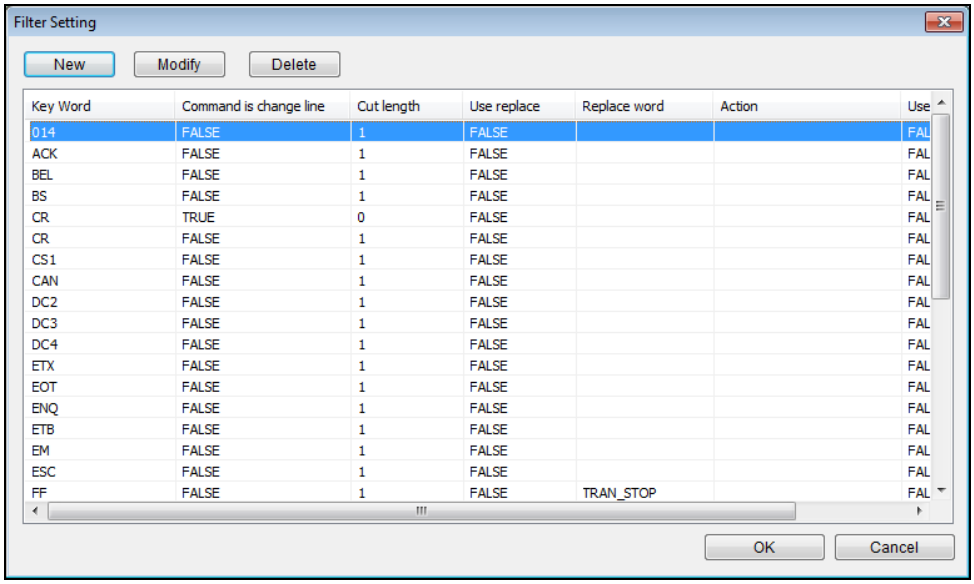


a. Under Select Sample, select the type of printer attached to the POS device or the GeoVision program installed in the POS device.

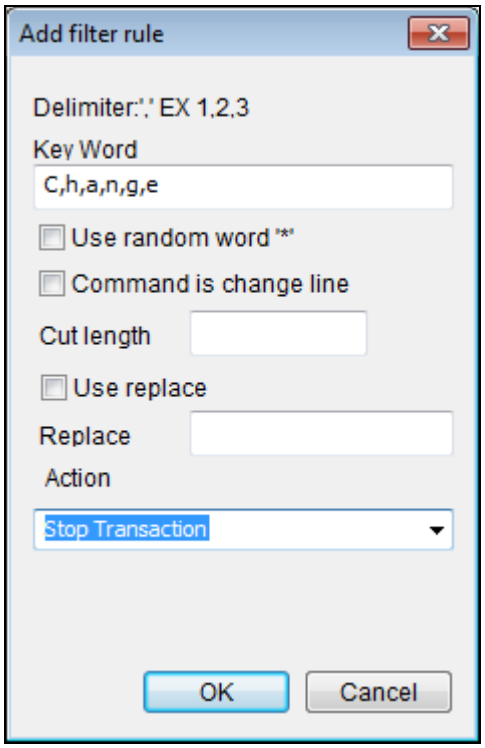
b. Under Filter Name, name the filtering criteria. In this example, we will define how a transaction ends on a receipt, so we will name it “End of Transaction”.

7. Click the **Add** button. The Filter Name appears in the list.

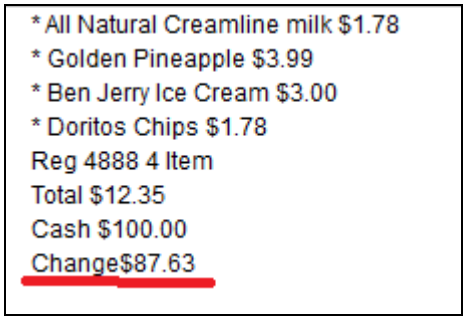
8. Select the created filter name and click the **Modify** button. This dialog box appears.



9. Click the **New** button. This dialog box appears.

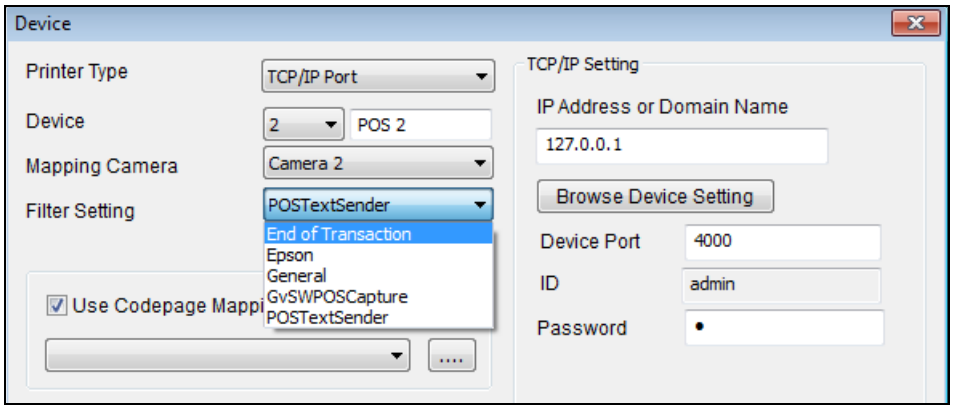


10. Type the **keyword** indicating the end of a transaction, and add comma (,) between every letter. In this example, the keyword is “Change” which appears at the end of every transaction, so type C,h,a,n,g.e.



11. Under Action, select **Stop Transaction**.
12. Click **OK** several times to return to the POS Server Setup dialog box.

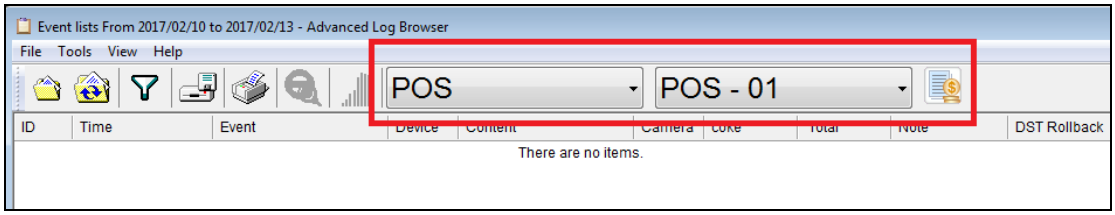
13. Select the POS device in the list applied for the filter setting, and click the **Modify** button. The Device dialog box appears.
14. Under Filter Setting, select the filter setting you set up for the end of a transaction. In this example, its “End of Transaction”.



15. Click **OK**.

Step 3: Displaying Receipt Details of a Transaction

16. Select **ViewLog** > **Toolbar** > **Tools** > **Advanced System Log**. The Advanced Log Browser Open Database dialog box appears.
17. Define a period of time to retrieve the POS data.
18. From the left side of the toolbar, select **POS** data, select which **POS** device, and click to have a list of transactions during the defined period of time.

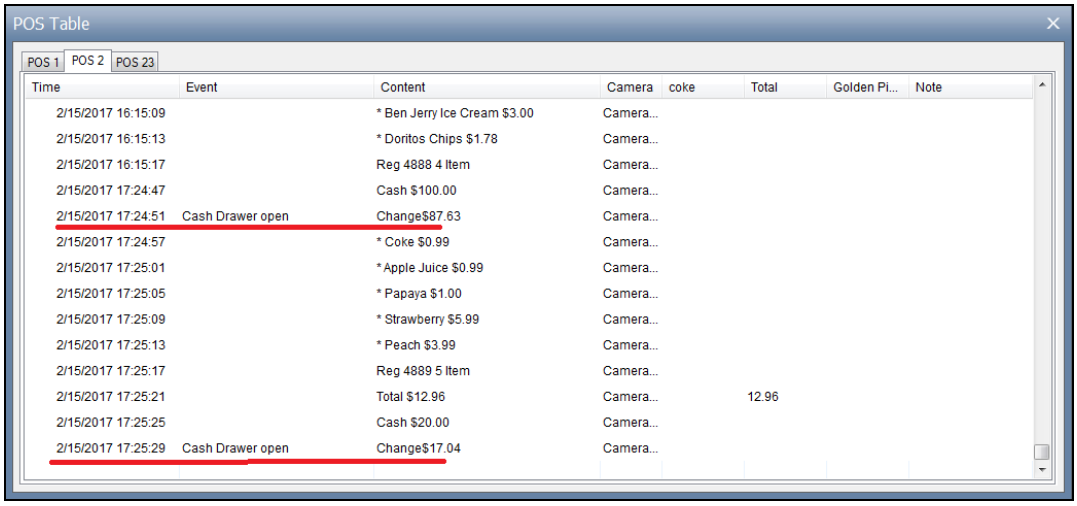


19. When you click a transaction on the List, its related receipt content will be displayed.

10.8 Filtering Transactions by a Keyword

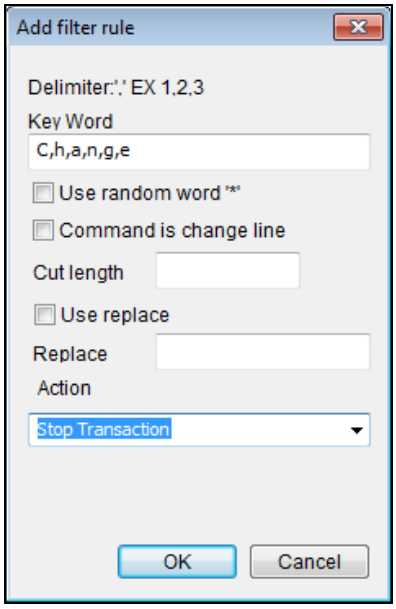
You can filter transactions by a keyword to have the following functions: to start a new line after the keyword, to remove unwanted text before the keyword, to replace a keyword with another, and/or to be noted as Event, such as Cash Drawer Open, in the System Log when the keyword appears.

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:

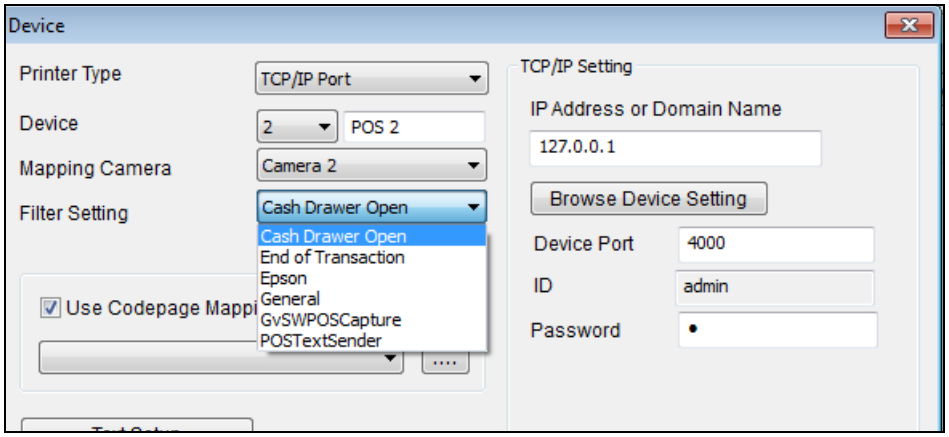
1. To open the following dialog box, follow Step 5 to 8 in *Step 2: Defining How a Transaction Ends on the Receipt, 10.6 Displaying Receipt Details of a Transaction*.



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.

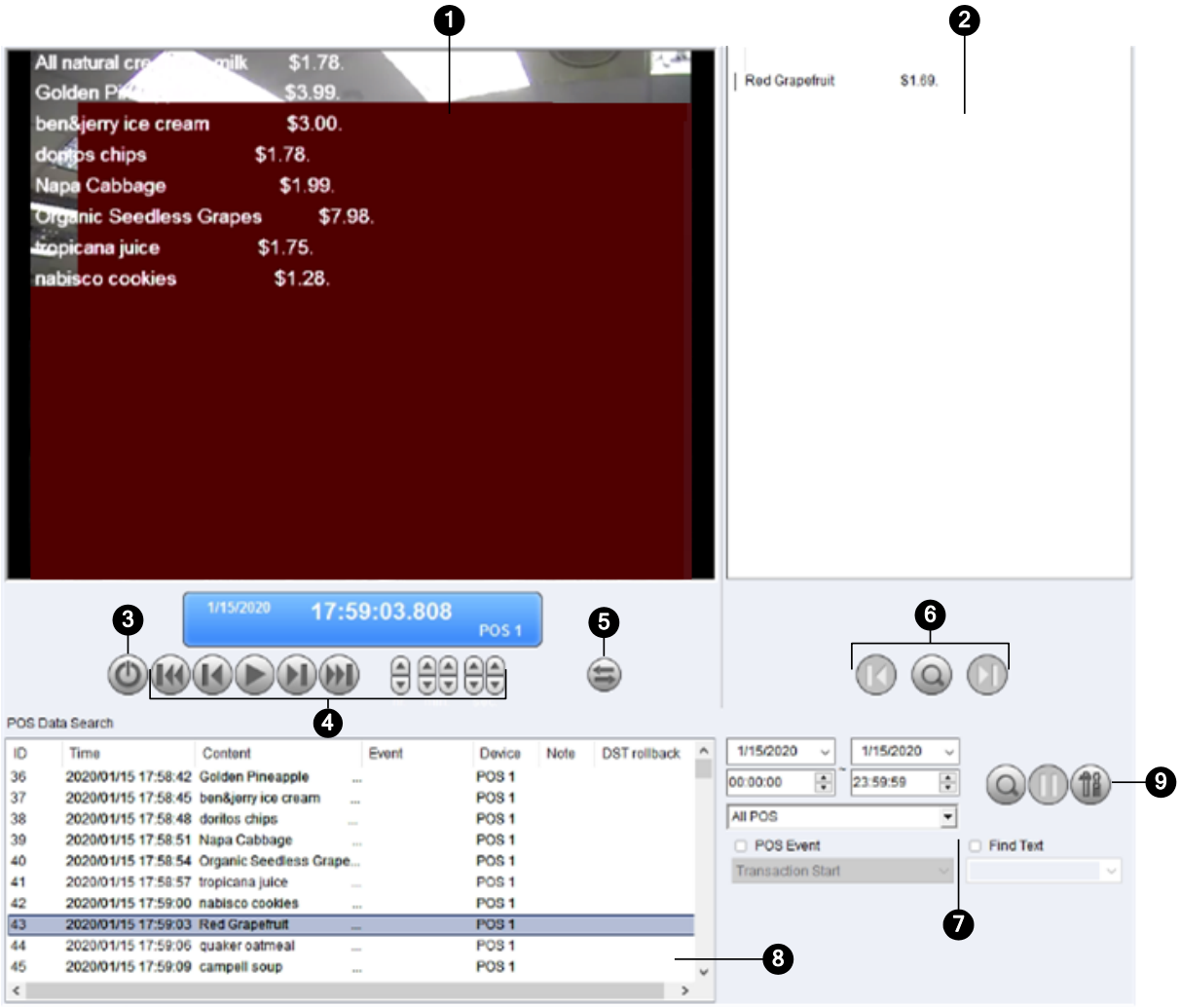


11. Click **OK**.

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, you can instantly search for and play back 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 the 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 window 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 time 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 of 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.