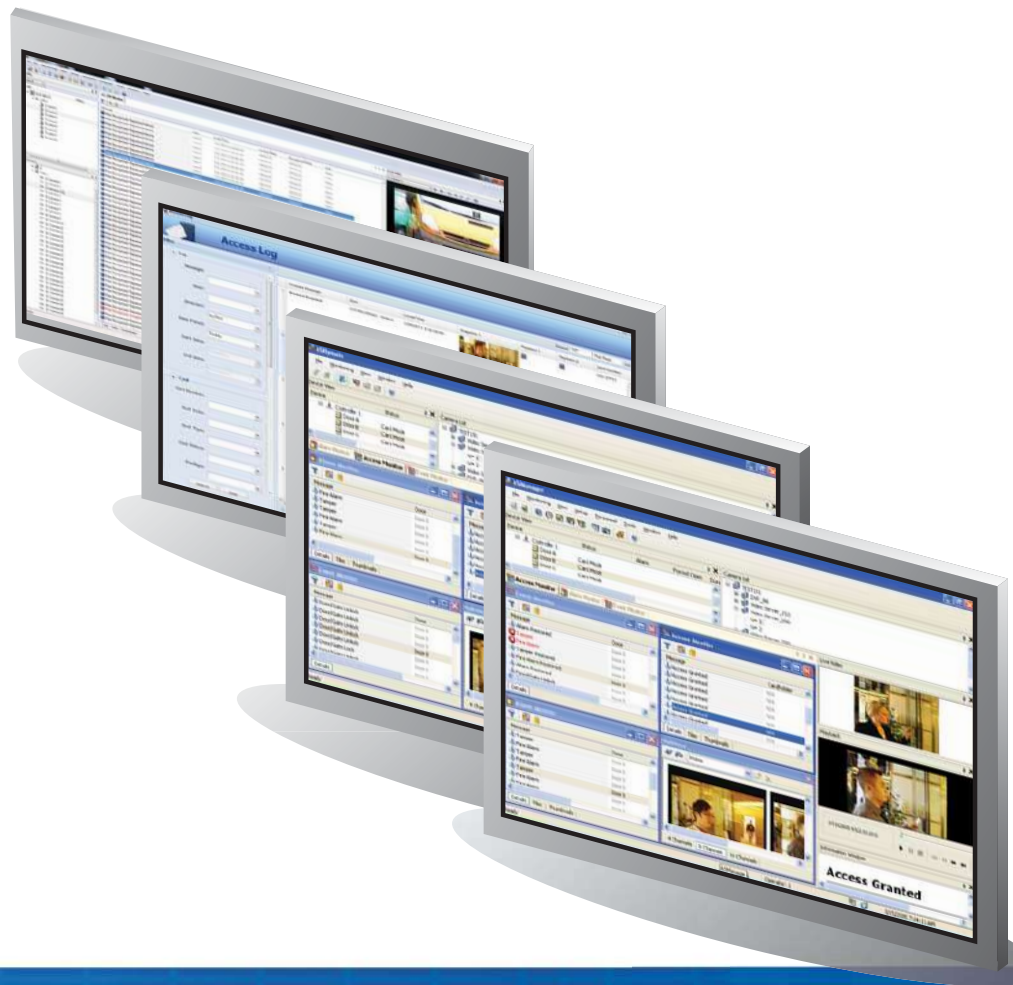




GV-ASManager

User's Manual





© 2025 GeoVision, Inc. All rights reserved.

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

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

GeoVision, Inc.
9F, No. 246, Sec. 1, Neihu Rd.,
Neihu District, Taipei, Taiwan
Tel: +886-2-8797-8377
Fax: +886-2-8797-8335
<http://www.geovision.com.tw>

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

December 2025

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



[Warranty]



[Technical Support Policy]

Contents

Note for Users to Upgrade GV-ASManager	vi
Firmware and Software Compatibility	vii
Naming and Definition.....	xi
Chapter 1 Introduction.....	1
1.1 Main Features	2
1.2 Concepts.....	5
1.3 Optional Devices	7
Chapter 2 Installation.....	8
2.1 System Requirements	8
2.2 Licensing.....	8
2.3 Installing GV-ASManager	9
2.4 Login	10
Chapter 3 The Main Screen of GV-ASManager.....	12
3.1 Main Screen	12
3.1.1 Toolbar	14
3.2 View Windows.....	15
3.2.1 Controls on the Window	15
3.3 Monitoring Windows	17
3.3.1 Controls on the Monitor Window.....	18
3.3.2 Customizing a Monitor Window	19
3.3.3 Arranging Monitor Windows	20
Chapter 4 Settings	21
4.1 Setup Flowchart	21
4.2 Adding Controllers.....	22
4.2.1 Configuring a Controller	22
4.2.2 Configuring Doors or Elevator Floors	25
4.3 Adding Cards	32
4.3.1 Adding a Single Card	32
4.3.2 Adding a Special Card.....	36
4.3.3 Adding a Group of Cards.....	37
4.3.4 Adding a Passcode	38
4.3.5 Importing/Exporting Card Data	39
4.3.6 Customizing a Card Data Field.....	40
4.3.7 Adjusting Columns on the Card List	41
4.4 Adding Weekly Schedules.....	42
4.4.1 Step 1: Adding Time Zones	43
4.4.2 Step 2: Adding Weekly Schedules.....	44

4.4.3	Step 3: Adding Holidays	46
4.5	Adding Access Groups.....	47
4.6	Adding Users	49
4.6.1	Adding a User	49
4.6.2	Customizing a User Data Field	51
4.6.3	Importing/Exporting User Data	52
4.3.4	Adjusting Columns on the User List.....	52
4.7	Adding I/O Boxes	53
4.7.1	Connecting GV-I/O Box.....	53
4.7.2	Configuring Input and Output Functions	55
Chapter 5	Video Integration	57
5.1	Mapping Cameras.....	58
5.2	Accessing a Live View.....	61
5.2.1	Live Video Window.....	62
5.3	Accessing Captured Images.....	63
5.4	The MultiView Window	63
5.5	Retrieving Recorded Videos.....	65
5.6	Applying Text Overlay	67
Chapter 6	Anti-Passback.....	69
6.1	Anti-Passback	70
6.2	Local Anti-Passback.....	71
6.3	Global Anti-Passback	73
6.3.1	Step 1: Enabling Global Anti-Passback	74
6.3.2	Step 2: Configuring Areas	74
6.3.3	Step 3: Configuring Readers	75
6.3.4	Step 4: Configuring Door Contacts	76
6.3.5	Step 5: Monitoring Areas.....	76
6.3.6	Step 6: Locating Users	77
Chapter 7	Patrol Tour	78
7.1	Creating Patrol Tour.....	78
7.2	Creating Rolling Patrol Tour	80
7.3	Activating the Patrol Tour	82
7.4	Monitoring Patrol Activities	84
7.5	Accessing Patrol Log.....	85
Chapter 8	Other Functions.....	86
8.1	Adding System Users.....	86
8.2	Setting up Alert Notifications	88
8.2.1	Setting up SMS Server.....	88
8.2.2	Setting up E-Mail Server	89

8.2.3	Setting up Notifications.....	90
8.3	Startup Settings.....	92
8.4	Setting up GV-GF Fingerprint Readers	94
8.5	Setting up GV-FR Face Recognition Readers	95
8.6	Scanning Driver's Licenses and Business Cards.....	96
8.7	Defining Hot Keys	98
8.8	Using Remote Lock Down App.....	99
8.9	Defining New Card Formats	102
8.10	Monitoring Emergency Exits with Input Sensors.....	103
8.11	Designing and Printing Access Card Template.....	105
8.12	Utilizing Job Codes	110
8.13	Defining Occupancy Limit.....	113
Chapter 9	GV-ASRemote	116
9.1	Installing GV-ASRemote	116
9.2	The GV-ASRemote Window.....	117
9.2.1	Windows Toolbar	118
9.3	Connecting to GV-ASManager	119
9.4	GV-ASRemoteWeb.....	121
Chapter 10	GV-ASWeb.....	122
10.1	Connecting to GV-ASManager	122
10.2	Functions on GV-ASWeb	124
10.3	Monitoring GV-ASManager	126
10.4	Accessing Logs.....	128
10.4.1	Defining Search Criteria	128
10.4.2	Log Window Icons	128
10.4.3	Exporting Logs	129
10.4.4	Defining Columns	130
10.5	Creating Maps.....	132
10.6	Setting up Export Schedule for Lists and Logs	135
10.7	Accessing GV-ASWeb using Mobile Devices	136
Chapter 11	GV-TAWeb for Workforce Schedule and Payroll	140
11.1	Connecting to GV-ASManager	141
11.2	Setting up Workforce Schedule	143
11.2.1	TA Shift: Setting up a Daily Schedule.....	143
11.2.2	TA Template: Setting up a Schedule Template	145
11.2.3	TA Holidays: Setting Certain Dates as Holidays	146
11.2.4	TA Schedule: Assigning Schedules to Employees.....	147
11.3	TA User: Specifying Hourly Pay	151
11.4	TA Report: Looking up Records	152

11.5	Creating Accounts to Manage GV-TAWeb	158
Chapter 12	GV-VMWeb for Visitor Management	159
12.1	Connecting to GV-ASManager	159
12.2	The GV-VMWeb Window	160
12.3	Creating Accounts to Manage GV-VMWeb	161
12.4	Creating Visitor Profiles	162
12.5	Granting Visitor Access	163
12.6	Searching GV-VMWeb Database	166
12.7	Visitor Self Registration	166
12.7.1	Setting up Mail Server in GV-VMWeb.....	167
12.7.2	Creating a Visitor Account	169
12.7.3	Creating a Visit Request.....	170
Chapter 13	License Plate Recognition	172
13.1	Installing PC LPR	173
13.1.1	Installing LPR Plugin	174
13.1.2	Inserting LPR Dongle	174
13.1.3	Accessing Recognition Results in PC LPR.....	175
13.2	Adding PC LPR	176
13.2.1	Step 1: Enabling LPR Functions in PC LPR	177
13.2.2	Step 2: Adding a PC LPR to GV-ASManager	178
13.2.3	Step 3: Configuring a Channel	180
13.2.4	Exporting LPR Data.....	186
13.3	Adding Standalone LPR	191
13.3.1	Step 1: Enabling Connection with GV-ASManager.....	192
13.3.2	Step 2: Adding a Standalone LPR to GV-ASManager	193
13.3.3	Step 3: Configuring a Channel	195
13.4	Adding Vehicles	197
13.5	Monitoring LPR Activities	200
13.5.1	LPR View Window	200
13.5.2	Monitoring Windows	201
13.6	Receiving Notifications for LPR Activities	202
13.7	Setting up Vehicle Hotlist	202
13.7.1	Setting up the Hotlist Database	202
13.7.2	Adding License Plates to the Hotlist	204
13.8	Managing Parking Lots.....	207
13.8.1	Setting up a Parking Lot	207
13.8.2	Monitoring Parking Lots.....	211
13.9	Calculating Average Speed	214
13.9	LPR Functions on GV-ASWeb	214

13.9.1	LPR List	215
13.9.2	Vehicle List.....	216
13.9.3	LPR Log.....	217
Chapter 14	Face Recognition.....	220
14.1	GV-Face Recognition Camera	221
14.1.1	Adding GV-Face Recognition Camera.....	222
14.2	GV-AI FR	223
14.3	Managing Face Recognition Access Data	225
Chapter 15	GV-Access Mobile App	229
Chapter 16	GV-ASNotify	230
16.1	Installing GV-ASNotify.....	230
16.2	Connecting to GV-ASManager	231
16.3	Utilizing GV-ASNotify	238
Chapter 17	Database Settings	234
17.1	Starting the Database Tools	234
17.2	Creating a Database	235
17.3	Other Database Settings	236
17.4	Mapping Source Database	236
17.4.1	Converting Data from the Active Directory Database.....	241
17.4.2	Converting Data from the OLE Database	247
17.4.3	Converting Data from an Excel File	247
Chapter 18	Firmware Upgrade	248
Chapter 19	Troubleshooting	249
Appendix	255
A.	Event Notifications	255
B.	E-Mail and SMS Alert Symbols	260
C.	Controller Status.....	261
D.	Supported Number of Connections.....	262

Note for Users to Upgrade GV-ASManager

If for any reason the system is not responding correctly after the software upgrade, you can restore your current database. Follow the steps below to back up the current database before upgrading to the latest version.

1. Run **ASDBManager.exe** from the GV-ASManager program folder at **C:\Access Control\ASManager** (by default, the folder is created in drive C).
2. Select **ASManager Database and Path Setting > Backup Database** to back up your current database.
3. Download the latest version from [GeoVision website](#) and upgrade GV-ASManager.

Note: After upgrading GV-ASManager, it is recommended to also upgrade the GV-AS / GV-EV Controller firmware. To upgrade the controller firmware, see the [Firmware Upgrade Instructions](#).

Firmware and Software Compatibility

The software versions compatible with GV-ASManager are listed below.

- **GV-DVR / NVR:** V8.5.9.0 or later
- **GV-VMS:** V15.10 or later
- **GV-Recording Server:** V1.4.2 or later
- **GV-Control Center:** V4.0.0 or later
- **GV-AI Guard:** V2.0 or later

The GV-AS / GV-EV Controller firmware versions compatible with GV-ASManager are listed below.

Models	GV-ASManager						
	V4.2.3	V4.3	V4.35	V4.4	V4.4.1	V4.4.2	V4.4.3
GV-AS100	V1.08						N/A
GV-AS110 / 120	V1.07						N/A
GV-AS400	V1.06						
GV-AS1010	V1.0	V1.1	V1.2		V1.3		V1.31
GV-AS1110	V1.0	V1.1	V1.2				V1.21
GV-AS1520 / 1620	N/A						N/A
GV-AS410	V1.23	V1.3	V1.4				V1.41
GV-AS210 / 810							
GV-AS2110 / 4110 / 8110							
GV-AS4111 / 81111							
GV-AS2120	N/A	V1.35					
GV-CS1320	N/A		V1.0	V1.10			V1.11
GV-EV48	V1.12	V1.3		V1.4			V1.41
GV-ASBox / GV-ASNet (Optional devices)	V1.07						N/A

	GV-ASManager											
Models	V5.0.0	V5.0.1	V5.0.2	V5.1.0	V5.1.1	V5.2.0	V5.3.0	V5.3.1	V5.3.2	V5.3.3	V5.3.4	V6.0.0
GV-AS100	N/A											
GV-AS110 / 120	N/A											
GV-AS400	V1.06											
GV-AS1010	V1.32						V1.40					
GV-AS1110	V1.21											
GV-AS1520	N/A	V2.00	V2.01	V2.02	V2.04	V2.05	V2.06					
GV-AS1620	N/A					V1.00	V1.02	V1.03	V1.04	V1.05		
GV-AS210 / 2110 / 2120	V2.00	V2.11	V2.12	V2.15	V2.20	V2.21	V2.31	V2.32	V2.40	V2.41		
GV-AS410 / 4110 / 4111									V2.32			
GV-AS810 / 8110 / 8111			V2.32									
GV-CS1320			V2.20		V3.0	V3.03	V3.04	V3.05	V3.06- V3.07	V3.08	V3.09- V3.10	V3.10
GV-EV48	V1.41		V1.43			V2.31						
GV-ASBox / GV-ASNet (Optional devices)	N/A											

	GV-ASManager					
Models	V6.0.1	V6.0.1A	V6.0.2	V6.1.0	V6.1.1	V6.1.2 V6.2.0
GV-AS100	N/A	N/A	N/A	N/A	N/A	N/A
GV-AS110 / 120	N/A	N/A	N/A	N/A	N/A	N/A
GV-AS400	V1.06	V1.06	V1.06	V1.06	NA	NA
GV-AS1010	V1.40	V1.40	V1.40	V1.40	V1.40	V1.40
GV-AS1110	V1.21	V1.21	V1.21	V1.21	V1.21	V1.21
GV-AS1520	V2.06	V2.06	V2.06	V2.06	V2.06	V2.06
GV-AS1620	V1.10 V1.11	V1.11	V1.11	V1.11	V1.13	V1.14
GV-AS210 / 2110 / 2120	V2.50	V2.50	V2.60	V2.60	V2.80 V2.82	V2.82
GV-AS410 / 4110 / 4111						
GV-AS810 / 8110 / 8111		V2.60	V2.60			
GV-CS1320	V3.10	V3.12	V3.12	V3.13	V3.13	V3.13
GV-EV48	V2.31	V2.31	V2.31	V2.31	V2.32	V2.32
GV-ASBox / GV-ASNet (Optional devices)	N/A	N/A	N/A	N/A	N/A	N/A

Naming and Definition

GV-DVR / NVR	GeoVision Analog and Digital Video Recording Software. GV-DVR / NVR also refers to Multicam System , GV-NVR System , GV-Hybrid DVR System and GV-DVR System at the same time.
GV-VMS	GeoVision Video Management System for IP cameras.
PC LPR	The PC LPR refers to GV-NVR LPR and GV-VMS LPR. A GV-NVR or GV-VMS can be turned into a GV-NVR LPR and GV-VMS LPR simply by installing the LPR Plugin and an LPR Dongle. The PC LPR is capable of comparing captured license plates with the database from GV-ASManager.
Standalone LPR	The standalone LPR refers to GV-DSP LPR, GV-LPR1200, GV-LPR2800-DL and GV-LPR2811-DL. These devices have built-in LPR processor, capable of comparing captured license plates with the database from GV-ASManager.

Chapter 1 Introduction

The integration of GV-ASManager, GV-AS Controller (door controller) and GV-EV Controller (elevator controller) offers full control of entrances of your premise. Up to 1,000 units of controllers can be monitored and controlled by one GV-ASManager.

The following diagram is an example of how GV-ASManager and controllers are set up.

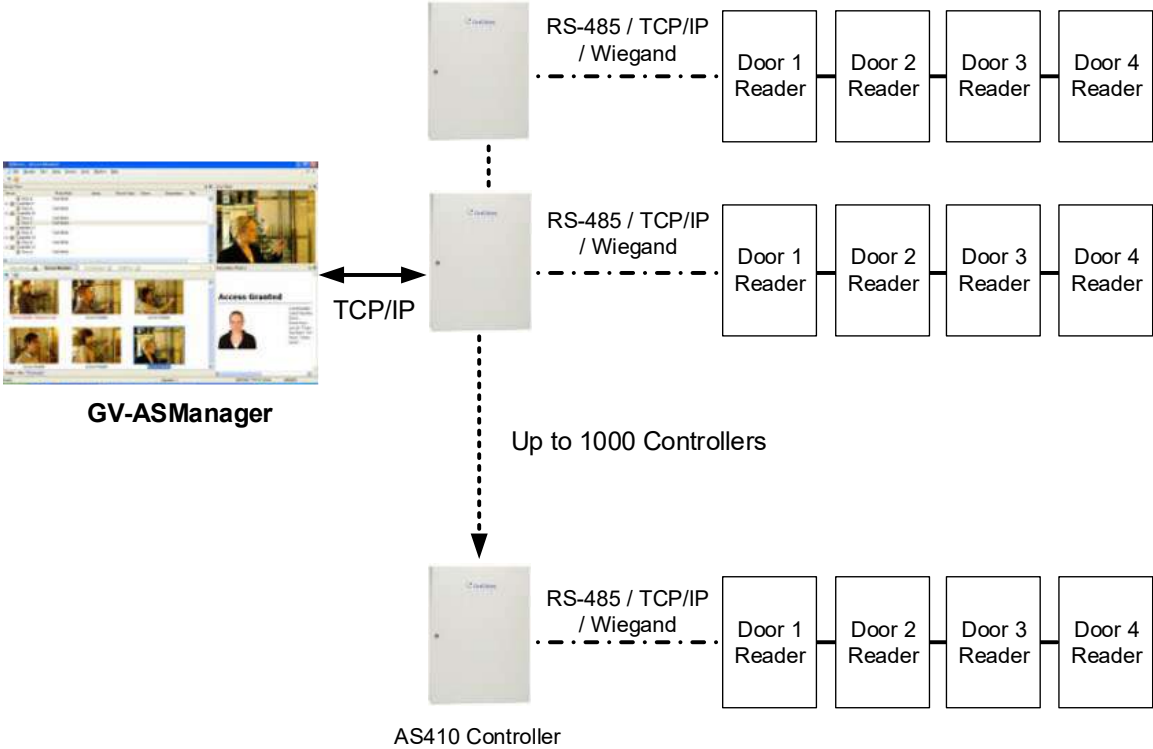


Figure 1-1

1.1 Main Features

Access Control

- Up to 1,000 GV-AS / GV-EV Controllers supported
- Four access modes: Card only, Card and PIN Code, Card or Common mode, Release mode
- Alarm conditions: door held open, door forced entry, tamper, access denied, duress, fire alarms
- SMS or E-Mail notification with user-defined content, video snapshot and user photo
- Up to 100,000 cards supported for GV-AS Controllers
- Up to 1,000 system users and 10,000 access groups
- Up to 256 time zones, weekly schedules and holiday planning for 14 months
- Multiple cards per user
- Enroll cards in batch mode
- Anti-Duress operation
- Anti-Passback capabilities
- Door interlock
- Man trap in double-door configuration
- Import/export of card and user data in Access or Excel file format
- User-defined screen layout and dual monitor display support
- Support Microsoft Access or SQL database
- Patrol Tour requiring security personnel to check in at the specified locations
- Integration of face recognition into security management with support for GV-Face Recognition Cameras / GV-AI FR (software) / GV-FR Panel (reader)
- User interface supported in Czech, English, French, Hebrew, Italian, Japanese, Portuguese, Russian, Serbian, Spanish, Traditional Chinese, Turkish, and Ukrainian

Video Integration

- Video integration with GeoVision software, IP devices and third-party IP cameras for live viewing
- Support for third-party IP devices using ONVIF, PSIA and RTSP protocols
- User-defined matrix of 16-channel multi-views
- Instant event playback

GV-ASRemote

- Monitor unlimited GV-ASManager over Internet
- Remote door monitoring, video playback, door operation

GV-TAWeb

- Flexible workforce schedule arrangement
- Payroll calculation
- Attendance and payroll report search

GV-ASWeb

- Remotely watch live view from connected devices
- Remotely control doors and LPR lanes
- Remotely add or delete cards, users, controllers, access groups, cameras
- Remotely set up operator accounts, patrol tours, parking lots, and notification settings
- Web interface for historical log search with corresponding video and snapshot
- Log export in Excel, Text, HTML, Zip and PDF file formats
- View access data on Google Maps in the order of access time

GV-VMWeb

- Web interface for creating visitor database and granting access
- Visitor record search
- Visitor self-registration

GV-LPR

- Up to 255 GV-DSP LPR, Edge GV-IP LPR Camera, and PC-based LPR
- Up to 8 recognition channels per PC LPR (GV-DVR / NVR / VMS / AI Guard LPR)
- Up to 100,000 vehicles supported
- Up to 100 Web browser connections supported
- Multiple vehicles assigned to a single user
- Import / export of vehicle data in Access or Excel file format
- Vehicle hotlist to identify stolen vehicles or vehicles of interest
- Parking lot management to regulate vehicle access, parking space availability, parking duration allowed, anti-passback, and shared parking

- Various notifications upon LPR events: e-mail, alarm, trigger recording, push notification, popup message
- GV-ASWeb to remotely access LPR settings and logs
- GV-Access mobile app to remotely monitor the alert status of each lane, open parking gates, and access live view

GV-Access Mobile App

- Support up to 5 GV-ASManager systems
- Provide the connection and alert status of each controller, door, LPR device and lane
- Access live views of cameras mapped to a door or lane
- Lock or unlock a door
- Open an LPR gate
- Clear an alert event
- Push notifications upon any access control, LPR, I/O box, system and user activity events from GV-ASManager
- Push notifications and live view call when the touchpad is activated in GV-CR1320 (reader) / GV-CS1320 (controller)

GV-Patrol Mobile App

- Access patrol tours created from GV-ASManager
- Check in at patrol points
- View patrol status and historical tours

1.2 Concepts

Understanding the following concepts may help you read through the manual.

Weekly Schedule	<p>A weekly schedule is certain days of the week when a user is granted access to a secure site.</p> <p>For details, see <i>4.4 Adding Weekly Schedules</i>.</p>
Access Group	<p>An access group is a group of users with identical location restrictions during the same time restraints.</p> <p>For details, see <i>4.5 Adding Access Groups</i>.</p>
Alarm Condition	<p>An alarm condition is a condition monitored through sensors, and alarms will be activated when the condition is detected by sensors. For example, GV-AS210 controller can monitor up to 8 sensors, such as door status sensor, smoke detector and tamper detector. GV-AS210 controller also provides output relays for activating and deactivating electric lock, siren and emergency door release when the alarm condition occurs.</p> <p>GV-AS100 / 1010 / 110 / 1110 / 120 have built-in sensors to detect whether the controller is being physically tampered with (i.e. opening of the controller or sustaining strong impact). For GV-AS210 / 2110 / 2120 / 410 / 4110 / 810 / 8110 / 1620, the tampering alarm sensor needs to be installed separately and triggering conditions depend on the type of sensor installed.</p> <p>For settings of alarm conditions, see <i>4.2.2 Configuring Doors and Elevator Floors</i>. For configuring inputs and outputs see GV-AS / GV-EV Controller User's Manual.</p>
Anti-Duress	<p>If a person is forced to open the door under threat, he or she can enter a PIN plus 1 to activate an alarm and inform the ASManager to dispatch the police. For example, the PIN is 5555 and you enter 5556. The door will open normally (access granted) and the alarm will be activated. The function is enabled by default.</p>
Anti-Passback	<p>The feature is designed to prevent card sharing and to enforce use of entrance and exit readers. If a card is used at an entrance reader, it must be used at an exit reader before it will be valid at the entrance reader again. For settings, see <i>4.2.2 Configuring Doors and Elevator Floors</i>.</p>

Interlock	<p>The feature is also called “mantrap” or interlocking”. The feature interlocks a door with one or multiple doors connected to the same controller. For example, if door A is set to interlock with Door B and C, neither of Door B or C will unlock when Door A is open/unlocked. When either of Door B or C is open/unlocked, Door A will not unlock.</p> <p>For settings, see <i>4.2.1 Configuring a Controller</i>.</p>
Two-person A/B rule	<p>The door unlocks only when two assigned cards are presented in order.</p> <p>For settings, see <i>4.3.1 Adding a Single Card</i>.</p>
IP device	<p>The video device connects to GV-ASManager through network. GV-ASManager displays live video from not only GeoVision IP devices (GV-DVR / NVR / VMS, GV-AI Guard, GV-Recording Server, GV-Video Server, GV-Compact DVR and GV-IP Camera) but also third-party IP cameras through ONVIF, PSIA and RTSP protocols.</p> <p>For details, see <i>Chapter 5 Video Integration</i>.</p>
Device Group	<p>The feature allows the system administrator to restrict a user account to only be able to read, write or execute the controllers, cards, users, access groups, time zones and weekly schedules assigned under a device group. For example, the administrator can create a device group for the sales department and assign related cards and controllers under the device group. Employees in the sales department will only have access to the cards and controllers of their own department.</p> <p>For details, see <i>8.1 Adding System Users</i>.</p>
Door Group	<p>When a large number of controllers are connected to GV-ASManager, the doors of different controllers can be organized into door groups. The door group allows you to quickly upload fingerprints and user data to the doors installed with fingerprint or face recognition readers.</p> <p>For details, see <i>Uploading Fingerprints to Controllers Using Door Groups</i> section in Chapter 3 of GV-GF Fingerprint Reader User's Manual.</p>

1.3 Optional Devices

Optional devices can expand the capabilities and versatilities of your GV-ASManager. Consult your sales representative for more information.

<p><u>GV-FWC</u></p>	<p>GV-FWC integrates GeoVision face-recognition-based cameras, software and readers into an access control system by sending access card data, paired to Face IDs, to controllers either through TCP/IP or Wiegand.</p>
<p><u>GV-IO Box Series</u></p>	<p>GV-IO Box series provides 4 / 8 / 16 inputs and relay outputs, and supports both DC and AC output voltages, with optional support for Ethernet module and 4E additionally supporting PoE connection.</p>
<p><u>GV-PCR Enrollment Reader</u></p>	<p>GV-PCR1251 / 1352 is a USB card reader, supporting 125 kHz / 13.56 MHz, designed to assist with GV-AS ID Card / Key Fob enrollment to GV-ASManager.</p>

Chapter 2 Installation

2.1 System Requirements

For GV-ASManager V4.2.1 or later, the following is the minimum system requirements.

Number of Controllers		0-50	51-100	101-1000
OS	64-bit	Windows 10 / Windows 11 / Server 2016 / Server 2019 / Server 2022		
CPU		Intel Core i3, 3.4 GHz (2 Cores, 2 Threads)	Intel Core i5, 3.4 GHz (2 Cores, 2 Threads)	Intel Core i7, 3.0 GHz (4 Cores, 8 Threads)
Memory		8 GB RAM		16 GB RAM
Hard Disk		500 GB		1 TB
Database		MDB or Microsoft SQL database		Microsoft SQL database
Program		.NET Framework 4.5 Microsoft SQL Server 2005 Express (optional)		
Browser		Internet Explorer 9.0 or later, Edge, Chrome, Firefox		
Note: The program .NET Framework 4.5 is required to run GV-ASManager.				

2.2 Licensing

Free License		4 controllers
Maximum License		1000 controllers
Increment for Each License		1 controller
Optional Combination		GV-AS Controllers + GV-Patrol
Type	GV-USB Dongle	External or Internal
	Software License	GV-ASManager V5.3.0 or later only

Note:



1. The Maximum License is a paid service.
2. Starting from GV-ASManager 5.3.0, Software Licenses can be purchased and registered in place of USB dongles, see [Software Licensing for GV-ASManager](#).
3. Software licensing is not compatible with GV-USB dongle, and ONLY supports the following controllers.
 - GV-AS210 series / 410 series / 810 series firmware V2.30 or later
 - GV-AS1520 firmware version V2.03 or later
 - GV-AS1620 firmware version V1.01 or later
 - GV-CS1320 firmware V3.01 or later
 - GV-EV48 firmware V2.30 or later

2.3 Installing GV-ASManager

Starting from version 4.2.1, the GV-ASManager software supplied with GV-AS / GV-EV Controllers can connect with up to 4 controllers for free. If you need to manage more than 4 controllers, a **USB dongle** or **Software License** is required. GV-ASManager supports connections with up to 1,000 GV-AS / GV-EV Controllers.

Note: Starting from GV-ASManager 4.2.1, no USB dongle is needed to connect to IP cameras.

You can install the driver and GV-ASManager from the GeoVision website.

4. Go to the Download page of [GV-ASManager](#).
5. If the USB dongle of licensing is used:
 - 5.1 Insert the USB Dongle to your computer.
 - 5.2 To install USB driver, select **Driver & F/W** from the dropdown list and click the **Download** icon  of **GV-Series Card Driver / USB Devices Driver**.
6. To install GV-ASManager, select **Primary Applications** from the dropdown list and click the **Download** icon  of **GV-ASManager**.
7. To download and install **Microsoft DirectX End-User Runtimes (November 2008)**, visit [here](#).
8. To download and install **.Net Framework 4.5**, visit [here](#).

2.4 Login

Before using GV-ASManager, you need to set the login ID and password, and create a database.

1. In the **Start** menu, select **Access Control** and click **ASManager**. When starting the system for the first time, the system will prompt you for a Supervisor ID and Password.

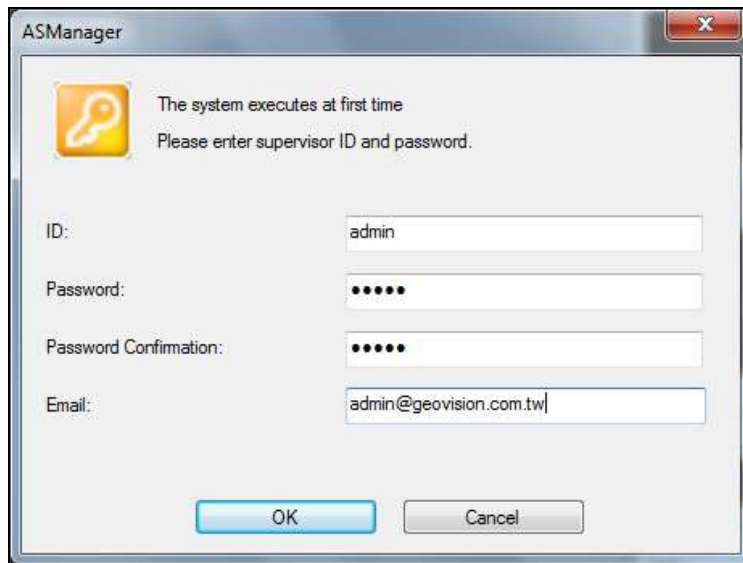


Figure 2-1

2. Type an **Email** address so that your password can be sent to the email address when forgotten. Remember to set up the email server after you log in. See *8.2.2 Setting up E-Mail Server* for details.
3. Type a desired ID name and password for the Supervisor account. This dialog box appears.



Figure 2-2

4. Re-type the **ID** and **Password**. If you want to skip the login process in the future, select **Auto Login**.
5. Click **OK**. The message “*Can’t open database. Would you like to set up database?*” appears.
6. Select **Yes** to create a database. The ID and password you have configured in Step 1 are required to access the feature. This dialog box appears.

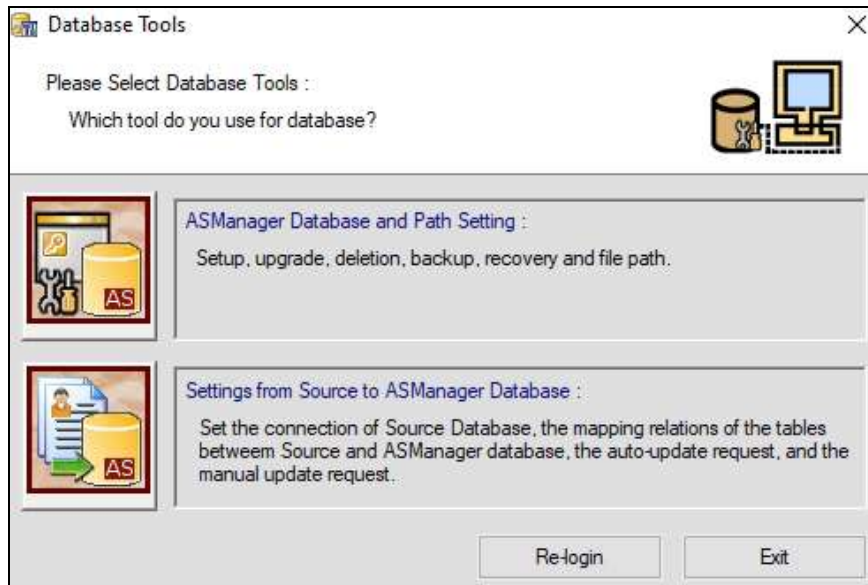


Figure 2-3

7. Select **ASManager Database Setting and Path Setting**. The ASManager Database Setting dialog box appears.
8. You can create either a Microsoft Access database or a Microsoft SQL database.
 - To create a Microsoft SQL database, see *Chapter 17 Database Settings*.
 - To create a Microsoft Access database for first-time users of GV-ASManager, Select **Setup MDB / MSSQL Database for ASManager**. The Setup Database Connection dialog box appears. Select **Microsoft Office Access Database**, and click **OK**. The program starts creating a database. When it is complete, the message “Setup database connection successfully” will appear.
9. Restart **ASManager**. You can see the main screen of GV-ASManager.

Note: By default, the Access database is created at C:\Access Control\ASManager\ASRes.

Chapter 3 The Main Screen of GV-ASManager

After you run GV-ASManager, the following main screen appears. Get yourself familiar with the main screen as it will help you when you read further into the following sections.

Note: After closing the main screen, GV-ASManager will continue to run in Windows Task Manager.

3.1 Main Screen

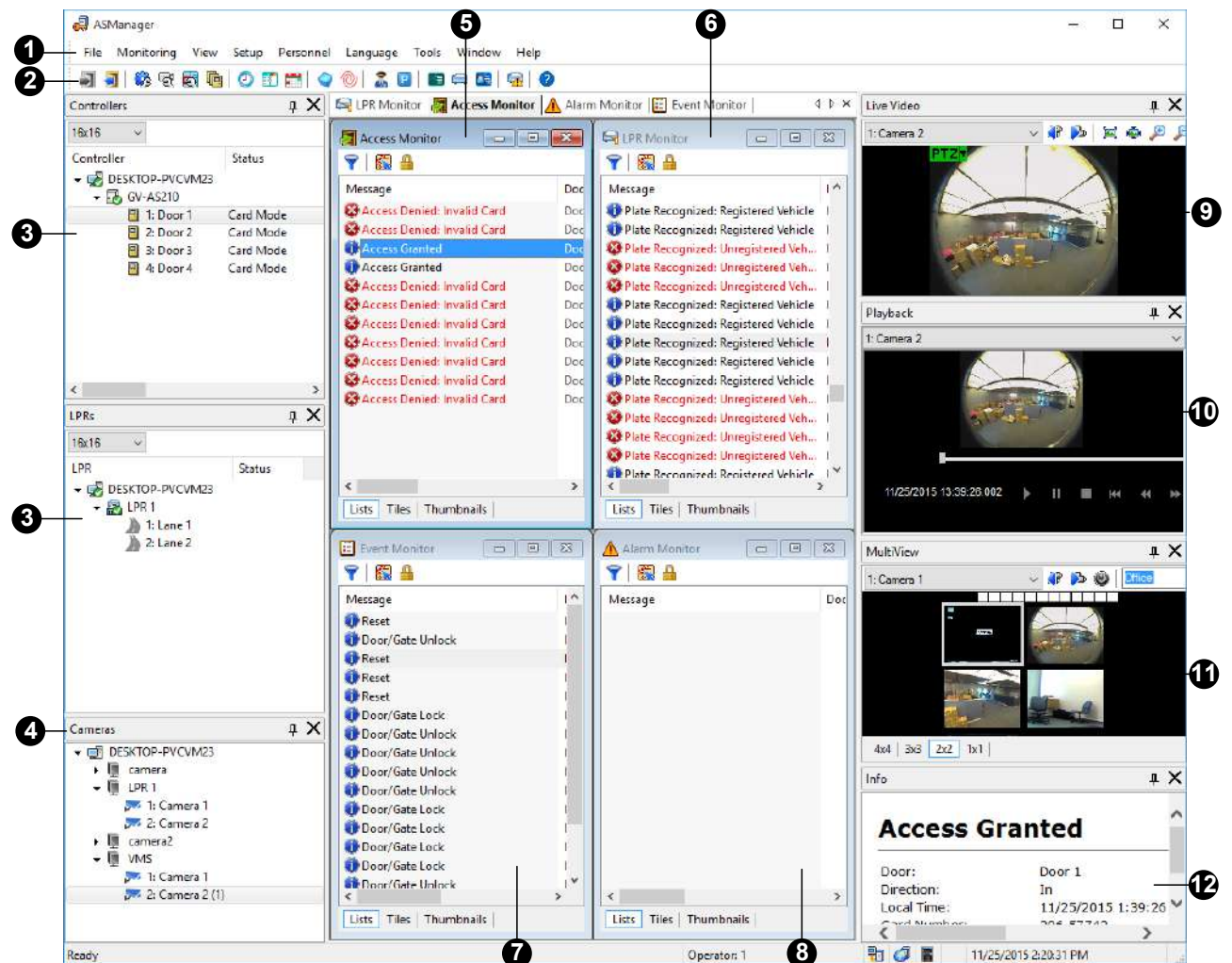


Figure 3-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of File (log in / out GV-ASManager), Monitoring (display monitoring windows), View (display the function windows), Setup (set up connected devices and schedules), Personnel (set up the users' accounts), Language (select language of user interface), Tools (set up notification and log) and Window (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of Login, Logout, Devices, Cameras, Areas, Door Groups, Time Zones, Weekly Schedules, Holidays, Access Groups, Feature Access, Patrol Tours, Parking Lots, Cards, Vehicles, Users, Hotlist, and About.
3	Controller / LPR View Window	Displays a list of connected controllers / LPR devices and their current status. You can change the size of icons to 16 x 16, 24 x 24 or 32 x 32 from the dropdown list.
4	Camera View Window	Displays a list of connected cameras.
5	Access Monitor	Displays access activities of doors.
6	LPR Monitor	Displays LPR activities and status.
7	Event Monitor	Displays monitored events of doors.
8	Alarm Monitor	Displays alarm events of doors.
9	Live View	Displays the live view of one connected camera. For details, see <i>5.2 Accessing a Live View</i> .
10	Playback	Plays back recorded events from a compatible GeoVision IP device. For details, see <i>5.5 Retrieving Recorded Video</i> .
11	MultiView	Displays live views of multiple IP devices connected. For details, see <i>5.4 The MultiView Window</i> .
12	Information Window	Displays the information of doors, card readers and monitored events.

3.1.1 Toolbar



Figure 3-2

No.	Name	Function
1	Login	Logs in GV-ASManager.
2	Logout	Logs out GV-ASManager.
3	Monitoring Windows	Open a desired Monitoring window. See <i>3.3 Monitoring Windows</i> .
4	Devices	Defines controllers, doors, LPR devices, I/O boxes and cameras. See <i>4.2 Adding Controllers</i> .
6	Areas	Configures Global Anti-Passback. See <i>6.3 Global Anti-Passback</i> .
12	Feature Access	Uploads the enrolled fingerprints and user data to the controllers and face recognition readers respectively. See <i>Chapter 3 Fingerprint Only Mode</i> in GV-GF Fingerprint Reader User's Manual or Uploading to the Face Recognition Reader in <i>Chapter 5</i> of GV-FR Face Recognition Reader User's Manual .
13	Patrol Tours	Creates patrol tours to require security staff to check in at the specified locations. See <i>Chapter 7 Patrol Tour</i> .
15	Cards	Creates and edits a database of card information. See <i>4.3 Adding Cards</i> .
16	Vehicles	Creates and edits a database of vehicle information. See <i>Chapter 13 License Plate Recognition</i> .
17	Users	Creates and edits a database of user information. See <i>4.6 Adding Users</i> .
18	Hotlist	Sets up vehicle hotlist to identify stolen vehicles or other vehicles of interest. See <i>13.7 Setting up Vehicle Hotlist</i> .
19	About	Displays the version of GV-ASManager.

3.2 View Windows

To see the status of a list of connected controllers, LPRs, cameras, and I/O Boxes, click **View** on the menu bar and select **Controllers**, **LPRs**, **Cameras** or **I/O Boxes**.

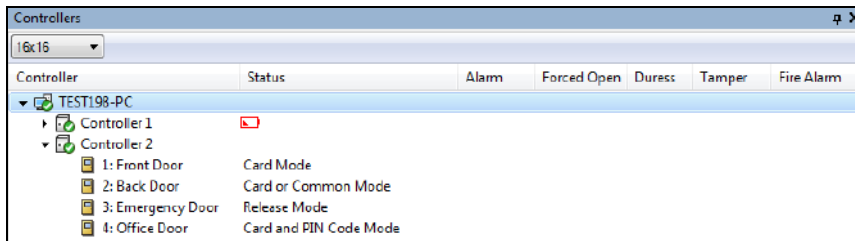


Figure 3-3

3.2.1 Controls on the Window

You can control the connected controller or door by right-clicking it in the Controller List window. The following control options are available when right-clicking the GV-ASManager's PC, Door and/or Controller:

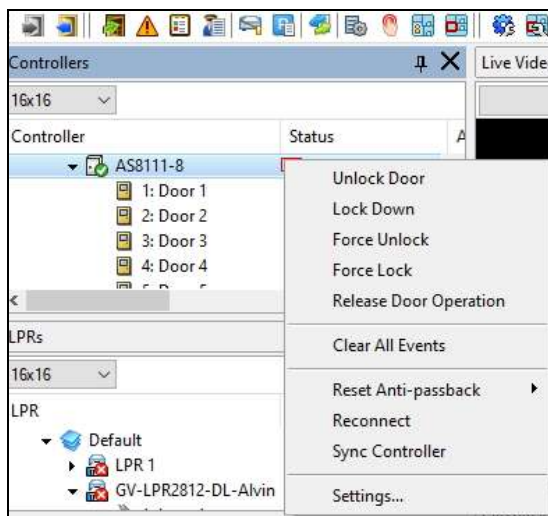


Figure 3-4

Name	Function	Available
Unlock Door, Lock Down, Force Unlock, Force Unlock with Timer Force Lock, Release Door Operation	Control the selected door or all doors associated with the selected controller. The Force Unlock and Force Lock keep the door stay open or locked until you select Release Door Operation . The Force Unlock with Timer allows you to set a time in minutes, after which the door will be locked.	PC Controller Door

	<p>The Unlock Door unlocks the door temporarily for the time interval specified. See “Lock Reset Time” at Step 2 in <i>4.2.2 Step 2: Configuring the Doors</i>.</p> <p>The Lock Down is only supported by GV-AS1010 / 1110 / 210 / 2110 / 2120 / 410 / 4110 / 810 / 8110 / 1620. It locks down the selected door or all doors associated with the selected controller. This function overrides the Authentication Schedule and the door(s) can only be opened by presenting the assigned access card.</p>	
Clear All Events	<p>Clear all alarm events of the selected PC / door / controller.</p> <p>When clearing any events, users are prompted to add a note for this action, which is recorded within User Action Monitor (Monitoring > New User Action Monitor).</p>	PC Controller Door
Reset Anti-Passback	<p>Enable a user to re-access the entrance or exit reader. See <i>Chapter 6 Anti-Passback</i>.</p>	PC Controller
Sync Controller	<p>Sync the settings between the controller and GV-ASManager immediately.</p>	PC Controller
Reconnect	<p>Reconnect to the controller.</p>	Controller
Settings	<p>Access the Controller setup dialog box.</p>	Controller Door
ASWeb	<p>Link to GV-ASWeb.</p>	PC
Stop Alarm, Clear Forced Open, Clear Duress, Clear Tamper, Clear Fire Alarm, Clear Held Open, Clear Access Denied	<p>Clear the alarm conditions. For alarm settings, see <i>4.2.2 Configuring Doors or Elevator Floors</i>.</p>	Door
Sync GV-GeoFinger / GV-FR2020 / GV-VD8700 / GV-FD8700-FR / GV-AI FR / GV-FR Panel	<p>Add the selected user data to and replace the current databased on the device or program.</p>	Door

3.3 Monitoring Windows

The Monitor windows allow you to monitor various activities.

- To open the Monitor window, click **Monitoring** on the menu bar, and select the desired one.

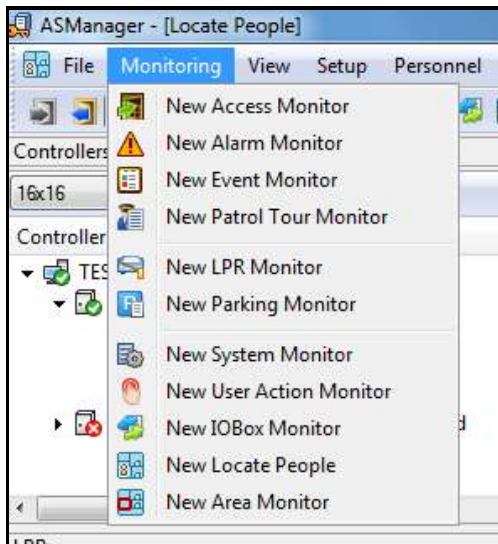


Figure 3-5

3.3.1 Controls on the Monitor Window

The controls available on the Monitor windows vary. Here we use the Access Monitor window as example to explain the controls.

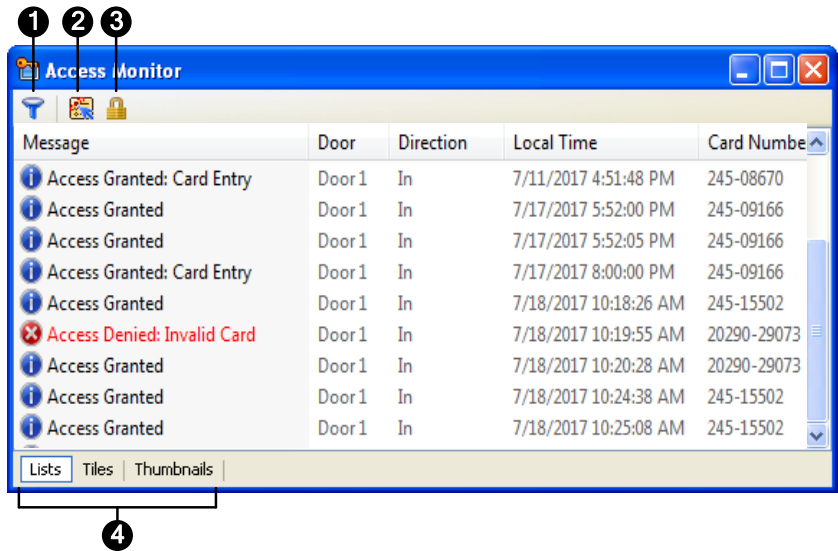


Figure 3-6

No.	Name	Function
1	Filter	Sets filter criteria to only display the desired activity information. See 3.3.2 Customizing a Monitor Window.
2	Auto Select	Focuses on the latest data display.
3	Lock	Suspends the current data display.
4	Lists / Tiles / Thumbnails	Decides how events are displayed on the window. In Tiles and Thumbnails views, user profile photos and snapshots captured will be displayed if available.

In some Monitor windows, you can right-click a message to have more options or detailed information. Below is an example of the options available when right-clicking a message in the Access Monitor window.

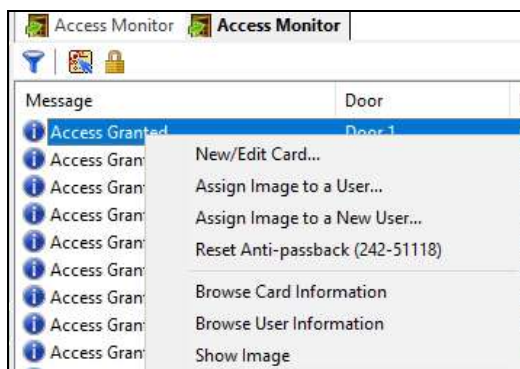


Figure 3-7

3.3.2 Customizing a Monitor Window

You can customize the messages displayed on a Monitor window by defining filter criteria. Multiple custom Monitor windows can be added for your specific requirements.

1. To add one Monitor window, click **Monitoring** on the menu bar, and select one.
2. Click the **Filter** button on the Monitor window. This dialog box appears.

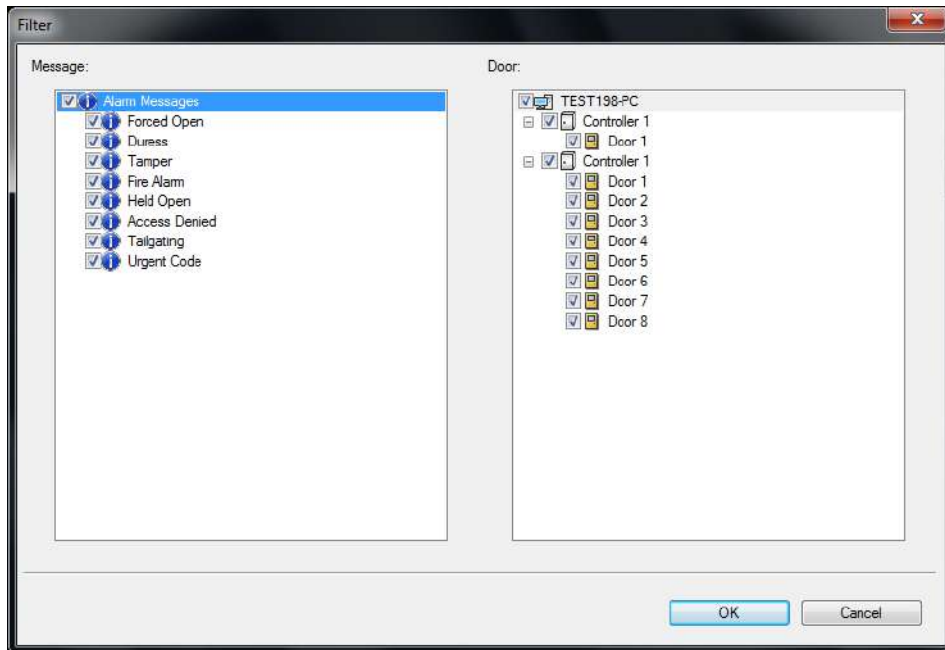


Figure 3-8

3. Select the desired messages and devices for monitoring, and click **OK**. The Monitor window will only display the messages based on the defined criteria.
4. Right-click the **Monitor** tab on the main screen, and select **Rename** to name the window.

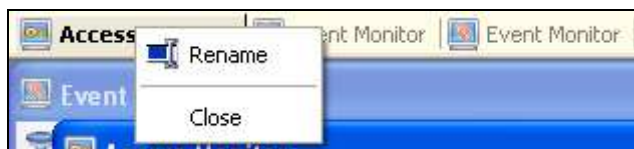


Figure 3-9

Note: The added windows are only for one-time use, and they cannot be saved after the Monitor window is closed.

3.3.3 Arranging Monitor Windows

The Monitor windows can be arranged on screen in several ways. On the menu bar, click **Window**, and select one of the following options to arrange them:

- **Cascade:** Overlaps the open windows and shows their title bars.
- **Tile Horizontally:** Arranges the open windows horizontally.
- **Tile Vertically:** Arranges the open windows vertically.
- **Arrange Icons:** Arranges the minimized windows on the bottom.

You can also place the Monitor windows on a different computer monitor. On the menu bar, click **Window > New Window** and drag the Window to another computer monitor.

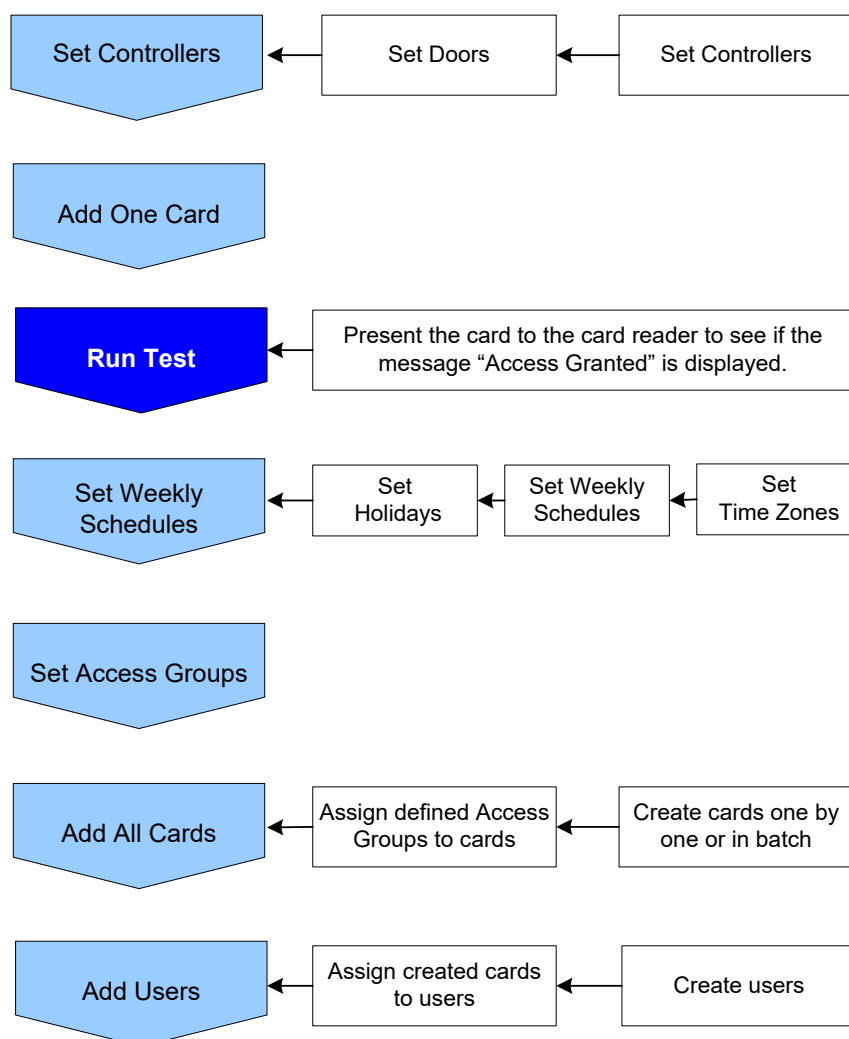
Chapter 4 Settings

This section describes the following settings:

- Adding Controllers
- Adding Cards
- Adding Weekly Schedules
- Adding Access Groups
- Adding Users

4.1 Setup Flowchart

To get started quickly with GV-ASManager settings, follow the process illustrated below.



4.2 Adding Controllers

To add door or elevator controllers to GV-ASManager, follow these steps:

- **Step 1 Configuring a Controller**

Establish the connection between the controller and GV-ASManager. See *section 4.2.1*.

- **Step 2 Configuring Doors or Elevator Floors**

Define doors on a door controller or floor buttons on an elevator controller. See *section 4.2.2*.

4.2.1 Configuring a Controller

1. On the menu bar, click **Setup > Devices**. This window appears.

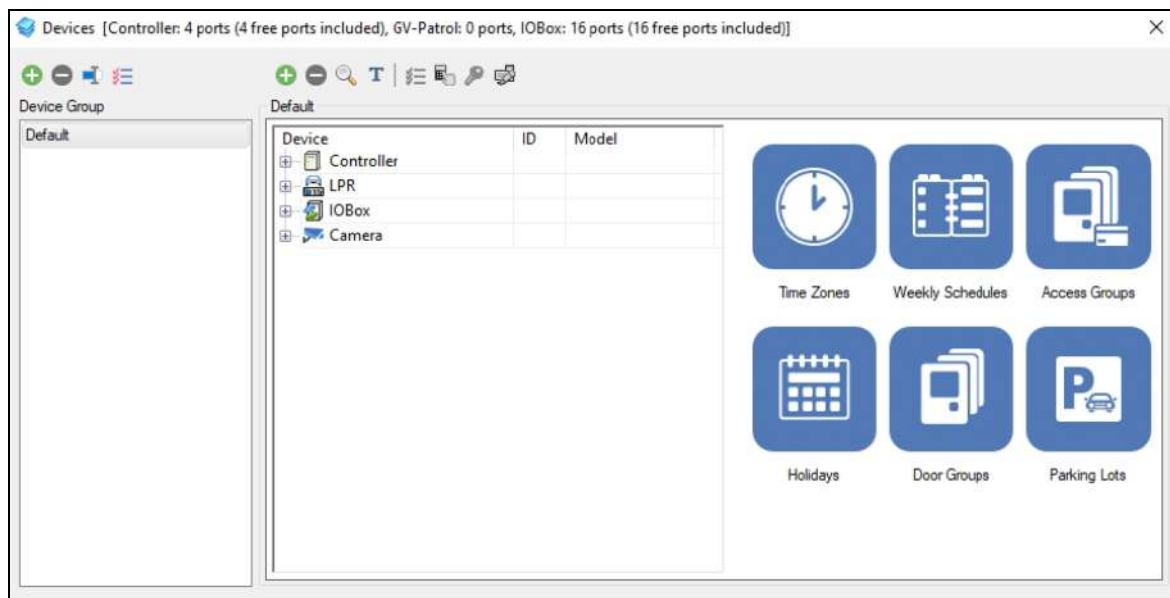


Figure 4-1

2. Under **Device Group**, define a group for the controller to be added. Otherwise, use the **Default** group.

Note: The devices (Controller, LPR, I/O Box and Camera) under the same Device Group will be applied with the identical settings of Time Zones, Weekly Schedules, Access Groups, Holidays, Door Groups and Parking Lots.

3. Right-click **Controller** > **New Controller**.

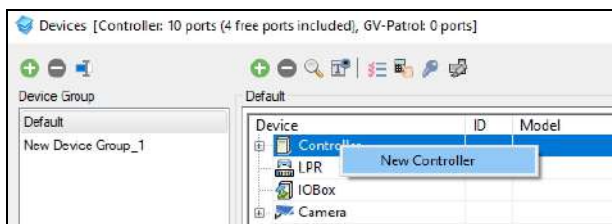



Figure 4-2

4. Type **ID** and **Name** of the controller, select its **Model** and click **OK**.



Figure 4-3

Note: The Controller ID must match the Controller ID set ahead on the Web interface of the controller. See [GV-AS / GV-EV Controller User's Manual](#).

5. Under **Connection**, select **TCP / IP** or **Local DDNS** as communication mode between the controller and GV-ASManager. Type the connection information of the controller, such as IP address, login credentials and Crypto Key (3DES code). You can also click the **Search** button  besides the IP to search for controllers detected in the same LAN.

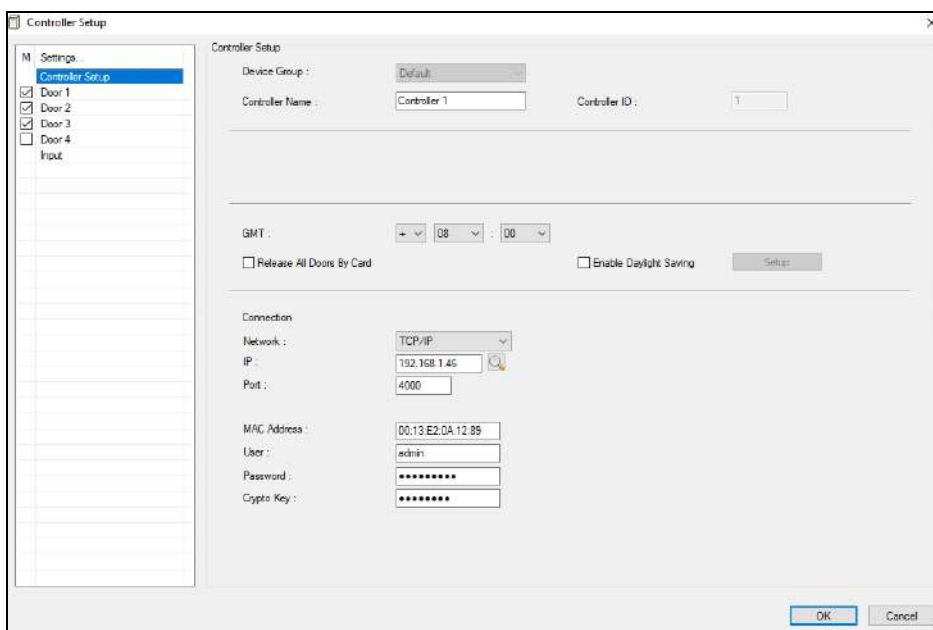




Figure 4-4

Note: The default values of GV-AS / GV-EV Controller are: IP address **192.168.0.100**; username **admin**; password **admin**; Crypto Key (3DES code) **12345678**.

6. To verify if the connection settings are correct, click **OK** at this step and back to the main screen. If the icon  appears in the Controller view window, it indicates the connection between the controller and GV-ASManager has been established. If the icon  appears, it indicates the connection failed. Then make sure the above connection setup is correctly configured.

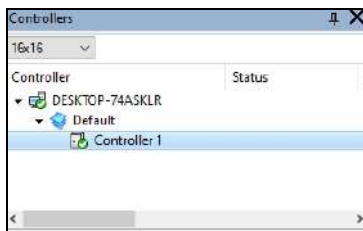


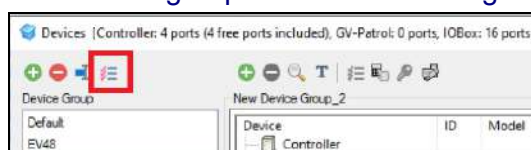
Figure 4-5

7. The following settings are OPTIONAL:

- **GMT:** The current time at the host computer.
- **Release All Doors by Card:** When a card is presented, all doors set to **Release by Card** mode will open until the end of Release by Card mode set in the Authentication Schedule. For Authentication Schedule, see *4.2.2 Step 2: Configuring the Doors*.
- **Enable Daylight Saving:** Enable the Daylight Saving Time by selecting your time zone. The system will automatically adjust for daylight saving time.

Note:

1. The **Release All Doors by Card** function is not available for GV-EV48.
2. For details on disconnection messages displayed on the Status field (Figure 4-5), see *Appendix D. Controller Status*.
3. To quickly create another Device Group, you can use the **Apply Settings to Device Groups** option to replicate the settings (Holiday, Time Zone and Weekly Schedule) of one device group onto other device groups.



4.2.2 Configuring Doors or Elevator Floors

A. GV-AS Controller: Doors

To define doors on the controller, click one **Door** on the left list of the Controller Setup dialog box.

To define the general settings of a door under the **General** tab:

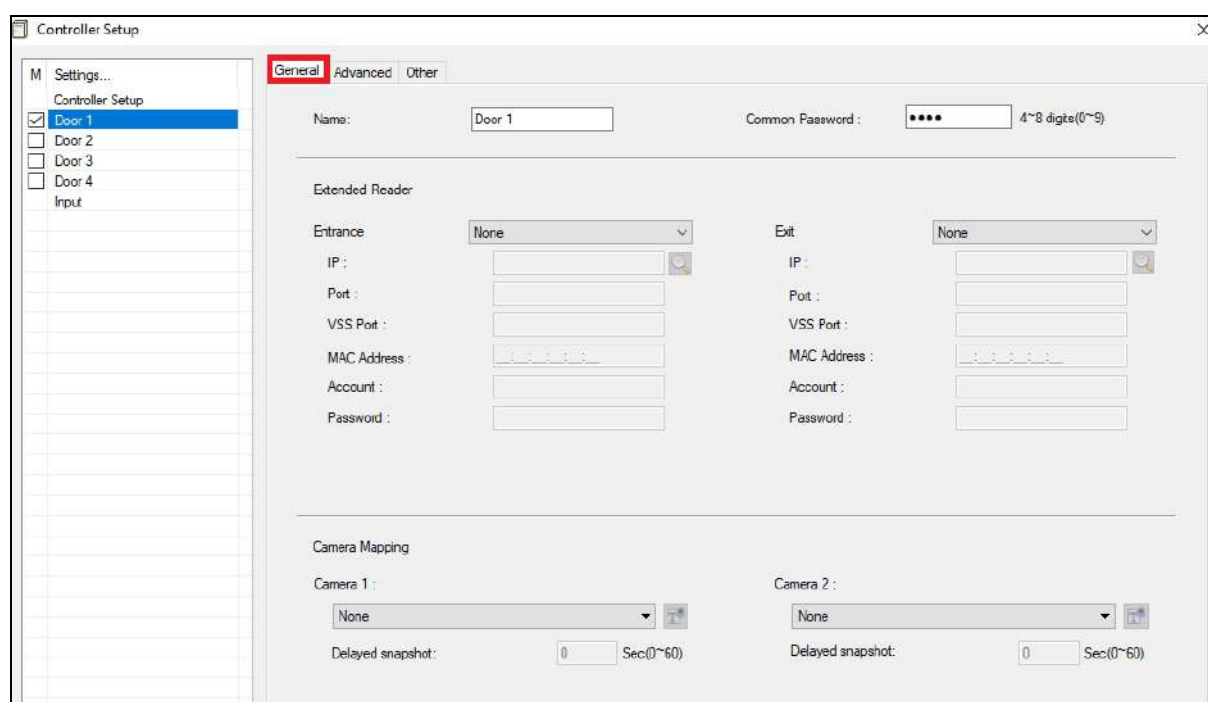


Figure 4-6

- **Name:** Name the door.
- **Common Password:** Set a password for the door. When under **Card or Common Mode**, the user can gain access by entering this password, plus # to enter the setting, using a keypad. The default password is **1234**. See Figure 4-8 for Card or Common Mode.

[Extended Reader]

- **Entrance / Exit:** Set up the card readers connected to the entrance and exit of the door through network. If the card reader is connected through Wiegand, skip the Extender Reader settings.
 - ⊙ **GeoFinger:** Connect to the fingerprint reader. The access granted when presented fingerprints match those enrolled in GV-ASManager. See *Chapter 3 Fingerprint Only Mode* in [GV-GF Fingerprint Reader User's Manual](#) for details.

- ⊙ **GV-CR1320 / CR420:** Connect to the GV-CR1320 / 420 camera reader.
- ⊙ **GV-FR2020:** Connect to the face recognition reader. The access granted when recognized faces match those saved in GV-ASManager. See *Chapter 4 Access Control Configurations* in [GV-FR Face Recognition Reader User's Manual](#) for details.
- ⊙ **GV-VD8700 / FD8700-FR:** Connect to the face recognition cameras, through **GV-FWC**. The access granted when recognized faces match those registered in GV-ASManager. See *14.1 GV-Face Recognition Camera*.
- ⊙ **GV-AI FR:** Connect to the face-recognition-based Server. The access granted when recognized faces match those registered in GV-ASManager. See *14.2 GV-AI FR*.
- ⊙ **GV-FR Panel:** Connect to the face-recognition-based panel. The access granted when recognized faces match those registered in GV-ASManager. See *3.1 Setting up GV-ASManager* in [GV-FR Panel User's Manual](#) for details.

[Camera Mapping] The settings are OPTIONAL unless a camera is installed at the door. For details, see *Chapter 5 Video Integration*.

To define the advanced settings of a door under the **Advanced** tab:

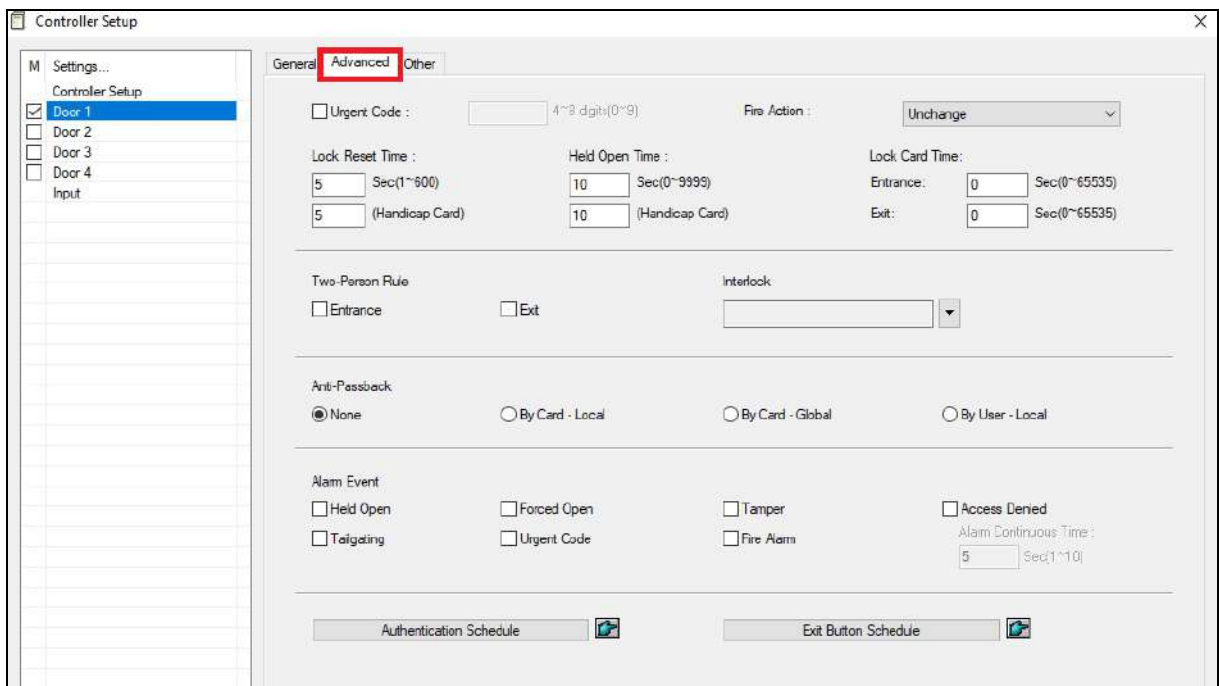


Figure 4-7

- **Urgent Code:** When the Urgent Code is entered on the reader, the associated door will unlock. However, the door will not unlock if the door is in Release by Card Mode and has not been unlocked by a card. The Urgent Code function is only supported by GV-AS1010 / 1110 and readers connected to GV-AS210 / 2110 / 2120 / 410 / 4110 / 810 / 8110 / 1620.
- **Fire Action:** Set the door to be locked or unlocked when fire alarm occurs.
- **Lock Reset Time:** If the door is monitored, type the number of seconds the door can be held open. After the specified time expired, the door will automatically be locked. Next to **Handicap Card**, type the number of seconds the door will be held open when a Handicap Card is swiped.
- **Held Open Time:** If the door is monitored, type the number of seconds the door can be held open before a Door Held Open alarm is generated. Next to **Handicap Card**, type the number of seconds the door can be held open after a Handicap Card is swiped before a Door Held Open alarm is generated.
- **Lock Card Time:** The user will be denied access if he or she tries to re-access the door more than 1 time within the specified Lock Card Time. For example, if the Lock Card Time of a cafeteria entrance is set to 7200 seconds, someone who entered the cafeteria at 9 am will be prevented from re-entering the cafeteria until 11 am.
- **Two Person Rule:** Select **Entrance** and/or **Exit** to require presenting Two Person A Card and then Two Person B Card to unlock the entrance and/or exit door. To set a card to Two Person A/B Card, see *4.3.1 Adding a Single Card* section.
- **Interlock:** Select door(s) for interlocking. Doors that are interlocked cannot be open at the same time. The door only unlocks when the other door is closed. For example, Door 1 ~ Door 3 are interlocked. Door 1 will not unlock if either of Doors 2 and 3 is open/unlocked, and when Door 1 is open/unlocked, Doors 2 and 3 will not unlock. The function is not available for GV-EV48.
- **Anti-Passback:** For details, see *Chapter 6 Anti-Passback*.
- **Alarm Event:** The settings are OPTIONAL unless an alarm device is installed on the controller. Select the alarm conditions to trigger the alarm device: **Held Open, Force Open, Tamper, Fire Alarm, Access Denied, Tailgating** and **Urgent Code** (entered).
 - ⊙ **Alarm Continuous Time:** Type the duration of the alarm sounds in seconds for Access Denied alarm.

- **Authentication Schedule:** Optionally set separate access modes for different time periods.

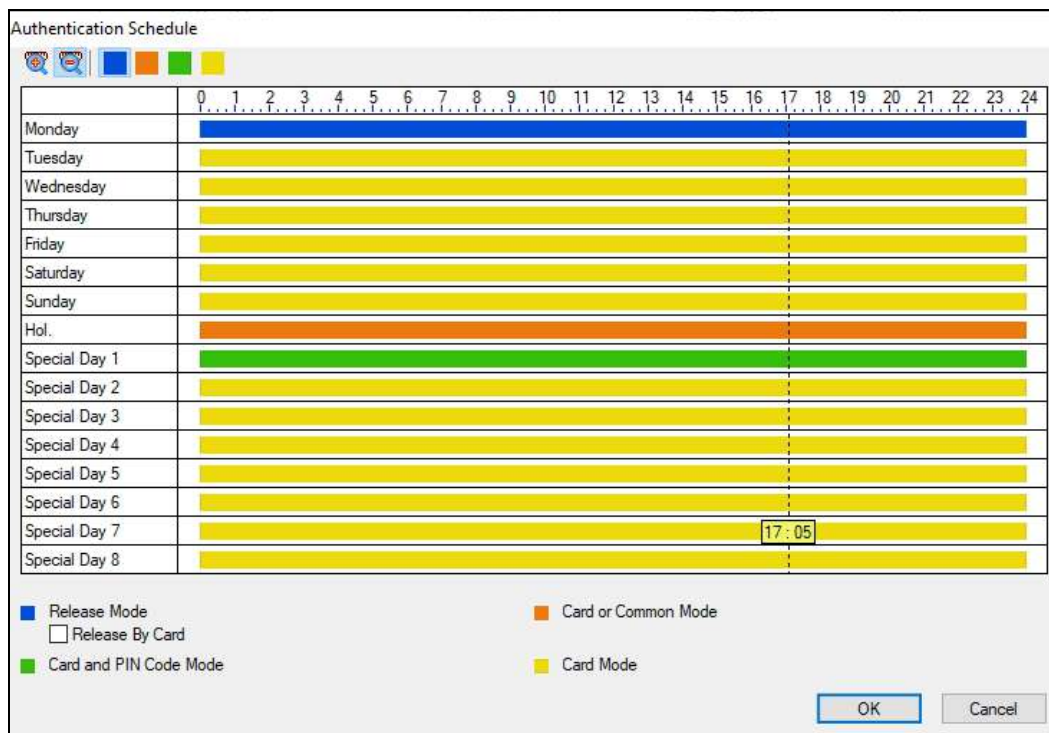


Figure 4-8

Select one Schedule access mode on the toolbar and drag the mouse over the timelines. Four (4) access modes are available:

- ⊙ **Card Mode:** Enabled by default. This mode only requires the user to present his or her card to be granted access. Alternatively, the user can enter a passcode to gain access if the reader comes with a keypad. To set up a passcode, see *4.3.3 Adding a Passcode*.
- ⊙ **Release Mode:** Keep the door in an unlock status.
 - **Release by Card:** The door unlocks only after a card is presented and remains unlocked during the time specified for Release Mode. This option is for preventing unattended doors from opening during the Release Mode.
- ⊙ **Card and PIN Code Mode:** This mode requires the user to enter the card's PIN code on the keypad and then present the card. To set up a PIN code, see *4.3.1 Adding a Single Card*.

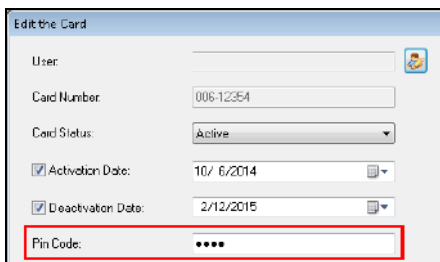



Figure 4-9 Pin Code setting on the Edit the Card dialog box

- Card or Common Mode:** This mode requires the user to present the card **or** enter the door's common password (see Figure 4-4), plus # to enter the setting, using the keypad.

- Exit Button Schedule:** Optionally set the time periods during which the Exit button is accessible. By default, access to the Exit button is always granted. To create a schedule, click the **Delete Access Time** button  and drag the mouse over the timelines for when you want the Exit button to be locked. The function is only supported by GV-AS1010 / 1110 / 210 / 2110 / 410 / 4110 / 810 / 8110 / 1620.

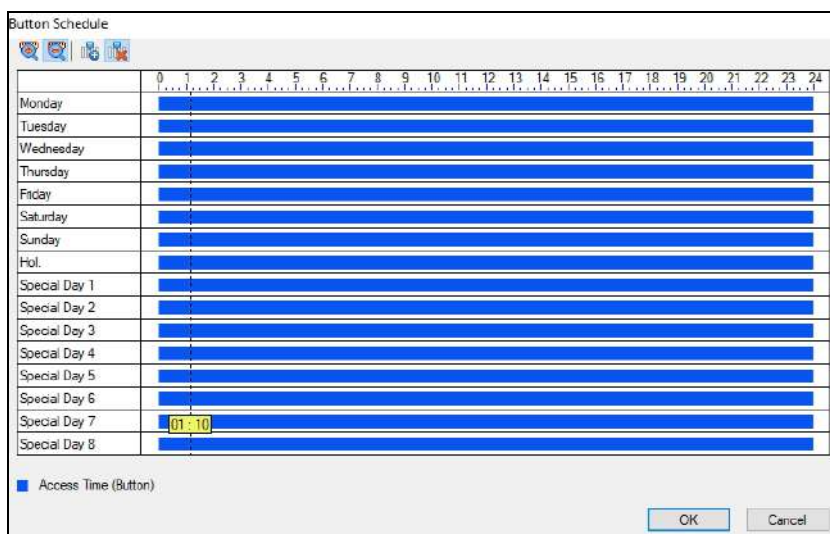


Figure 4-10

To define the settings of a door under the **Other** tab:

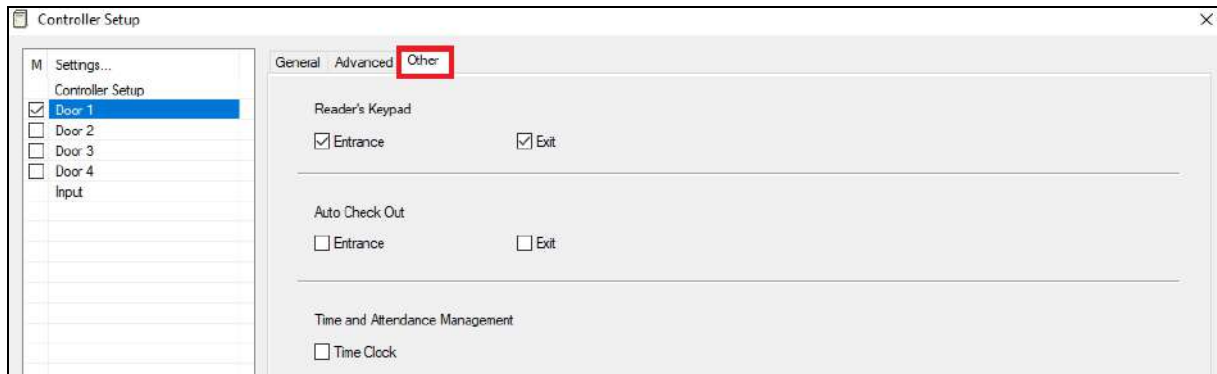



Figure 4-11

The settings at the Other tab are **OPTIONAL** and are only applicable when related settings are also configured:

- **Disable Keypad:** This option works together with the **Card and PIN Code Mode**. Deselect **Entrance** or **Exit** to allow access by swiping card only.
- **Auto Check Out:** Record the check-out time of visitor card on GV-VMWeb when a visitor presents the card at the entrance / exit door. To set a card as Visitor Card, see *Adding a Single Card* section later in this chapter.
- **Time Clock:** This option must be selected to enable GV-TAWeb. See *Chapter 11 GV-TAWeb for Workforce Schedule* for details.

Tip: After completing the settings of a door, you can click the **Apply All** button  on the Devices dialog box (Figure 4-1) to apply the Authentication Schedule and/or Exit Button Schedule to other device groups.

B. GV-EV Controller: Floors

To define the general setting of an elevator and floors under the **Floors** tab:

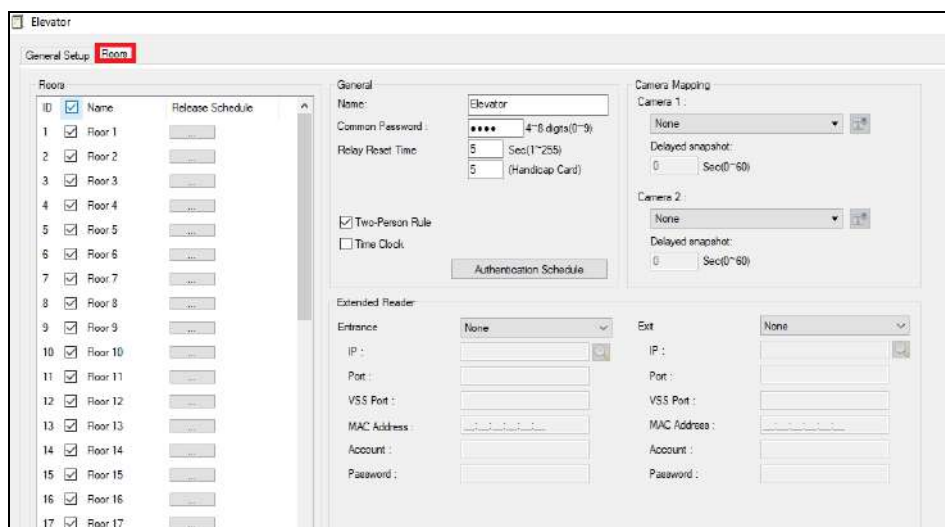


Figure 4-12

- **Name:** Name the elevator.
- **Common Password:** Set a password to unlock the floor button. When under **Card or Common Mode**, the user can gain access by entering this password, plus # to enter the setting, using a keypad. The default password is **1234**.
- **Relay Reset Time:** Type the number of seconds the floor button will remain accessible after card is presented. After the specified time expired, the floor button will automatically be locked. Next to **Handicap Card**, type the number of seconds the floor button will remain accessible when a Handicap Card is swiped.
- **Two Person Rule:** Require presenting Two Person A Card and Two Person B Card in order to unlock the floor button. To set cards as Two Person A/B Card, see 4.3.1 *Adding a Single Card*.
- **Time Clock:** This option must be selected to enable GV-TAWeb. See *Chapter 11 GV-TAWeb for Workforce Schedule* for details.
- **Authentication Schedule, Extended Reader and Camera Mapping:** The settings are the same with those of configuring a controller. See *A GV-AS Controller: Doors* in section 4.2 for Authentication Schedule and Extended Reader. See *Chapter 5 Video Integration* for Camera Mapping.
- **Release Schedule:** Click next to a **Floor** to specify time periods allowing access to a floor button.

Note: The **Release Schedules** have priority over the **Authentication Schedule**.

4.3 Adding Cards

Once you have configured a controller, you can start enrolling cards. All new cards must be enrolled into GV-ASManager before access is granted. Up to 100,000 cards can be stored.

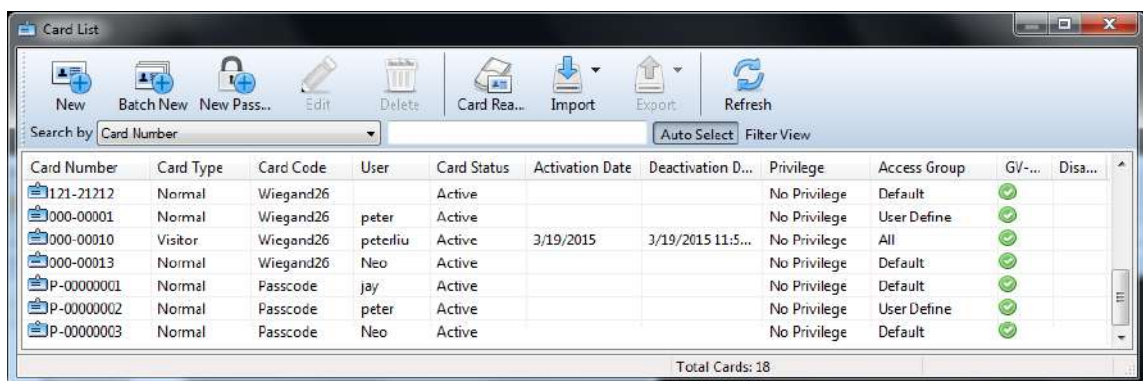
Depending on how many cards you need to program, you can simply add them one at a time or use the batch function to add a group of cards.

Note: To use **Mobile Card** credentials, see [GV-QR1352 / DES1352 User's Manual](#) for details.

4.3.1 Adding a Single Card

1. To add one card, use one of these ways:

- Present a card to the reader. The message *Access Denied: Invalid Card* is displayed. Right-click the message and select **New / Edit Card**. The New a Card dialog box appears (Figure 4-14). Then follow Step 3 to complete other settings.
- On the menu bar, click **Personnel > Cards**. This window appears.



Card Number	Card Type	Card Code	User	Card Status	Activation Date	Deactivation D...	Privilege	Access Group	GV-...	Disa...
1121-21212	Normal	Wiegand26		Active			No Privilege	Default	✓	
000-00001	Normal	Wiegand26	peter	Active			No Privilege	User Define	✓	
000-00010	Visitor	Wiegand26	peterliu	Active	3/19/2015	3/19/2015 11:5...	No Privilege	All	✓	
000-00013	Normal	Wiegand26	Neo	Active			No Privilege	Default	✓	
P-00000001	Normal	Passcode	jay	Active			No Privilege	Default	✓	
P-00000002	Normal	Passcode	peter	Active			No Privilege	User Define	✓	
P-00000003	Normal	Passcode	Neo	Active			No Privilege	Default	✓	

Total Cards: 18

Figure 4-13

2. Click the **New** button on the toolbar > **Add a New Card**. This dialog box appears.

The 'New a Card' dialog box contains the following fields and options:

- User: [Text Field] [Assign User Icon]
- Card Number: [Text Field] [GV-PCR1251 / 1352 Enrollment Reader Icon]
- Card Status: [Active] [Dropdown]
- Card Code: [Wiegand26] [Dropdown]
- Card Type: [Normal] [Dropdown]
- Activation Date: [11/15/2021] [Calendar Icon]
- Deactivation Date: [11/15/2021] [Calendar Icon]
- Auto Inactive (Days): [60] [Text Field]
- Pin Code: [Masked Field]
- Privilege: [No Privilege] [Dropdown]
- Disable Lock Card / Disable APB / Allow Access during Lockdown Mode: [Checkbox]
- Card User Defined Field 01-06: [Dropdown Menus]

Assign Access Groups:


Device Group	Access Group
<input checked="" type="checkbox"/> Default	Default
<input type="checkbox"/> New Device Group_1	Default

Copy to User Define

Controller 1

Figure 4-14

3. These settings are available for a card:

- **User:** Click the **Assign User** button  to assign the card to a user.
- **Card Number:** Type a card number. You can also use the GV-PCR1251 / 1352 Enrollment Reader to detect and fill in card numbers automatically. See [GV-PCR1251 / 1352 Enrollment Reader's Installation Guide](#) for details.
- **Card Code:** Select the code format of the card.
- **Card Type:** Select one of the following card types.
 - **Normal:** The card opens the door when it is under Card Mode, the default mode.
 - **Patrol:** The card is assigned to the person in charge of patrolling a location, e.g. a guard. When the patrol card is presented to the reader, the access will be recorded but the door will remain locked. The feature can be set together with **Privilege** in the dialog box. The patrol card user can have the privilege to stop alarms and clear alarm events during patrolling.

- **Two-person A Card:** Two-person A/B rule. The card is defined as Card A. Card B must be presented after Card A to unlock the two-person-rule enabled door.
 - **Two-person B Card:** Two-person A/B rule. The card is defined as Card B. Card A must be presented before Card B to unlock the two-person-rule enabled door.
 - **Visitor:** This card is assigned to a visitor and the visitor's access is managed using GV-VMWeb. See *Chapter 10 GV-ASWeb*.
 - **Security:** The security card can enable the Security Mode where no cards can be granted access. Only the security card can disable the Security Mode.
 - **Handicap:** When the handicap card is used, the door will remain unlocked for the time specified in **Lock Reset Time** and **Held Open Time** options for handicap card. For the two options, see *4.2.2 Configuring Doors or Elevator Floors*.
- **Activation / Deactivate Date:** Specify the date to activate or deactivate the card.
 - **Auto Inactive (Days):** When the card has not been used for access for the specified days, it will be deactivated.
 - **PIN Code:** Enter a four-digit PIN code for the card. When the authentication mode is set to **Card and PIN Code Mode**, the user needs to enter the PIN code and then present the card. The default setting is 1234.

For the controllers listed below, the user can gain access by entering the card number and the set pin code. For example, if the card number is 12345678 and the Pin is 0000, the command will be 000012345678 for GV-AS210.

Models	Supported Firmware	Command (Example: Card 12345678, Pin 0000)
GV-AS100	V1.04 or later	Card Number + Pin Code
GV-AS1010	V1.0 only	Example: 123456780000
GV-AS110	V1.04 or later	*Card Number + Pin Code #
GV-AS1110	V1.0 only	Example: *123456780000#
GV-AS210 / 410 / 810	V1.0 - V1.23	Pin Code + Card Number
GV-EV48	V1.0 – V1.12	Example: 000012345678

- **Privilege:** Assign one of these privileges to the user:
 - **Stop Alarm:** The user can stop alarms by presenting the card.
 - **Clear Event:** The user can clear alarm events by presenting the card. All alarms in the Controller view window will be erased, but a record of these alarms is kept in the Alarm Monitor.

- **Disable Lock Card / Disable APB / Allow Access during Lockdown Mode:** When the option is selected, the card will be exempt from **Lock Card Time** and **APB** settings. In addition, the card will be allowed access to doors when **Lockdown Mode** is activated.

For details on Lock Card Time, see *4.2.2 Configuring Doors or Elevator Floors*. For details on Lockdown Mode, see the **Lock Down** button in *3.3.2 Controls on the Window*.

Note: The Allow Access during Lockdown Mode only works with:

- GV-AS210 / 2110 / 410 / 4110 / 810 / 8110 with firmware V1.23 or later
 - GV-AS2120 with firmware V1.35 or later
 - GV-AS1010 / 1110 with firmware V1.0 or later
 - GV-AS1620
-

- **Supported Devices:** GV-ASManager supports up to 100,000 cards. The first 40,000 cards created are labeled as **40K** and cards 40,001 ~ 100,000 are labeled as **100K**.
- **Assign Access Group:** Select **Device Group** and then click its **Access Group** dropdown list to assign one predefined access group. For details, see *4.5 Adding Access Groups*.
- **Controller:** The Controller box displays the associated doors with Access Groups.

4. Present the enrolled card to the reader. Once the card is accepted, the message *Access Granted* will be displayed.

Tip: For first-time users of GV-ASManager, you can click the **Copy to User Define** button and select **24-hour access** for each door for test run.

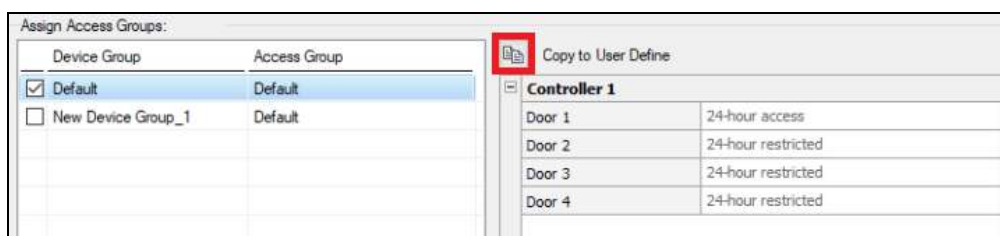


Figure 4-15

4.3.2 Adding a Special Card

You can create up to 100 Special Cards for separately applying Lock Reset Time and Held Open Time when swiping the card to a door. This function only works with GV-AS210 / 410 / 810 firmware V2.80 or later

1. On the menu bar, click **Personnel > Cards**. The Card List window appears.
2. Click the **New** button on the toolbar > **Add a New Special Card**.
3. Set **Lock Reset Time** in seconds after which the door will be locked automatically, and **Held Open Time** in seconds before a Door Held Open alarm is generated.

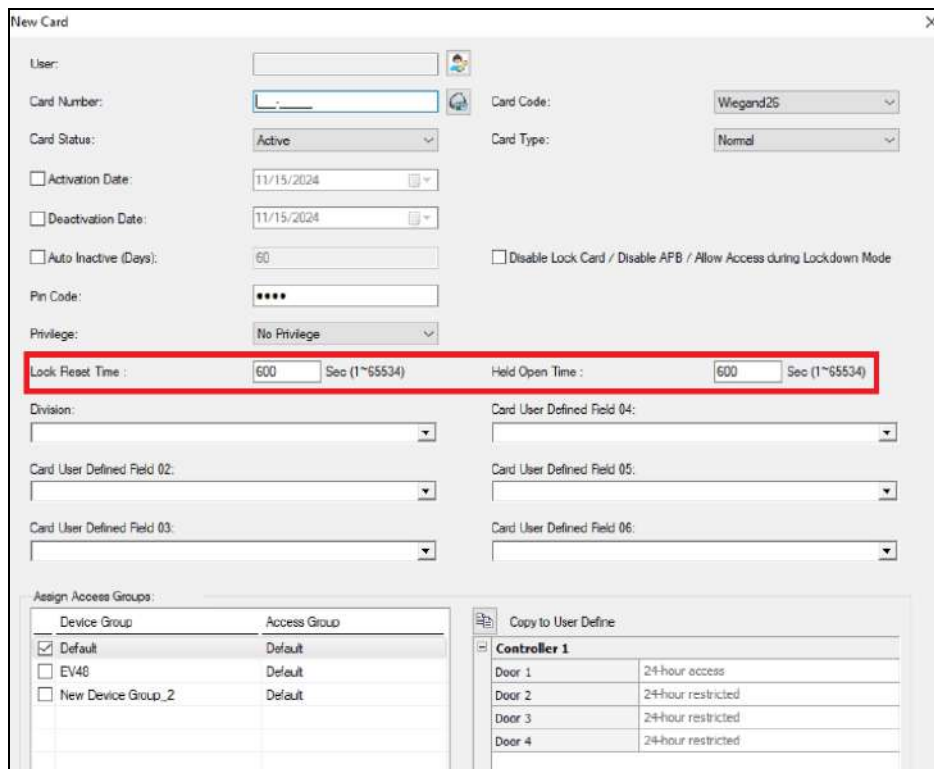


Figure 4-16

4. Other settings in the dialog box are identical to those of adding a single card. See Step 3 in 4.3.1 *Adding a Single Card*.

Note: The default Lock Reset Time is 5 seconds and Held Open Time is 10 seconds.

4.3.3 Adding a Group of Cards

You can create a mass number of cards, with card numbers in sequence, at a time.

1. On the menu bar, click **Personnel > Cards**. The Card List window appears.
2. Click the **New** button on the toolbar > **Batch New Cards**. This dialog box appears.

Device Group	Access Group
<input checked="" type="checkbox"/> Default	Default
<input type="checkbox"/> New Device Group_1	Default

Figure 4-17

3. Type a range of card numbers.
4. Other settings in the dialog box are identical to those of adding a single card. See Step 3 in 4.3.1 *Adding a Single Card*.

Note: The cards enrolled using the Batch function have the same PIN. To change the PIN of a card, click the **Edit** button on the Card List window.

4.3.4 Adding a Passcode

When the authentication mode is set to **Card Mode**, the user can either present a card or enter a passcode to gain access. Follow the steps below to create a passcode.

Note: The Passcode function is only supported by:

- GV- AS1010 / 1110 firmware V1.1 or later
 - GV-AS210 / 2110 / 410 / 4110 / 810 / 8110 & GV-EV48 firmware V1.3 or later
 - GV-AS2120 firmware V1.35 or later
 - GV-CS1320 firmware V1.0 or later
 - GV-AS1620
-

1. On the menu bar, click **Personnel > Cards**.
2. Click the **New** button on the toolbar > **Add a New Passcode**.
3. Type a **Passcode** consisting of 4 to 8 numbers.



Figure 4-18

4. Other settings in the dialog box are identical to those of adding a single card. See Step 3 in 4.3.1 *Adding a Single Card*.

After the passcode is created, a card number will be assigned to the passcode.

4.3.5 Importing/Exporting Card Data

You can import and export card data in mdb, xls, xlsx, or csv format.

To export card data:

1. On the Card List window, select desired cards using Ctrl + left click.
2. Click the **Export** button > **Export to Access** or **Export to Excel**.
3. Assign the file path, and optionally enter password to export card data.

Note:

1. The Excel file format does not support the password protection.
2. The Passcode cannot be exported.

To import card data:

1. On the Card List window, click the **Import** button and select one of import formats: **Access, Excel, CSV, or Others**.
2. Locate the file and type the **Password** if necessary. Click **OK**. This dialog box appears.

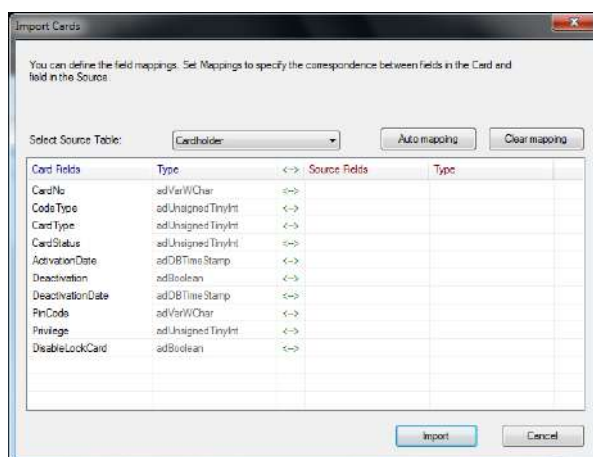


Figure 4-19

3. Select the **Source Table** you want to import.
4. Click the **Auto mapping** button to automatically map the Source fields to the current card data fields.
5. You can also manually map the fields by clicking the columns under **Source Fields**.
6. Click **Import** to import card data.

4.3.6 Customizing a Card Data Field

You can customize data fields for cards. Up to six fields can be created for card data entry.

1. On the Card List window, click **Card User Define Fields Setting**.
2. Select one **User Define** field, and type the text to be displayed as the field label. In this example, a Division field was created.

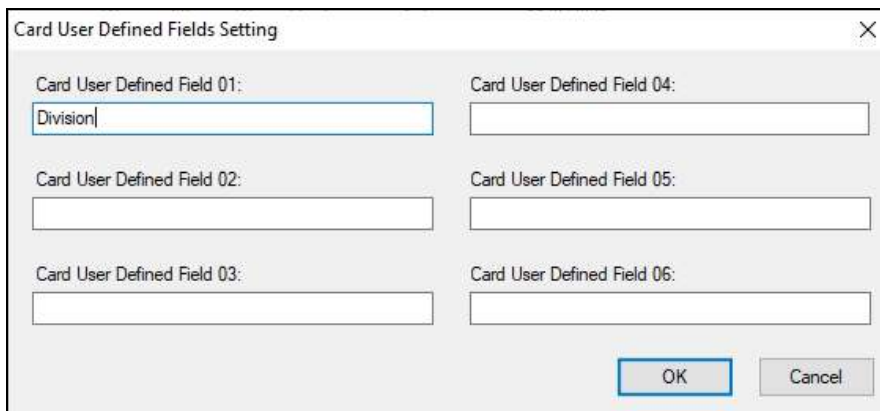


Figure 4-20

3. On the Card List window, click the **New** button on the toolbar or double-click a created card to edit.
4. Click in the custom data field and enter the appropriate information. In this example, human resources is entered in the created Division field.

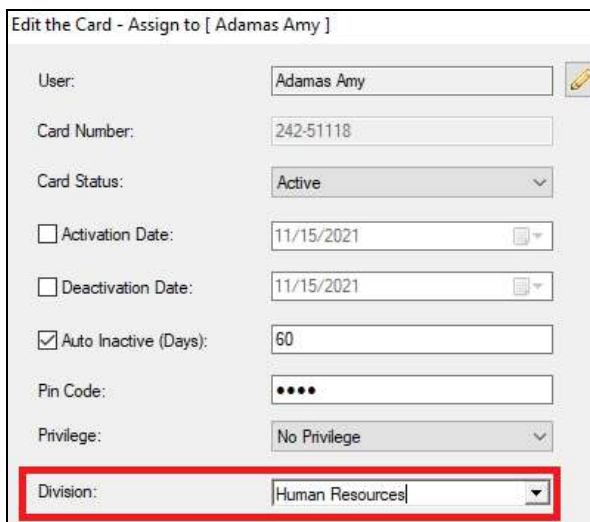


Figure 4-21

4.3.7 Adjusting Columns on the Card List

You can adjust column items on the Card List window by enabling or disabling an item, or move a column by dragging

1. To adjust column items, right-click any items and select **Columns**.

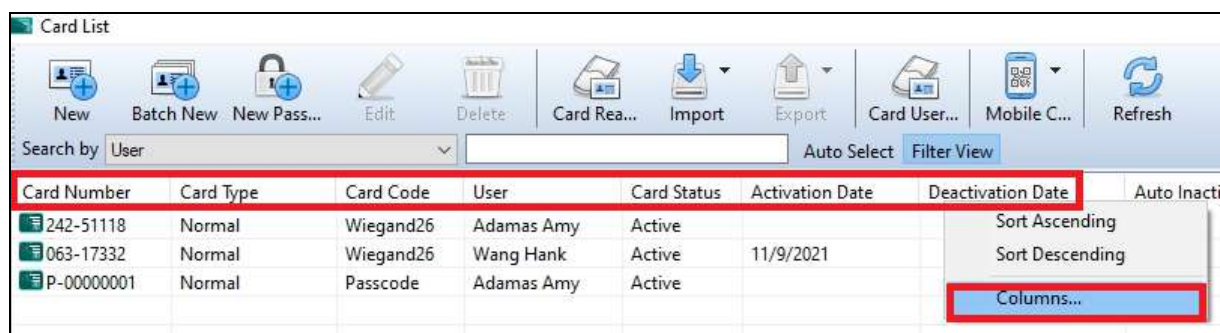


Figure 4-22

2. Enable or disable desired items.
3. To move a column, select a column item, click and hold the left mouse button, and move the column to the new position.

4.4 Adding Weekly Schedules

This section helps you define daily and holiday access times. Up to 254 weekly schedules can be defined with two default schedules for “Deny Access” and “Full Access”.

Before creating weekly schedules, it is helpful to map out all possible usages of weekly schedules for the site. For example: consider the variety of access hours for employees, consider requirements for janitorial personal who may need night access, consider requirements for service or repair personnel who may need all hours’ access, consider requirements for supervisory staff who may need extended hours access and etc.

- **Step 1 Adding Time Zones**

Define the minutes and hours of the day when a user is granted access to a secure site. The minimum time duration is 5 minutes.

- **Step 2 Adding Weekly Schedules**

Define the days of the week when a user is granted access to a secure site.

- **Step 3 Adding Holidays**

Define specific dates as holidays and special days.

4.4.1 Step 1: Adding Time Zones

This section provides examples of adding the following time zones:

- Day shift – 09:00 to 19:00 hours
- Night shift – 19:00 to 9:00 hours (cross midnight)

1. On the menu bar, click **Setup > Devices**, and select a **Device Group**. The devices under the Device Group will be applied with identical Time Zones.
2. Select **Time Zones** on the left of the Devices dialog box. This dialog box appears.

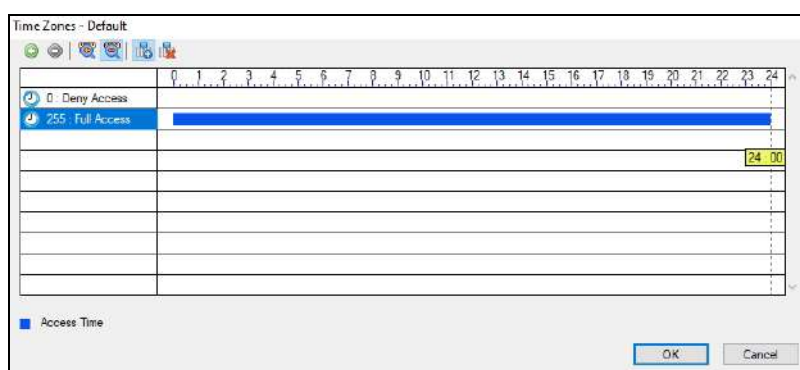



Figure 4-23

3. Click **Add** . This dialog box appears.

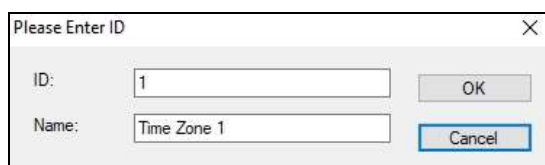



Figure 4-24

4. The **ID** is the number of the time zone, which is automatically assigned by the system in ascending order. Name the time zone and click **OK**.

For example, name Time Zone 1 as **Day Shift**.

5. Click and drag the mouse on the timeline of the created time zone to mark the access time.

For example, the time of Day Shift is **from 09:00 to 19:00**.

6. To create another time zone, click **Add**  and name it, e.g. **Night Shift**. Then click and drag the mouse on the timeline to mark the access time, e.g. **from 19:00 to 24:00** and **from 00:00 to 09:00**.

7. Click **OK**. The two time zones are created and defined.

4.4.2 Step 2: Adding Weekly Schedules

This section provides examples of adding the following weekly schedules:

- Schedule-Day Shift – Monday through Friday, 09:00 to 19:00 hours
- Schedule-Night Shift – Monday through Friday, 19:00 to 9:00 hours

1. On the menu bar, click **Setup > Devices**, and select a **Device Group**. The devices under the Device Group will be applied with identical Weekly Schedules.
2. Select **Weekly Schedules** on the left of the Devices dialog box. This dialog box appears.

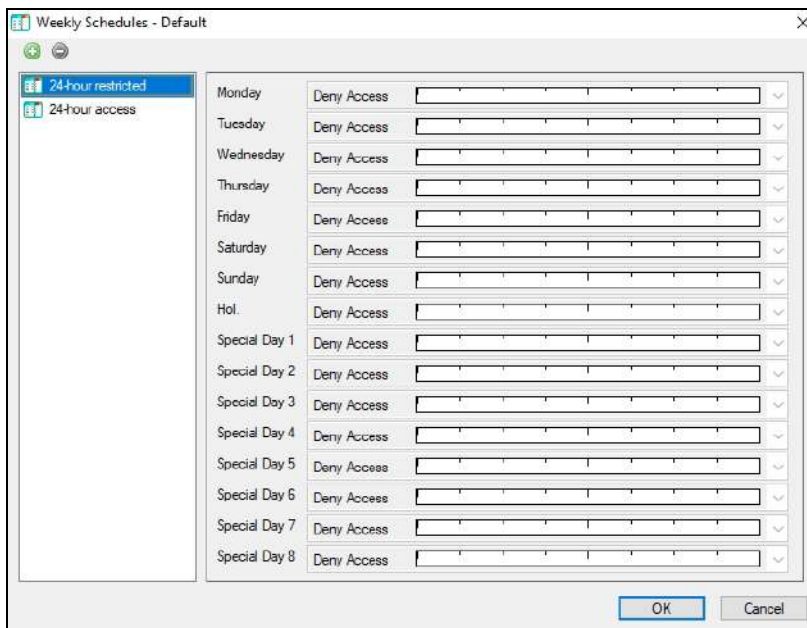



Figure 4-25

3. Click **Add** . This dialog box appears.

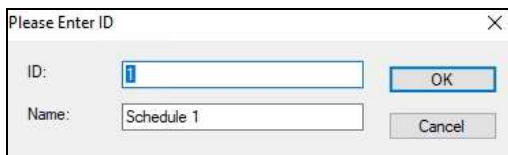


Figure 4-26

4. The **ID** is the number of the weekly schedule, which is automatically assigned by the system in ascending order. Name the weekly schedule and click **OK**. For example, name the Schedule 1 as **Schedule-Day Shift**.

- From the dropdown lists of **Monday** to **Friday**, select the **Day Shift** time zone you have created. No access is allowed on Saturday, Sunday and Holiday.

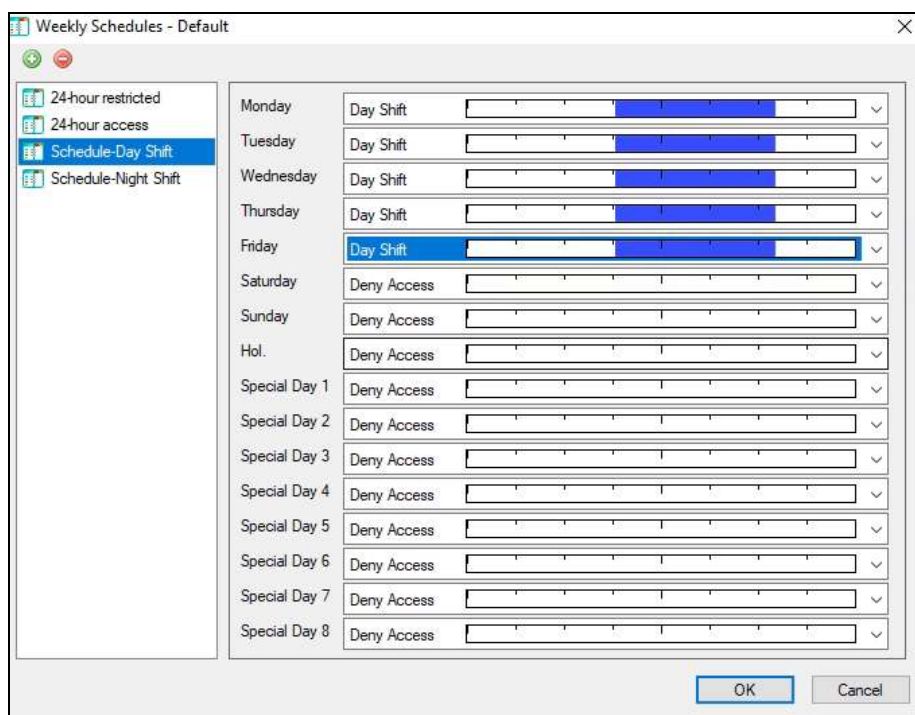



Figure 4-27

- To create a second time schedule, click **Add**  and name it as **Schedule-Night Shift**. From the dropdown lists of **Monday** to **Friday**, select the **Night Shift** time zone you have created. No access is allowed on Saturday, Sunday and Holiday.
- Click **OK**. The two weekly schedules are created and defined.

4.4.3 Step 3: Adding Holidays

To designate specific dates as holidays and special days on the system:

1. On the menu bar, click **Setup > Devices**, and select a **Device Group**. The devices under the Device Group will be applied with identical Holidays.
2. Select **Holidays** on the left of the Devices dialog box. This dialog box appears.

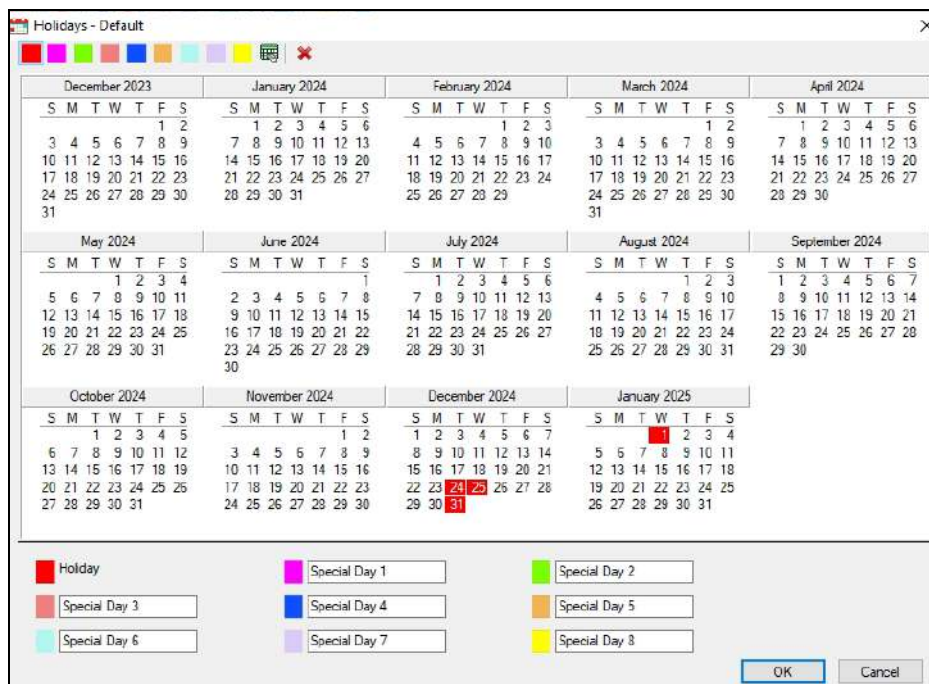


Figure 4-28

3. Click the **Holiday** icon and click the dates you want to set as holidays. For example,
 - Dec 24, 2024 – Christmas Eve
 - Dec 25, 2024 – Christmas Day
 - Dec 31, 2024 – New Year’s Eve
 - Jan 01, 2025 – New Year’s Day
4. You can designate up to 8 special days for Authentication Schedule and Exit Button Schedule by clicking the color blocks and selecting the dates.

Note: Holiday dates and special days can cross over to the following year, and certain holiday dates change from year-to-year. Administrators should review and update the holiday settings prior to the beginning of a new year to ensure proper holiday coverage.

4.5 Adding Access Groups

An access group defines which doors or lanes can be accessed at what times. You can create multiple access groups to suit the schedules of different groups of employees. Instead of setting the access rights of each card one by one, you can quickly assign a card to an access group and the access rights of that access group will be applied to the card.

This section describes how to create an access group and assign a card to the access group.

To create an Access Group:

1. On the menu bar, click **Setup > Devices**, and select a **Device Group**. The devices under the Device Group will be applied with identical Access Groups.
2. Select **Access Groups** on the left of the Devices dialog box. This dialog box appears.

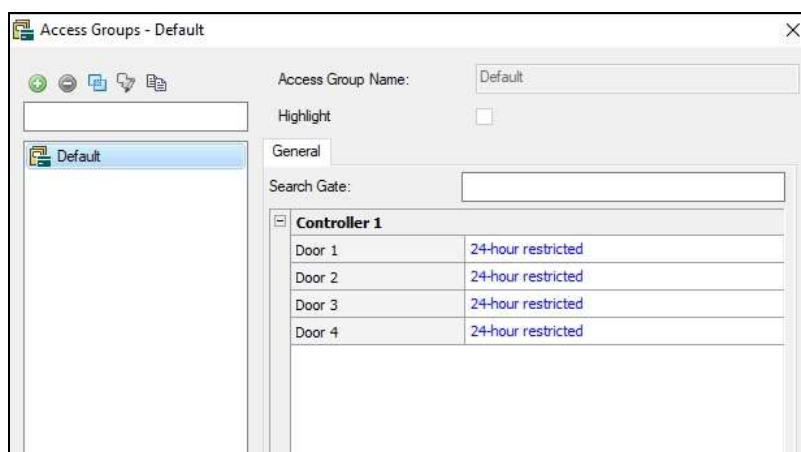




Figure 4-29

3. Click **New** , and name the access group, e.g. *Daytime Staff* and *Nighttime Staff*.
4. To define door access for the access group, click the dropdown list next to each door and select one of the predefined Weekly Schedules. For example, select *Schedule-Day Shift* or *Schedule-Night Shift* created in 4.4.2 Step 2: Adding Weekly Schedule.
5. Optionally, users can click **Merge**  to create an access group containing all the access schedules of multiple access groups selected.

For example, merging *Daytime Staff* and *Nighttime Staff* to create an access group of *Supervisors*.

6. Optionally, enable **Highlight** to highlight all the access messages of the access group in the **Access Monitor** window.

To assign a card to an Access Group:

7. Click **Personnel** on the menu bar > **Cards**. The Card List dialog box appears.
8. Double-click one listed card. The Edit Card dialog box appears.
9. Select **Device Group**, and from its **Access Group** dropdown list, select one predefined access group, e.g. *Daytime Staff*. The Weekly Schedules assigned to the access group are displayed on the fields of associated doors.

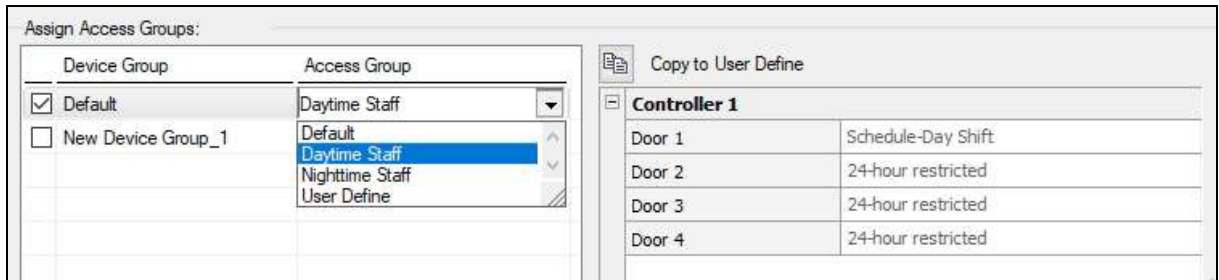


Figure 4-30

Tip: To search for an access group or a door, you can type its keyword in the respective search boxes.



Figure 4-31


4.6 Adding Users

This section describes how to create a database of user accounts and assign cards to users.

4.6.1 Adding a User

1. On the menu bar, click **Personnel > Users**. The User List window appears.
2. Click the **New** button on the toolbar. This dialog box appears.

Figure 4-32

3. Type a name under **Display**, which is a required setting. Other user information are of optional entries.
4. To assign a card or vehicle to the user, click **Add**  to create a new card or vehicle, or assign an existing one.

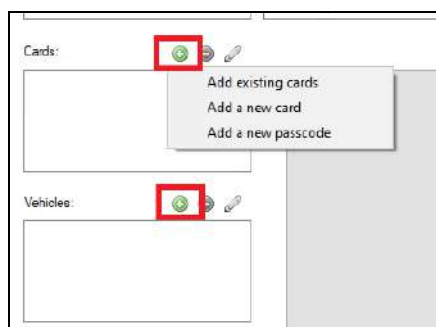


Figure 4-33

- To send e-mail alerts whenever any of the cards / vehicles assigned to the user is presented to the reader, select **Send Email**.

Note: To send e-mail alerts, see [8.2.2 Setting up E-Mail Server](#) to configure the e-mail server first.

The **Home** and **Business** tabs allow you to enter personal information for the user account. Under the Business tab, if you enable **Separation Date**, the cards for this user will be deactivated on the day after the specified date.

Tip: To edit the Business and User Define tabs of multiple users at a time, use Shift + left click to select multiple users from the User List, right-click the selected users, and click **Edit**.



Figure 4-34

You can enroll fingerprints under the **Features** tab using GV-GF1911 / 1921 / 1922. For details, see [Chapter 3 Fingerprint Only Mode](#) in [GV-GF Fingerprint Reader User's Manual](#).

4.6.2 Customizing a User Data Field

You can customize data fields for users. Up to ten data fields can be created for user data entry.

1. On the menu bar, click **Personnel > User**. The User List window appears.
2. Click the **User Define Fields Setting** button on the toolbar. The User Define Fields Setting dialog box appears.
3. Select one **User Define** field, and type the text to be displayed as the field label. In this example, a Parking Space Number field was created.

Figure 4-35

4. On the Card List window, click the **New** button on the toolbar or double-click a created user to edit.
5. Click the **User Define** tab. The custom data field created now is displayed.

Figure 4-36

4.6.3 Importing/Exporting User Data

From the User List window, you can import and export user data in mdb, xls or xlsx format. For details, see *4.3.4 Importing / Exporting Card Data*.

4.3.4 Adjusting Columns on the User List

You can adjust column items on the User List window by enabling or disabling an item, or move a column by dragging. For details, see *4.3.6 Adjusting Columns on the Card List*.

4.7 Adding I/O Boxes

To add one GV-I/O Box to GV-ASManager over network for I/O management, follow these steps:

- **Step 1 Connecting GV-I/O Box**

Establish the communication between GV-I/O Box and GV-ASManager. See *section 4.7.1*.

- **Step 2 Configuring Input and Output functions**

Define the input and output pins to be used by GV-I/O Box. See *section 4.7.2*.

Note: GV-ASManager supports up to 16 GV-I/O Boxes. Over 16 box connections require a license.

4.7.1 Connecting GV-I/O Box

1. On the menu bar, click **Setup > Devices**. The Devices dialog box appears.
2. Under **Device Group**, define a group for the I/O Box to be added. Otherwise, use the **Default** group.

Note: The devices (Controller, LPR, I/O Box and Camera) under the same Device Group will be applied with the identical settings of Time Zones, Weekly Schedules, Access Groups, Holidays, Door Groups and Parking Lots.

3. Right-click **IO Box > New IO Box**.

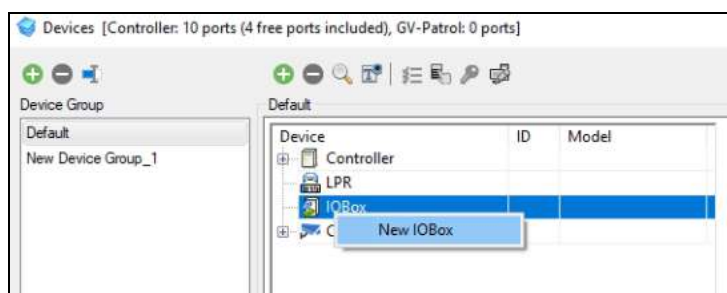


Figure 4-37

4. Type an **ID** number and **Name** for the I/O Box, select **Type** of the I/O Box and click **OK**.



Figure 4-38

5. Under **Connection**, select the communication mode between the I/O Box and GV-ASManager.

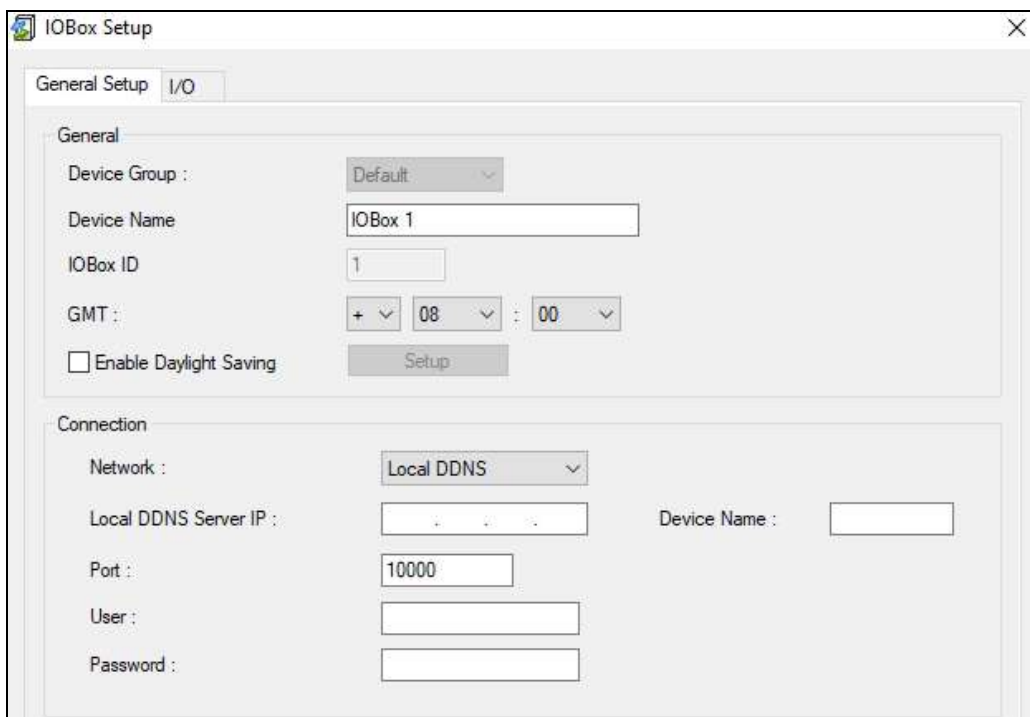





Figure 4-39

- If selecting **TCP / IP**, type the IP address, port number and login credentials. You can also click the **Search** button  to search for I/O Boxes detected in the same LAN.
 - If selecting **Local DDNS**, type the IP address of the LocalDDNS Service, the device name to match that on the I/O Box's Web interface registered from the LocalDDNS Server, the port number and login credentials.
6. To verify if the connection settings are correct, click **OK** at this step and back to the main screen. If the icon  appears in the IO Box view window, it indicates the connection between the I/O Box and GV-ASManager has been established. If the icon  appears, it indicates the connection failed. Then make sure the above connection setup is correctly configured.

7. OPTIONAL settings in the **General Setup** tab:

- **GMT:** The current time at the host computer.
- **Enable Daylight Saving:** Enable the Daylight Saving Time by selecting your time zone. The system will automatically adjust for daylight saving time.

4.7.2 Configuring Input and Output Functions

1. To define the input and output devices, click the **I/O** tab. This dialog box appears.

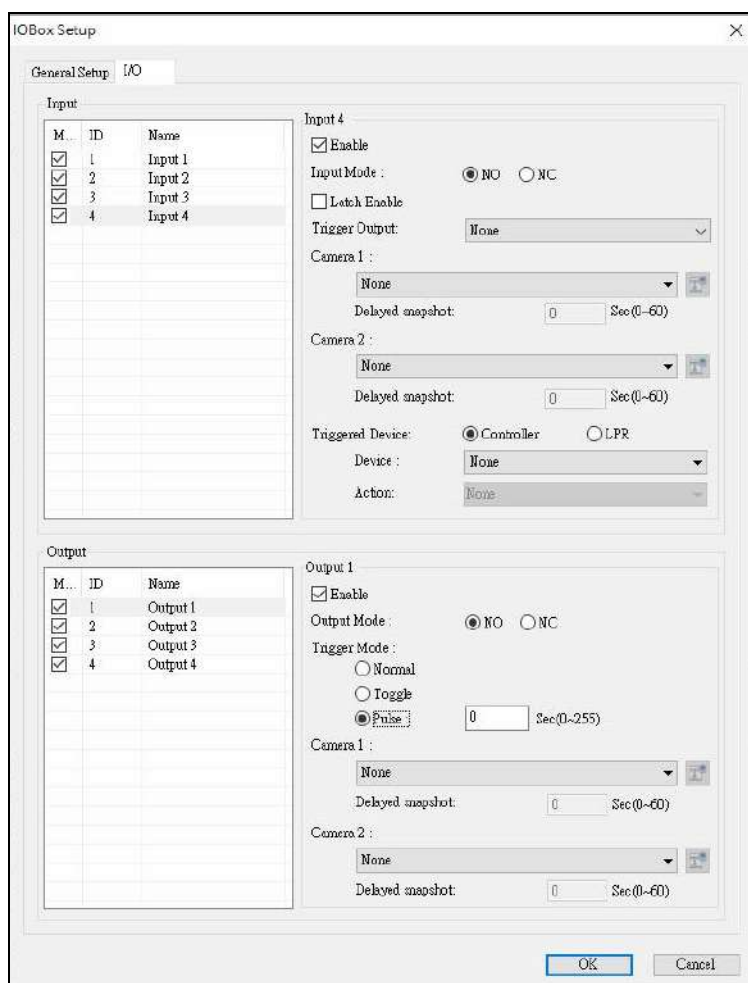


Figure 4-40

2. On the left panes, select one input or output to be defined.

[Input]

- **Enable:** Enable this Input function.
- **Input Mode:** Configure the input to **NC** (normally closed) or **NO** (normally open) mode.
- **Latch Enable:** Instead of constant output alarm in N/O and N/C, the option provides a momentary alarm when triggered.
- **Trigger Output:** Select an output to trigger when the input is activated.
- **Camera 1 / 2:** Select cameras to take snapshots upon input trigger.
- **Delayed snapshot:** Type the number of seconds to delay capturing a snapshot after input is triggered.
- **Trigger Device:** Specify the controller or LPR device to trigger a door or lane operation.

[Output]

- **Enable:** Enable this Output function.
- **Output Mode:** Configure the input to **NC** (normally closed) or **NO** (normally open) mode.
- **Trigger Mode:**
 - **Normal Mode:** Output continues to be triggered until the source of the output condition is stopped.
 - **Toggle Mode:** Output continues to be triggered until a new input trigger ends the output.
 - **Pulse Mode:** Output is triggered for the amount of time specified in the **Sec** field.
- **Camera 1 / 2:** Select camera(s) to take snapshots upon output trigger.
- **Delayed snapshot:** Type the number of seconds to delay capturing a snapshot after output is triggered.

Chapter 5 Video Integration

GeoVision IP devices, software and third-party IP cameras can be connected to GV-ASManager over a network. Live videos can then be accessed and snapshots will be captured when the events of access control, LPR and I/O devices occur.

GV-ASManager provides the following video features:

- Live view
- Video playback
- Monitor up to 16 cameras simultaneously
- Text Overlay

Note:

1. GeoVision IP devices and software include GV-DVR / NVR / VMS, GV-AI Guard, GV-Recording Server, GV-Video Server, GV-Compact DVR and GV-IP Camera.
 2. GV-ASManager is compatible with third-party IP devices using RTSP, ONVIF and PSIA protocols.
 3. GV fisheye dewarping is only supported when using MultiView, and only available on Single View mode.
 4. To add a camera from GV-DVR / NVR / VMS, GV-AI Guard, it is required to enable Control Center Server (CCS) on these hosts.
-

5.1 Mapping Cameras

Following the steps below to associate a camera with the door, floor, lane or input/output device.

To add a camera:

1. On the menu bar, click **Setup > Devices**.
2. Select the desired Device Group, right-click **Camera > New Camera**.

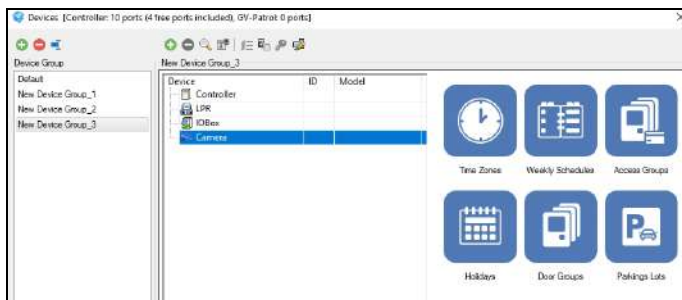


Figure 5-1

3. In the Host Setting dialog box, select the type of the IP device and define its connection information, including IP, login credentials, port(s) and number of cameras connected with.

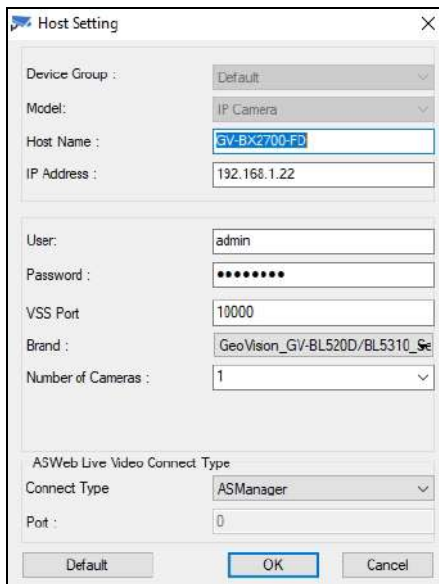


Figure 5--2

Note: To connect IP devices through RTSP, ONVIF and PSIA protocols, select **IP Camera** from the **Model** drop-down list, and then **Protocol** from the **Brand** drop-down list to choose the type of protocol.

4. Optionally, define how the live view of camera is streamed to GV-ASWeb.
 - **ASManager:** Enabled by default. The live view is streamed from GV-ASManager to GV-ASWeb.
 - **Motion-JPEG:** The live view is streamed from the IP device to GV-ASWeb in JPEG format.
 - **Web Socket or Web Socket Secure (Recommended):** The live view is streamed from the IP device to GV-ASWeb, through port **80** or **443** respectively.
5. Click **OK** and return to the main screen.

To associate a camera:

6. Double-click a Device, and select one Door, Floor, Lane or I/O for setup.

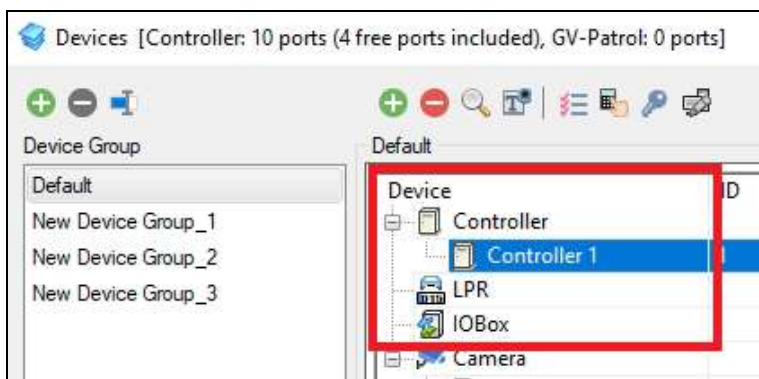


Figure 5-3

7. Use the drop-down list to select a camera you just added. Take GV-AS Controller as an example as below.

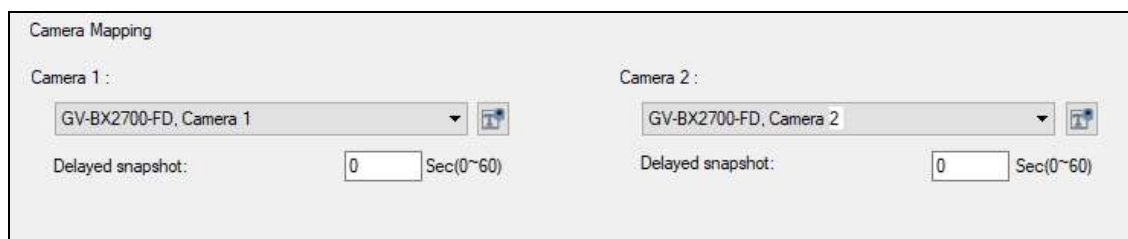


Figure 5-4

8. Optionally, enable **Delayed snapshot** by defining the number of seconds to delay capturing snapshots after an event is triggered. For example, if the camera is installed 10 meters away from a card reader and it takes 5 seconds for a user to walk pass the camera after presenting the card, you can delay the snapshot for 5 seconds.

Once set up, the camera will take snapshots when a card reader, LPR camera or I/O device is triggered. You can access the snapshots from the corresponding Monitor window in Thumbnails view.

Tip: You can associate two cameras of entrance and exit, respectively, with one door. Or you can associate two cameras with a door with different view angles.

5.2 Accessing a Live View

After mapping cameras to a door, floor, lane or I/O device, use one of the following methods to access live view on the Live Video window:

- On the Controller / LPR / IO Boxes List window, click the desired door, floor, lane or input / output. Its associated live view will appear.
- On the Camera List window, click the desired camera. Its associated live view will appear.
- On the Access / Alarm Monitor window, click the desired event. Its associated live view will appear.

To access live views from multiple IP devices simultaneously, see *5.4 The Multi View Window*.

5.2.1 Live Video Window



Figure 5-5

No.	Name	Function
1	Camera List	Switches between two cameras when you have mapped two cameras to the selected door.
2	Previous / Next Camera	Switched to the previous or the next camera.
3	Best Fit	Rescales the image to fit any resized window.
4	Actual Size	Displays the image in its original size.
5	Zoom	Zooms in or out the image.
6	Thumbnail	Displays a thumbnail view (No. 7). When the image size is larger than the Live Video window, drag the box in the thumbnail view to have a close look at the image.
7	Thumbnail View	See the description in No. 6.

5.3 Accessing Captured Images

You can access the images captured after the access and alarm triggered event.

- On the Access Monitor or Alarm Monitor window, double-click the desired event to display the captured image. Or, right-click the desired event and select **Show Image** to display the image.

5.4 The MultiView Window

The MultiView window provides a live view of up to sixteen cameras on one window.

- On the menu bar, click **View > MultiView**. The MultiView window appears.
- Drag the desired camera from the Camera List window, and drop it to a grid on MultiView.

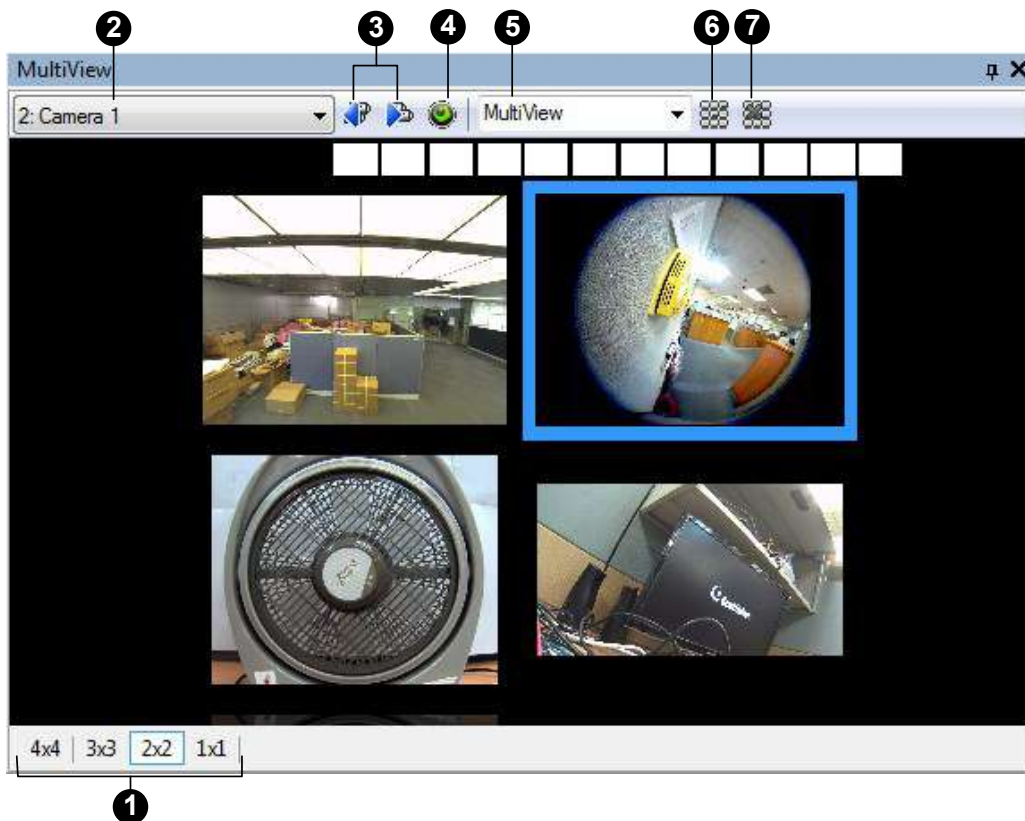


Figure 5-6

No.	Name	Function
1	Layout	Select the number of channels to display.
2	Camera List	Select the desired camera.
3	Previous / Next Camera	Go to the previous or next camera view.
4	Fisheye	Select the installation site of the fisheye camera, and then right-click the camera view to dewarp the circular source image into single view.
5	Multi View	Switch to a different Multi View. To add a Multi View: <ol style="list-style-type: none"> 1. In the drop-down list, type a name for the Multi View. 2. Click the Add Multi View button. The Multi View is created. 3. Drag the desired camera from the Camera List window to the Multi View. 4. Repeat above steps to add more than one Multi View.
6	Add Matrix	Add a Matrix View.
7	Remove Matrix	Remove a Matrix View.

Note: When multiple monitors are set up in the system, you can drag and drop the Multi View window to another computer monitor.

5.5 Retrieving Recorded Videos

Recorded videos can be retrieved and played back from the hosts of GV-DVR / NVR / VMS, GV-AI Guard and GV-Recording Server. For remote playback to work, you need to enable the following functions on the hosts to allow remote access:

- For GV-DVR / NVR / VMS, GV-AI Guard, enable **Remote ViewLog Service** under Control Center Server
- For GV-Recording Server, enable **Remote ViewLog** under Network

To play back a video:

- On the Access Monitor or Alarm Monitor window, click the desired event. If a recorded video exists, the Playback window will be enabled. Click the **Play** button to play the video clip.

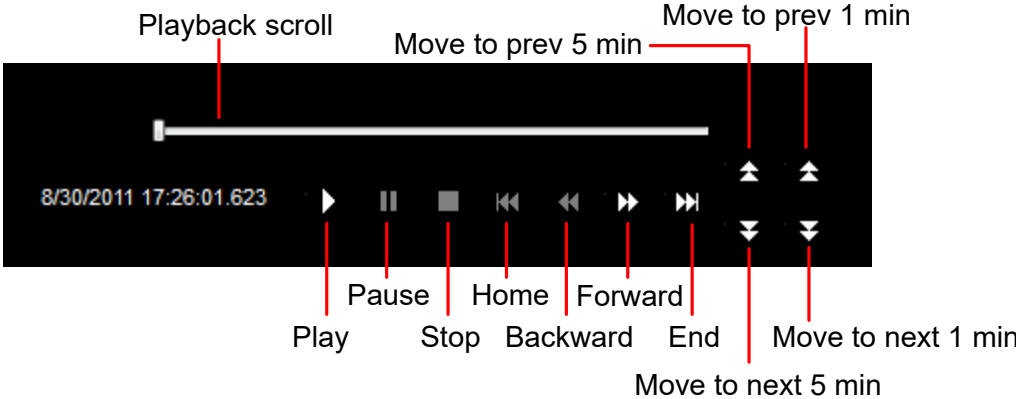
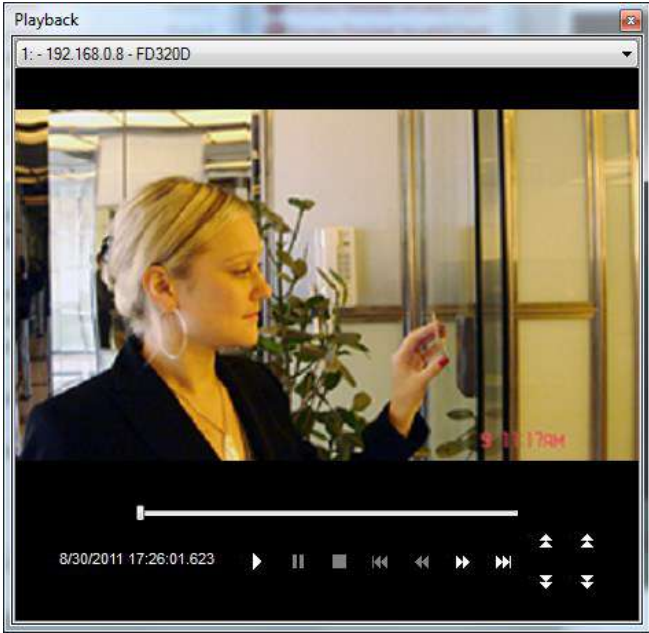


Figure 5-7

Right-click the window to have the following features:


<p>Play Mode</p>	<p>Includes these options:</p> <ul style="list-style-type: none"> • Frame by Frame: Plays back video frame by frame. • Real Time: Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback. • Auto Play Next 5 Minutes: Plays back video up to 5 minutes. • Audio: Turns on or off the video sound.
<p>Render</p>	<p>Includes these options:</p> <ul style="list-style-type: none"> • Deinterlace: Converts the interlaced video into non-interlaced video. • Scaling: Smoothens mosaic squares when enlarging a playback video. • Deblocking: Removes the block-like artifacts from low-quality and highly compressed video. • Defog: Enhances image visibility. • Stabilizer: Reduces camera shake. • Text overlay's camera name and time: Overlays camera name and time onto the video. • Text overlay's POS/GV-Wiegand: Overlays POS or GV-Wiegand Capture data onto the video. • Full Screen: Switches to the full screen view.
<p>Tools</p>	<ul style="list-style-type: none"> • Snapshot: Saves a video image. • Save as AVI: Saves a video as avi format. • Download: Downloads the video clip from a GeoVision IP device to the local computer.

5.6 Applying Text Overlay

Once the mapped cameras from GV-VMS are triggered, the event messages of Controller / LPR / I/O can be overlaid on the camera view of GV-VMS. For details on mapping GV-IP cameras, see *5.1 Mapping Cameras*.

Note: The function is only supported by GV-VMS V16.10.3.0 or later.

To enable Text Overlay:

1. On the menu bar, click **Setup > Devices** and double-click a Device.
2. Select a Door, Floor, Lane or I/O for setup. Here we use GV-I/O Box as an example.
3. After selecting one **Input** or **Output**, in the Camera Mapping section, click the **Text Overlay** icon  besides cameras.

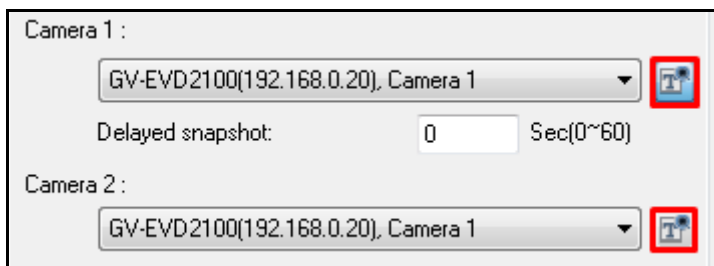



Figure 5-8

4. Click **OK** to return to the Device List.
5. Click the **Camera Text Overlay** icon .

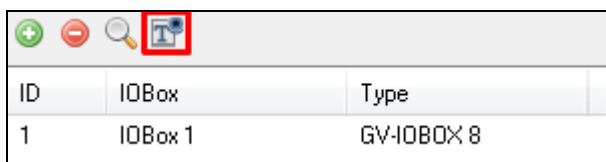


Figure 5-9

6. Enter your own messages, or use the buttons on the text window to send out the programmed information.

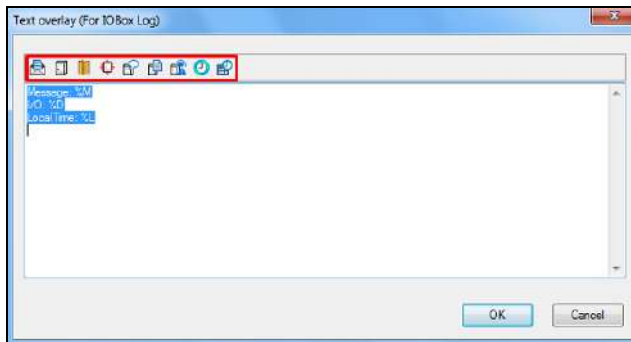


Figure 5-10

Make sure the Text Overlay setting is also enabled in GV-VMS (**Home > Toolbar > Configure > Video process > Text Overlay Setting > Print ASManager Text on Screen**).

Note: For how to text overlay a standalone LPR's data on GV-VMS's live view, see the [technical notice](#).

Chapter 6 Anti-Passback

The Anti-Passback is used to ensure one-card and one-way access into and then out of a controlled area. This function prevents users from passing their cards back to a second person to gain entry into the same controlled area. Depending on the number of controllers and communication link, there are three types of Anti-Passback operations: **Anti-Passback**, **Local Anti-Passback** and **Global Anti-Passback**, which will be explained more fully in the upcoming sections.

Anti-Passback is performed only on one controller, while Local Anti-Passback and Global Anti-Passback can be performed on multiple controllers. Anti-Passback is performed through either RS-485 or TCP/IP connection, while Local Anti-Passback and Global Anti-Passback are performed only through TCP/IP connection. The following table lists the supported operations among GV-AS / GV-EV Controllers.

Model	Anti-Passback	Local Anti-Passback & Global Anti-Passback
GV-AS100 / 110 / 120	Yes	Yes (GV-ASBox or GV-ASNet required)
GV-AS1010 / 1110 GV-AS210 / 410 / 810 GV-AS2110 / 2120 GV-AS4110 / 8110	Yes	Yes
GV-CS1320	Yes	Yes
GV-AS1520	Yes	Yes
GV-AS1620	Yes	Yes

6.1 Anti-Passback

Anti-Passback is used on **one controller only**. For this application, select **by Card – Local** or **by User – Local** at the **Door** tab of the Controller Setup dialog box.

- **By Card – Local:** Select this option to monitor the access into the controlled area by cards. This option enables multiple cards to be used simultaneously by the same user.
- **By User – Local:** Select this option to monitor the access into the controlled area by users. This option prevents the same card from using by multiple users.

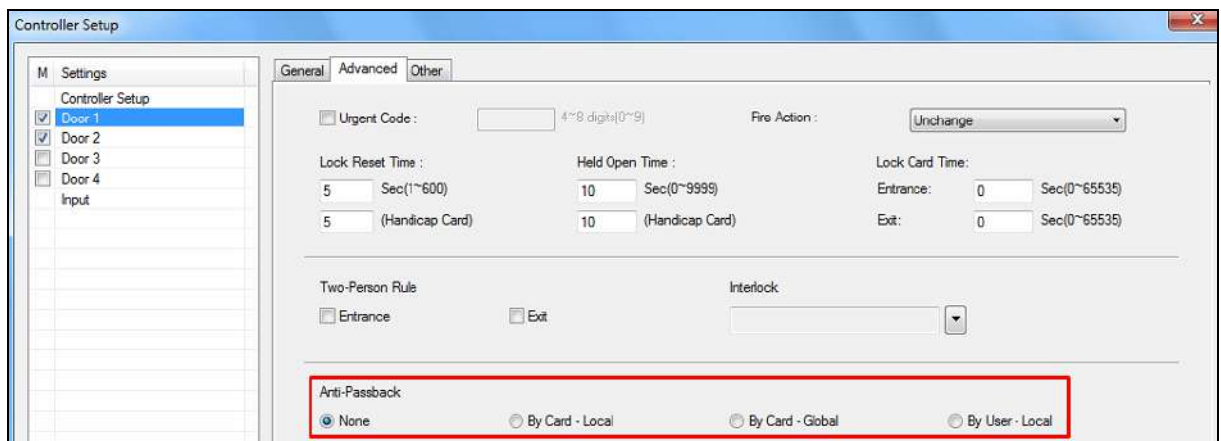


Figure 6-1

To reset Anti-Passback on GV-ASManager, right-click one **Host** or **Controller** on the Controller view window (Figure 3-3) and select **Reset Anti-Passback**.

Note: The **By User – Local** option is only supported by GV-AS2 / 4 / 8 series controllers and GV-AS1520 firmware V2.0 or later.

6.2 Local Anti-Passback

Local Anti-Passback is used on **multiple controllers which are associated with network connections**. Before you start, the following conditions must be true:

- The communication mode between GV-ASManager and the controller is Ethernet.
- LAN environment is applied.

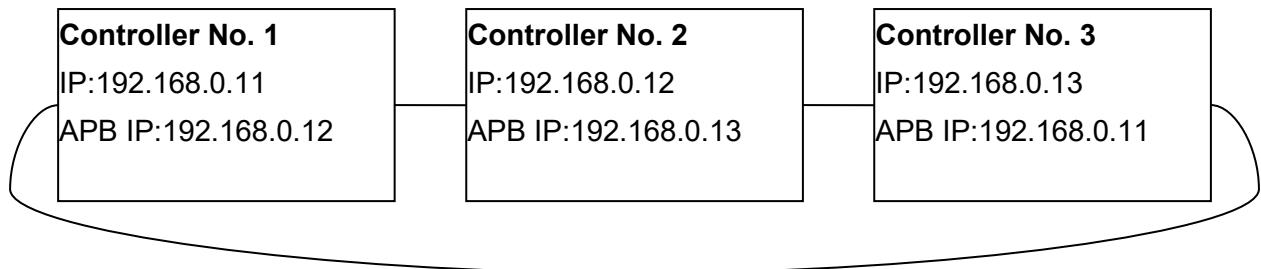
This section explains how to combine three controllers to implement the Anti-Passback (APB) function. Because Anti-Passback is performed across a network, each controller is assigned a unique IP address. When three controllers are connected for Anti-Passback, an APB IP address is used for interaction.

For example, Controller No. 1, No. 2 and No. 3 are combined in the order shown below. APB IP is the IP address of the associated controller.

IP of Controller No. 1 is 192.168.0.11; APB IP of Controller No. 1 is IP of Controller No. 2.

IP of Controller No. 2 is 192.168.0.12; APB IP of Controller No. 2 is IP of Controller No. 3.

IP of Controller No. 3 is 192.168.0.13; APB IP of Controller No. 3 is IP of Controller No. 1.



To configure Anti-Passback for the three Controllers:

Step 1: Configuring Door Contacts

This step defines the door contact sensor for each door. When a door contact sensor is triggered, GV-ASManager knows which door is open.

To configure door contact sensors, go to the Web interface of each controller and select **Input Configuration**. In this example, Input 01 is set as Door Contact of Door 1, Input 02 is set as Door Contact of Door 2 and etc.

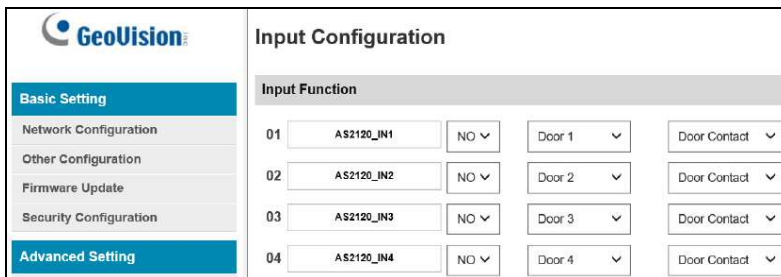


Figure 6-2-1

Step 2: Configuring APB IP Addresses

1. Access the **Function Configuration** page of the Controller No. 1's Web interface. In the Series Function (APB & Fire) section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 2, e.g. 192.168.0.12.



Figure 6-2-2

2. Access the **Function Configuration** page of the Controller No. 2's Web interface. In the Series Function (APB & Fire) section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 3, e.g. 192.168.0.13.
3. Access the **Function Configuration** page of the Controller No. 3's Web interface. In the Series Function (APB & Fire) section, select **Enable** and enter **Info IP** that is the IP address of Controller No. 1, e.g. 192.168.0.11.
4. In GV-ASManager, select **Local Anti-Passback** (Figure 6-1) to start the function.

6.3 Global Anti-Passback

Global Anti-Passback can not only prevent the use of a card to gain successive entries, but track the user around the site.

The plan below shows a typical site controlled by access control.

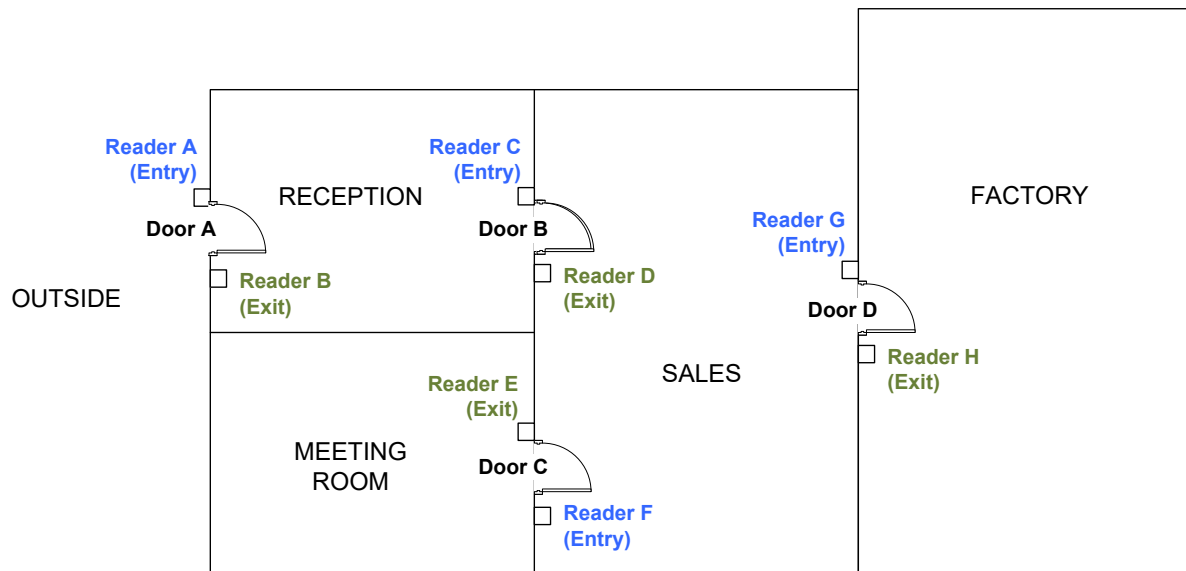


Figure 6-3

To configure the above site as example of Global Anti-Passback, you must complete the following six steps:

- **Step 1: Enabling Global Anti-Passback**
Select **By Card – Global** at each **Door** tab (*section 6.3.1*).
- **Step 2: Configuring Areas**
Define the Entrance and Exit areas for each door (*section 6.3.2*).
- **Step 3: Configuring Readers**
Define the Entrance and Exit readers for each door (*section 6.3.3*).
- **Step 4: Configuring Door Contacts**
Define the door contact sensor for each door (*section 6.3.4*).
- **Step 5: Monitoring Areas**
How to monitor the areas for each door (*section 6.3.5*).
- **Step 6: Locating Users**
How to locate a user in the control area (*section 6.3.6*).

6.3.1 Step 1: Enabling Global Anti-Passback

Select **By Card – Global** at each **Door** tab of the Controller Setup dialog box (Figure 6-1).

6.3.2 Step 2: Configuring Areas

This step is to define the Entrance and Exit areas for each door and name the areas properly.

- On the menu bar, click **Setup > Areas**. This dialog box appears. Then select a **Door** to define its area by specifying **Enter to** and **Exit from**.

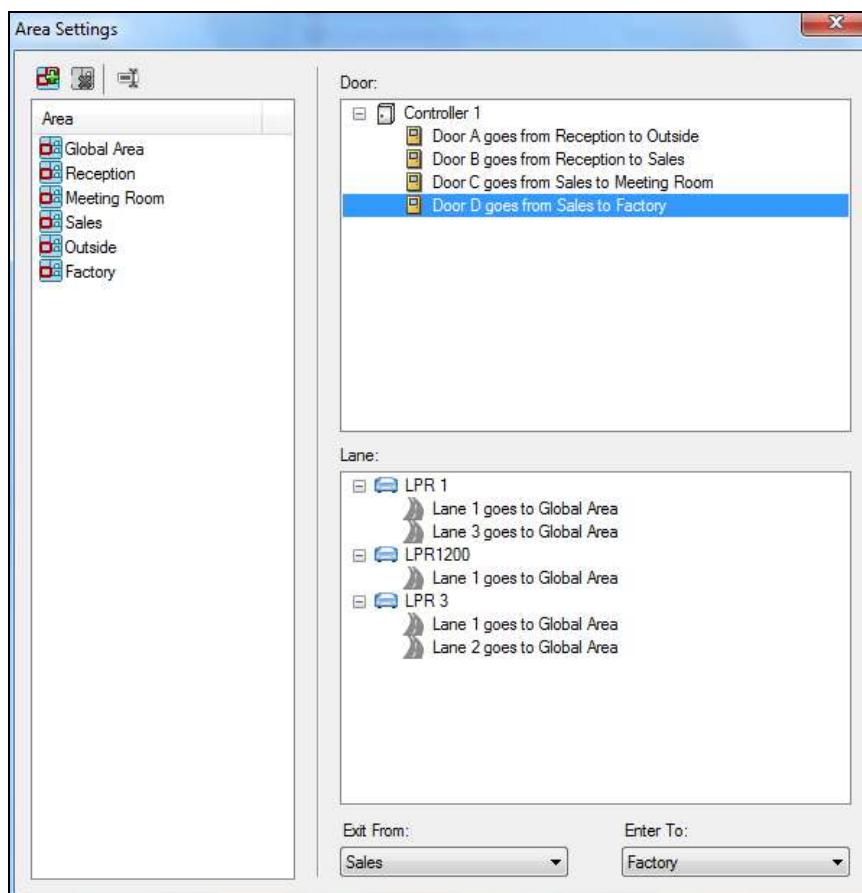


Figure 6-4

Enter to is the area where a user enters by accessing the Entrance reader of the door. **Exit from** is the area where the user is from. In this example, based on the plan of Figure 6-3, we set up like this:

Door A: **Enter to** Reception; **Exit from** Outside

Door B: **Enter to** Sales; **Exit from** Reception

Door C: **Enter to** Meeting Room; **Exit from** Sales

Door D: **Enter to** Factory; **Exit from** Sales

6.3.3 Step 3: Configuring Readers

This step is to define the Entrance and Exit readers for each door. The reader defining tells GV-ASManager which reader controls the access across the area boundaries. When users access unauthorized readers, the message **Access Denied: APB (Wrong Area)** will be displayed and the door will remain locked. When users access the same reader successively, the message **Access Denied: APB (Double Entry)** will be displayed and the door will remain locked.

To define readers, go to the Web interface of controller. On the left menu, click **Wiegand Setting** for Wiegand readers or **Extended Reader** for RS-485 / TCP/IP readers. In the example below, based on the plan of Figure 6-3, Wiegand reader A (Entry) goes from Outside to Reception, Wiegand reader B (Exit) goes from Reception to Outside and etc.

Wiegand Function	
Wiegand A	Door/Gate A Entry
Wiegand B	Door/Gate A Exit
Wiegand C	Door/Gate B Entry
Wiegand D	Door/Gate B Exit
Wiegand E	Door/Gate C Entry
Wiegand F	Door/Gate C Exit
Wiegand G	Door/Gate D Entry
Wiegand H	Door/Gate D Exit

Figure 6-5

6.3.4 Step 4: Configuring Door Contacts

This step is to define the door contact sensor for each door. When a door contact sensor is triggered, GV-ASManager can tell which door is open.

To define door contact sensors, go to the Web interface of controller and select **Input Configuration**. In this example, Input 01 is set as Door Contact of Door 1, Input 02 is set as Door Contact of Door 2 and etc.

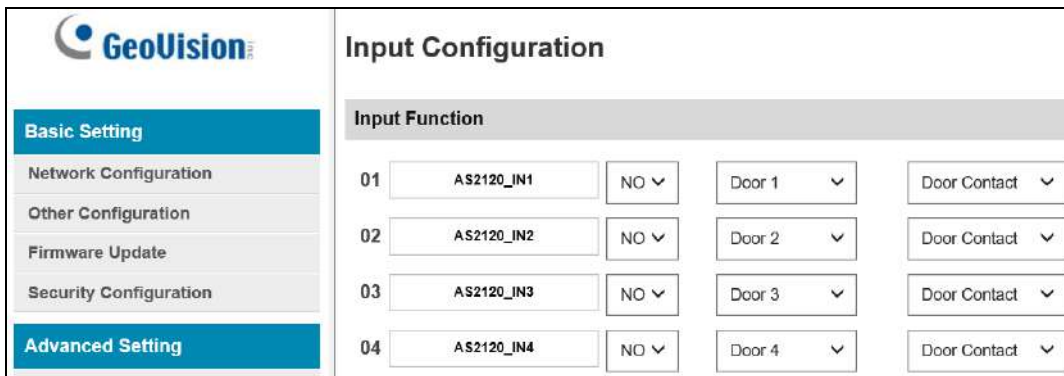


Figure 6-6

6.3.5 Step 5: Monitoring Areas

To monitor the area for each door, on the menu bar, select **Monitoring > New Area Monitor**. When a card is swiped to enter an area, GV-ASManager can tell which user is granted access to which area. In this example, the access from the card number 244-36572 belonging to the user Ian Anston is granted to the meeting room.

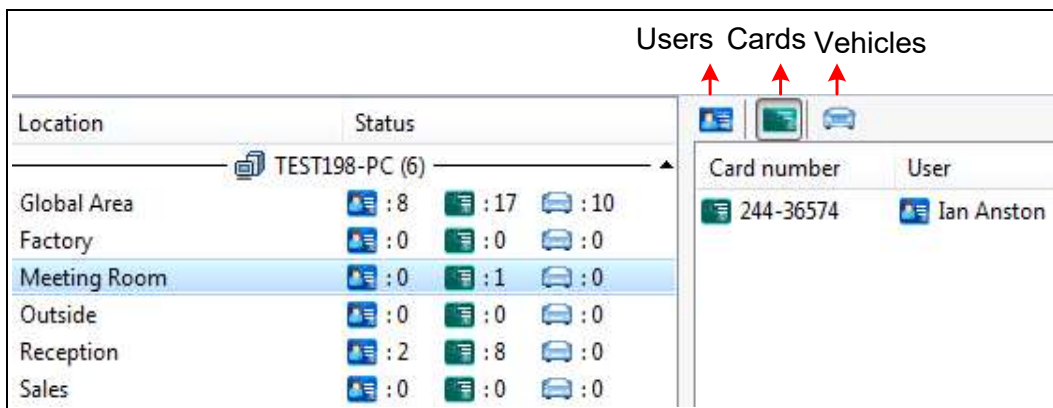


Figure 6-7

6.3.6 Step 6: Locating Users

To locate a user, on the menu bar, select **Monitoring > New Locate People**.

When the Entrance or Exit reader is triggered, GV-ASManager can tell if the user follow Anti-Passback rules and then grant or deny access. In this example, based on the plan of Figure 6-3, Christine Downes is granted access from Door A and now she is in the reception area.

User	Location	User: Christine Downes			
TEST198-PC (12)		Message	Door	Direction	Local Time
Brendy Williams	Global Area	Access Granted	Door A	Out	9/15/2017 4:59:10 PM
Ian Anston	Global Area	Access Granted	Door A	In	9/15/2017 5:00:09 PM
Tom Hiddleston	Reception				
Rachel Mill	Global Area				
David Wang	Global Area				
Scarlett Johansson	Global Area				
Blake Lively	N/A				
Chris Hemsworth	Global Area				
Alex Urda	Global Area				
Brad Macal	Global Area				
Christine Downes	Reception				
Joyce Change	N/A				

Figure 6-8

Tip: To reset Anti-Passback in GV-ASManager or GV-ASRemote, right-click one **Host** or **Controller** icon on the Controller view window (Figure 3-4) and select **Reset Anti-Passback**.

Chapter 7 Patrol Tour

Patrol Tour can be created to require security staff to check in at the specified locations during a certain time period.


7.1 Creating Patrol Tour

Create weekly Patrol Tours by specifying the doors where the security staff needs to check in during the specified time period. If the security staff does not present their cards at the specified door on time, an alert notification can be sent using e-mail or SMS message.

1. On the menu bar, click **Setup > Patrol Tours**. This dialog box appears.



Figure 7-1

2. To create a new Patrol Tour, click the **Add Patrol Tour** button  on the left toolbar. The **Group Patrol Tour** option enables any patrol cards in the group presenting at the patrol point to be counted as attendance. For **Rolling Patrol Tours**, see 7.2 *Creating Rolling Patrol Tour*.

3. Select a day in the timeline and click the **Add Patrol Point** button  above the timeline. This dialog box appears.

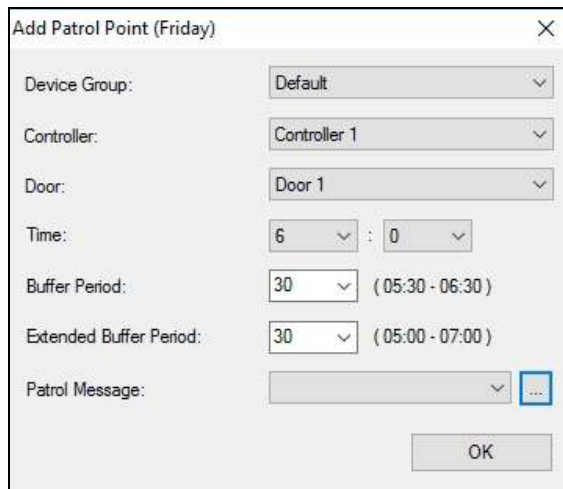



Figure 7-2

4. To define the location and check-in time of the Patrol Point, select the **Device Group**, **Controller** and **Door** that the security staff needs to patrol, and complete the following settings:
- **Time:** Select the time when the security staff should check in at the selected door by presenting the card.
 - **Buffer Period:** Specify the Buffer Period in minutes, which will be added before and after the check-in time specified above. Security staff checking in during the buffer period will be considered on time. Using *Figure 7-2* as an example, the security staff needs to check in between 5:30am and 6:30am to be considered on time.
 - **Extended Buffer Period:** The Extended Buffer Period will be added before and after the Buffer Period specified above. Security staff who checks in during the Extended Buffer Time is considered late or early, and alert notifications can be set off if enabled. Using *Figure 7-2* as an example, check-ins between 4:50am - 5:30am will be marked as Early, while check-ins between 6:30am – 7:10am are considered late.
 - **Patrol Message:** Click the ... button and type an alert message to be sent using e-mail or SMS when the security staff is on time, early, late or absent.

Note: Security staff checking in outside the Extended Buffer Period will be marked as absent.

5. Click **OK**.

- To add more Patrol Points, repeat the steps 3~5. You can also drag a Patrol Point to another day of week or click  to create a copy.

Below is an example of a completed Patrol Tour, where the dark green zone is when the security staff needs to check in and the light green zone is the extended buffer period.

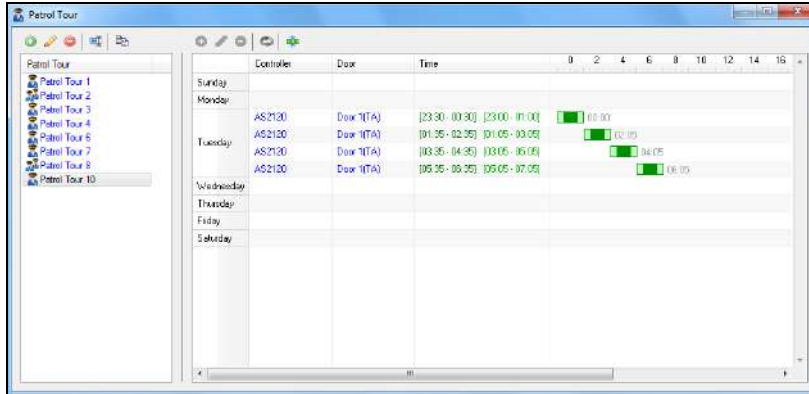


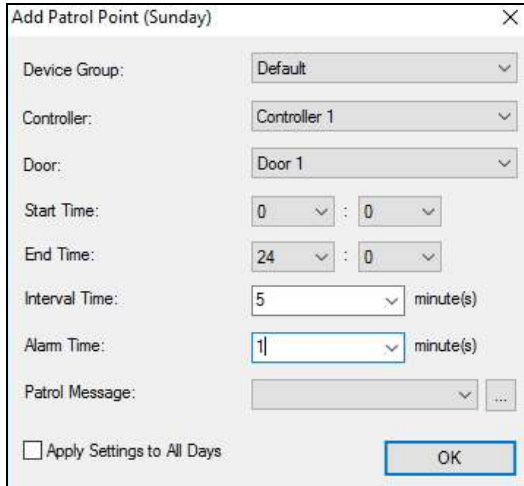
Figure 7-3

7.2 Creating Rolling Patrol Tour

Rolling Patrol Tours are weekly schedules used to specify patrol points where the security staff is required to check in repeatedly at the time interval set, e.g. every 10, 20 minutes or every hour. If the security staff does not present the card at the specified door on time, an alert notification can be sent using e-mail or SMS message.

- On the Patrol Tour window, click the **Add Patrol Tour** button  > **Add Rolling Patrol Tour**.


2. Select a day in the timeline and click the **Add Patrol Point** button  above the timeline. This dialog box appears.



The screenshot shows a dialog box titled "Add Patrol Point (Sunday)". It contains several configuration options:

- Device Group:** Default
- Controller:** Controller 1
- Door:** Door 1
- Start Time:** 0 : 0
- End Time:** 24 : 0
- Interval Time:** 5 minute(s)
- Alarm Time:** 1 minute(s)
- Patrol Message:** (empty field with a ... button)
- Apply Settings to All Days
- OK** button

Figure 7-4

3. To define the location and patrol time of the Patrol Point, select the **Device Group**, **Controller** and **Door** that the security staff needs to patrol, and complete the following settings:
- **Start Time:** Specify the first time, within the day, when the security staff should check in at the selected door by presenting the card.
 - **End Time:** Specify the last time, within the day, when the security staff should check in at the selected door by presenting the card.
 - **Interval Time:** Specify the time interval in minutes, in which the security staff needs to check in at the same door again after their last check-in time.
 - **Alarm Time:** Specify the alarm time, counting down in minutes, in which to remind the security staff to check in at the door selected. For example, if the Alarm Time is set as 1 minute and the security staff needs to check in at 5:00, they will be alerted at 4:59. The Alarm Time must be smaller than the Interval Time.
 - **Patrol Message:** Click the ... button and type an alert message to be sent using e-mail or SMS when the security staff is on time, early, late or absent.
 - **Apply Settings to All Days:** Select to apply the Patrol Point settings to all days of the week.
4. Click **OK**.
5. To add more Patrol Points, repeat the step 2. You can also drag a Patrol Point to another day of week or click  to create a copy.

7.3 Activating the Patrol Tour

1. After you have created the Patrol Tour, double-click the Patrol Tour. This dialog box appears.

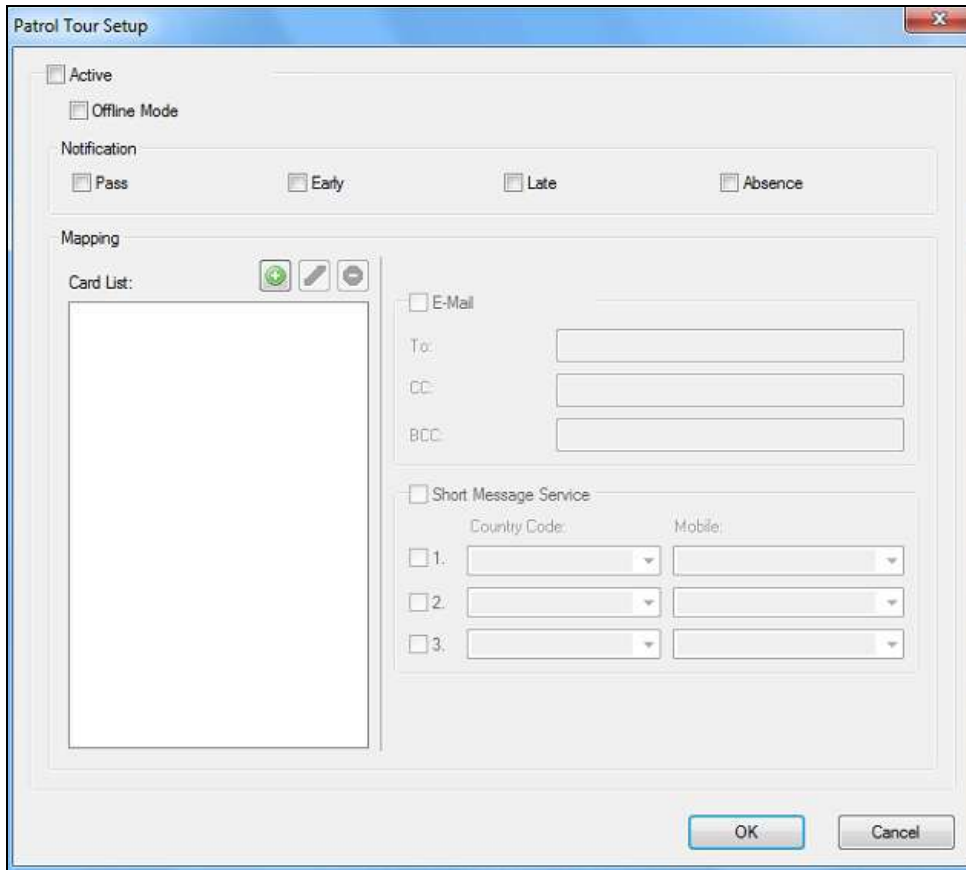



Figure 7-5

2. Click **Add**  and select a card. You can add multiple cards if needed and the security staff will be required to present one of the cards listed here.

Note: When the security staff presents the card, the controller may grant or deny door access according to the settings of the card. For example, if the security staff is using a Patrol Card, the door will remain locked and the security staff will check in without opening the door. See [4.3 Adding Cards](#) to see how to add the cards.

3. Double-click a card and select to notify by **E-Mail** and/or **Short Message Service**.

The screenshot shows a 'Mapping' window with a 'Card List' on the left containing two entries: [026] 123-45678 and [026] 234-56789. On the right, there are two notification sections. The first is 'E-Mail' with checkboxes for 'To:', 'CC:', and 'BCC:'. The second is 'Short Message Service' with checkboxes for 'Country Code:' and 'Mobile:', followed by three rows of input fields for each. At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 7-6


4. To set up alert notifications, select the notification conditions to send alert.

The screenshot shows a notification settings window. At the top, there is a 'Active' checkbox which is checked, and an 'Offline Mode' checkbox which is unchecked. Below this is a 'Notification' section, which is highlighted with a red rectangular box. This section contains four checkboxes: 'Pass', 'Early', 'Late', and 'Absence', all of which are currently unchecked.

Figure 7-7


5. Optionally, click **Offline Mode** to be able to check in by the scheduled Patrol times without an Internet connection through [GV-Patrol mobile app](#).
6. Click **Active** to activate the Patrol Tour and click **OK**.

Note:

1. Once the Patrol Tour is activated, the Patrol Points cannot be modified again.
 2. Once the Patrol Tour has been de-activated, the Patrol Tour Setup page will also become unchangeable. Instead of re-configuring a new Patrol Tour from the beginning, you can use the **Copy Patrol Tour** button  to create a new patrol tour with the same settings as the de-activated Patrol Tour.
-

7.4 Monitoring Patrol Activities

To monitor Patrol activities, on the menu bar, click **Monitoring > New Patrol Tour Monitor**.

Next, click  to select the Patrol Tour you want to monitor. The current status of each Patrol Point will be displayed. A red zone indicates Absence, an orange zone indicates Early or Late, and a green zone indicates On Time.

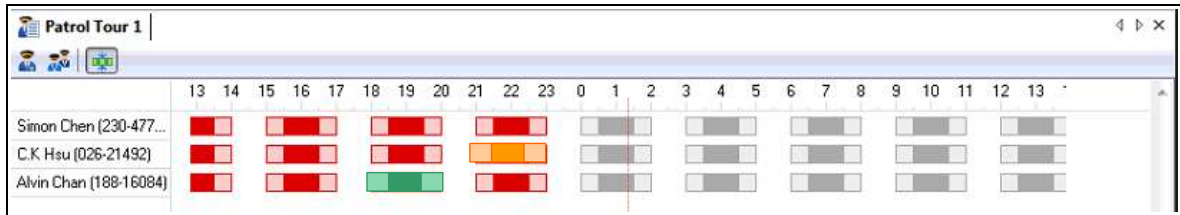


Figure 7-8

7.5 Accessing Patrol Log

Using Patrol Log on GV-ASWeb, you can set search criteria to look up patrol records. For how to log in GV-ASWeb, see *10.1 Connecting to GV-ASManager*.

1. On GV-ASWeb, click the **Patrol Log** icon. This window appears.

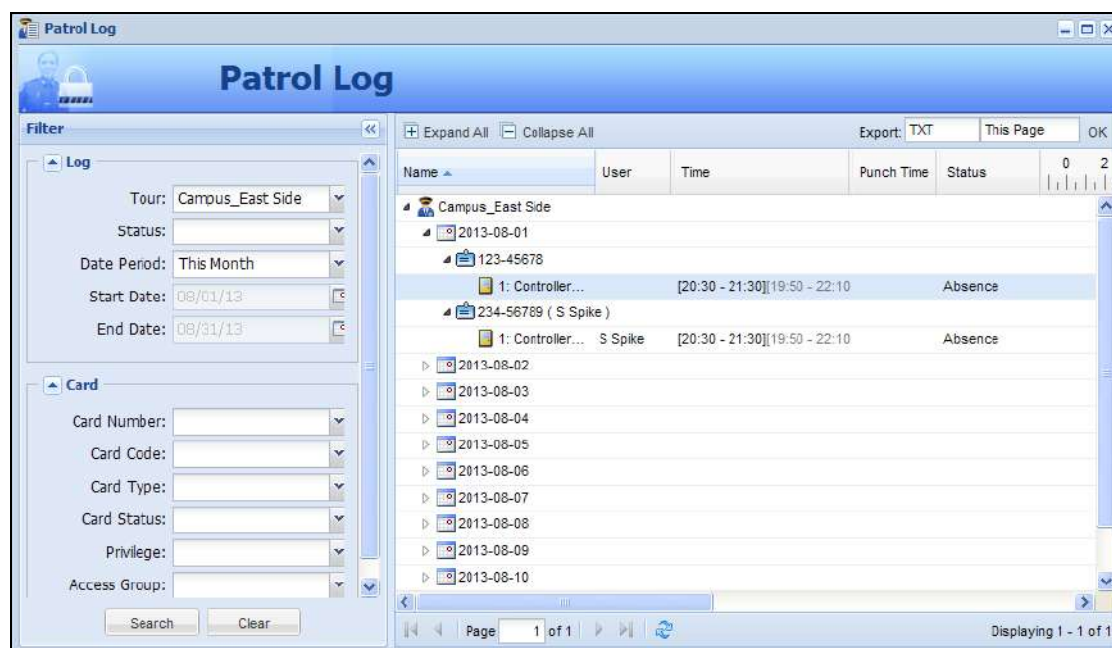


Figure 7-9

2. Under **Filter** in the left pane, define the search criteria. For example, you can use the **Status** drop-down list to search for all patrol records listed as “Absence.”
3. Click the **Search** button to start the log search.

To export logs, see *10.6 Setting up Export Schedules for Lists and Logs* for details. To customize the columns of search results, see *10.4.4 Defining Columns* for details.

Chapter 8 Other Functions

8.1 Adding System Users

A system user is a person using GV-ASManager to monitor door controllers, enroll users or program the system. Using this function, the system administrator can create new system users with different access rights. Up to 1,000 user accounts can be created.

1. On the menu bar, click **Tools > Operators**. This dialog box appears.

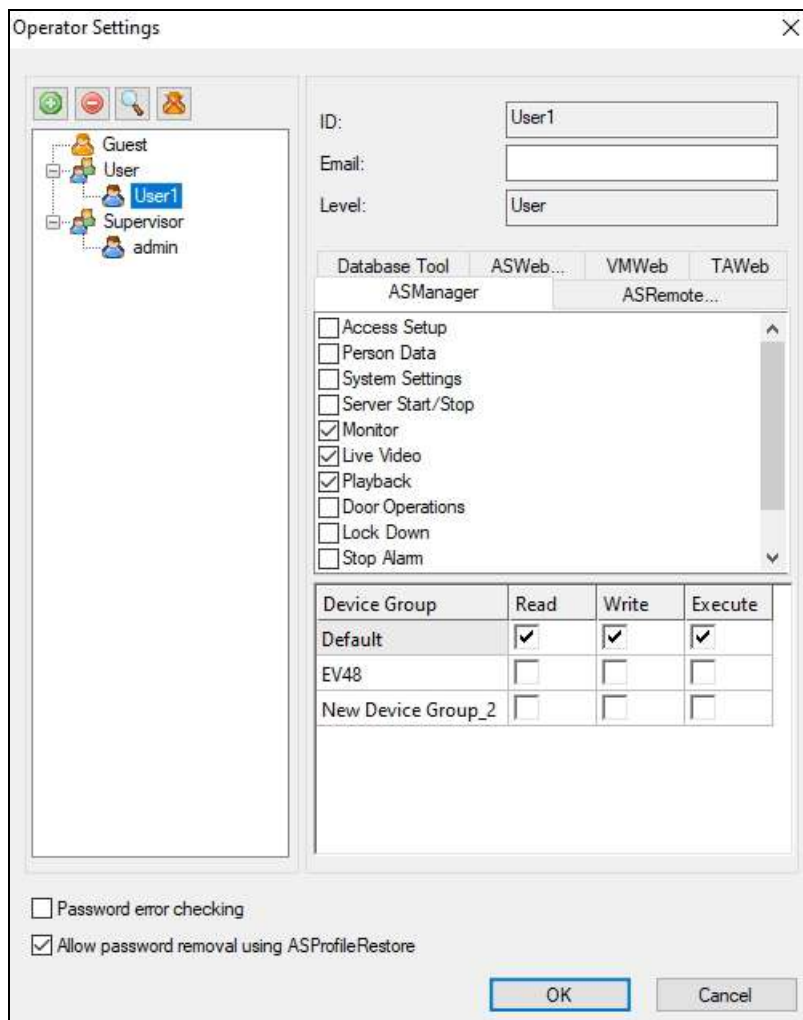




Figure 8-1

2. Click the **New** button  at the top left corner. The Add Account dialog box appears.
3. Type the user's **ID** and **Password**. Re-enter the same password in the Password Confirmation field.
4. Type an email address so that the user's password can be sent to the email if forgotten.
5. Set the user's authorization level to **Supervisor** or **User**. By default, users belonging to the Supervisor level have full rights and permissions to system settings. Users belonging to the User level are restricted from all system settings, and have only limited access to certain functions.
6. Click **OK** to add the user.
7. Click any of the following tabs in the middle of the window: **ASManager**, **Database Tool**, **VMWeb**, **TAWeb ASRemote/ASNotify/Locakdown App/ASManager SDK**, and **ASWeb/GV-Access/Web SDK/ASMobile/ASRemote Web/GV-Patrol**. Select the corresponding functions to grant access to the system user.
8. In the **Device Group** section, you can optionally select a device group and specify whether the user account will be able to read, write and execute the functions assigned under the device group. A device group may include controllers, cards, users, access groups, time zones and weekly schedules. Up to 32 device groups can be created. You can click the name of a device group to rename it.
 - **Read:** Privilege to view settings.
 - **Write:** Privilege to view and change settings. When Write is selected, Read will automatically be selected.
 - **Execute:** Privilege to open door, close door and turn off alarm.

For example, if you select Device Group 4 and only select **Write**, the user will be able to view and change only the settings of the controllers, cards, users, access groups, time zones and weekly schedules assigned under Device Group 4.
9. Optionally select **Password error checking** to show remaining attempts and wait time for login errors.
10. Optionally select **Allow Password Removal using ASProfileRestore**. You can erase all user and supervisor accounts by running **ASProfileRestore.exe** from the software installation folder.

To edit an existing user, select a user from the user list to display its properties. Or, click the **Search Account** button  for a quick search. Only supervisors can edit the information of a system user.

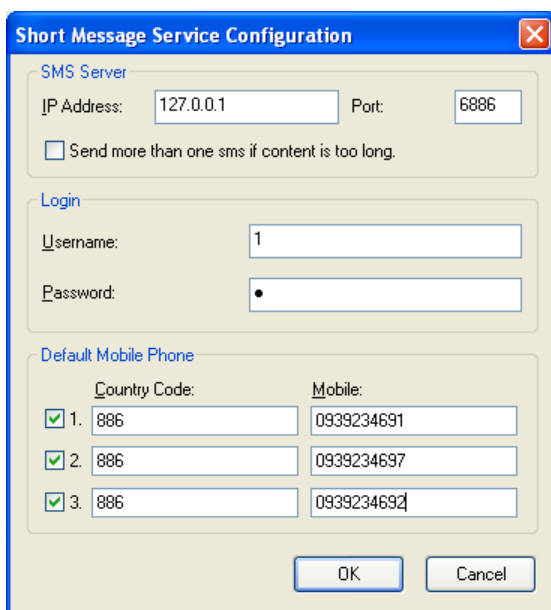
8.2 Setting up Alert Notifications

When alert conditions occur, the system can automatically send SMS and e-mail alerts to one or multiple recipients, as well as activating computer alarms.

8.2.1 Setting up SMS Server

Before you can send out SMS alerts, you should configure the SMS server.

1. On the menu bar, click **Tools > SMS Server Settings**. This dialog box appears.



The dialog box titled "Short Message Service Configuration" contains the following fields and controls:

- SMS Server**
 - IP Address: 127.0.0.1
 - Port: 6886
 - Send more than one sms if content is too long.
- Login**
 - Username: 1
 - Password: •
- Default Mobile Phone**

	Country Code:	Mobile:
<input checked="" type="checkbox"/> 1.	886	0939234691
<input checked="" type="checkbox"/> 2.	886	0939234697
<input checked="" type="checkbox"/> 3.	886	0939234692

Buttons: OK, Cancel

Figure 8-2

2. Type the IP address of the SMS server, its login username and password. Then assign up to three mobile numbers, including country code, which SMS alerts should be sent to. Click **OK**.
3. To enable the SMS connection, click **Tools** on the menu bar > **Connect to SMS Server**.

Note: For ASCII encoding (English language), SMS text messages are limited to 160 characters; for Unicode encoding (other languages), SMS text messages are limited to 70 characters. If you want to send longer text messages, select **Send more than one sms if content is too long**. The long messages will be split up to 9 segments and go out as multiple SMS messages.

8.2.2 Setting up E-Mail Server

Before you can send out e-mail alerts or send lost password to an email account, you need to configure the e-mail server.

1. On the menu bar, click **Tools > Email Server Settings**. This dialog box appears.



Figure 8-3

2. Select **Google** or **Microsoft** to link your email account, or select **Others** to enter your own server information.
3. To set up your own mail server, configure the following options:
 - **Name:** Type the sender's name.
 - **E-Mail Address:** Type the sender's e-mail address.
 - **Authentication:** If your mail server requires authentication for sending e-mails, select one type of authentication, and type the valid username and password.
 - **Host Name/Address:** Type the name of the mail server.
 - **Command Port:** Keep the default port 25, or modify it to match that of the mail server.

- **SSL:** Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of Internet connection. When the option is enabled, the Command Port is changed to 465.
- **Message Priority:** Assign the message a priority so the recipient knows to either look at it right away (high priority) or read it when time permits (low priority). A high priority message has an exclamation point next to it. Low priority is indicated by a down arrow.
- **Send to:** Type a valid e-mail address and click the **Test** button to check if the server setup is correctly configured.

8.2.3 Setting up Notifications

1. On the menu bar, click **Tools > Notifications**. This dialog box appears.

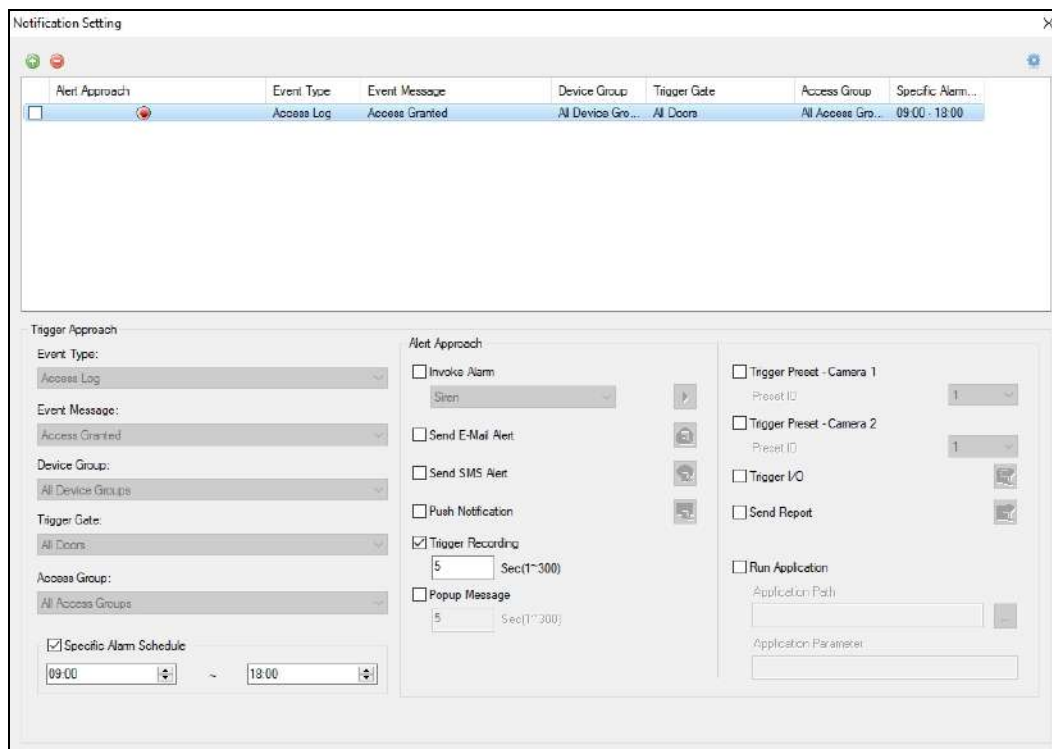



Figure 8-4

2. Click **Add**  to add an **Alert Approach**.
3. Define **Trigger Approach** for under which Event Type, Event Message, Device Group, Triggered Gate and/or Access Group, the notifications should be sent.
4. Optionally, select **Alarm Schedule** to send the notifications only during the specified time period.

5. Select **Alert Approach** for what alert or alarm should be triggered when the defined event occurs.
6. You can set up more than one Alert Approach rule, and enable or disable the desired rule anytime.

[Alert Approach]

- **Invoke Alarm:** Enable a computer alarm when the defined event occurs.
- **Send E-Mail Alert:** If you haven't set up the e-mail server, you will be prompted to set it up when you click this option. Then the E-Mail setup dialog box appears. Enter the recipient's e-mail address and alert subject. You can enter your own content, or use the buttons on the text window to send out the programmed information. For details, see *C. E-Mail and SMS Alert Symbols in Appendix*.
- **Send SMS Alert:** If you haven't set up the SMS server, you will be prompted to set it up when you click this option. Then the SMS setup dialog box appears. Ensure the preset mobile number(s). Select Text Code Type. You can enter your own messages, or use the buttons on the text window to send out the programmed information. For details, see *C. E-Mail and SMS Alert Symbols in Appendix*.
- **Push Notification:** Send push notifications to the GV-Access mobile app when the defined event occurs. For details, see [GV-Access Installation Guide](#).
- **Trigger Recording:** Enable recording of DVR / NVR / VMS, Video Server or Compact DVR when the defined event occurs. You can specify the recording time between 1 and 300 seconds. For the function to work, you must activate monitoring on the IP devices ahead.
- **Popup Message:** An associated live view will pop up for alert when the defined event occurs. Specify the duration of live view remains on the screen between 1 and 300 seconds.
- **Trigger Preset:** Direct the camera(s) to a preset point, if the camera supports the preset function, when the defined event occurs.
- **Trigger I/O:** Enable an associated output when the defined event occurs.
- **Send Report:** Enable to send the reports of lists and logs when the defined event occurs. For this function to work, you must set up which list and/or log to be sent and how to send on GV-ASWeb ahead. See *10.6 Setting up Export Schedule for Lists and Logs*.
 - For the **Fire Status** (Event Type: System Log > Event Message: Fire Status), specify the time interval (under Send Report) between each fire alarm to avoid receiving repeated reports.

- **Run Application:** Specify the **Application Path** and the designated application will run when the defined event occurs. Typing a command under **Application Parameter** can execute a function of that application.

Note: For text code type, select **ASCII** for English that is limited to 160 characters and select **Unicode** for text of other languages that is limited to 70 characters.

8.3 Startup Settings

To run programs automatically upon Windows or GV-ASManager startup, on the menu bar, click **Tools > Options**. This dialog box appears.

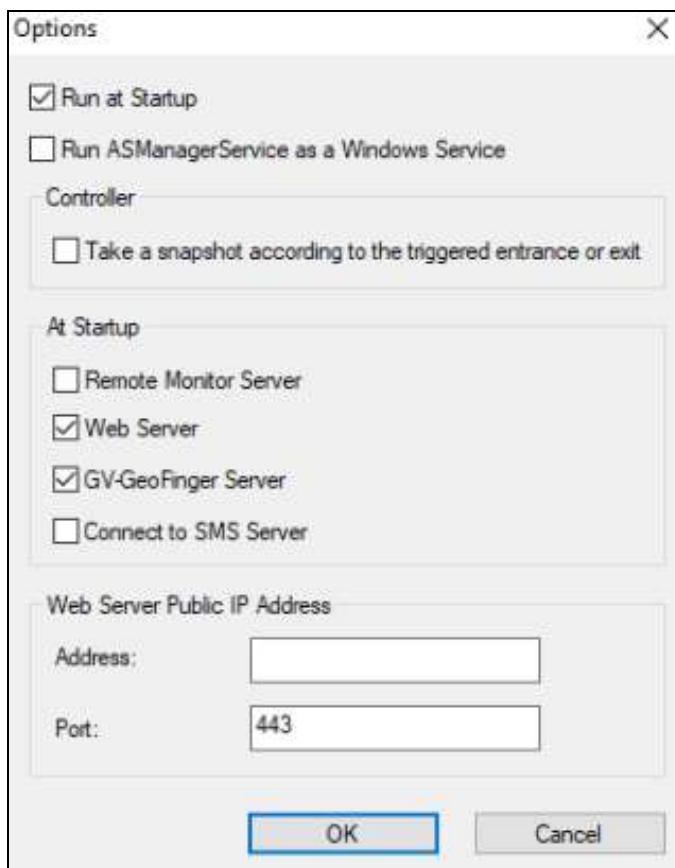


Figure 8-5

- **Run at Startup:** Run GV-ASManager at Windows startup.
- **Run ASManager Service as a Window Service:** Under Service Mode, GV-ASManager can start automatically after system startup and run in the background without logging into a Windows user account.

- **Take a snapshot according to the triggered entrance or exit:** If you associate two cameras to the entrance and exist of a door, respectively, GV-ASManager will take snapshots of both entrance and exit regardless of which direction is triggered. When the option is selected, GV-ASManager will only take a snapshot of the triggered entrance or exit.

[At Startup]

- **Remote Monitor Server:** Enable Remote Monitor Server upon GV-ASManager startup. The Remote Monitor Server needs to be enabled to utilize GV-ASRemote.
- **Web Server:** Enabled by default, start Web Server upon GV-ASManager startup. The Web Server needs to be enabled to access GV-ASManager from GV-ASWeb and GV-Access app.
- **GV-GeoFinger Server:** Enabled by default, start GeoFinger Server upon GV-ASManager startup. The GeoFinger Server needs to be enabled to enroll fingerprints remotely through TCP/IP.
- **Connect to SMS Server:** Enable SMS Server upon GV-ASManager startup. The SMS Server needs to be enabled to receive alert notifications through SMS messages.

8.4 Setting up GV-GF Fingerprint Readers

GV-ASManager can enroll users' fingerprints using **GV-GF1911 / GV-GF1921 / GV-GF1922** and upload the fingerprint data to the **GV-GF Fingerprint Readers** installed on the controllers. To gain access, the user's fingerprints must match the enrolled ones.

There are two ways to enroll fingerprints: locally and remotely.

For **local fingerprint enrollment**, a GV-GF1911 / 1921 / 1922 needs to be connected to GV-ASManager, and the user needs to register his or her fingerprints at the site of GV-ASManager.

For **remote fingerprint enrollment**, first enroll empty fingerprints for a user on GV-ASManager. The user can then go to a connected GV-GF1921 / 1922 at a later time, and register his or her fingerprints using an assigned card. This function is useful when the user is not around GV-ASManager.

Note:

1. GV-GF1911 / 1912 / 1921 / 1922 is only supported in GV-ASManager 4.2.1 or later.
 2. For **remote fingerprint enrollment** through TCP/IP, a separate GV-GF1921 / 1922 is required to enroll fingerprints. GV-GF1921 / 1922 used for fingerprint enrollment cannot be applied as a fingerprint reader at the same time.
 3. The enrolled fingerprints will be saved on the fingerprint reader instead of on GV-ASManager for remote fingerprint enrollment.
-

For details on how to enroll fingerprints and how to upload fingerprint data to GV-GF Fingerprint Reader, see *Chapter 3 Fingerprint Only Mode* in [GV-GF Fingerprint Reader User's Manual](#).

8.5 Setting up GV-FR Face Recognition Readers

GV-ASManager can synchronize users' faces enrolled from **GV-FR2020** for access control. The user data is uploaded from GV-ASManager to the assigned **face recognition reader** for face enrollment. After enrollment, the user's face must match the enrolled face to gain access.

Note:

1. GV-FR2020 is only supported in GV-ASManager 4.4.2 or later.
 2. The enrolled face images will be saved both on the face recognition reader and GV-ASManager.
-

For details on how to integrate with GV-ASManager for face enrollment, see *Chapter 4 Access Control Configurations* and *Chapter 5 User Management* in [GV-FR Face Recognition Reader](#).

8.6 Scanning Driver's Licenses and Business Cards

GV-ASManager can work with **SnapShell ID Scanner** to let you acquire and edit the personal data from driver's licenses and business cards.

Note: This function only supports SnapShell ID Scanner with SDK driver version.

1. Consult the Scanner's documentation to connect the Scanner with GV-ASManager.
2. On the menu bar, click **Personnel > Users**. The User List dialog box appears.
3. Click the **New** button. The User Setup dialog box appears.
4. Click the **Scan** tab. This dialog box appears.

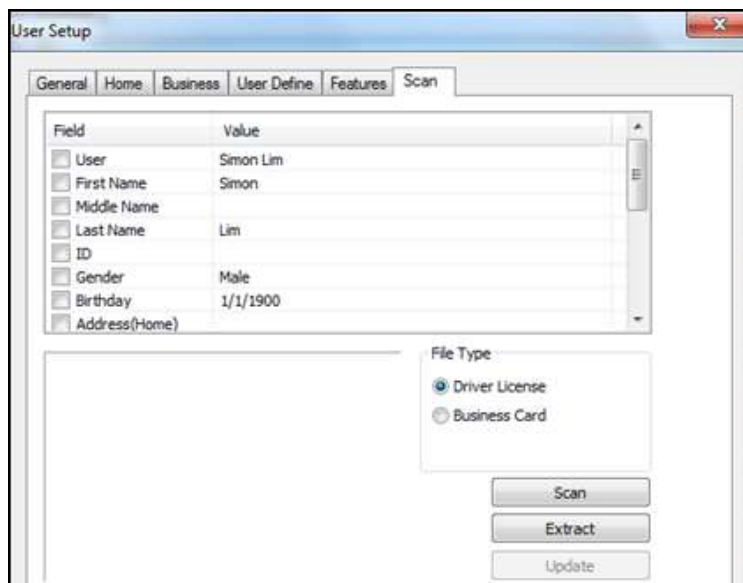


Figure 8-6

5. In the File Type field, select **Driver License** or **Business Card**. Here we use the Driver License as the example to demonstrate the following steps.

- Place a driver's license on the Scanner and click **Scan**. The license image is displayed.



Figure 8-7

- Click the **Extract** button to read the license data. The data is displayed in the **Value** column.
- To modify the data, click the desired **Value** column and type the next texts. Click anywhere in the dialog box when you are finished with the modification.



Figure 8-8

- Click the **Update** button. This driver's license is saved to the GV-ASManager's database.
- Now you can click the **Home** tab to view the information of the driver's license, or click the **Business** tab to view the information of the business card if scanned.

8.7 Defining Hot Keys

You can assign hot keys to quickly control doors, lanes and trigger output devices.

1. On the menu bar, click **Tools > Hotkey Settings**. This dialog box appears.

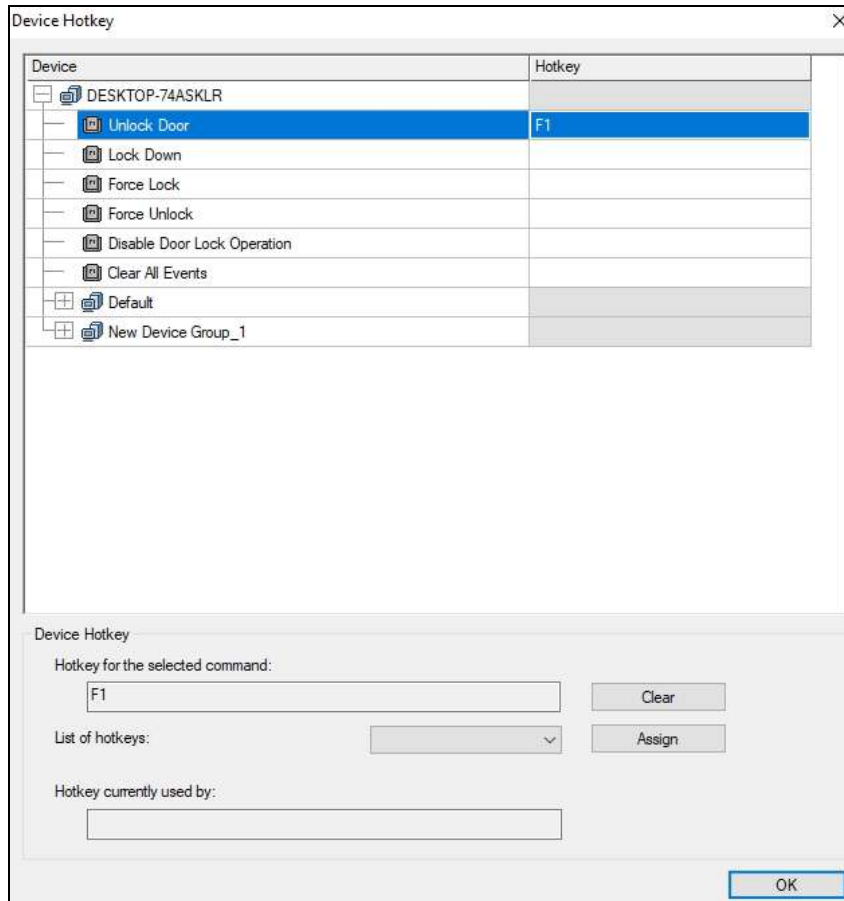


Figure 8-9


2. Under **Device**, select a host, a controller, a door, a lane, or an output and select the command, e.g. Unlock Door, you want to assign a hot key.
3. Select a hot key from the **List of hotkeys** drop-down list and click **Assign**.
4. Click **OK**.

8.8 Using Remote Lock Down App



The Remote Lock Down App allows a security personnel to quickly lock down or force unlock all the doors of multiple GV-ASManager systems connected to the app. Up to 255 GV-ASManager systems can be supported.

Note: Remote Lock Down App is only supported by GV-AS1010 / 1110 / 210 / 2110 / 2120 / 410 / 4110 / 810 / 8110 / 1620 with GV-ASManager V4.2.3 or later.

The Remote Lock Down App can be downloaded from the GeoVision website. Go to the [Download Page](#) of GV-ASManager. Select **Utility** in the drop-down list and click the

Download icon  of **GV-LockDownApp**.

Running Remote Lock Down APP

1. On the menu bar of GV-ASManager, click **Tools > Servers > Remote Monitor Server**. When the server is started, the icon  appears at the bottom-right of the main screen.
2. Run **Remote Lock Down App**. The LockDownApp window appears.
3. To connect to GV-ASManager, click the **Add Host** button . This dialog box appears.

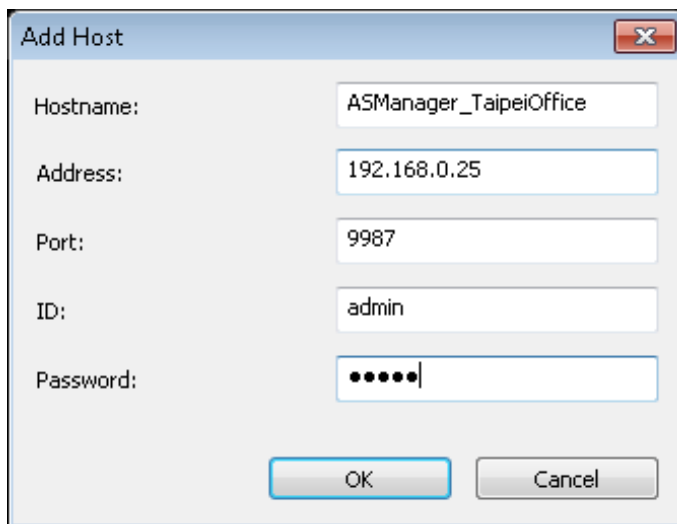


Figure 8-10


4. Type a **Hostname** to identify the GV-ASManager, and type its **IP Address**, **Port**, **ID** and **Password**.
5. Click **OK**. The GV-ASManager and its controllers are now listed.
6. To add more GV-ASManager systems, repeat above steps.
7. To lock down the doors of all connected GV-ASManager, click the **Lock Down** button . The doors that are locked down are now highlighted in red.



Figure 8-11



- To force the doors of all connected GV-ASManager to unlock, click the **Force Unlock** button . The unlocked doors are highlighted in green.



Figure 8-12

- To see doors that have not been locked down due to disconnection, click the **Filter** button  > **Unlock**. To see doors that have not been forced open due to disconnection, select **Lock**.

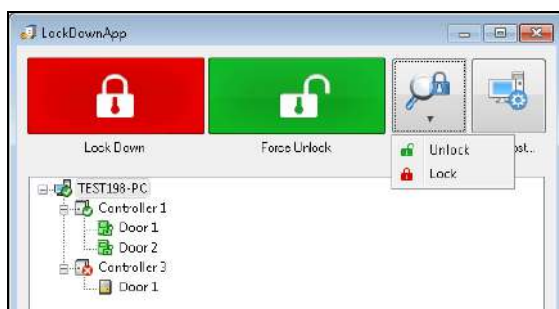


Figure 8-13

If you want to cancel the lock down for a single GV-ASManager, on the GV-ASManager, right-click the server / controller in the following Controller view window, and select **Release Door Operation**.

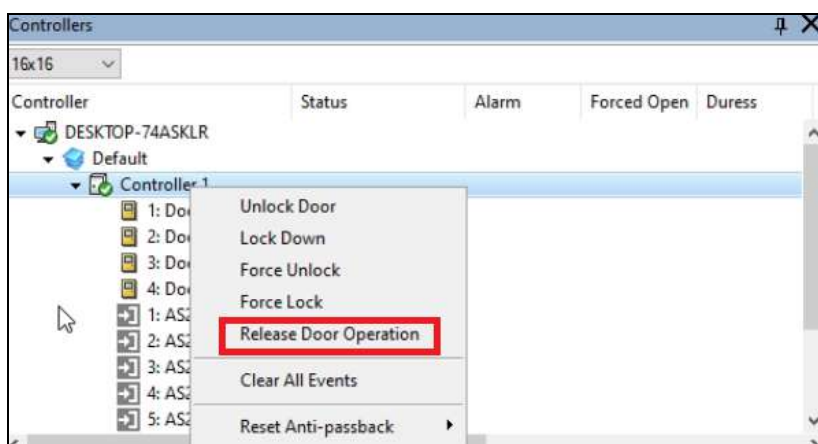
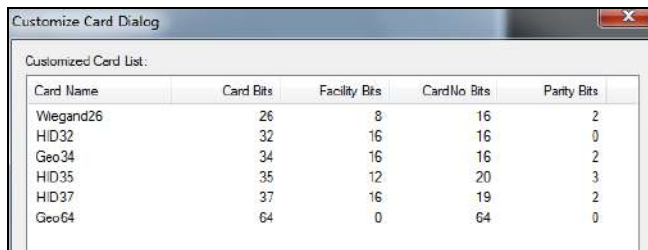


Figure 8-14

8.9 Defining New Card Formats

By default, GV-ASManager only recognizes access cards of certain bit formats that have been pre-defined. To use cards with other data formats, you will need to define the card format for GV-ASManager to recognize it.

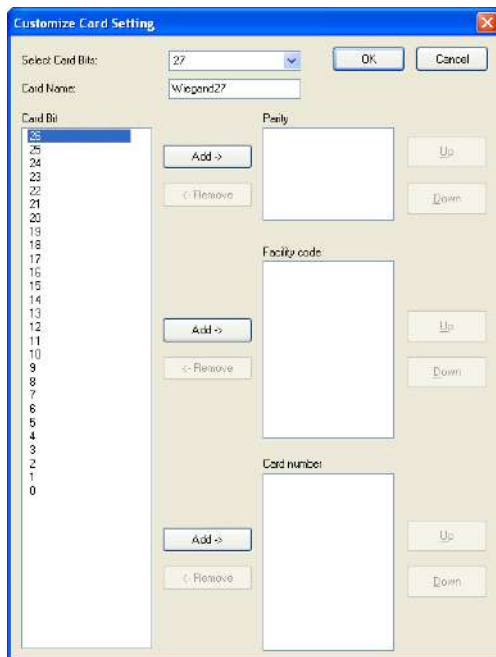
1. On the menu bar, click **Tools > Code Format Settings**. The pre-defined card formats are listed.



Card Name	Card Bits	Facility Bits	CardNo Bits	Parity Bits
Wiegand26	26	8	16	2
HID32	32	16	16	0
Geo34	34	16	16	2
HID35	35	12	20	3
HID37	37	16	19	2
Geo64	64	0	64	0

Figure 8-15

2. To define a new card format, click the **New** button. This dialog box appears.



The 'Customize Card Setting' dialog box contains the following elements:

- Select Card Bits:** A dropdown menu currently set to '27'.
- Card Name:** A text field containing 'Wiegand27'.
- Card Bit:** A list of bit positions from 0 to 25. Bit 27 is highlighted.
- Parity:** A text field with 'Add ->' and '<- Remove' buttons, and 'Up' and 'Down' navigation buttons.
- Facility code:** A text field with 'Add ->' and '<- Remove' buttons, and 'Up' and 'Down' navigation buttons.
- Card number:** A text field with 'Add ->' and '<- Remove' buttons, and 'Up' and 'Down' navigation buttons.
- Buttons:** 'OK' and 'Cancel' buttons at the top right.

Figure 8-16

3. Next to **Select Card Bits**, select the card bit.
4. For each number under **Card Bit**, define whether it is **Parity**, **Facility Code** or **Card Number** by clicking the **Add** button. The exact steps to defining card format vary from card format to card format.
5. When you are done, click **OK**.

8.10 Monitoring Emergency Exits with Input Sensors

If there are emergency exits on premises that must always remain closed, you can connect the exits to the input sensors on GV-AS Controller and monitor them using the functions below.

- Monitor the status of input devices on the Controller view window
- Assign up to two cameras to an input device to capture snapshots upon input trigger

Note that these functions are only supported by the following GV-AS Controllers.

Models	Supported Firmware	Number of Inputs Supported
GV-AS210 / 2110 / 2120	V1.3 or later	8
GV-AS410 / 4110 / 810 / 8110	V1.3 or later	16
GV-AS2120	V1.35 or later	16

To set up:

1. On the Web interface of controller, make sure the input is set to **Normal Input**. You can modify the input name if needed.

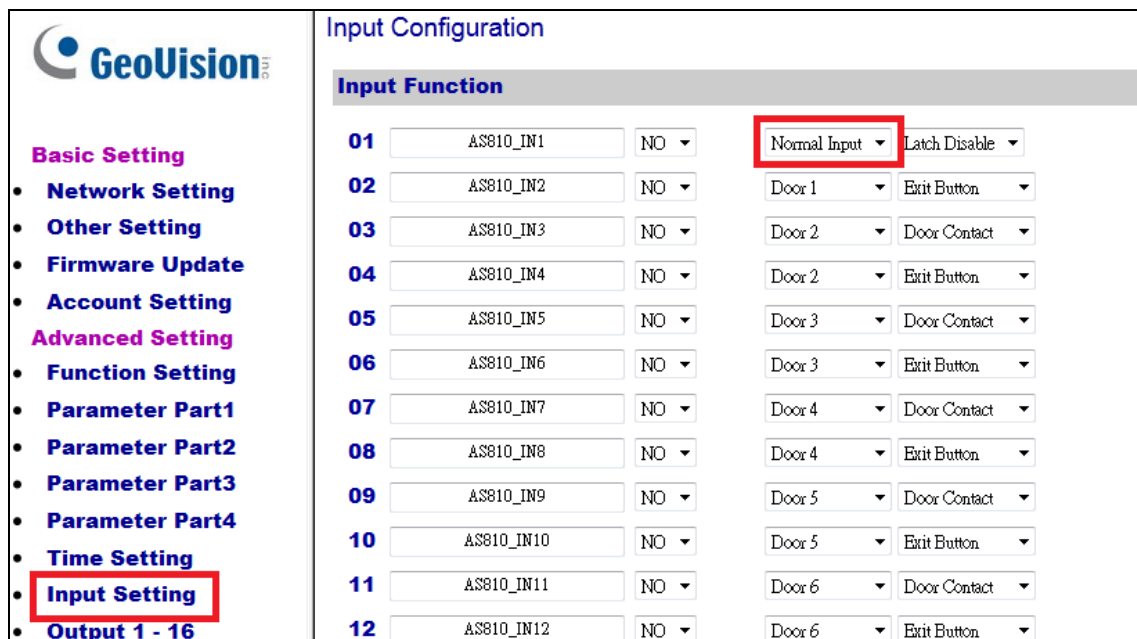


Figure 8-17

2. In GV-ASManager, right-click the controller in the Controller view window and click **Settings**.

3. Click **Input**.

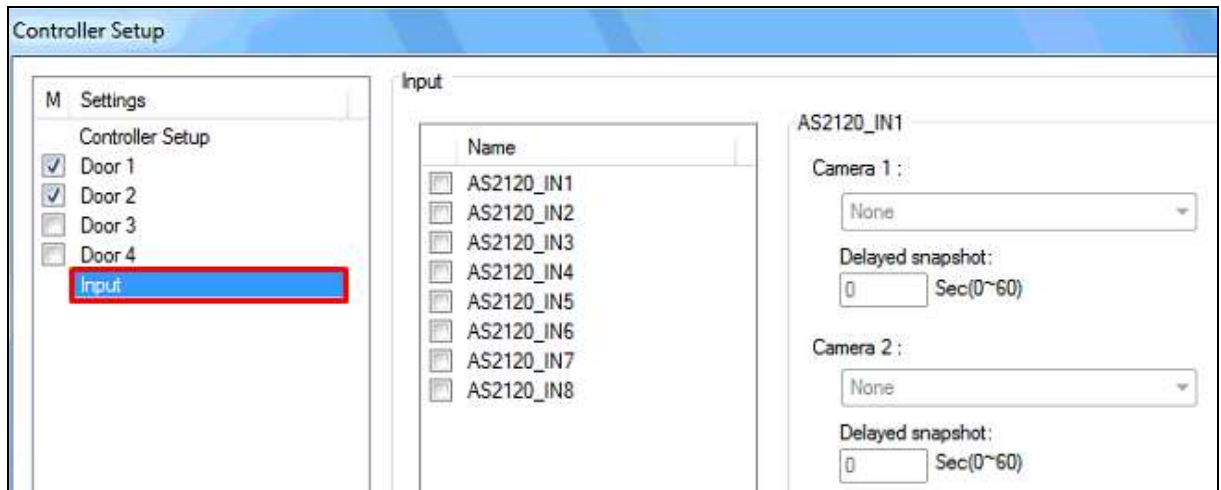


Figure 8-18

4. On the left pane, select input devices to monitor their status in the Controller view window (Figure 8-19).
5. On the right pane, use the drop-down list to assign up to two cameras to the input. You can enable **Delayed snapshot** by typing the number of seconds to delay capturing a snapshot after the input is triggered. For example, if the camera is installed 10 meters away from the emergency exit and it takes 5 seconds for a user to walk pass the camera after triggering the input, you can delay the snapshot for 5 seconds.
6. Click **OK**.

The inputs will now be listed in the Controller view window (left in Figure 8-19), and the input status will change to “Active” when the emergency exit is opened, triggering the input. The event will also be shown in the Event Monitor.

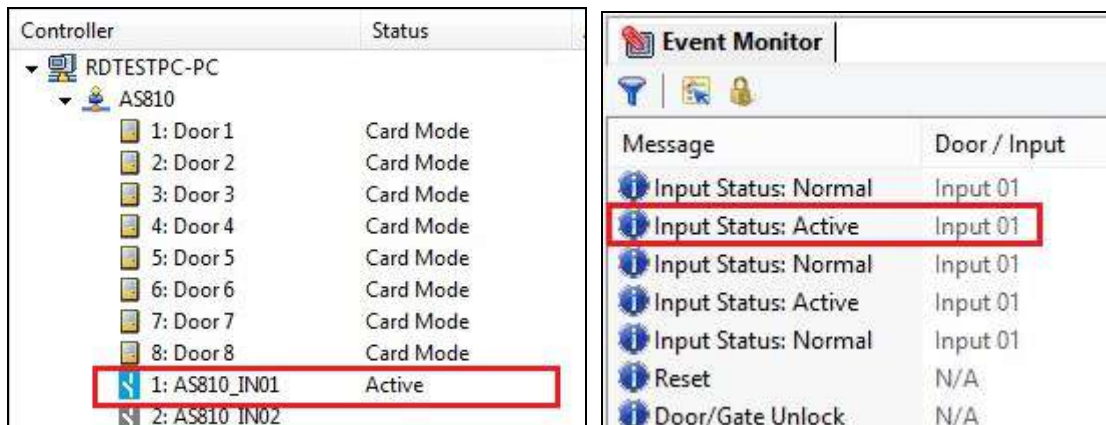


Figure 8-19

8.11 Designing and Printing Access Card Template

You can design a card template for your access cards by adding text and images. The text and images in the template can be linked to the users' personal information (ex: user's last name) and photo in the user database.

1. On the menu bar, click **Personnel > Users**. The User List window appears.
2. Click the **Design Card Template** button on the toolbar. This dialog box appears.

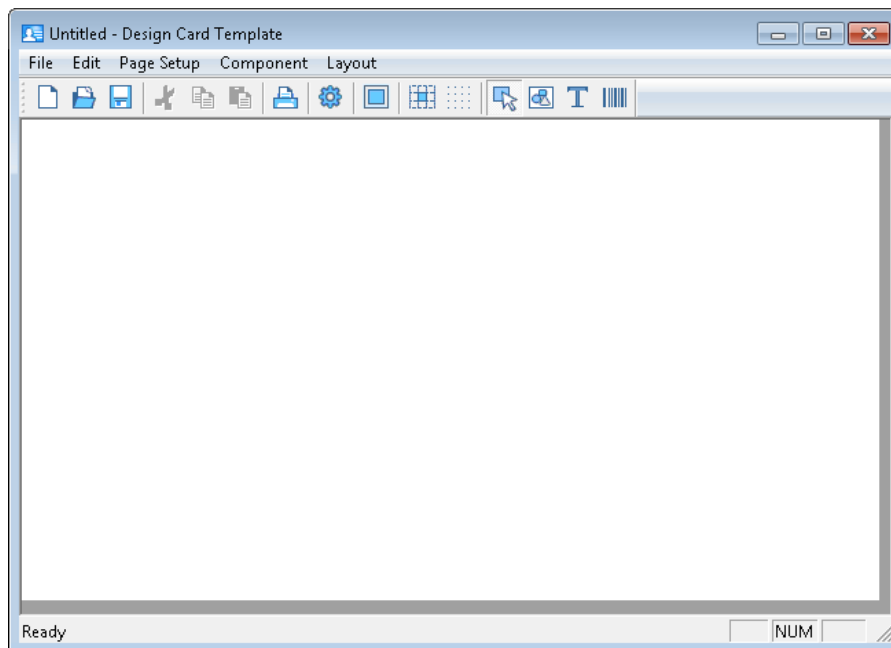


Figure 8-20

3. Click the **New** button  to create a new template.

Tip: If you do not want to design a template from scratch, click **File > Template Sample** to use the template sample.

4. To set the orientation and margins of the card template, click **Panel > Settings**.

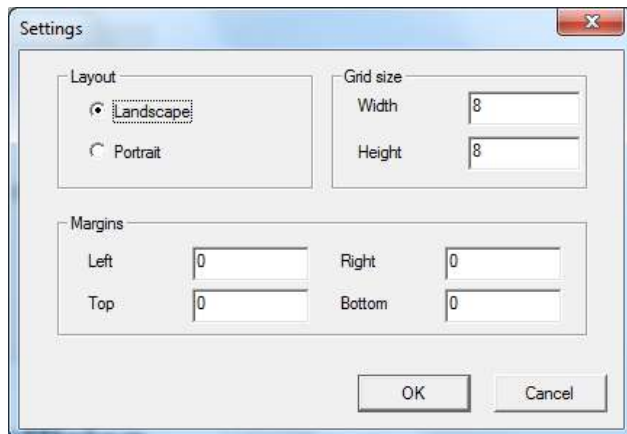



Figure 8-21

5. To add an image such as a background picture, user photo, or company logo, follow the steps below.
 - a. Click the **Image** button  and drag to define the size and location of the image.
 - b. Right-click the image > **Properties**. This dialog box appears.

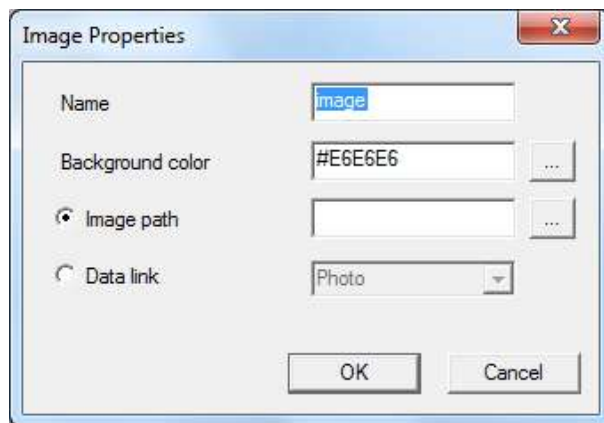


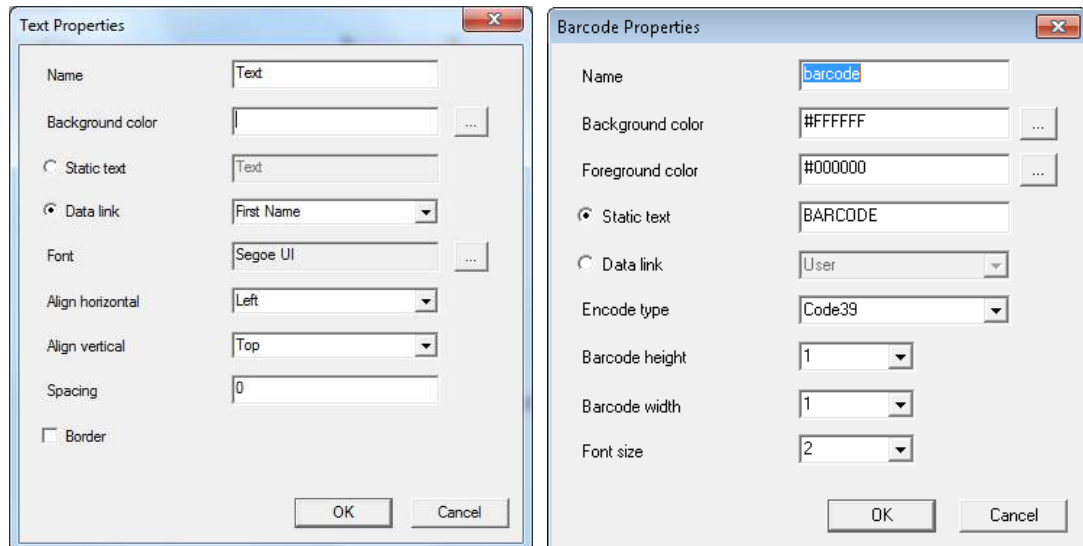


Figure 8-22

- c. Adjust the background color if needed.
- d. To insert a fixed image, select **Image Path** and locate an image. To insert the photo of each user, select **Data link**.
- e. Click **OK**.



6. To add a textbox or a barcode, follow the steps below.
- Click the **Text** button  or the **Barcode** button , and drag to define the size and location of the box.
 - Right-click the textbox or barcode, and select **Properties**. This dialog box appears.



Text Properties

Barcode Properties

Figure 8-23

- Adjust the background color, font, alignment, spacing and border if needed.
 - To add fixed text, select **Static text** and type the text. To insert the user information of each user, select **Data link** and select a field from the user profile (ex: Last name).
 - For barcode, you may need to adjust the **Encode type** according to the type of barcode you are using.
 - Click **OK**.
7. The following tools are available to help you align the images and text boxes:
- Select the multiple items, click **Layout** and select one of these options: **Align left**, **Align right**, **Align top**, **Align bottom**, **Make same size**.
 - Click the **Show Grid** button  and **Snap to Grid** button . You can adjust the size of the grid by clicking **Panel** and then select **Settings**.

- Click **File** and **Save** to save the template.

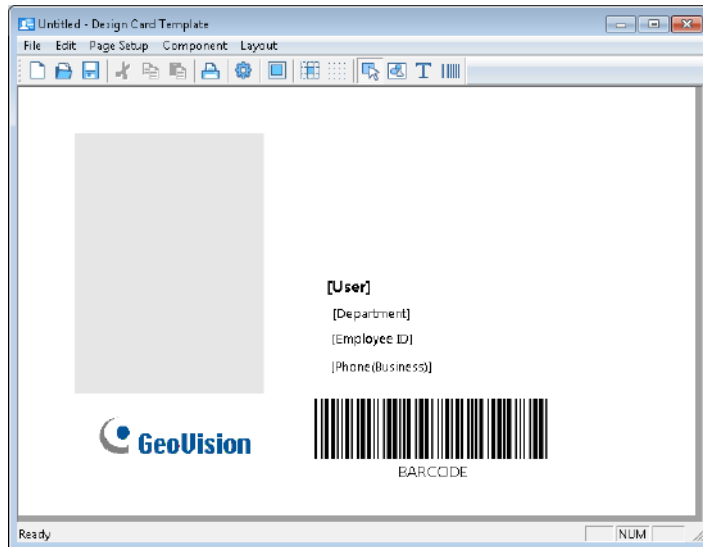


Figure 8-24

- To preview the template with actual user information and photo, select one or more users in the user list, right-click, select **Print** and select **Print Preview and Setup**.
- To print the cards, select one or more users in the user list, right-click, select **Print** and select **Print Cards**.

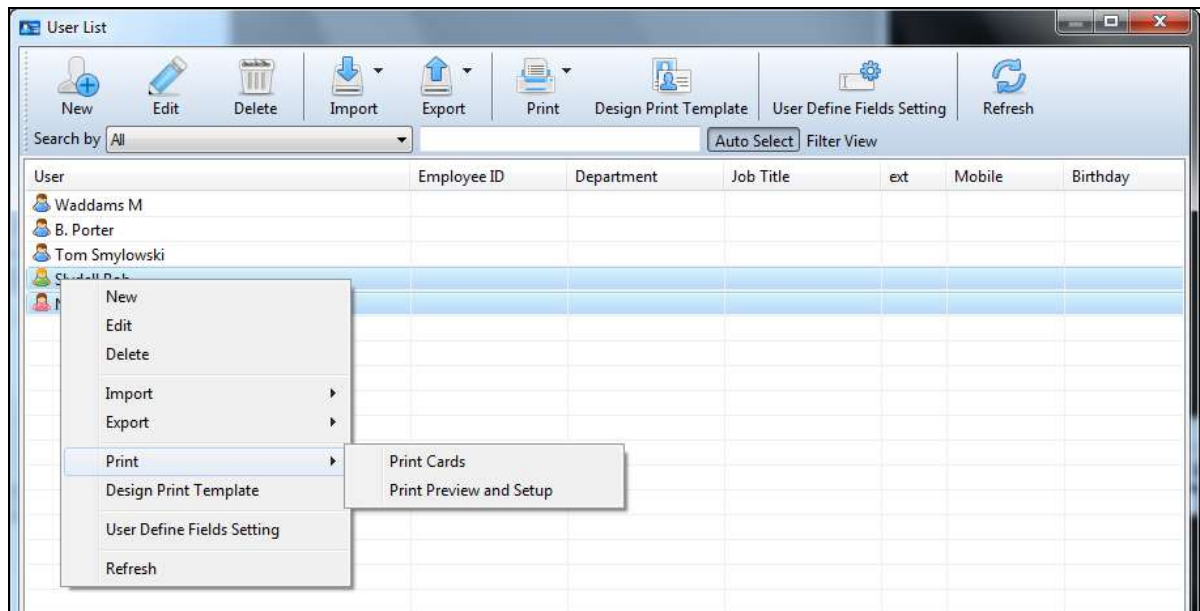
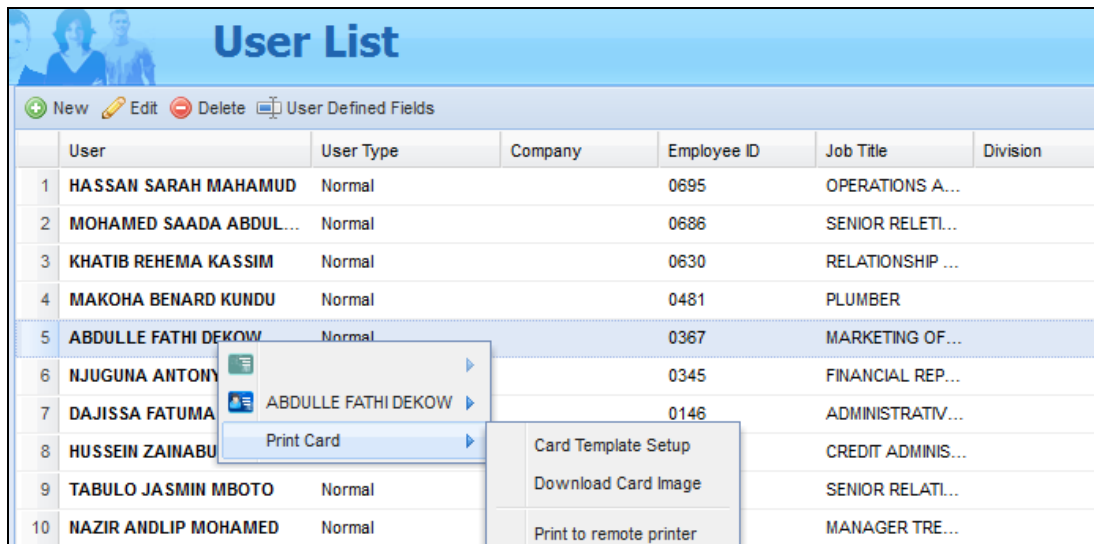


Figure 8-25

*

Note: You can remotely print access cards through GV-ASWeb. Refer to Chapter 10 *GV-ASWeb* to see how GV-ASWeb works.

1. Right-click a user account, select **Print Card > Print to remote printer**.



	User	User Type	Company	Employee ID	Job Title	Division
1	HASSAN SARAH MAHAMUD	Normal		0695	OPERATIONS A...	
2	MOHAMED SAADA ABDUL...	Normal		0686	SENIOR RELETI...	
3	KHATIB REHEMA KASSIM	Normal		0630	RELATIONSHIP ...	
4	MAKOHA BENARD KUNDU	Normal		0481	PLUMBER	
5	ABDULLE FATHI DEKOW	Normal		0367	MARKETING OF...	
6	NJUGUNA ANTONY			0345	FINANCIAL REP...	
7	DAJISSA FATUMA			0146	ADMINISTRATIV...	
8	HUSSEIN ZAINABU				CREDIT ADMINIS...	
9	TABULO JASMIN MBOTO	Normal			SENIOR RELATI...	
10	NAZIR ANDLIP MOHAMED	Normal			MANAGER TRE...	


Figure 8-26

2. If you would like to change the printing preferences for printing access cards on GV-ASWeb, you must modify the printer default settings from your local computer.

8.12 Utilizing Job Codes

Using the function keys on **GV-AS1010**, an employee with multiple types of jobs can specify the start and the end of each type of job by entering different job codes on GV-AS1010.

Follow the steps below to set up.

1. On the menu bar, click **Setup > Devices**. The Devices dialog box appears.
2. Select a Controller and click the **Job Code** button .

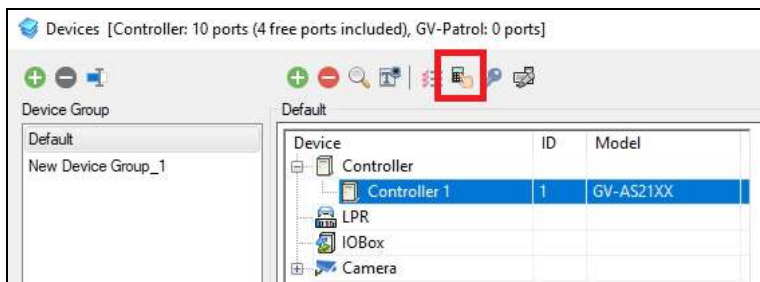


Figure 8-27

3. Select a checkbox, and type the **Job Code** and **Description**.

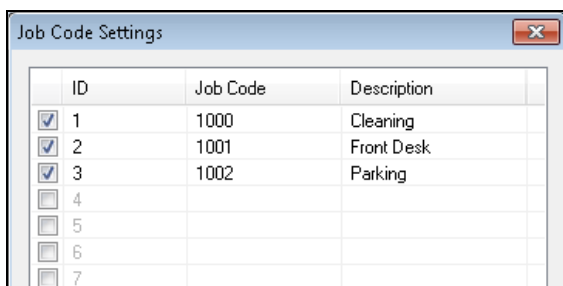


Figure 8-28

4. Click **OK**.
5. On the Web interface of GV-AS1010, set two function keys to **Job Code (Start)** and **Job Code (End)**.

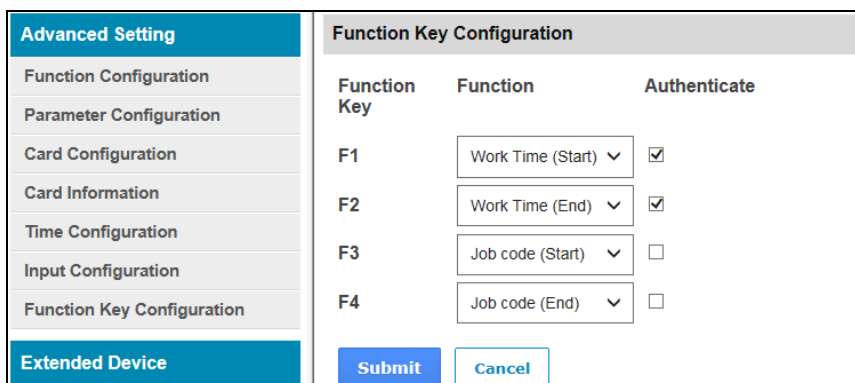


Figure 8-29

Example:

Employee A has a 9:00 to 17:00 workday, but the workday consists of two job codes: Cleaning from 9 am to noon and being a front desk receptionist from 1 pm to 5 pm.

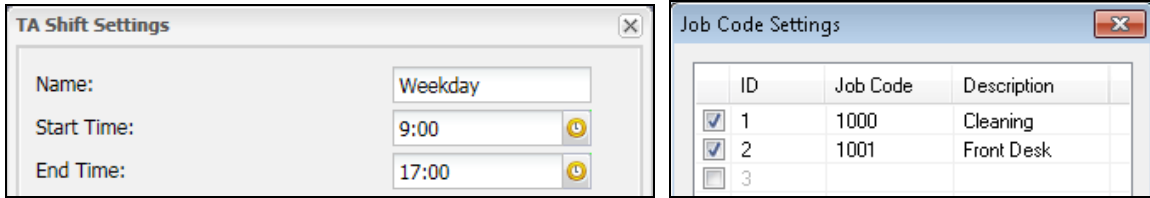


Figure 8-30

To differentiate the two jobs in the records, employee A enters different job codes on the GV-AS1010 reader at the start and end of each job.

Time	Operation on GV-AS1010	Explanation
9:00	F1 key > Swipe Card	Work Time (Start)
9:00	F3 key > 1000 > Swipe Card	Job Code (Start) for Cleaning
12:00	F4 key > 1000 > Swipe Card	Job Code (End) for Cleaning
13:00	F3 key > 1001 > Swipe Card	Job Code (Start) for Front Desk
17:00	F4 key > 1001 > Swipe Card	Job Code (End) for Front Desk
17:00	F2 key > Swipe Card	Work Time (End)

You can look up the records in TA Report of GV-TAWeb using **Job Code** and **Job Code Summary**. See *Chapter 11 GV-TAWeb* for details.

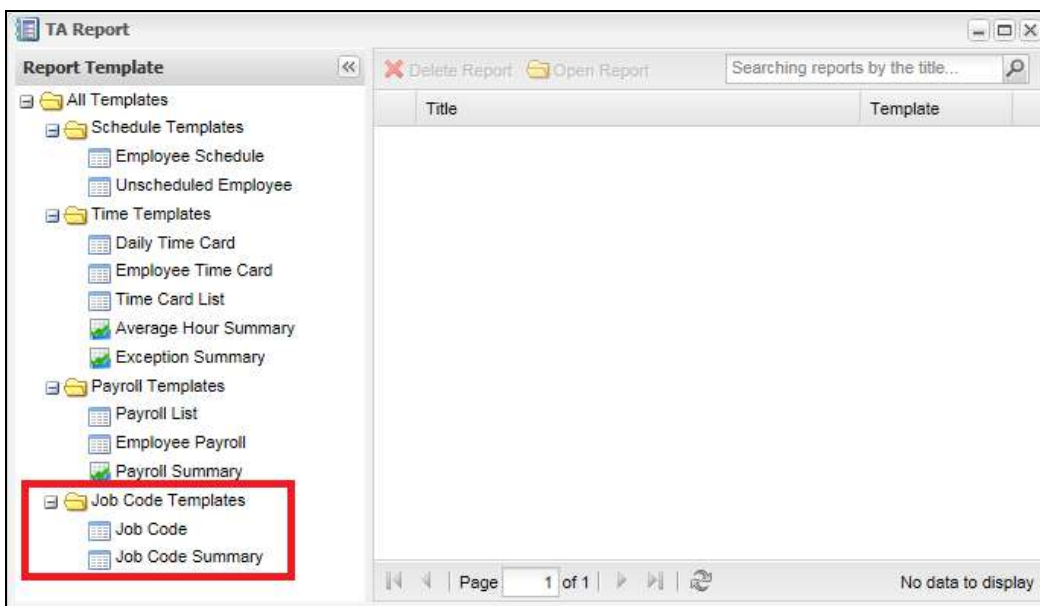


Figure 8-31

Job Code shows the punch-in and punch-out time of the different job codes.



	Date	Job Code	Name	Division	Department	Job Title	Employee ID	Punch In Time	Punch Out Time
1	2016/07/27 (W)	[1000] Job Code - Clean	a				0000010	09:00:26	12:05:52
2	2016/07/27 (W)	[1001] Job Code - Front Desk	a				0000010	13:00:02	17:05:18

Figure 8-32

Job Code Summary shows the total work hours of different job codes.



	Job Code	Name	Division	Department	Job Title	Employee ID	Work Time
1	[1000] Job Code - Clean	a				0000010	03:05:26
2	[1001] Job Code - Front Desk	a				0000010	04:05:16

Figure 8-33

8.13 Defining Occupancy Limit

You can define the occupancy limit of an area to trigger a highlight on the screen of GV-ASManager for alert when the specified number of users within the area has been reached.

Note: The function is only supported by GV-AS210 / 2110 / 2120 / 410 / 4110 / 810 / 8110 firmware V2.41, GV-AS1620 firmware V1.05, GV-CS1320 firmware V3.10 and later versions of these products.

To define the Area of a door:

1. On the menu bar, click **Setup > Areas**. The Area Settings dialog box appears.
2. Select a **Door** and define its belonging area by specifying **Enter to** and **Exit From**. **Enter to** is the area where a user enters by accessing the Entrance reader of the door, and **Exit from** is the area where the user is from.

To set up Occupancy Limit:

3. Set up the following functions. When the set thresholds are reached, the area will be highlighted on the screen of GV-ASManager for alert.
 - **Occupancy Limit (Cards):** Specify the maximum number of users allowed to stay in an area for alert.
 - **Area Card Warning:** Specify the number of users already entered for pre-alert.

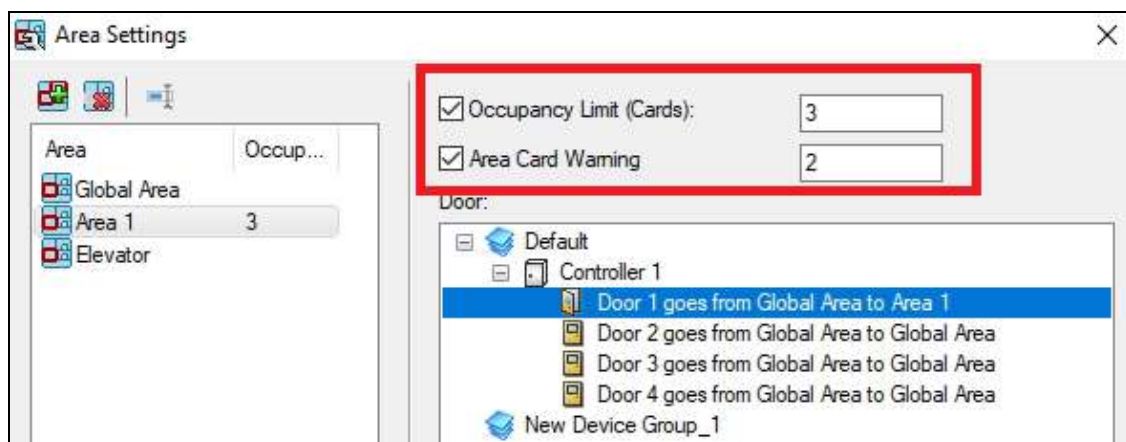


Figure 8-34

To set up Door Contact:

For GV-ASManager to tell the location of a user, it is required to set up a door contact sensor for the door to detect if it is open. To define the door contact sensor, go to the Web interface of controller > **Input Configuration**.

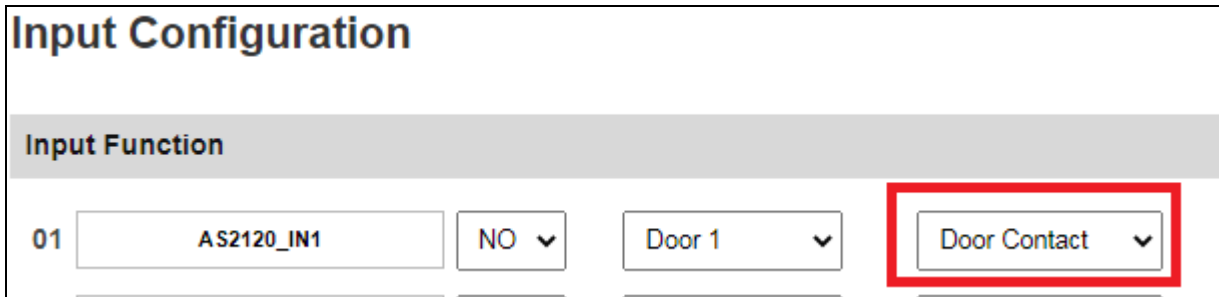


Figure 8-35

To monitor an Area:

When the number of users entered has reached the pre-alert threshold (**Area Card Warning**), the area will be highlighted in *orange* as below. In this case, the number for pre-alert is set to 2. When 2 users have entered the Area 1, the orange highlight will be displayed.

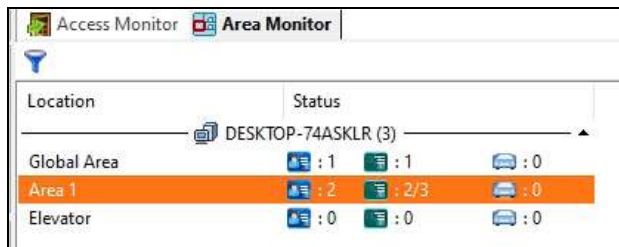


Figure 8-36

When the number of users entered has reached the **Occupancy Limit**, the area will be highlighted in *red* as below. In this case, the limit is to only allow 3 users to enter the Area 1.

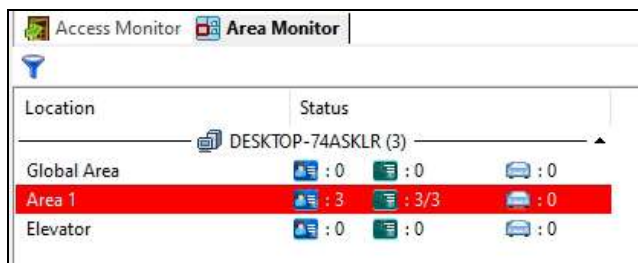


Figure 8-37

When users exit an area by accessing its Exit reader, the number of users in the area will decrease accordingly and where users go will be indicated. In this case, 3 users exit from Area 1 and enter to Global Area.

Location	Status
DESKTOP-74ASKLR (3)	
Global Area	: 3 : 3 : 0
Area 1	: 0 : 0/3 : 0
Elevator	: 0 : 0 : 0

Figure 8-38

Note: In the following example, 0/3 indicates that the area has an occupancy limit of 3 users and no one is in the area now.

Area 1	: 0 : 0/3 : 0
--------	---


Figure 8-39

Chapter 9 GV-ASRemote

The client software GV-ASRemote is designed to monitor multiple GV-ASManager systems over a network. GV-ASRemote provides the following features:

- Remote monitoring
- Remote live view and playback
- Remote control: stop alarms and force the door to lock/unlock
- Remote access to Access Log and LPR Log

9.1 Installing GV-ASRemote

Visit the [Download Page](#) of GV-ASManager. Select **Primary Applications**, click the **Download icon**  of **GV-ASManager**, follow on-screen instructions to complete the installation.

9.2 The GV-ASRemote Window

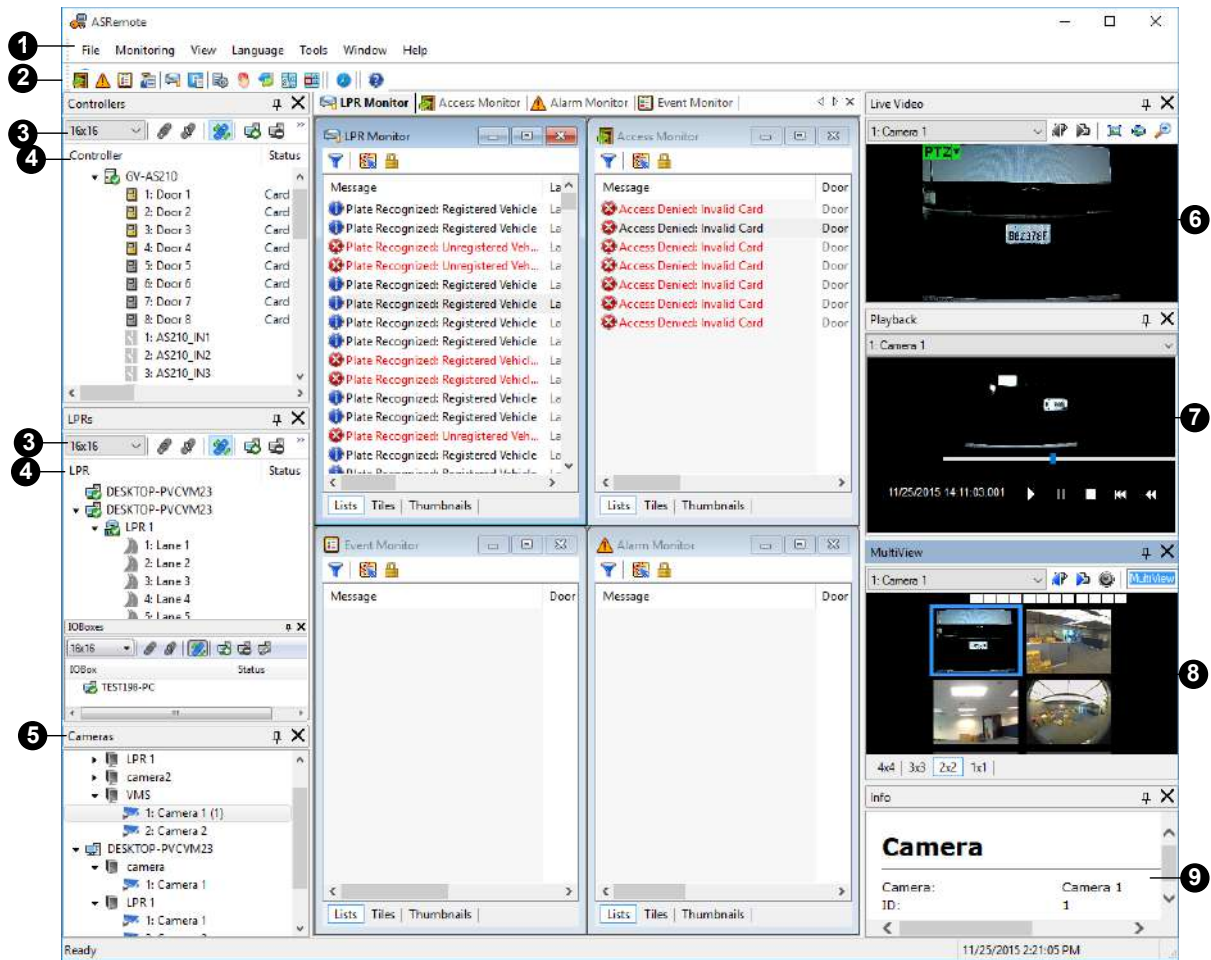


Figure 9-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of File (log in / out GV-ASManager), Monitoring (display monitoring windows), View (display the function windows) and Window (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of various monitoring windows and Web Browser (open GV-ASRemoteWeb).
3	Windows Toolbar	The Windows Toolbar includes the options of Connect , Disconnect , Auto Connect , Add Host , Remove Host , Settings and Resolution . You can change the size of icons to 16 x 16, 24 x 24 or 32 x 32 from the drop-down list. For details, see <i>9.2.2 Windows Toolbar</i> .

4	Controller / LPR / I/O boxes View	Displays a list of connected controllers / LPR devices / I/O boxes and their current status.
5	Camera List	Displays a list of connected cameras.
6	Live View	Displays live views of one connected camera. For details, see the same operations in <i>5.2 Accessing Live View</i> .
7	Playback	Plays back recorded events from a compatible GeoVision IP device. For details, see the same operations in <i>5.5 Retrieving Recorded Video</i> .
8	MultiView	Displays live views of connected cameras from multiple IP devices. For details, see <i>5.4 The MultiView Window</i> .
9	Information Window	Displays the information of doors, card readers and monitored events.

9.2.1 Windows Toolbar




Figure 9-2

No.	Name	Function
1	Connect	Starts the connection with GV-ASManager.
2	Disconnect	Ends the connection with GV-ASManager.
3	Auto Connect	Retries to build the connection with GV-ASManager.
4	Add Host	Adds a GV-ASManager host to the list.
5	Remove Host	Deletes a GV-ASManager host on the list.
6	Settings	Edits the settings of GV-ASManager hosts.
7	Resolution	Changes the size of icons to 16 x 16, 24 x 24 or 32 x 32.

9.3 Connecting to GV-ASManager

Before GV-ASRemote can connect to a GV-ASManager system, the GV-ASManager must allow remote access:

- Click **Tools** on the menu bar > **Servers** > **Remote Monitor Server**. When the server is started, the icon  appears at the bottom-right of the main screen.

To create a GV-ASManager host and enable connection:

1. On the toolbar, click the **Add Host** button. This dialog box appears.

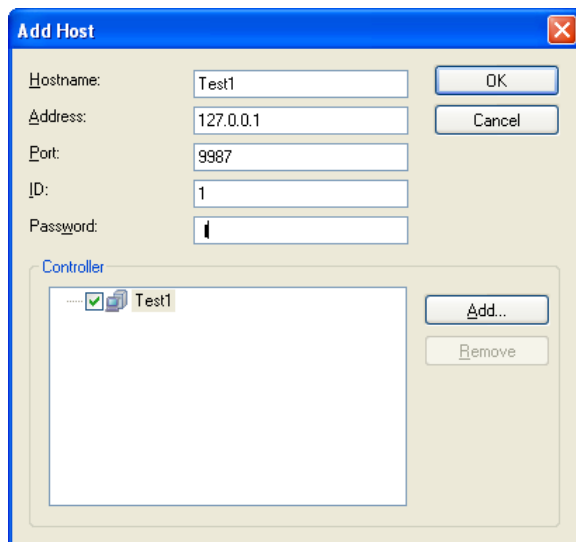


Figure 9-3

2. Name the host, type the IP address of GV-ASManager', modify the port number if necessary, and type its login credentials.
3. Click **Add**. This dialog box appears.




Figure 9-4


4. Type the ID of the controller associated with the GV-ASManager and click **OK**.
5. To add more controllers, repeat Steps 3-4.

6. Click **OK** and return to the main screen. A host folder will be displayed on the Controller View window as example below.



Figure 9-5

If the icon  appears, it indicates the connection between GV-ASManager and GV-ASRemote has been established.

If the icon  appears, it indicates the connection failed. Make sure GV-ASManager is enabled for the Remote Monitor Server function.

Note: For the disconnection messages displayed on the Status column, see *Appendix D. Controller Status*.

9.4 GV-ASRemoteWeb

GV-ASRemoteWeb enables remote access to Access Log and LPR Log of multiple GV-ASManager systems over a network.

1. To open GV-ASRemote, click the **Web Browser** button  on the toolbar. This dialogue box appears.

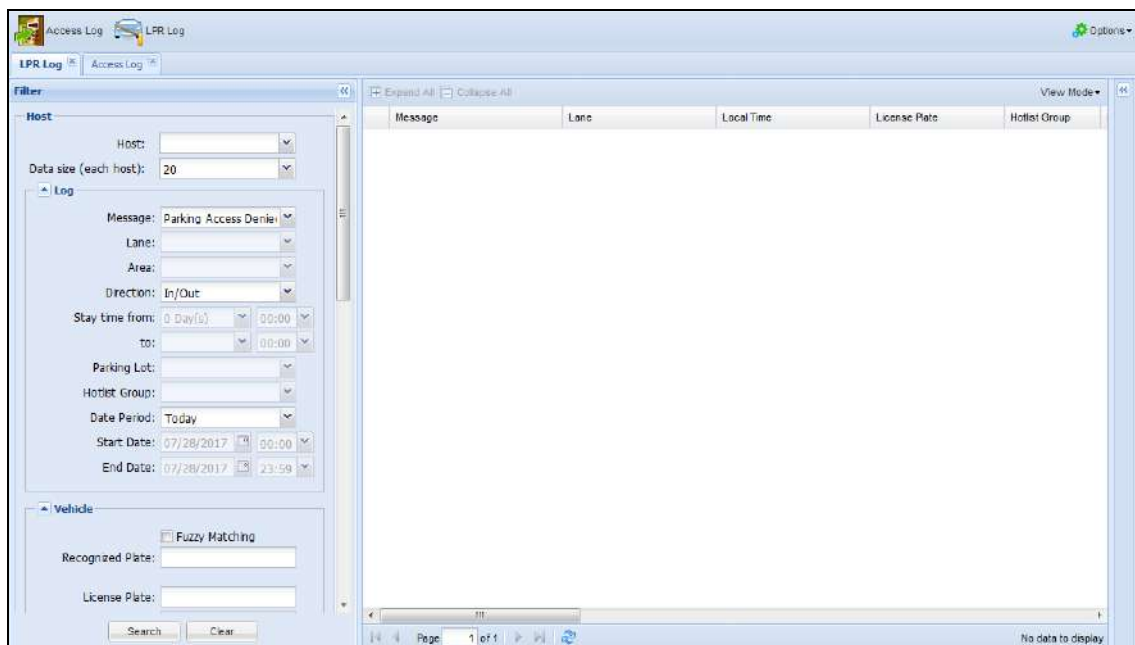


Figure 9-6

2. Select a log you want to view on the top-right corner.
3. Select a connected host from **Host** and the number of logs from **Data size** to display in the search results.
4. Set the search criteria. For example, you can use the **Message** drop-down list to search the records that match the conditions of “Parking Access Denied”.
5. Click the **Search** button to start the log search.

Chapter 10 GV-ASWeb

GV-ASWeb allows you to access data and settings of GV-ASManager over a network using a Web browser. You can remotely watch live video, access logs, and configure system settings using Web interfaces.

10.1 Connecting to GV-ASManager

Before GV-ASWeb can connect to one GV-ASManager, the GV-ASManager must be set to allow remote access:

- On the menu bar, click **Tools > Servers > Web Server**. This dialog box appears.

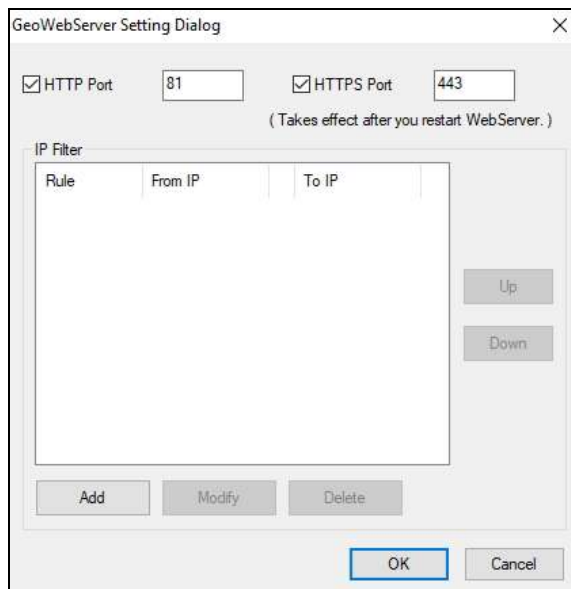



Figure 10-1

To grant or deny access of certain IP addresses, click **Add**, and type the IP addresses. Otherwise click **OK** to start the connection. When the server is started, the icon  appears at the bottom-right of the main screen.

To start GV-ASWeb:

1. There are two ways to link to GV-ASWeb:
 - Under the device list, right-click the host PC >**ASWeb** or **ASWeb with SSL**.

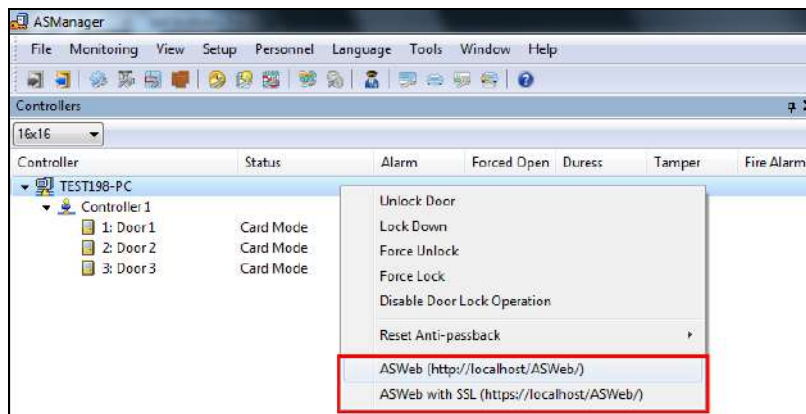


Figure 10-2

- Open an Internet browser, and type the IP address of GV-ASManager to be connected. This web page appears.



Figure 10-3

2. Optionally click **https://** for SSL encrypted connection.
3. Enter the login credentials. The GV-ASWeb page appears.

Note: To change the UI theme, click the  icon on the top right of the login page (Figure 10-3) and select **Dark** or **Light**.

10.2 Functions on GV-ASWeb

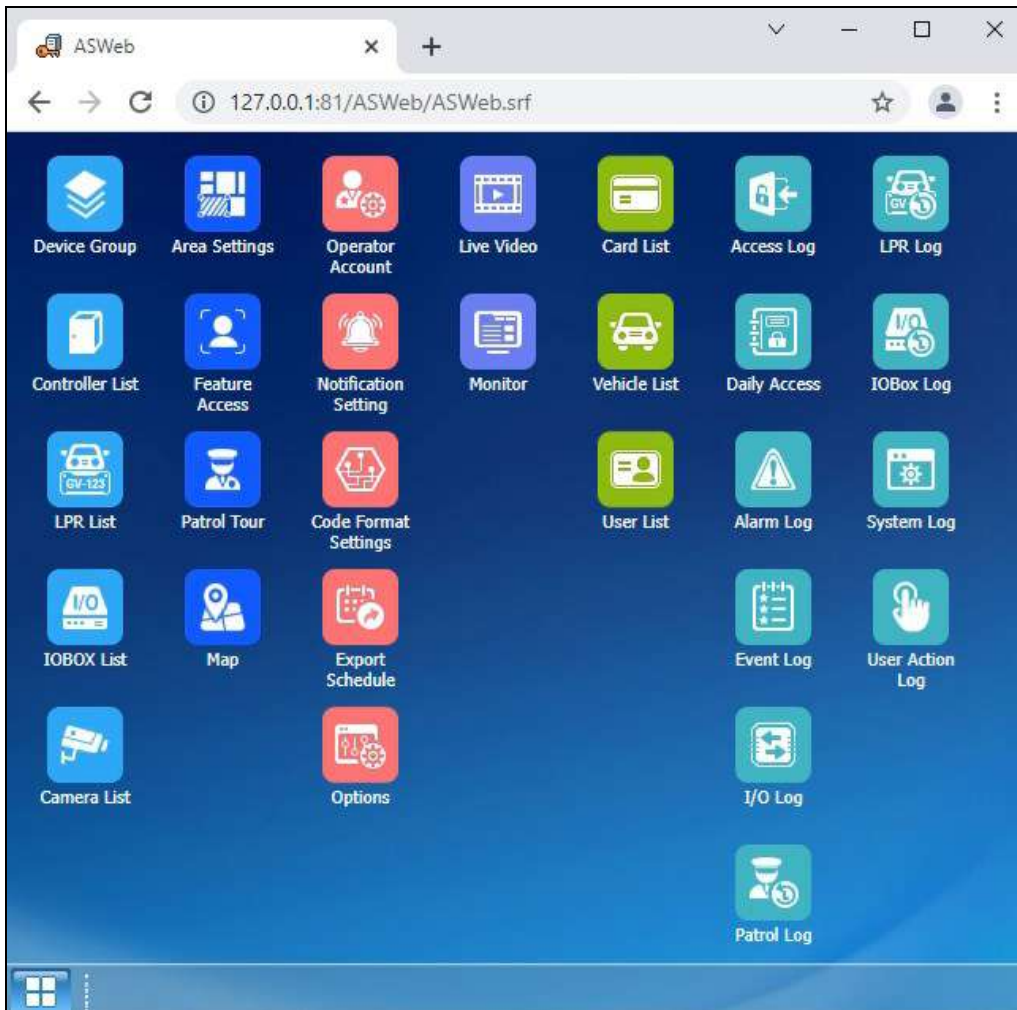



Figure 10-4

You can access the following functions by clicking icons on the Web interface or selecting them from the menu  on the bottom-left corner.

Name	Details
Monitor	Remotely monitor GV-ASManager. See <i>10.3 Monitoring GV-ASManager</i> .
Live Video	Remotely watch live view of a camera connected to GV-ASManager. Note that live view will be displayed with MJPEG codec and a frame rate of 5 fps.
Device Group Controller List LPR List IO Box List Camera List Area Settings	Remotely set up the mentioned functions, also available on the host PC. Also see: <ul style="list-style-type: none"> • <i>Adding Controllers</i> • <i>13.2 Adding PC LPR</i> • <i>4.7 Adding I/O Boxes</i> • <i>5.1 Mapping Cameras</i>

<p>Feature Access Patrol Tour Map</p>	<ul style="list-style-type: none"> • <i>6.3.2 Configuring Areas</i> • <i>14.3 Managing Face Recognition Access Data</i> • <i>7.1 Creating Patrol Tour</i> • <i>10.5 Creating Maps</i> <p>Tip: You can right-click a door and select Accessible Card or Accessible User to see the cards and users that are granted access to the door.</p>
<p>Card List User List Vehicle List</p>	<p>Remotely set up the mentioned functions, also available on the host PC.</p> <p>Also see:</p> <ul style="list-style-type: none"> • <i>4.3 Adding Cards</i> • <i>4.6 Adding Users</i> <p>Note: Batch and Import/Export functions are not supported in the Card List of GV-ASWeb.</p>
<p>Access Log, Daily Access, Alarm Log, Event Log IO Box Log, IO Log LPR Log, Patrol Log System Log, User Action Log</p>	<p>Remotely access the mentioned logs, also available on the host PC.</p> <p>Also see:</p> <ul style="list-style-type: none"> • <i>10.4 Accessing Logs.</i>
<p>Operator Account Short Message Service Configuration Mail Configuration Notification Settings Code Format Settings Export Schedule Options</p>	<p>Remotely access the mentioned functions, also available on the host PC.</p> <p>Also see:</p> <ul style="list-style-type: none"> • <i>8.1 Adding System Users</i> • <i>8.2.1 Setting up SMS Server</i> • <i>8.2.2 Setting up E-Mail Server</i> • <i>8.2.3 Setting up Notifications</i> • <i>8.9 Defining New Card Formats</i> • <i>10.6 Setting up Export Schedule for Lists and Logs.</i> • <i>8.3 Startup Settings</i>
<p>Note: Any changes made on GV-ASWeb will be reflected in GV-ASManager.</p>	

10.3 Monitoring GV-ASManager

You can use GV-ASWeb to remotely monitor controller status, control doors / lanes, areas, and watch the following logs updating in real time: Access Log, Alarm Log, Event Log, LPR Log and Patrol Log.

1. On GV-ASWeb, select **Monitor**. The Monitor window appears.
2. To control doors / lanes, right-click the controller or LPR in the device list. The options available are similar to those on GV-ASManager. For details, see 3.2.1 Controls on the Window.

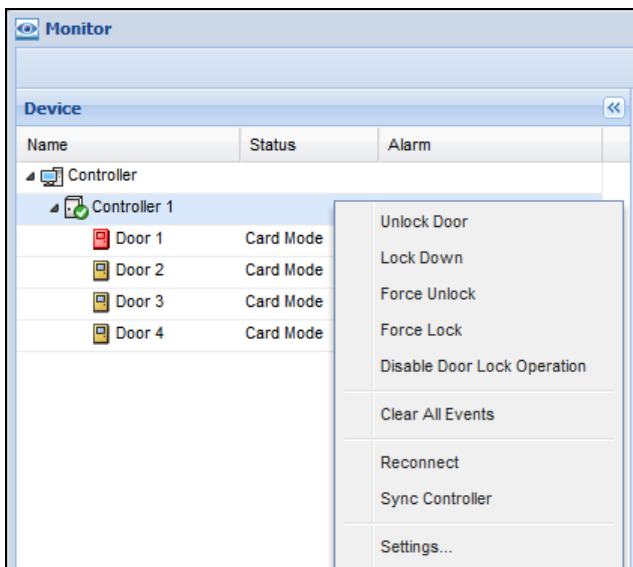


Figure 10-5

3. Click **Monitor** in the upper-right corner to select logs and functions to display. Activities will appear in real time without refreshing the page.

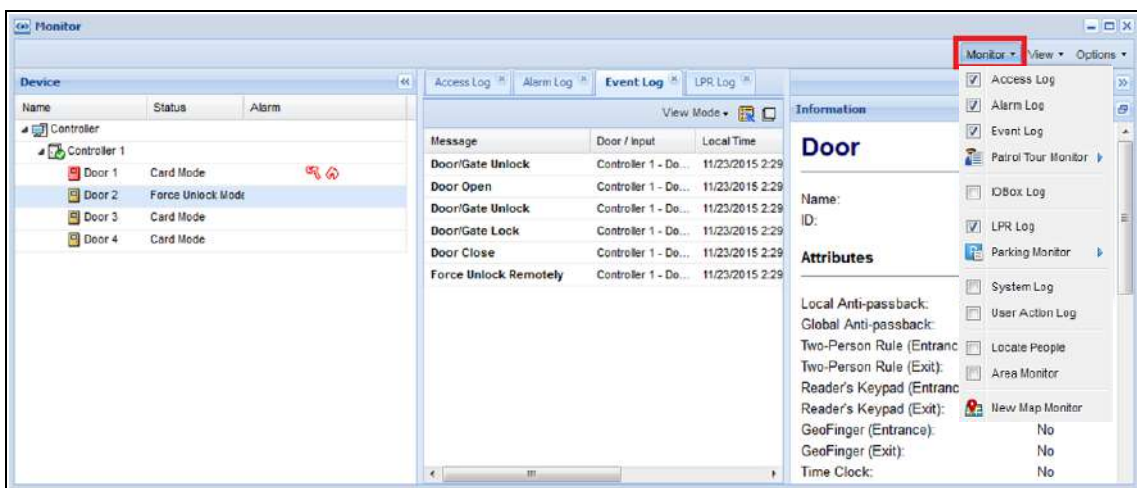


Figure 10-6

- To see a pop-up map of the associated device upon an alarm event, click **Options** in the upper-right corner > **Map (Alarm)**. Up to 6 pop-up events can be shown at a time. For details on how to set up the map, see *10.5 Creating Maps*.

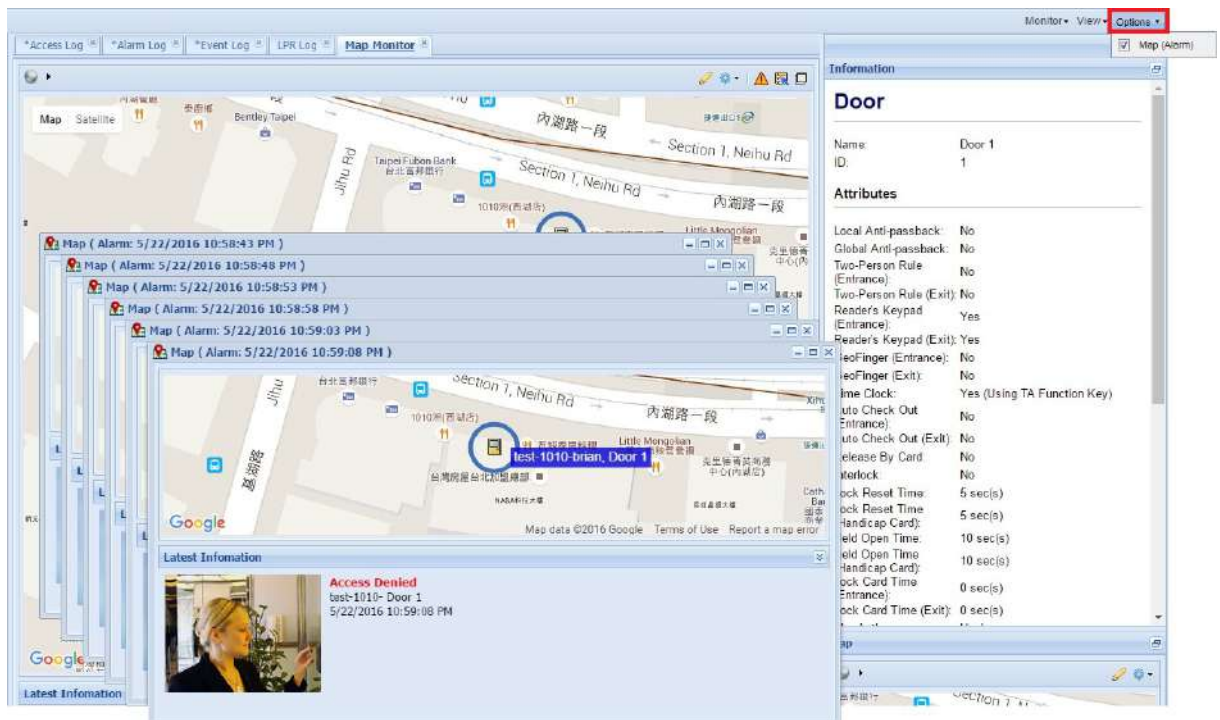
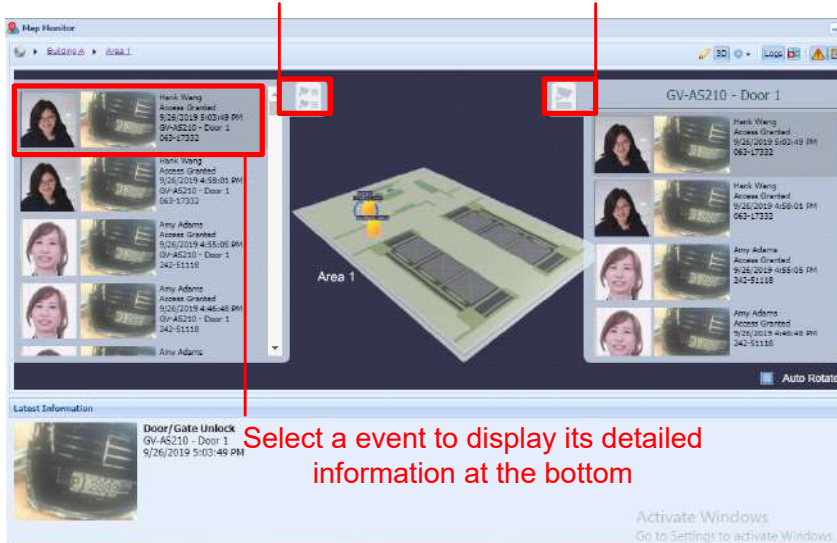


Figure 10-7

- To view the monitoring of event logs in the form of a map, which also supports 3D maps, click **Monitor > New Map Monitor**. The following window appears.

Click to display the left tab, where all events of the GV-ASManager are displayed

Click to display the right tab, where events of the device selected are displayed



Select a event to display its detailed information at the bottom

Figure 10-8

10.4 Accessing Logs

You can access the logs of the connected GV-ASManager, including Access Log, Alarm Log, Daily Access, Event Log, IO Box Log, I/O Log, LPR Log, Patrol Log, System Log, and User Action Log. In addition, you can set search criteria to filter the records efficiently.

10.4.1 Defing Search Criteria

1. Select a log of interest. Here we use Access Log as an example.
2. Under **Filter** on the left pane, type or select the desired filtering criteria. For example, we want to search the log for the records that match the conditions of “Access Granted”, Card Number “120-38620”, Gate A entrance of AS210, and dates from July 1st to July 31st. The resulting filter window may look like this.

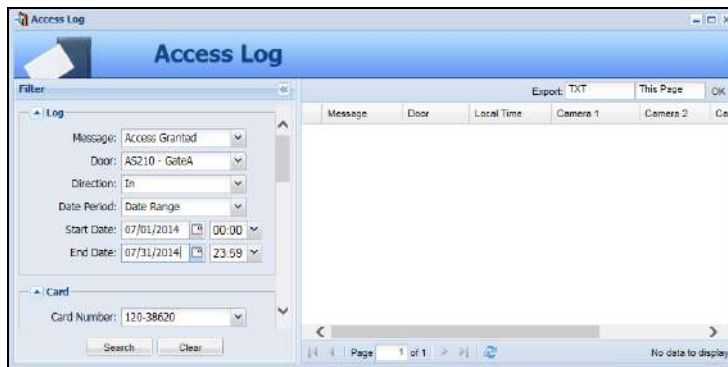


Figure 10-9

3. Click the **Search** button to start the log search.



Note: The maximum date range for all logs is 3 months.

10.4.2 Log Window Icons

The icons in the Log window can display the detailed information of that category. Click the icon to view the details.

: Indicates the availability of the recorded video.

: Indicates the availability of the video image.

In Access Log and Daily Access, you can right-click each search result to access more information such as card information  or user information .

Note:

1. Enable **Control Center Server** and **Remote ViewLog Service** on GV-NVR / VMS or GV-AI Guard hosts to allow remote access from GV-ASManager.
 2. To allow non-IE users to view and play video from GV-NVR / VMS or GV-AI Guard via GV-ASWeb, select **Web Socket** when adding the hosts to GV-ASManager. For the option, see Step 4, *5.1 Mapping Cameras*.
-

10.4.3 Exporting Logs

You can download the logs of the connected GV-ASManager to the local computer in four formats: **txt**, **html**, **xls**, **html (zip)**, and **PDF**. The Logs in html format and the snapshots captured will be exported in a .zip file.

1. Use the **Export** drop-down list on the top-right corner and select the file format.
2. Use the next drop-down list to select **This Page** to save the current log page, or **All** to save all logs.
3. Click **OK** to download the logs.

10.4.4 Defining Columns

You can define the displayed columns of the search results for each type of log. The desired column must be first enabled on GV-ASManager before it becomes searchable on GV-ASWeb.

1. On the menu bar of GV-ASManager, click **Tools > ASWeb Field**. This dialog box appears.

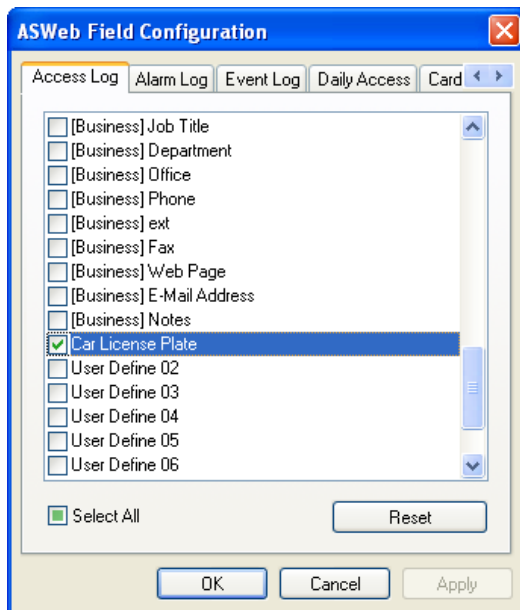


Figure 10-10

2. Select the columns to enable and click **OK**.
3. On GV-ASWeb, click on the arrow button next to an existing column and select **Columns**.

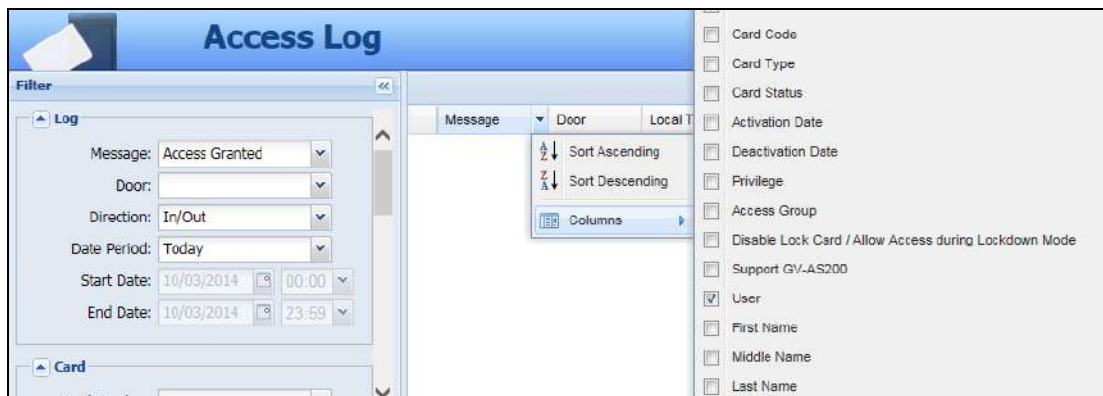


Figure 10-11

4. Select a column to display it in the search results.

For example, we added a user-defined column “Parking Space Number” to the Access Log. The resulting window on GV-ASWeb may look like this:

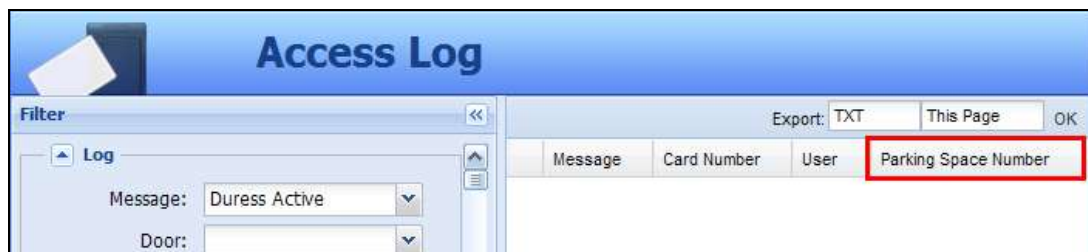



Figure 10-12

10.5 Creating Maps

You can place the icons of connected controllers, LPR lanes, LPR cameras and I/O devices on the Google Maps or on a map you uploaded to GV-ASWeb. The map will help you quickly pinpoint the location of an event or the devices you have installed.

1. On GV-ASWeb, click the **Map** icon . This window appears.

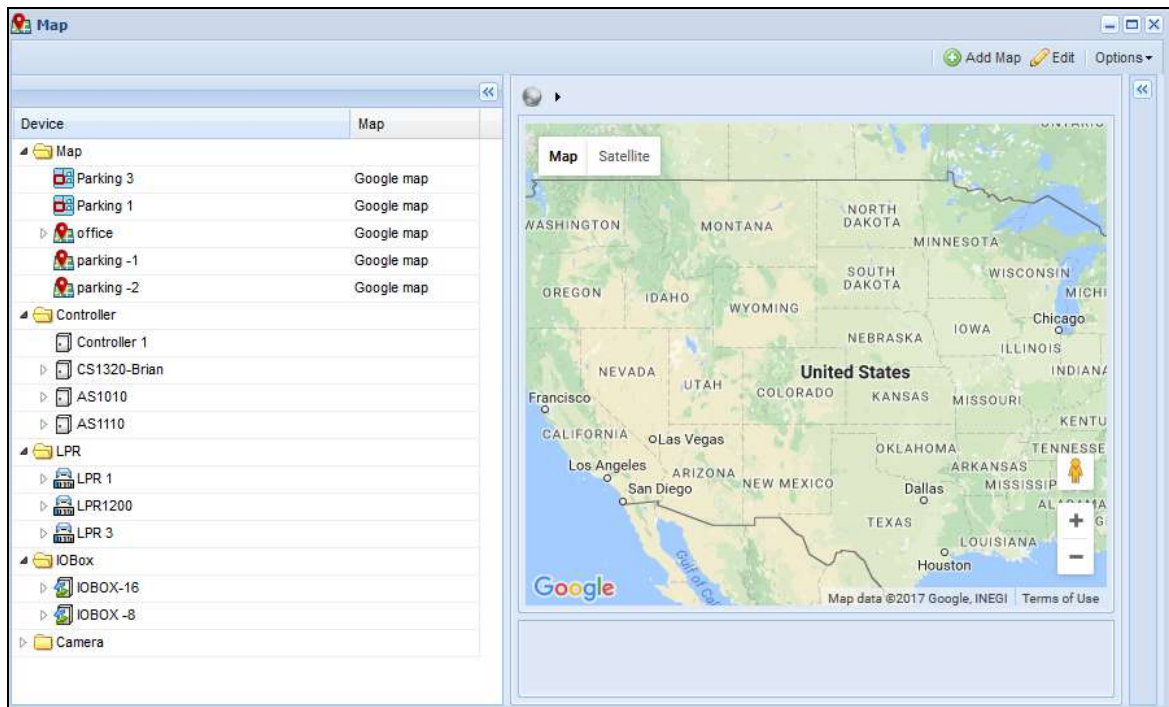


Figure 10-13

2. On the Google Maps, zoom in on location of the building or the monitored area. Skip to step 6 if you do not want to upload your own map.
3. To upload your own map, click **Add Map**. This dialog box appears.

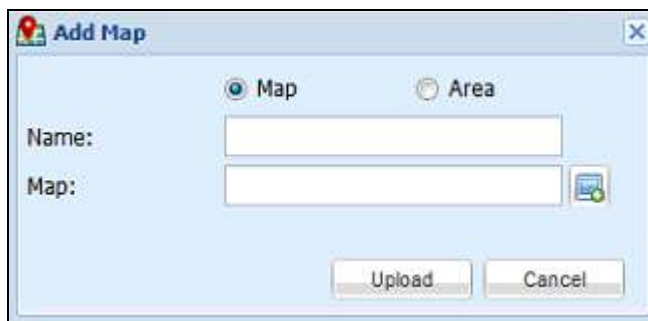



Figure 10-14

- Select **Map** to type a name for the map or select **Area** to choose an area created in *10.11 Configuring Areas for Anti-Passback* from the drop-down list.

- Click the **Add** button  to locate the file of the map.
 - Click **Upload**. A pin is placed on the map.
4. Click **Edit** in the top-right corner. If you have uploaded your own map, click the pin to open the map.
 5. Drag the controller, LPR lane, LPR camera and I/O device icons from the left menu onto the map according to their location.
 6. Click **Edit** again when you are finished. You can click the icon of the controllers, LPR lanes, LPR cameras or I/O devices to access their information.

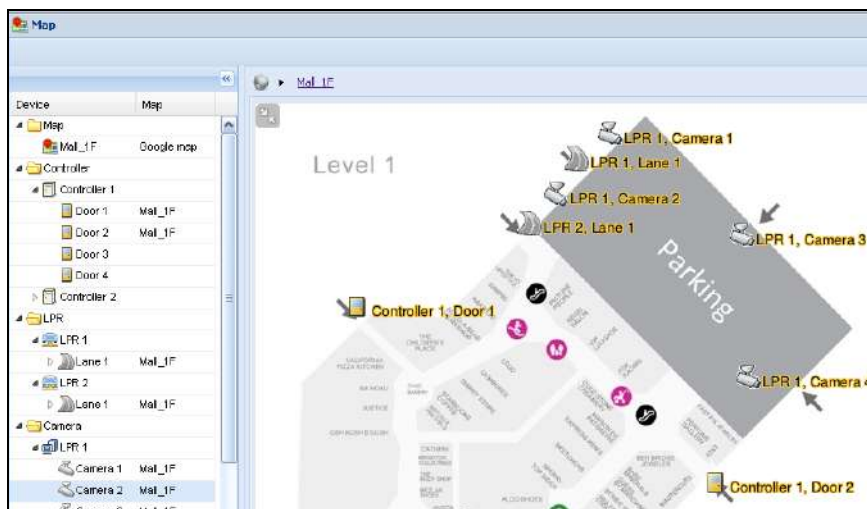



Figure 10-15

Next, you can look up activities at a door or LPR lane by clicking the arrow button  in the top-right corner. Select your search criteria and click **Search**.

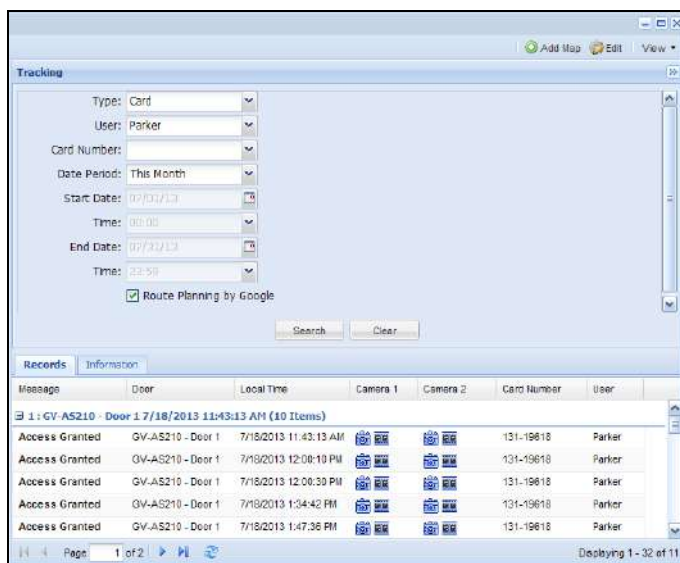



Figure 10-16

- You can double-click an event to locate the associated door or LPR lane on the map.
- You can select **Route Planning by Google** to see the suggested route between the access data of a card or a license plate in the order of access time.
- To view snapshots or play back recorded videos, click the snapshot or video button .

On the Google maps, you can also see the directions from one controller / monitored area / LPR cameras to another. The directions marked on the maps will also be displayed in LPR log.

1. Right-click the icon of your starting location, and select **Begin**.
2. Add as many destinations as you wish by right-clicking the icon and selecting **Through**.
3. For your last destination, right-click the icon and select **End**.



Figure 10-17

Note: For details on monitoring access status using the map created, see Step 4 and 5 in *10.3 Monitoring GV-ASManager*.

10.6 Setting up Export Schedule for Lists and Logs

You can set up a schedule to regularly export lists and logs, and send the report to specified e-mail addresses or a folder on the GV-ASManager system.

Note: The lists available for export include User List, Card List and Vehicle List.


1. On GV-ASWeb, click **Export Schedule**. This dialog box appears.

The screenshot shows the 'Export Schedule' dialog box. At the top, there are buttons for 'Add', 'Edit', 'Remove', and 'Refresh'. Below is a table with the following data:

Schedule Name	Report Type	Export Type	Operator Ac...	Frequency	Start time
Access Log (New)	Access Log	HTML	admin	Every Day	00:00

Below the table is the 'Set Send Information' section. It includes a 'Schedule Name' field with 'Access Log (New)', an 'Export Type' dropdown set to 'HTML', and a 'Frequency' section with radio buttons for 'None', 'Every Day' (selected), 'Every Week', and 'Every Month'. There is also a 'Start time' field set to '0:00'. Below this are sections for 'E-Mail' (with fields for To, CC, BCC, Subject, and Content) and 'Export To File' (with fields for Export Path and File Name).

Figure 10-18

2. Click **Add**  and select a list or log to be exported.

The screenshot shows the 'Export Schedule' dialog box with the 'Add' dropdown menu open. The menu lists the following options: User List, Card List, Vehicle List, Access Log, Alarm Log, Daily Access, Event Log, I/O Log, LPR Log, Patrol Log, System Log, and User Action Log. The background shows the 'Frequency' section with 'Every Month' selected.

Figure 10-19

- On the left pane, set the filter criteria for the desired data to be exported, and click **Save to Export Schedule**.

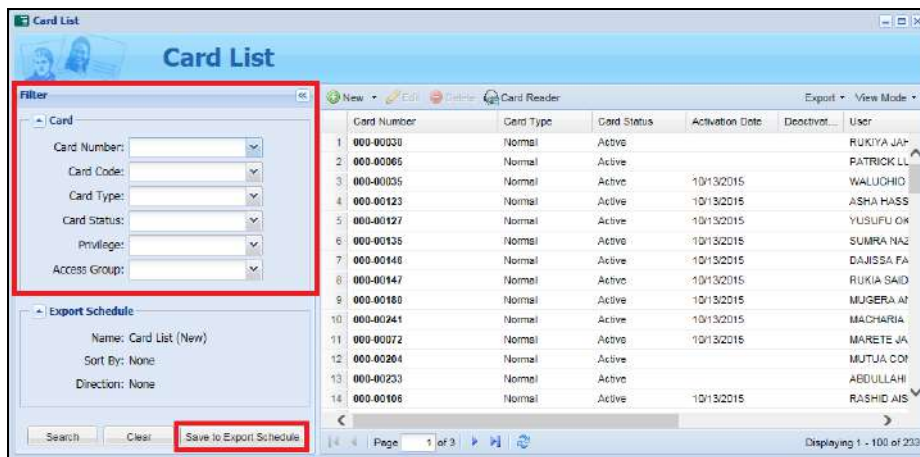


Figure 10-20

- Under **Set Send Information** of the Export Schedule dialog box, select **Export Type** for the file format, **Frequency** to export by day, week, month or a specific time.
- To send the report through e-mail, type the **E-mail** of the recipient.
- To send the report to a folder on the GV-ASManager system, specify the path and file name under **Export to File**.
- Click **Save** to apply.

10.7 Accessing GV-ASWeb using Mobile Devices

You can access GV-ASWeb using the Web browser on your mobile device.

1. Open the Web browser on your mobile device and type the IP address of GV-ASManager to be connected. This page appears.

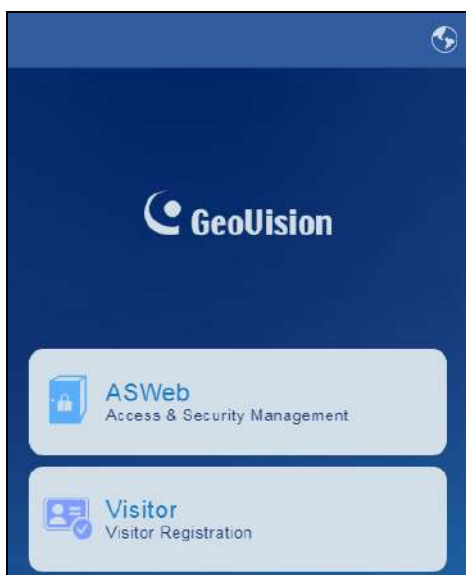


Figure 10-21

2. Click **ASWeb** and type login credentials. The Monitoring list is shown.

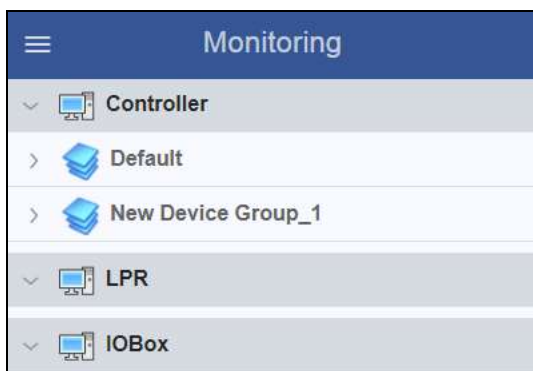


Figure 10-22

- Expand the Controller, LPR or IO Box list to see the status of doors, lanes or I/O boxes. When alert conditions occur, the alert icons will light up in red.

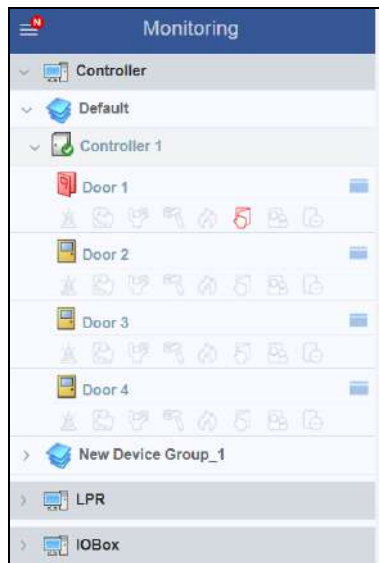


Figure 10-23

- To remotely control a device, tap on the device and select an action.

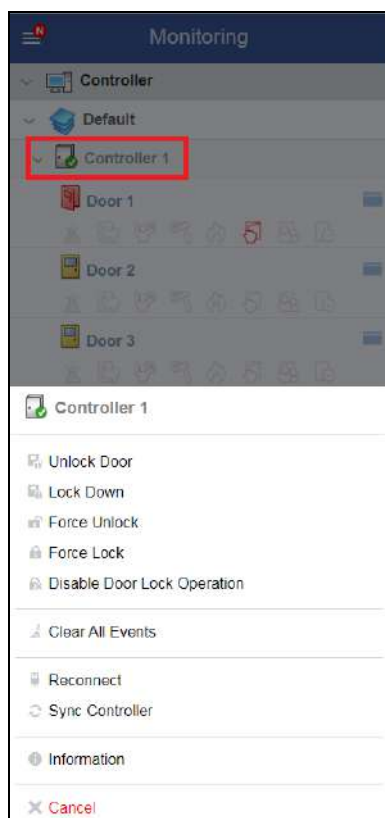



Figure 10-24

- To watch live view of a connected camera, tap the Menu button  > **Live Video** and select the device.

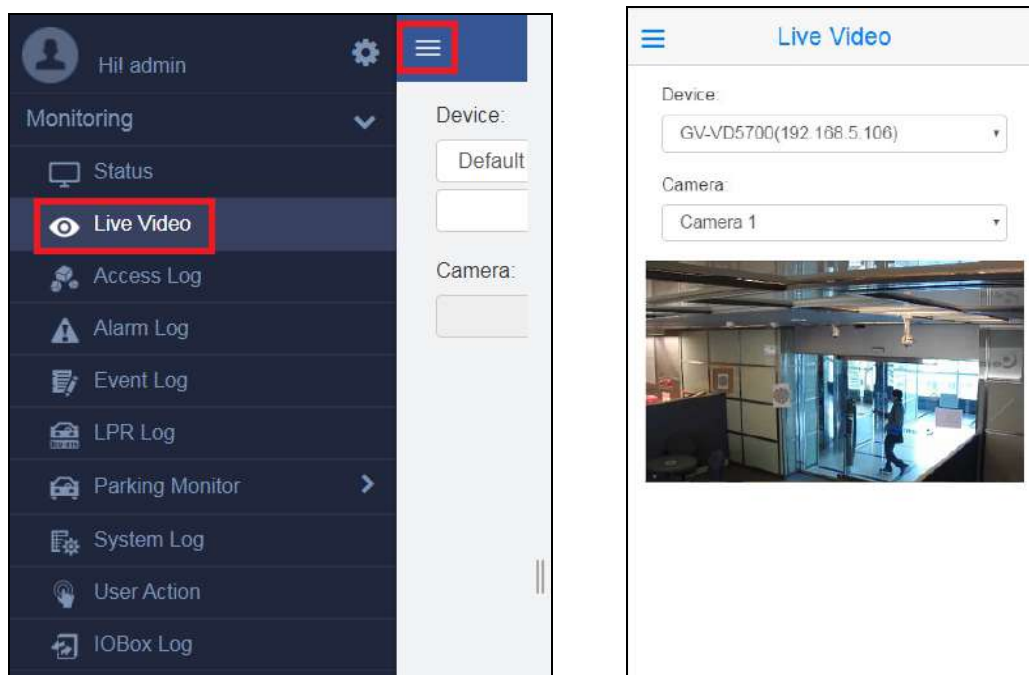


Figure 10-25

- To look up the logs, tap the Menu button  and select one log.

Chapter 11 GV-TAWeb for Workforce Schedule and Payroll

GV-TAWeb is a time and attendance management system that helps you assign work schedule, keep track of employee attendance and calculate salary. You must first enable GV-TAWeb function on GV-ASManager and then log in GV-TAWeb to access the following functions:

- **TA Report:** Look up workforce schedule, attendance records, and employee payroll.
- **TA Shift:** Set up different types of daily work schedules.
- **TA Template:** Arrange schedules of up to 45 days with daily schedules from TA Shift.
- **TA Holiday:** Designate which dates are holidays.
- **TA Schedule:** Assign work schedule to individual or a group of employees.
- **TA User:** Specify employee salary.
- **Export Schedule:** Set up a schedule to regularly export reports to specified e-mail addresses or a folder on the GV-ASManager system. See *10.6 Setting up Export Schedule for Lists and Logs*.

11.1 Connecting to GV-ASManager

To enable GV-TAWeb, the **Time Clock** option must be enabled on GV-ASManager and the **Web Server** must be started to allow remote access.

Note: The Time Clock option is not available for GV-AS1010. To use GV-AS1010 with GV-TAWeb, you must configure the built-in function keys on the Web interface of GV-AS1010. See the *Function Key Configuration* section in Chapter 8 of [GV-ASEV Controller User Manual](#).

1. On the menu bar of GV-ASManager, click **Setup > Devices**. In the Devices dialog box, double-click a Controller you want to track attendances, select a **Door**, click the **Other** tab and enable **Time Clock**.

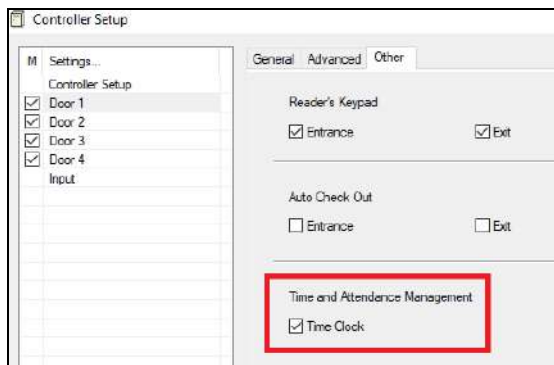



Figure 11-1

2. On the menu bar, click **Tools > Servers > Web Server**. The Geo Web Server Setting dialog box (Figure 10-1) appears.
3. Click **OK**. When the server is started, the icon  appears at the bottom-right of the main screen.

To start GV-TAWeb:

1. Open an Internet browser, and type the IP address of GV-ASManager to be connected.
This page appears.

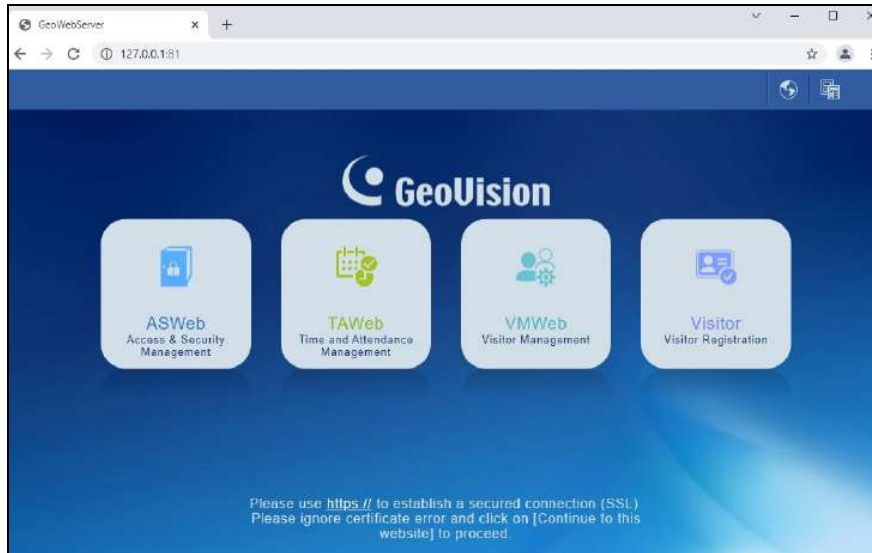


Figure 11-3

2. Click **https://** for SSL encrypted connection, or **TAWeb** for regular connection.
3. Enter the login credentials. The GV-TAWeb page appears.

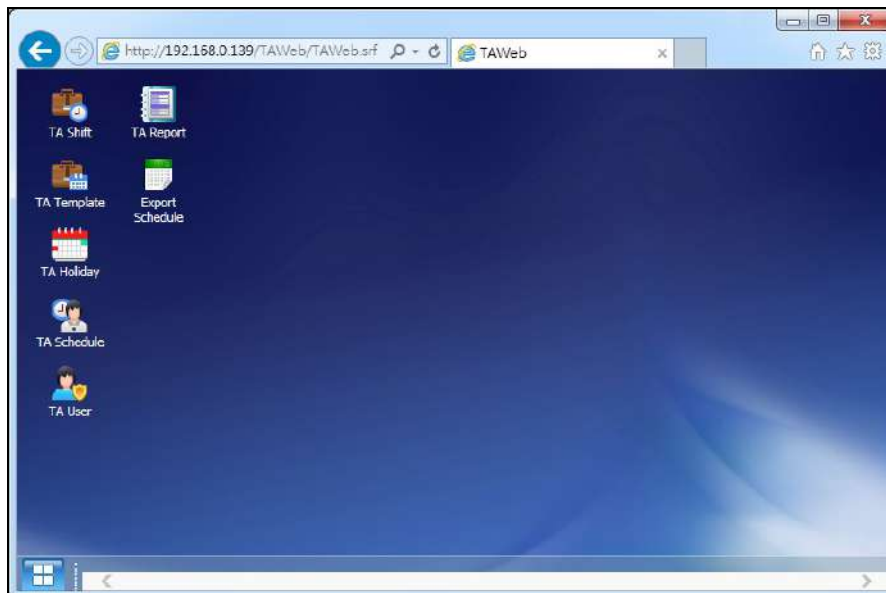


Figure 11-4

11.2 Setting up Workforce Schedule

To set up workforce schedule, first set up different types of daily work schedules using **TA Shift**, and then you can arrange the different types of daily work schedules into a cycle using **TA Template**. Next, specify the dates for holidays in **TA Holiday**. Lastly, **TA Schedule** allows you to assign work schedules to an employee or a group of employees using daily schedules in TA Shift or using long-term schedules from TA Template.

11.2.1 TA Shift: Setting up a Daily Schedule

1. Click the **TA Shift** icon. This dialog box appears.

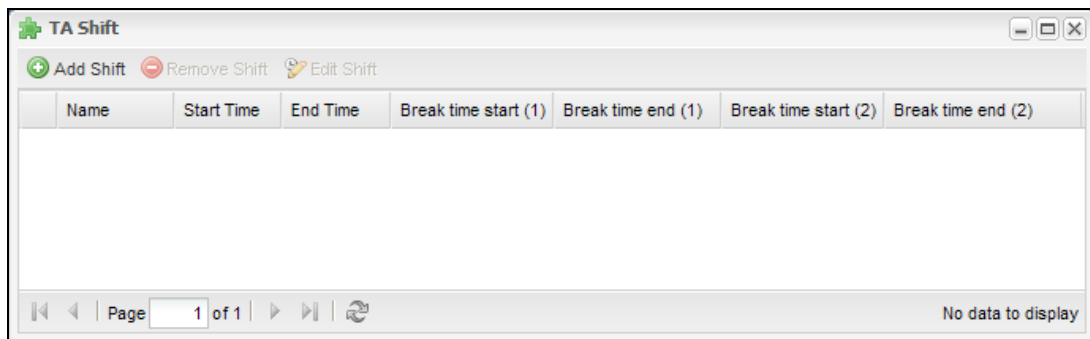


Figure 11-5

2. Click **Add Shift** to add a new daily shift schedule. This dialog box appears.

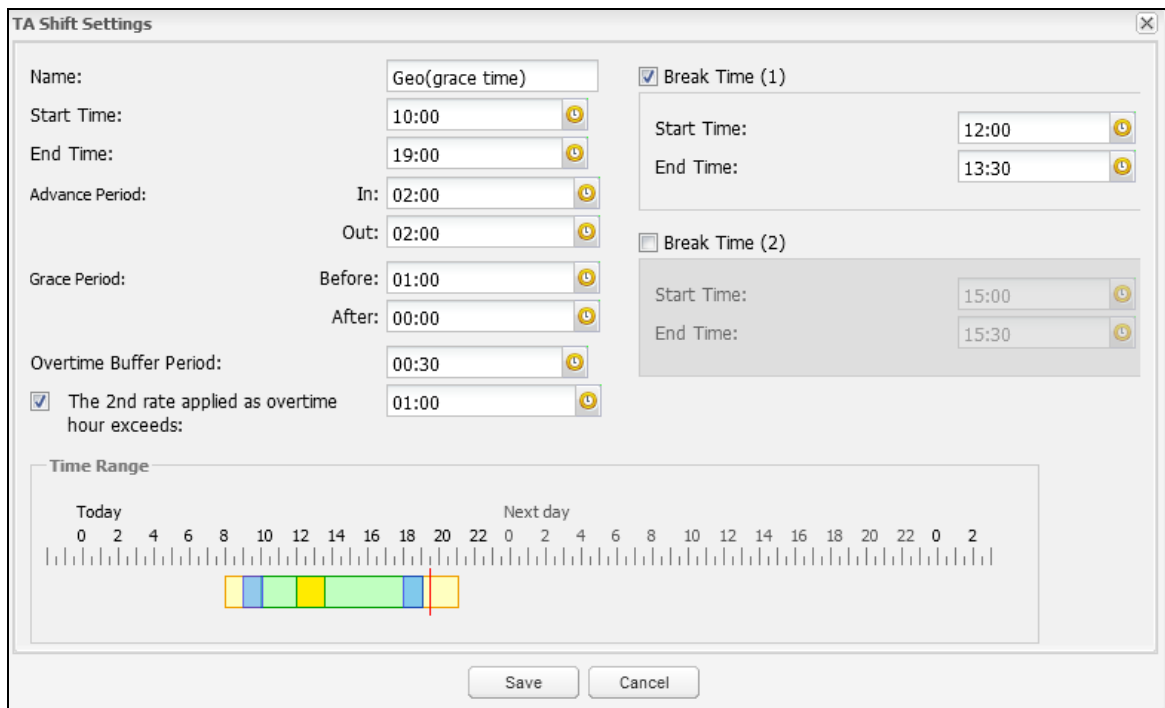


Figure 11-6

3. Type a **Name** for the daily shift to help you identify it.
4. Select a **Start Time** and **End Time** to specify when the work shift starts and ends.
5. Specify an **Advance Period** to set the amount of time before and after the regular work hours an employee can work. Employees arriving before the Advance Period will be recorded as working during Not Scheduled time in TA Record.
6. Specify a **Grace Period** to set the amount of time in which employees can vary their start and end times of the regular work hours.
7. Specify the **Overtime Buffer Period** and an employee has to work passed the overtime buffer period to be counted toward overtime pay.
8. Select **The 2nd rate applied as overtime hour exceeds** if you want to specify the time an employee has to work passed after the Overtime Buffer Period to be counted toward the second overtime rate.
9. To specify when break time starts and ends, select **Break Time** and select the **Start Time** and **End Time**. You can set a second break time if needed. Note that Break Time will not be counted toward Work Hours.

The time range shows the start and end times of a shift schedule. Using the below figures as an example, an employee working 2 hours passed the 19:00 pm regular end time will receive overtime pay for 1.5 hours (19:30 ~ 21:00), while an employee working 20 minutes passed 19:00 will not receive overtime pay. The 2nd rate will be applied once the employee has worked passed 20:00, which is 1 hour after the Overtime Buffer Period.

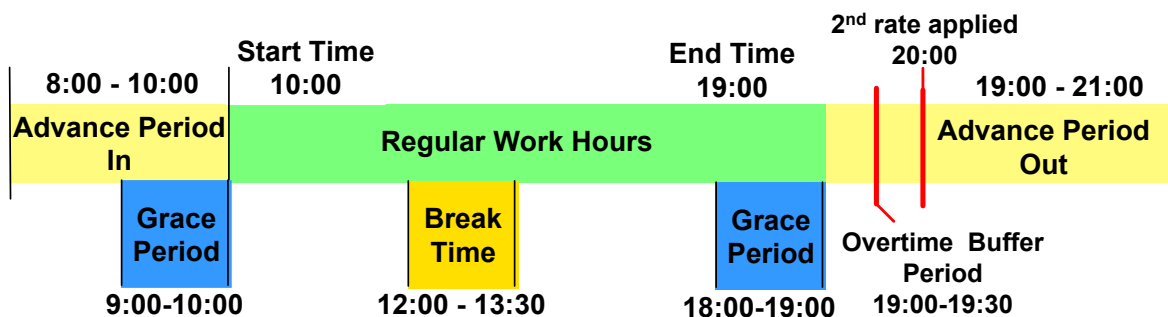


Figure 11-7

10. Click **Save** to confirm the shift settings.

11.2.2 TA Template: Setting up a Schedule Template

TA Template allows you to set a 1-45 day recurring schedule template composed of the daily shift schedule created in TA Shift.

1. Click the **TA Template** icon. This dialog box appears.

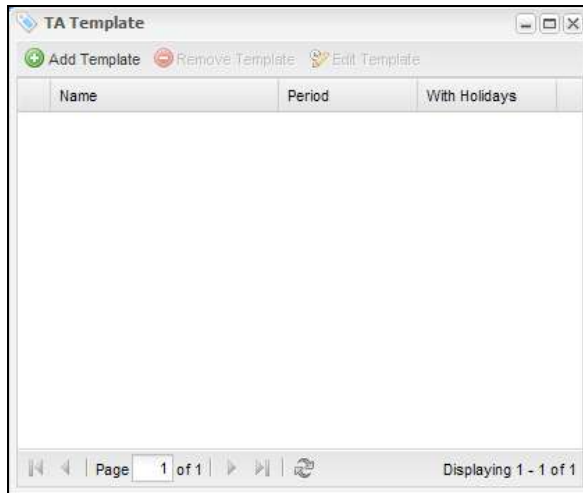


Figure 11-8

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

Figure 11-9

3. Type a **Name** to identify the template.
4. In the **Period** field, type a number between 1 and 45 to indicate the number of days in the schedule.
5. Select **With Holidays** to apply the holidays set up in TA Holiday.

- In the drop-down list below each day, select a daily shift schedule created in TA Shift.

A TA Template may look like this. In this example, the template is a 2-week work schedule, because the Period is set to 14 days. The drop-down list under each day indicates the daily work schedule selected for that day. A blank drop-down list means that no work schedule is assigned for that day.

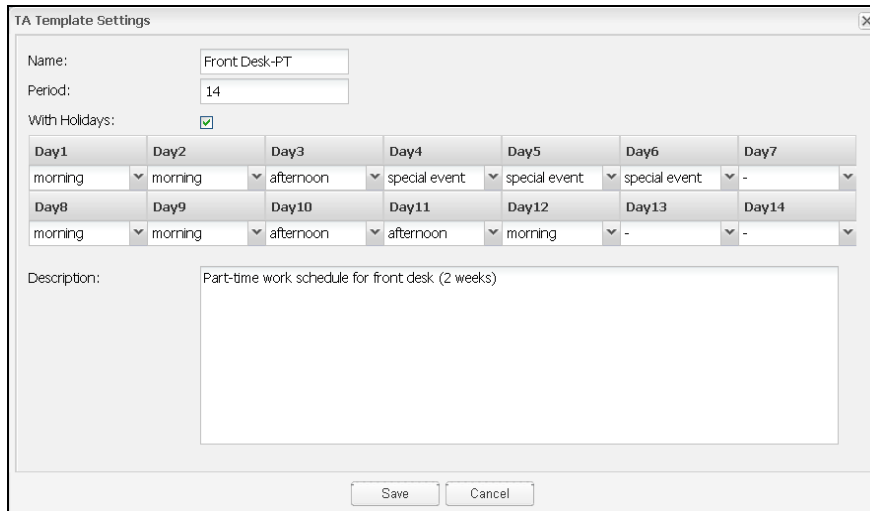


Figure 11-10

- Click **Save**.

11.2.3 TA Holidays: Setting Certain Dates as Holidays

- Click the **TA Holiday** icon. This dialog box appears.

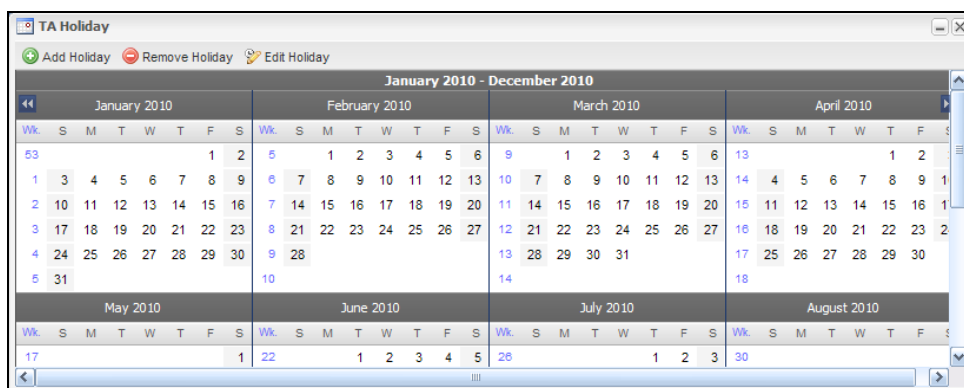


Figure 11-11

- Select a date and click **Add Holiday**.
- Type a name for the holiday.
- Click **OK** and that day will be designated as a holiday if **With Holidays** is selected in TA Template

11.2.4 TA Schedule: Assigning Schedules to Employees

After creating daily shift schedules in TA Shift or arranging a schedule template in TA Template, you can now assign the schedules you set up to an employee or an entire department and select a start date.

Note: The employees listed in TA Schedule are the users in **User List** on GV-ASManager. To assign employees to a group, open the employees' user information in User List and select the **Business** tab. In the **Division** field, type the division of the employee and all employees with the same division name will be grouped into one division in GV-TAWeb. Departments can be created under a division and offices can be created under a department if needed.

1. Click the **TA Schedule** icon. This dialog box appears.

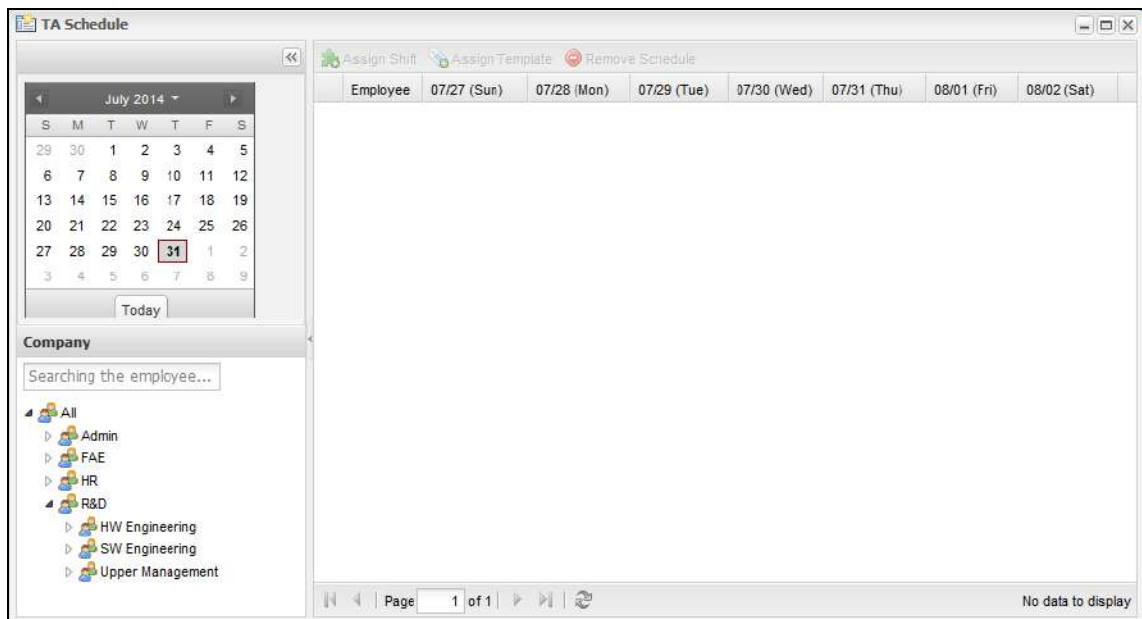


Figure 11-12

To assign daily shift schedules day by day:

- To assign daily schedules day-by-day, select an employee or a group of employees in the Company section and click **Assign Shift**. You can also press Shift or Ctrl to select multiple employees in a department. This dialog box appears.

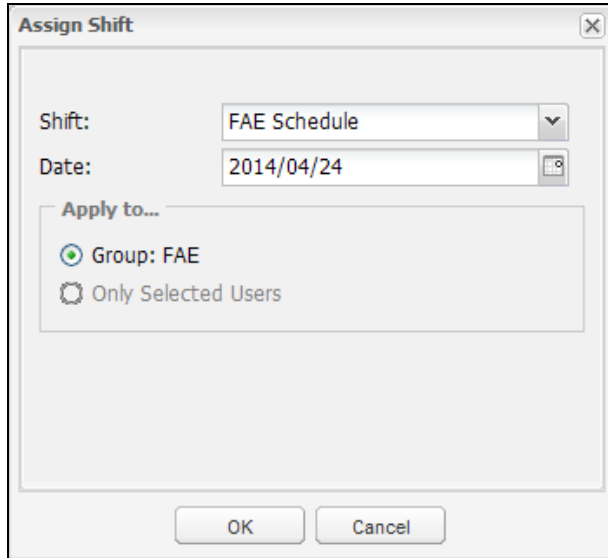
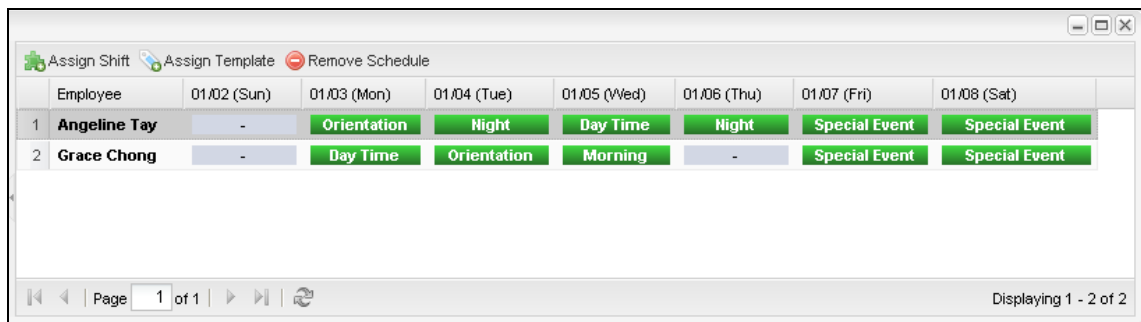


Figure 11-13

- Select a daily schedule and assign it to a date.
- You can choose to apply the schedule to the entire group or only the selected users.
- Repeat the steps for all the dates you want to schedule a shift.
- Click **OK**. A TA schedule window may look like this. In this example, different daily schedules created in TA Shift are assigned from Monday to Saturday to two employees.



	Employee	01/02 (Sun)	01/03 (Mon)	01/04 (Tue)	01/05 (Wed)	01/06 (Thu)	01/07 (Fri)	01/08 (Sat)
1	Angeline Tay	-	Orientation	Night	Day Time	Night	Special Event	Special Event
2	Grace Chong	-	Day Time	Orientation	Morning	-	Special Event	Special Event

Figure 11-14

To assign a schedule template:

- To assign a schedule template from TA Template, select an employee or a group of employees and click **Assign Template**. This dialog box appears.

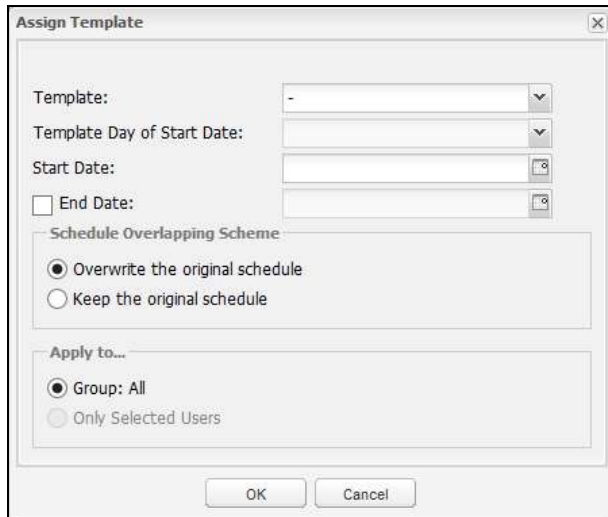


Figure 11-15

- Using the **Template** drop-down list, select a schedule template created in TA Template.
- Select a day from the **Template Day of Start Date** drop-down list and the template will start on that day.

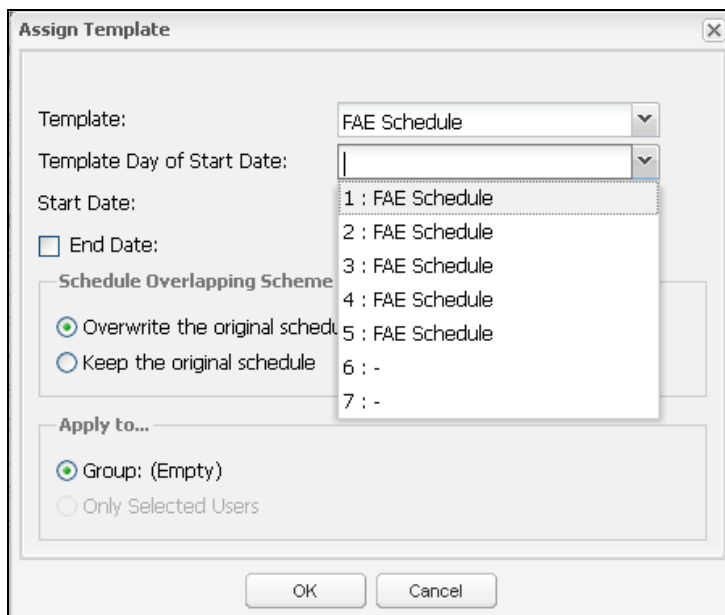


Figure 11-16

- Select a **Start Date** to begin applying the template and the schedule will begin with the day specified in Template Day of Start Date. Select an **End Date** to discontinue the schedule if needed.

11. In the Schedule Overlapping Scheme section, select **Overwrite the original schedule** if you want to overwrite the original schedule in the case of an overlap.
12. Select **Keep the original schedule** and the template will not be assigned if there is an existing schedule during the time period you specified.
13. Click **OK**. A TA schedule window may look like this. In this example, an FAE weekly schedule created in TA Template are assigned to two employees.

Employee	01/09 (Sun)	01/10 (Mon)	01/11 (Tue)	01/12 (Wed)	01/13 (Thu)	01/14 (Fri)	01/15 (Sat)
1 Shalynn Lee	-	FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	-
2 Jervonne Liao	-	FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	-

Figure 11-17

Hint: To set a weekly schedule with Saturday and Sunday as non-working days, set a 7-day Period and designate two consecutive days as non-working days by not selecting a daily shift.

Day1	Day2	Day3	Day4	Day5	Day6	Day7
FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	FAE Schedule	-	-

Figure 11-18

Then, in TA Schedule, match the first non-working day with a Saturday.

Select the first non-working day

Select a Saturday for Start Date

Figure 11-19

11.3 TA User: Specifying Hourly Pay

You can specify the hourly pay for regular work hours and overtime work hours using **TA User**.

1. Click the **TA User** icon. This dialog box appears.

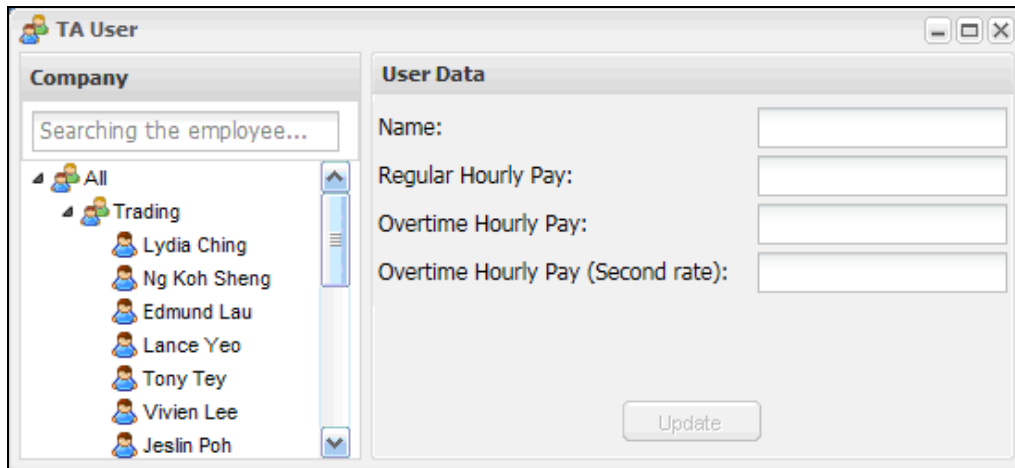


Figure 11-20

2. Select an employee from the list.
3. Type the **Hourly Regular Pay** and the **Hourly Overtime Pay**.
4. Type the **Overtime Hourly Pay (Second rate)** if you have set up the second overtime period. See *11.2.1 TA Shift: Setting up a Daily Schedule*.
5. Click **Update** to save the settings.

Note: The employees listed in TA User are the users in the User List. For how to create users, see *4.6 Adding Users*.

11.4 TA Report: Looking Up Records

TA Report allows you to look up workforce schedules, attendance record, payroll and summaries of each department's data.

1. Click the **TA Report** icon. This dialog box appears.

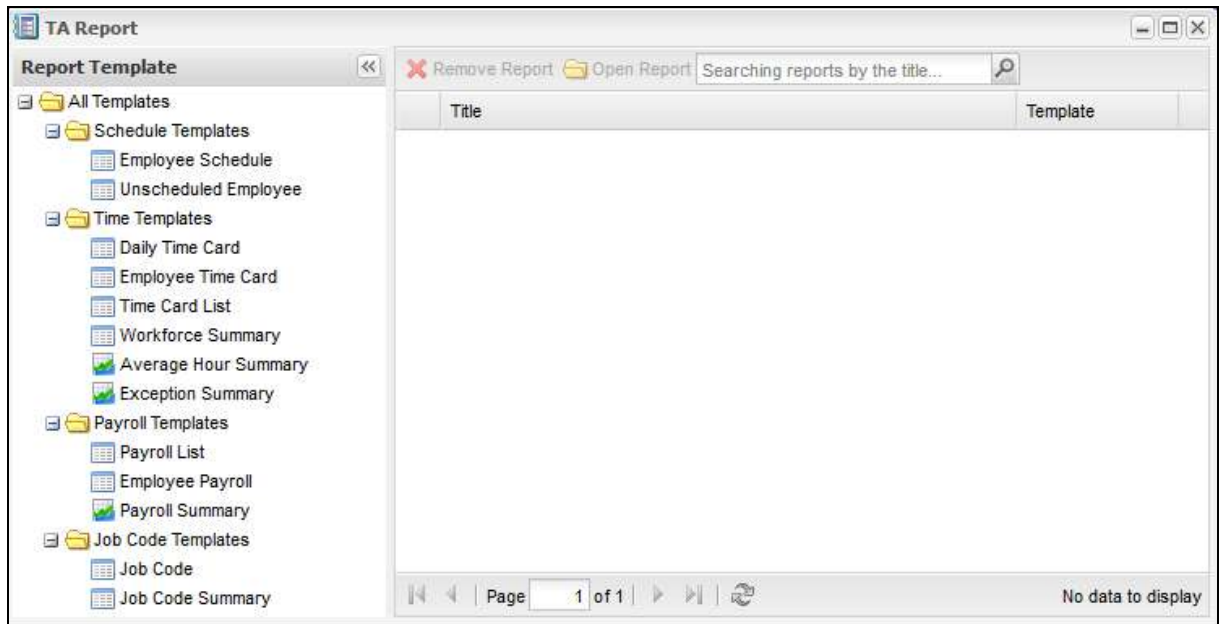


Figure 11-21

2. On the left pane, the following data and graphs are available:

Note: Accessing **Average Hour Summary**, **Exception Summary** or **Payroll Summary** requires Flash Player 10 or later.

[Schedule Templates]

- **Employee Schedule:** Shows the work schedule of an individual employee.
- **Unscheduled Employee:** Shows the days when employees are not scheduled to work.

[Time Templates]

- **Daily Time Card:** Shows the work schedule and the actual punch in/out time of employees in a department.

- **Employee Time Card:** Shows the work schedule and the actual punch in/out time of an individual employee.
- **Time Card List:** Searches for records within a department.
 - **Show Detailed Punch:** Click to display the detailed information of every punch time. For the option to work, **With direction** must be selected in the **Calculation** field.

Date	Name	Division	De...	Job Title	Employee ID	Exception	Punch Message	Punch In Time	Punch Out Time	Period Time
4 2017/05/04 (Thu)	Rachel Mill					A, D, I		12:00:00	18:13:31	
							Access Granted	12:00:00	18:13:31	06:13:31
							Access Granted	18:14:46	-	

Figure 11-22

To search for normal activities only, do not select any events. To search for abnormal activities, select one or more events under the Filter section. The following events are available.

- **In Late:** Punching in after the assigned start time.
 - **In Early:** Punching in before the assigned start time.
 - **Out Late:** Punching out after the assigned end time.
 - **Out Early:** Punching out before the assigned end time.
 - **Over Hours:** Working after the Overtime Buffer Period but before the Extended Period.
 - **Unscheduled Absence:** Absence during scheduled work day.
 - **Missed Punch:** Punching in without punching out or punching out without punching in.
 - **Not Scheduled:** Working on days when there is no assigned shift for that day.
 - **Below the required working hours:** Actual number of hours worked is below the assigned work hours.
- **Workforce Summary:** Shows each employee's total work time and days within the time period specified.
 - **Average Hour Summary:** Shows each department's average work hours per person during the time period specified and the percentage occupied in comparison to other departments.
 - **Exception Summary:** Displays a department's total counts of Exception Events within the time period specified.

[Payroll Templates]

- **Payroll List:** Shows the hourly pay, total work hours and total pay of the employees within a department during the time period specified.
- **Employee Payroll:** Shows the hourly pay, total work hours and total pay of an employee for each day of the time period specified.
- **Payroll Summary:** Shows the average total pay of each department during the time period specified and the percentage occupied within the company.

[Job Code Templates]

- **Job Code:** Shows the employee's punch in and punch out time of different job codes during the time period specified.
- **Job Code Summary:** Shows the employee's total work time of different job codes during the time period specified.

3. Using the Daily Time Card as an example, double-click **Daily Time Card** on the left menu. This dialog box appears.

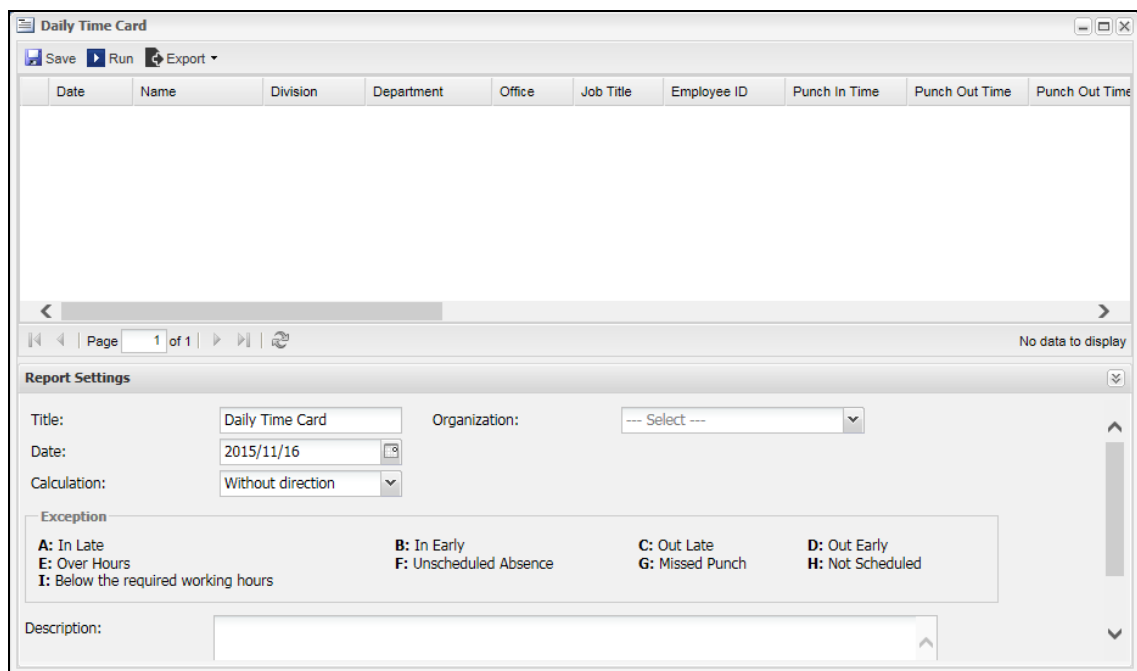


Figure 11-23

4. Select the **Date** and **Organization** to look up the employees' scheduled shift and actual attendance record.
5. You can use the **Calculation** drop-down list to further filter the search results.
 - **Without Direction:** Shows all attendance records.

- **With Direction:** Only shows attendance record registered from readers that have been set as entry readers (IN readers).
 - **With TA Function Key:** Only shows attendance record registered using the function keys of GV-AS1010.
6. Click the **Run** button toward the top. A dialog box similar to the one below appears. Using the fifth person as an example, Paul punched in at 10:01 and punched out at 16:56, even though his scheduled work time is from 9:00 to 17:00. He is therefore listed as A (In Late) and D (Out Early) in the **Exception** column. The number of hours he worked is listed under the **Work Time** column.

Name	Punch In Time	Punch Out Time	Work Time	Start Time	End Time	Duty Work Time	Exception
1. Corry	10:00	19:00	00:47	17:35	19:00	01:20	A, C, H
2. Irving	18:00	19:00	00:47	17:35	19:00	01:20	A, C, H
3. Iverson	17:52	18:16	00:18	17:35	19:00	01:20	A, D, H
4. Parker	10:01	16:56	06:55	09:00	17:00	08:00	A, D
5. Paul	10:01	16:56	06:55	09:00	17:00	08:00	A, D
6. Rick	-	-	-	-	-	-	-
7. Rondo	17:52	18:16	00:19	17:35	19:00	01:20	A, D, H

Report Settings

Title: Daily Time Card Organization: --- Select ---

Date: 2015/11/16



Calculation: Without direction

Exception

A: In Late B: In Early C: Out Late D: Out Early
 E: Over Hours F: Unscheduled Absence G: Missed Punch H: Not Sche
 I: Below the required working hours

Description:

Figure 11-24

7. You can click the **Access Log** icon  to see complete attendance records or click the **TA Log** icon  to see attendance records excluding records that are not during the scheduled work hours.

- To add/edit attendance records, click the **TA Log** icon . And click the **Add** or **Edit** buttons. The manually added and edited records are highlighted in green.

	Local Time	Message	Door	Direction	Camera 1	Camera 2
1	2017/05/04 09:00:00	Access Granted	AS1010 - Door 1	In		
2	2017/05/04 16:51:32	Access Denied: APB (Double Entry)	AS1010 - Door 1	In		
3	2017/05/04 16:51:35	Access Denied: APB (Double Entry)	AS1010 - Door 1	In		
4	2017/05/04 16:51:35	Time Attendance: Work Time Start	AS1010 - Door 1	In		
5	2017/05/04 16:52:00	Time Attendance: Work Time Start	AS1010 - Door 1	In		
6	2017/05/04 16:52:04	Access Denied: APB (Double Entry)	AS1010 - Door 1	In		
7	2017/05/04 16:52:04	Time Attendance: Work Time Start	AS1010 - Door 1	In		
8	2017/05/04 17:06:40	Access Denied: APB (Double Entry)	AS1010 - Door 1	In		
9	2017/05/04 17:06:40	Time Attendance: Work Time Start	AS1010 - Door 1	In		
10	2017/05/04 17:07:11	Access Denied: APB (Double Entry)	AS1010 - Door 1	In		
11	2017/05/04 17:07:11	Time Attendance: Work Time Start	AS1010 - Door 1	In		

Figure 11-25

- Click **Save** and a shortcut of the Daily Time Card for the specified department and date will be created in the TA Report main page.

Title	Template
1 Daily Time Card	Daily Time Card

Figure 11-26

- Click **Export** to export the data in excel (CSV), HTML or PDF format.
- To select which data to display, click the arrow next to the column title and click **Column**.

	Name	Punch In Time	Punch Out Time	Work Time	Start Time
1	Lydia Ching	09:56		40	09:00
2	Ng Koh Sheng	09:57		40	09:00
3	Edmund Lau	09:57			09:00
4	Lance Yeo	09:57			
5	Tony Tey	09:57	-	-	
6	Vivien Lee	09:57	18:37	08	
7	Jeslin Poh	09:56	18:37	08	

Figure 11-27

Note:

1. The **Export** function is only available after you have saved the report by clicking the **Save** button.
 2. In the Time Card List, you can select **CSV (individual)** or **HTML (individual)** to export the user records individually as an excel file or HTML page.
-

11.5 Creating Accounts to Manage GV-TAWeb

The administrator can create accounts with different privileges to manage GV-TAWeb.

1. On the menu bar, click **Tools > Operators**. The Account dialog box (Figure 8-1) appears.
2. Follow the instructions in *8.1 Adding System Users* to create an account.
3. Click the **TAWeb** tab.
4. Select the privileges you want to grant. The following options are available.
 - **Schedule Setup:** Access TA Shift, TA Template and TA Schedule.
 - **Report viewing:** Access TA Report.
 - **Payroll Setup:** Access TA User.
 - **Modify Log:** Able to modify and delete TA logs.
5. Click **OK**.

Chapter 12 GV-VMWeb for Visitor Management


GV-VMWeb is a visitor management system for internal business use where the administrator can create a visitor database and grant access to visitors over a LAN. GV-VMWeb can also allow visitors to register their own visitor accounts and create visit requests over the Internet using the Visitor service.



Figure 12-1

12.1 Connecting to GV-ASManager

Before GV-VMWeb can connect to GV-ASManager, remote access must be enabled on GV-ASManager as below:

1. On the menu bar, click **Tools > Servers > Web Server**. The Geo Web Server Setting dialog box (Figure 10-1) appears.
2. Click **OK** to start the connection. When the server is started, the icon  appears at the bottom-right of the main screen.

To start GV-VMWeb:

1. Open an Internet browser, and type the IP address of GV-ASManager to be connected. The login page (Figure 12-1) appears.
2. Click **https://** for SSL encrypted connection, or **VMWeb** for regular connection.
3. Enter the login credentials. The GV-VMWeb page appears.

12.2 The GV-VMWeb Window

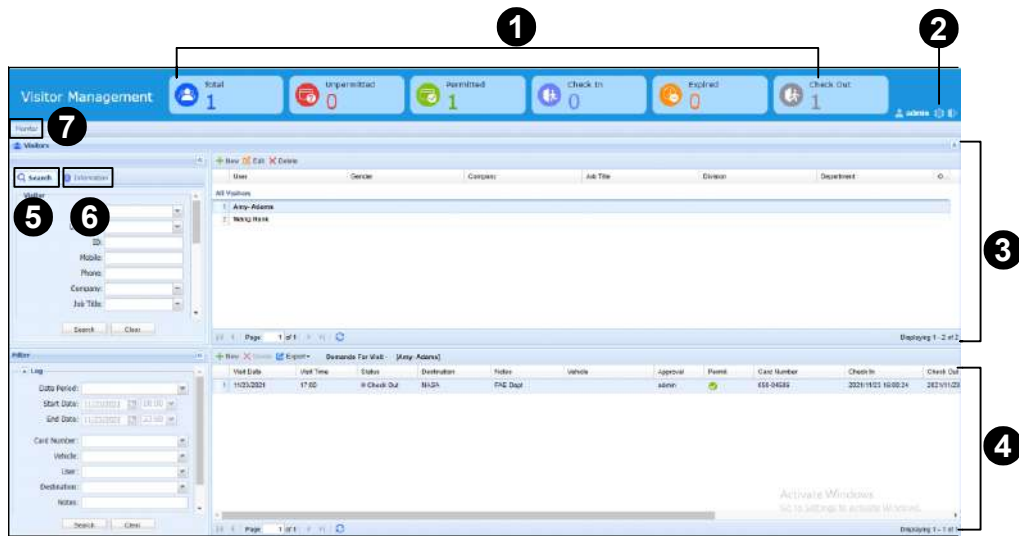
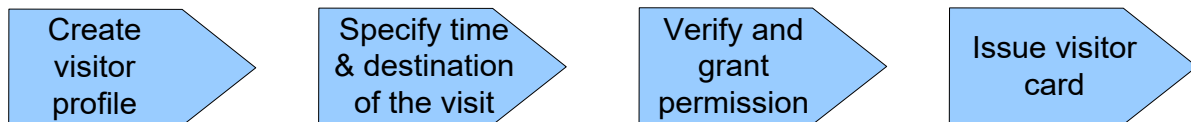


Figure 12-2

No.	Name	Function
1	Counter Banner	Display live counts of Total, Unpermitted, Permitted, Checked-in, Checked-out and Expired visit requests.
2	Options	Access the following functions: Auto Permit (permitting visit requests automatically when the requests are created), Visit record of issue cards is deletable (able to delete visit records under Demands for Visit (No 4, Figure 12-2)), Export Schedule (see 10.6 Setting up Export Schedule for Lists and Logs), Theme (changing the UI color theme), Visitor Web (see 12.6 Visitor Self Registration). Note: After selecting Export Schedule > Add , the Export Schedule will be minimized to the bottom-left side. Then click Save to Export Schedule to start setting.
3	All Visitors	List all the visitors created.
4	Demands for Visit	List all the visit requests of today.
5	Search	Search for visitors and visit records by defining criteria. See 12.5 Searching GV-VMWeb database.
6	Information	Display the user information of a selected visitor.
7	Monitor	List the visit records of a specified time period.

12.3 Creating Accounts to Manage GV-VMWeb

The administrator can create multiple accounts with different privileges to manage each step of granting access as shown below.



You can create a security staff account with privileges to create **Visitor Data** and **Visit Records**, while another account with privileges to **Verify** visitors and **Issue Card** can be assigned to a management staff. In this setup, the security staff can create visitor profiles and visit requests for visitors, but the management staff needs to approve the visits and issue cards, passcodes or QR codes to visitors before the visitors can be granted access.

Note: To create visitor cards, see [4.3 Adding Cards](#).

To create accounts:

1. On the menu bar of GV-ASManager, click **Tools > Operators**. The Account dialog box (Figure 8-1) appears.
2. Follow the instructions in [8.1 Adding System Users](#) to create an account.
3. Click the **VMWeb** tab.
4. Select the privileges you want to grant. The following options are available.
 - **Set Up Visitor Data:** Create and edit visitor profiles.
 - **View Visit Record:** Look up visit records in the past for each visitor.
 - **Edit Visit Record:** Create, edit and export visit records.
 - **Permit Visit:** Grant and edit visit permits.
 - **Issue Card:** Assign cards, passcodes or QR codes to visitors.
 - **System Settings:** Enable access to the GV-VMWeb setting options.
5. Click **OK**.

12.4 Creating Visitor Profiles

GV-VMWeb allows you to create visitor profiles and grant different accesses to each visitor.

To create a visitor profile:

1. In the Visitor section, click the **New** button. This dialog box appears.

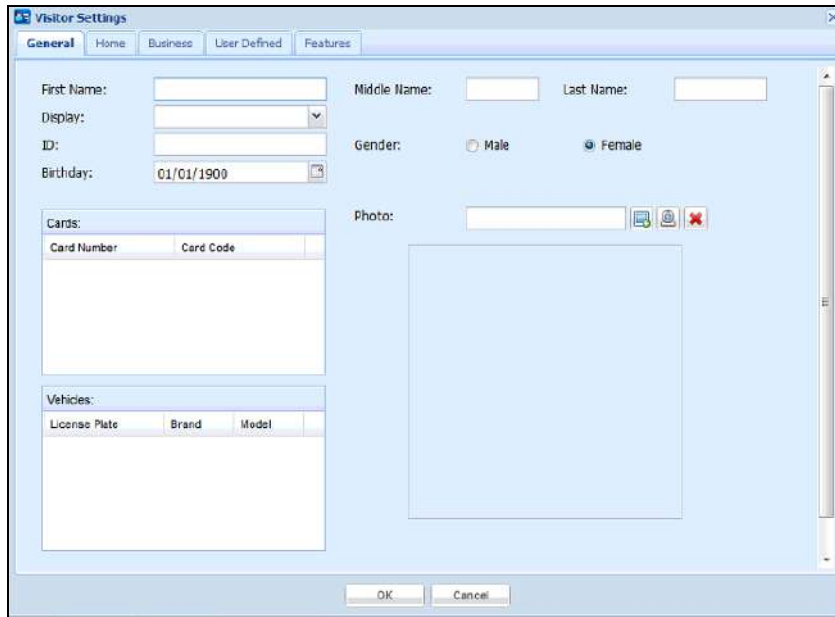


Figure 12-3

2. In the **General** tab, type the visitor's name and click **Browse** close to **Photo** to upload a photo of the visitor.
3. In the **Home** and **Business** tab, you can fill out other personal information about the visitor, such as phone number and address.
4. In the **User Defined** tab, the customized field labels will be displayed. To see how to customize the fields, see *4.6.2 Customizing a User Data Field*.
5. Click **OK**.

Note:

1. The visitor profile created will be updated to the User List in GV-ASManager.
 2. If you have a webcam installed, click the **Webcam** icon  to take a picture from the webcam. The webcam function requires Flash Player 10 or later.
-

12.5 Granting Visitor Access

After the visitor accounts are created, access permissions can be granted to visitors using the **Demands for Visit** section (No. 4, Figure 12-2). In this section, you can specify the date and time of a visit, assign an access card, a passcode or QR code to the visitor and view visit records.

To create a visit request:

1. Select a visitor account in the All Visitors section (No. 3, Figure 12-2) and click the **New** button in the Demands for Visit section (No. 4, Figure 12-2).

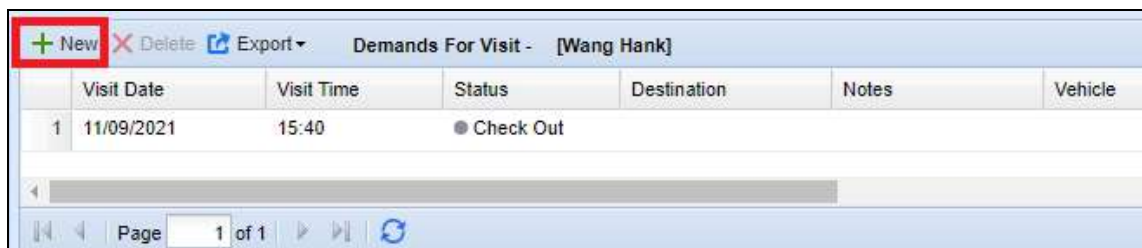


Figure 12-4

2. Select a **Visit Date** and **Visit Time** to note the time when the visitor will be visiting.
3. You can type a **Destination** and **Note** for your own reference.
4. Select the **Permit** checkbox and **Update** to grant access permission.
5. Under **Approval**, the account that permitted the access will automatically be recorded after permission is granted.

To assign a visitor card, passcode or QR code:

6. To assign a visitor card or passcode to the visitor, click the **Card Number** drop-down list. This dialog box appears.

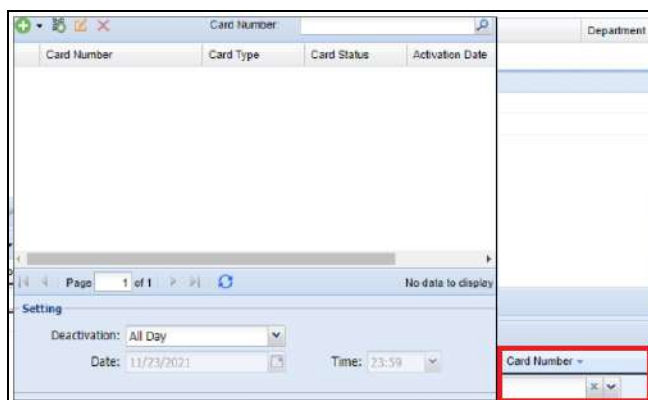





Figure 12-5

7. Click **Add**  and select **Add a New Card** or **Add a New Passcode** to create an access card or a passcode for the visitor.
8. Alternatively, to create a QR code for the visitor, click .
9. Use the **Deactivation** drop-down list to specify when the card will be deactivated.

Tip: If you have a GV-PCR310 Enrollment Reader installed, you can place the visitor card on GV-PCR310 and click **Card Reader**  to quickly identify the card number.

Note:

1. For details on adding access cards and passcodes, see [4.3.1 Adding a Single Card](#) and [4.3.3 Adding a Passcode](#), respectively.
2. The QR code function is only supported by GV-QR1352 readers and GV-FR Panel.

10. Click **Update** to continue editing the Demand for Visit entry.

To check out a visitor card:

11. The **Check In** time is when the Demand for Visit entry is created. After the visitor returns the visitor card, a security staff can return to this visit record and select the **Check Out** checkbox to record the check-out time of the visitor card on GV-VMWeb.



Figure 12-6

- Alternatively, you can choose to automatically check out the visitor card when the visitor presents the card at the entrance / exit door. For this function to work, it is required to enable the **Auto Check Out** options (On the Devices dialog box, select a controller / LPR > a Door / Lane > **Auto Check Out**).

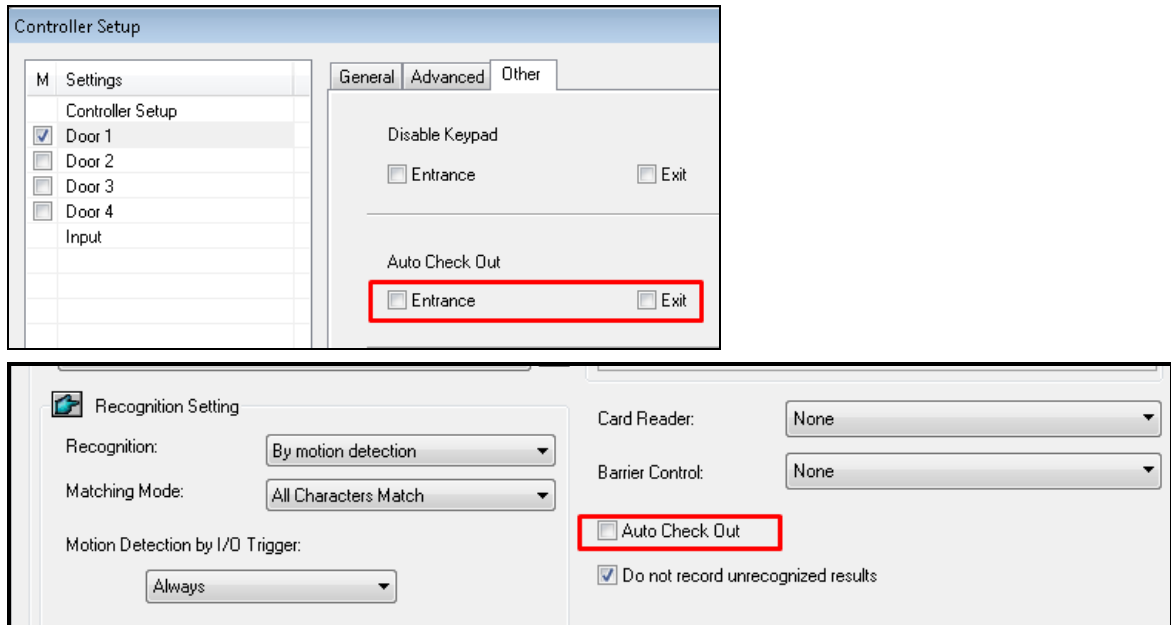


Figure 12-7

- Click **Update** to save the settings and the data will be updated to GV-ASManager.

Note:


- When using passcodes and QR codes for visitor access, the passcodes and QR codes will automatically be deleted upon checking out or after 24 hours from its check-in time.
- To edit the vehicle settings, click the  in the Vehicle field. When the visitor's vehicle enters the parking lot and the detected plate number matches the registered one, the check-in time will be recorded on GV-VMWeb.



Figure 12-8

12.6 Searching GV-VMWeb Database

To search for visitors, type the visitor's information in the **Visitor** section on the left and click the **Search** button. The search results will be listed in the **All Visitors** section. In the **Filter** section, you can filter the search of visit records by Card Number, Destination, Notes, User or the person who approved the visit.

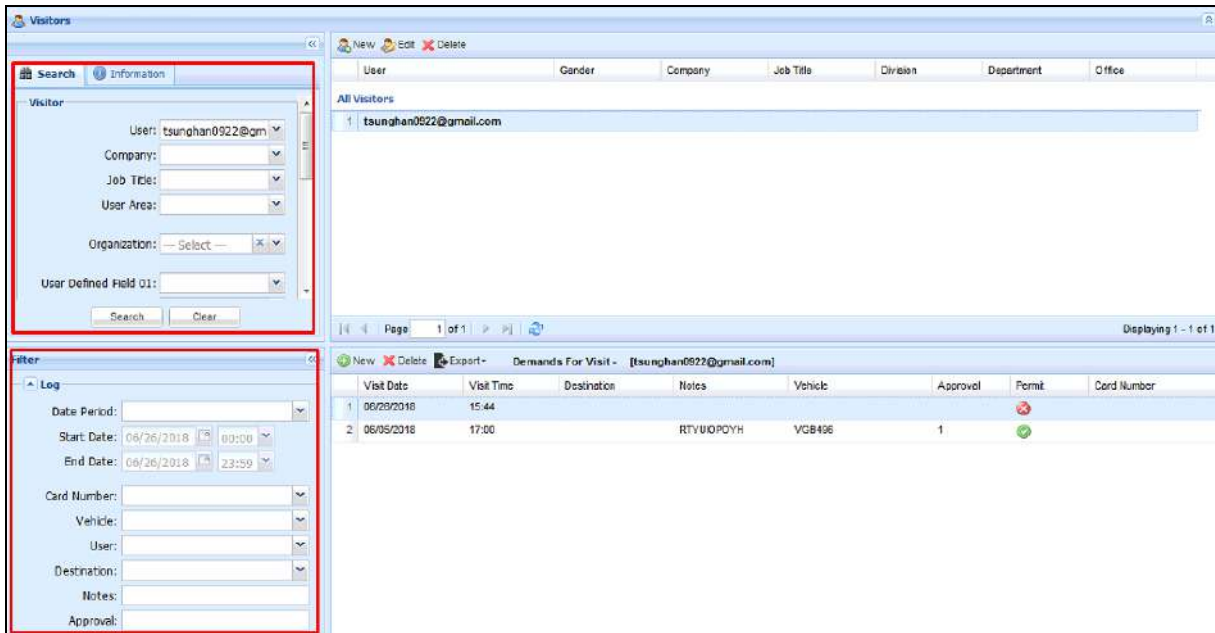


Figure 12-9

12.7 Visitor Self Registration

Visitors can create visitor accounts over the Internet and request permission to access the premises.

The administrator needs to first set up the mail server on GV-VMWeb. The visitor will be able to register a visitor account, activate the account and create a visit request. The visit request can trigger an e-mail notification to the administrator if set up, and automatically show up in GV-VMWeb for the administrator to grant or deny access.



12.7.1 Setting up Mail Server in GV-VMWeb

The mail server is used to send confirmation e-mails to visitors when they register visitor accounts. The administrator must first set up the mail server in GV-VMWeb.

1. Log in to GV-VMWeb.
2. At the upper-right corner, click **Options > Visitor Web**.

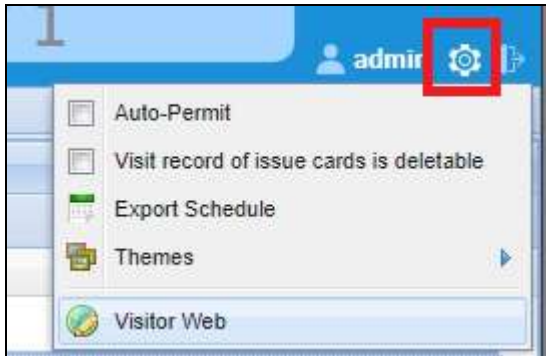


Figure 12-10

3. In the **Servers** tab, set up the mail server by entering its address, login details and port. For **HTTP Server Address**, type the IP address or the domain name of GV-ASManager.

Figure 12-11

4. In the **Confirmation E-Mail** tab, fill out the information of the **Sender** and the **Mail**. After registering a visitor account, a confirmation e-mail will be sent to the visitor and the visitor must click the activation link to confirm the account.
5. In the **Password E-Mail** tab, fill out the information of the **Sender** and the **Mail**. The visitor will be able to retrieve a forgotten password when clicking the “Forgot your password?” link on the login page. An e-mail with the password will be sent to the visitor.
6. In the **QR Code/ Passcode E-mail** tab, fill out the information of the **Sender** and the **Mail**. The visitor will be able to receive a QR code in the e-mail when the request for visit is permitted. Access will be granted when the visitor scans the QR code on the corresponding QR code reader.

Tip: To grant access through a QR code, register a visit on the **Visitor Registration** page (see *12.7.2 Creating a Visitor Account* & *12.7.3 Creating a Visit Request*) and the visitor will receive a QR code in the confirmation e-mail as a virtual visit card.

12.7.2 Creating a Visitor Account

1. Open an Internet browser, and type the IP address of GV-ASManager to be connected. The login page (Figure 12-1) appears.
2. Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** for regular connection. The Visitor Login page appears.



Figure 12-12

3. On the Visitor Login page, click **Register a Visitor Account**. This window appears.

 A screenshot of a web form titled "Register a Visitor Account". At the top left, there is a link "Back to the login page". The form has a light blue background. It contains the following fields:

- E-Mail Account: A text input field with a red border.
- Password: A text input field.
- Re-type Password: A text input field.
- Word Verification: A label "Type the characters you see in the picture below." followed by a CAPTCHA image showing the characters "aUFG4G" in a blue, stylized font. To the right of the image is a refresh icon.
- Below the CAPTCHA is another empty text input field.
- At the bottom center is a blue "Submit" button.

Figure 12-13

4. Type an e-mail address and a password for the visitor account.
5. Type the characters for word verification.
6. Click **Submit**. A confirmation e-mail will be sent to the specified e-mail address shortly. Click the activation link in the e-mail to activate the visitor account.


12.7.3 Creating a Visit Request

After the visitor account is activated, the visitor can now log into his or her account to create a visit request.

1. Open an Internet browser, and type the IP address of GV-ASManager to be connected. The login page (Figure 12-12) appears.
2. Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** for regular connection. The Visitor Login page appears.
3. Type the visitor account and password, and click **Login**. This window appears.



Figure 12-14

4. Click the **Visitor Setting** button at the upper-left corner to complete the visitor profile. See 12.3 Creating Visitor Profiles.
5. Click the **Add Visit** button . This dialog box appears.

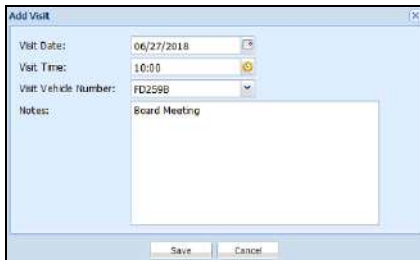


Figure 12-15

6. Specify the planned visit date, time and vehicle number if available.
7. Click **Save**.

The administrator will receive an e-mail notification if set up, and the visit request will also be displayed on GV-VMWeb. The administrator can then double-click the visit request to grant access and assign a visitor card passcode or QR code to the visitor.

Demands For Visit - [Alice]								
	Visit Date	Visit Time	Destination	Notes	Vehicle	Approval	Permit	Card Number
1	06/14/2018	10:00			G6QBB			

Figure 12-16

Note: For the administrator to receive e-mail notifications of visit requests, make sure to enter his/her e-mail address when creating the admin account. See *12.2 Creating Accounts to Manage GV-VMWeb*.

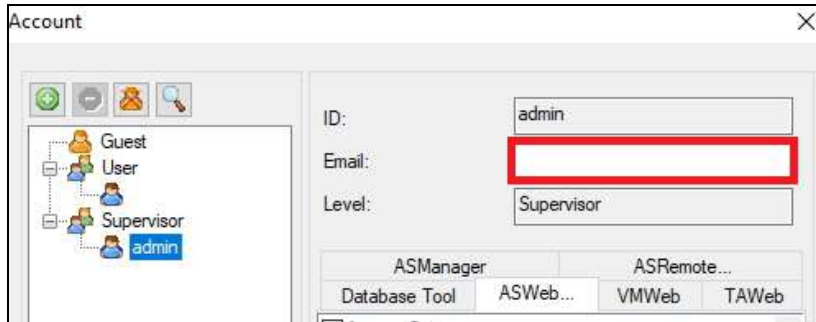


Figure 12-17

Chapter 13 License Plate Recognition

The License Plate Recognition (LPR) functions allow a **GV-LPR device** to grant access when detected license plate numbers match vehicles registered in the **GV-ASManager database**.

GV-ASManager supports connections with up to **255 devices**, including:

- Edge GV-IP LPR Cameras
- GV-DSP LPR units
- PC-based LPR systems

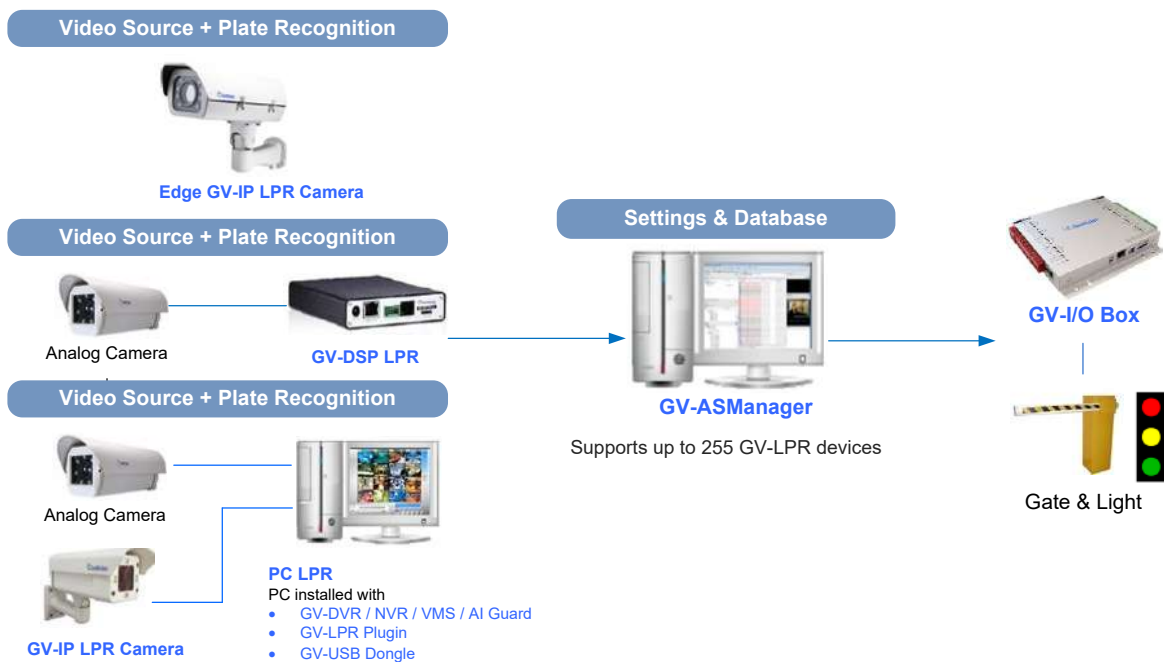


Figure 13-1

Main Screen

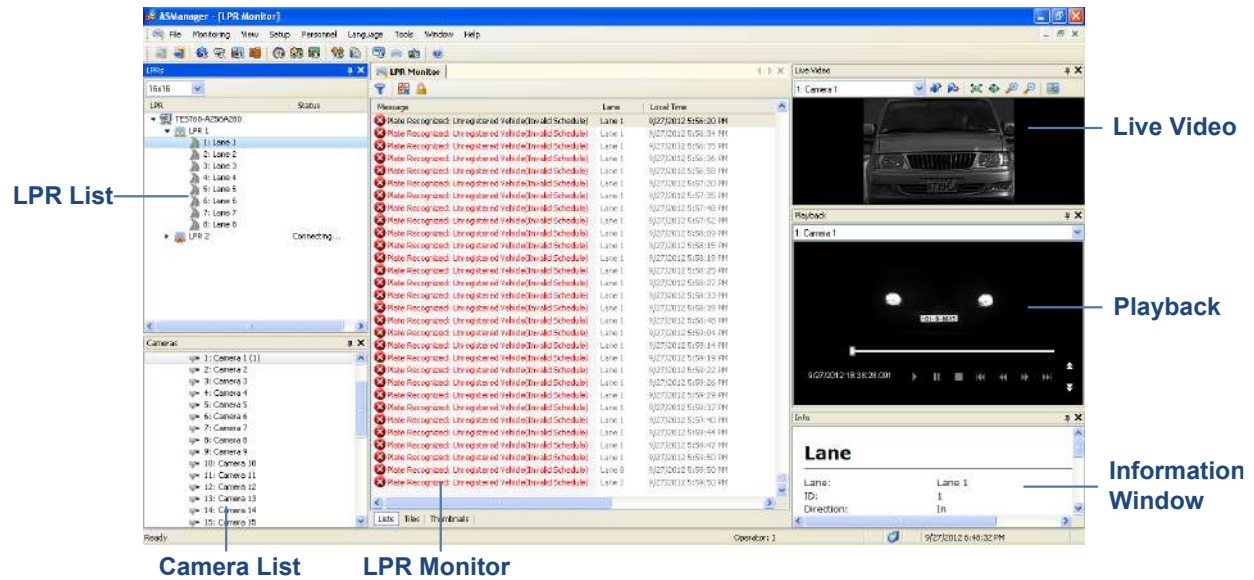


Figure 13-2

13.1 Installing PC LPR


A GV-NVR / VMS / AI Guard system can be turned into a **PC-based LPR system** simply by installing the **LPR Plugin** from the GeoVision [Website](#) and connecting an LPR Dongle.

Refer to the [datasheet](#) for the **minimum system requirements**, based on the type of LPR engine (machine learning or deep learning), the software used, and the number of channels:

1. GV-NVR / VMS V17 & V18 / AI Guard LPR (Machine Learning)
2. GV-NVR V17 & V18 / VMS / AI Guard LPR (Machine Learning) + 32CH 2MP Camera Monitoring
3. GV-VMS V17 & V18 / AI Guard LPR (Machine Learning) + 64CH 2MP Camera Monitoring
4. GV-NVR / VMS V17 & V18 / AI Guard LPR (Deep Learning)
5. GV-NVR / VMS V17 & V18 / AI Guard LPR (Deep Learning) + 32CH 2MP Camera Monitoring
6. GV-VMS V17 & V18 / AI Guard LPR (Deep Learning) + 64CH 2MP Camera Monitoring
7. GV-VMS V20 LPR (Deep Learning) + 64CH 2MP Camera Monitoring

Also refer to the [datasheet](#) for **compatibility between the software and GV-LPR Plugin**.

13.1.1 Installing LPR Plugin

1. Go to the [Download Page](#) of GV-LPR.
2. Select **Primary Applications** from the drop-down list, and
3. Click the **Download** icon  of **GV-LPR Plugin**.

Note: LPR Dongles can be used in conjunction with GV-VMS Software Licenses.

13.1.2 Inserting LPR Dongle

To see recognition results, the LPR Dongle needs to be inserted to the computer of GV-DVR / NVR / VMS / AI Guard. Both internal and external dongles are available. The dongle options include 1, 2, 3, 4, 5, 6, 7, 8 channels.

The following types of USB Dongles are available:

- GV-LPR with GV-DVR / NVR / VMS / AI Guard (Black, Blue)
- GV-LPR with Video Capture Card (Black, Blue)

Note:

1. Each recognition camera counts as 1 channel. For example, if you set up 4 recognition cameras for a single LPR lane, you will need a 4-ch LPR Dongle.
 2. When multiple LPR Dongles are inserted, the dongle that supports the most number of channels will be applied. The number of channels supported on each dongle will **not** be combined.
 3. If no LPR Dongle is inserted, license plates will be captured but the plate numbers will not be recognized.
-

13.1.3 Accessing Recognition Results in PC LPR

LPR Plugin comes with a tool that allows you to access the snapshots and recognized plate numbers of the detected license plate. When installing LPR cameras for the first time, you can use this tool to see the recognition results and make sure the cameras have been set up correctly.

1. Open the folder of GV-DVR / NVR / VMS / AI Guard and run **TestRecogPicView.exe**. The upper row is the live view of channels 1 to 4 and the lower row shows the snapshots of any license plates detected. The recognized plate numbers and the height of the captured license plate in pixels are displayed under the snapshots.



Figure 13-3

2. To see the results from channels 5 to 8, click **Switch Page** to switch to page 2.
3. To manually force a PC LPR to detect license plates, click the **Test** buttons.

13.2 Adding PC LPR

To add a PC LPR to GV-ASManager, follow the steps below:

- **Step 1 Enabling LPR Functions on a PC LPR**

Enable the recognition cameras and/or the overview cameras on a PC LPR.

- **Step 2 Adding a PC LPR to GV-ASManager**

Establish the communication between GV-ASManager and a PC LPR.

- **Step 3 Configuring a Channel**

Configure the recognition conditions of a camera channel.

Note: For optimal recognition results, the cameras used should be the ones designed for license plate recognition, such as [GeoVision's LPR Camera Series](#).

13.2.1 Step 1: Enabling LPR Functions in the PC LPR

To enable license recognition in GV-DVR LPR, click the **Configure** button > **Video Analysis**, > **License Plate Recognition** to access the following LPR functions.

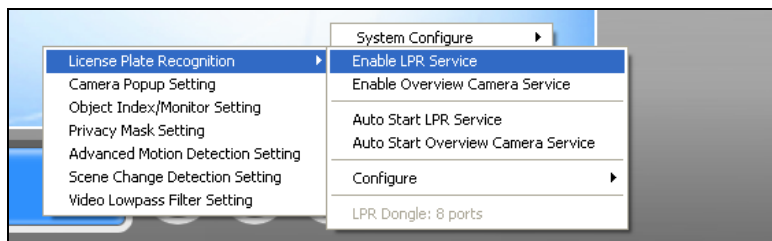





Figure 13-4

To enable license recognition in GV-VMS LPR, click the **Home** button  > **Toolbar**  > **Tools**  > **License Plate Recognition** to access the following LPR functions.

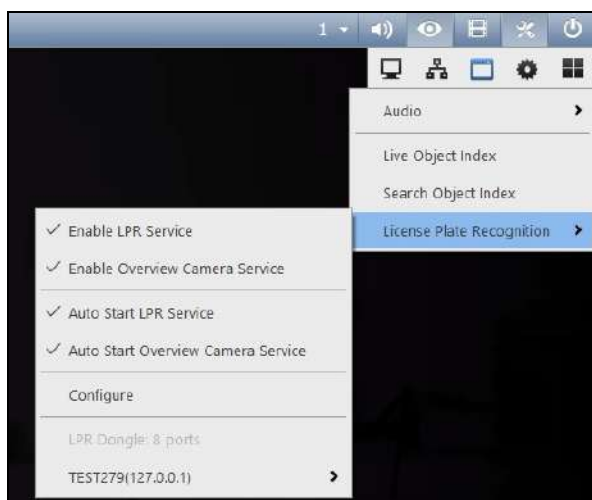


Figure 13-5

- **Enable LPR Service:** Enable recognition of license plates in the Recognition Camera.
- **Enable Overview Camera Service:** Allow GV-ASManager to use the cameras connected to GV-DVR/ NVR / VMS as overview cameras.
- **Auto Start LPR Service:** Automatically start LPR Service upon system startup.
- **Auto Start Overview Camera Service:** Automatically start Overview Camera Service upon system startup.
- **Configure:** Allow LPR data export. See 13.2.4 *Exporting LPR Data*.

13.2.2 Step 2: Adding a PC LPR to GV-ASManager

1. On the menu bar, click **Setup > Devices**. The Devices dialog box appears.
2. Under **Device Group**, define a group for the LPR device to be added. Otherwise, use the **Default** group.

Note: The devices (Controller, LPR, I/O Box and Camera) under the same Device Group will be applied with the identical settings of Time Zones, Weekly Schedules, Access Groups, Holidays, Door Groups and Parking Lots.

3. Right-click **LPR > New LPR**.

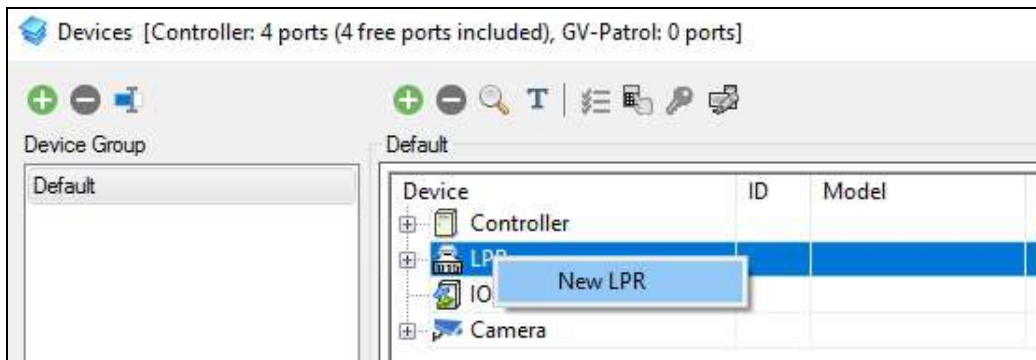


Figure 13-6

4. Type **ID** and **Name** of the LPR device, select **PC LPR** and click **OK**.

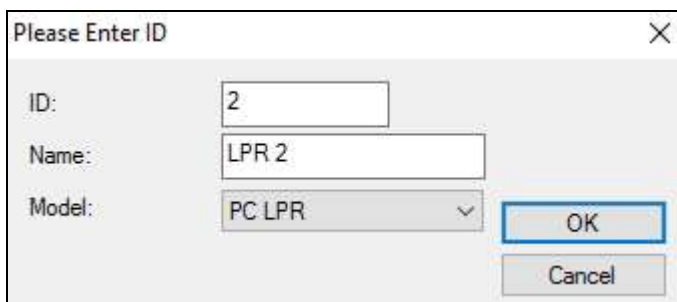



Figure 13-7

5. Set up the following connection information.

Name	Value
Country	Global
Version	6020
LPD Confidence	3
Hardware Acceleration	Enable
Max. number of logs per folder	999
Max. number of lines per log file	999
Log: API	Enable
Log: Recognition	Disable
Log: Recognition upon I/O tri...	Disable
Log: Video input	Disable
Log: Result export	Disable
Log: FPS	Disable
Saving image: Unidentifiable i...	Disable
Saving image: Identifiable ima...	Disable
Saving image: Min. free spac...	2048
Saving image: Number of ima...	1000

Figure 13-8

[Connection] Type the **IP Address**, **User Name** and **Password** of the PC LPR. You can also click the **Search** button  to search for PC LPR in the same LAN.

- **Command Port:** The default value is 3388.
- **Data Port:** The default value is 5611.
- **Log Port:** The default value is 5552.
- **Number of Cameras:** Select the number of cameras supported by the PC LPR.

[Camera Box] On the box, select a camera to modify its name.

[LPR Engine] Select the **Country** of the recognition engine. You can also modify the log-related settings to change how and what information is stored for debug purposes.

13.2.3 Step 3: Configuring a Channel

1. To configure a channel, select a **Lane** tab. This dialog box appears.

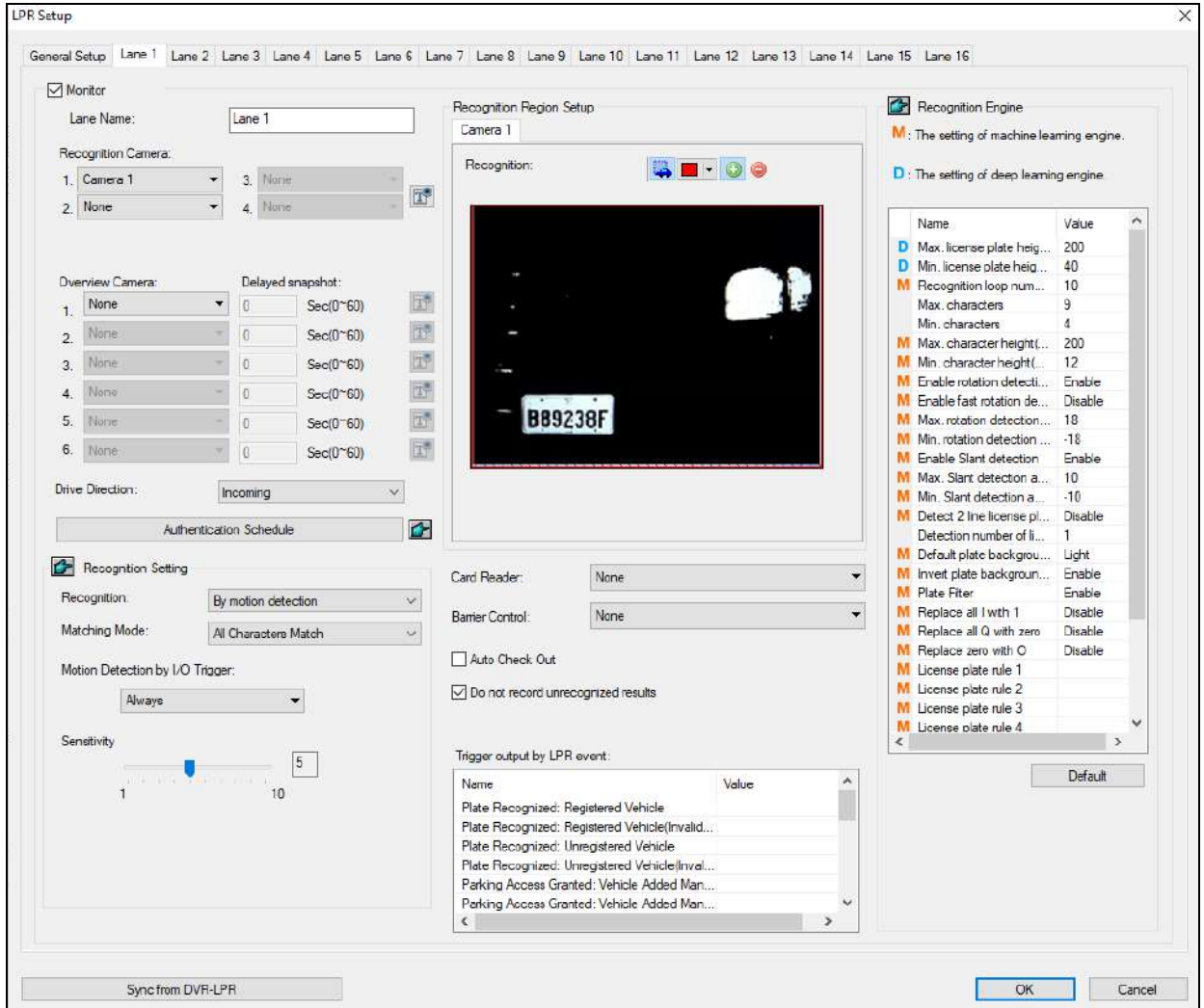


Figure 13-9

2. Select **Monitor** to enable the following settings.

Note: To apply the current settings of the connected PC LPR, click **Sync from DVR LPR** at the bottom-left side and skip to step 9.

[Recognition Camera] Select up to four **Recognition Cameras** connected to the PC LPR. Having more than 1 camera is useful when the width of the lane requires multiple cameras. If multiple cameras recognize the same license plate at the same time, the data will be recorded as 1 record.

Note: The resolution of the recognition camera needs to be at least D1. Each recognition camera counts as 1 channel. If you set up 4 recognition cameras for a single LPR lane, you will need a 4-ch LPR license.

[Overview Camera] Select up to six **Overview Cameras** connected to the PC LPR to capture the overall appearance of a vehicle. Under **Delayed snapshot**, you can type the number of seconds to delay the snapshot capturing after the license plate is recognized.

[Driver Direction] Select **Incoming** to designate the lane as the entrance of the parking lot or select **Outgoing** to set the lane as the exit of the parking lot.

[Authentication Schedule] Optionally, set up the schedule for different access modes at different time periods. By default, it is **License Plate Mode** that requires vehicles with authorized plate numbers to be recognized for access granted.

- **License Plate Mode:** Access can only be granted by license plate recognition for time periods defined under this mode.
- **Card Mode:** Access can only be granted by access cards for time periods defined under this mode.
- **License Plate or Card Mode:** Access can be granted by either license plate recognition or access cards for time periods defined under this mode.
- **License Plate and Card Mode:** Access requires both license plate recognition and access cards for time periods defined under this mode.

Note: The license plate number recognition is required to load logs containing the corresponding access card number under **License Plate or Card Mode** or **License Plate and Card Mode** when using standalone LPR devices.

[Recognition Setting]

- **Recognition:** Select to recognize license plates upon **motion detection** or **I/O detection**. For I/O detection, the PC LPR will only capture 1 license plate per I/O trigger.
- **Matching Mode:** Select **All Characters Match** to grant access when the recognized license plate matches a registered license plate completely. When **Allow 1 mismatched character** or **Allow 2 mismatched characters** is selected, 1 or 2 mismatched characters will be tolerated but not being the first and last characters. For example, license plate ABC-123 will be considered matching with AZC-223 when Allow 2 mismatched characters is selected.

- **Motion Detection by I/O Trigger:** When **Always** is selected, the PC LPR will always recognize license plates upon motion detection. If an **Input** is selected, the PC LPR will only recognize license plates when the assigned input is triggered. Multiple license plates can be captured during an input trigger.
- **Sensitivity:** Adjust the sensitivity level of motion detection.
- **Sensor:** Select the input sensor for I/O detection.
- **Delay after trigger:** Delay recognition for the number of milliseconds specified after I/O trigger.
- **Repeat Recognition:** Repeat recognition until the number of seconds specified in **Time out**. You can also set the PC LPR to **Continue recognizing until a registered vehicle is recognized**.

[Recognition Region Setup] Define the recognition area for each camera if needed.

[Card Reader] Optionally, use the drop-down list to select a card reader where the user is required to present a valid card when under Card Mode.



Note: For details on how to connect the PC LPR to a Wiegand Card Reader, click [here](#).

[Barrier Control] Use the drop-down list to select an output device to be a gate barrier. The output device will be triggered when the recognized license plate matches a registered license plate.

[Auto Check Out] Optionally, select this option to record the check-out time on GV-VMWeb when the visitor's vehicle exits the parking lot.

[Do not record unrecognized results] Enabled by default. Select to omit unrecognized results.

[Trigger output by LPR event] Optionally, click the fields under **Value** to assign output devices to trigger when the LPR events occur.

3. Click **OK** to apply the above settings and return to the main screen. If the icon  appears in the LPR view window, it indicates the connection between the PC LPR and GV-ASManager has been established. If the icon  appears, it indicates the connection failed. Then make sure the above connection setup is correctly configured.

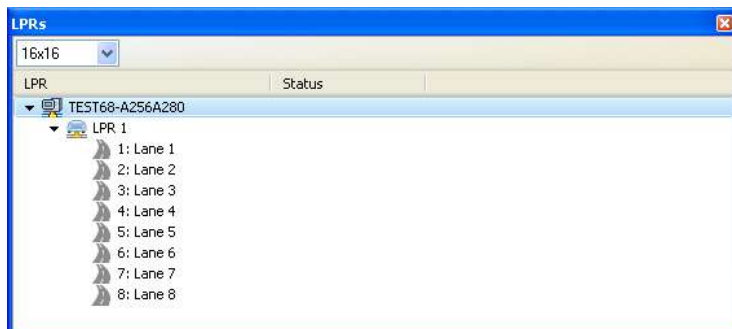


Figure 13-10

Under **Recognition Engine**, you can adjust the following settings of Recognition Engine when necessary.

IMPORTANT: Aside from changing the Country of recognition engine, it is highly recommended not to modify any parameters within Recognition Engine settings.

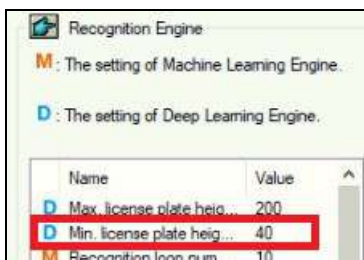
[LPR Engine] Settings for storing data/logs related to the LPR engine.

- **Max. number of logs per folder:** The maximum number of log files within each folder, from 200 ~ 999 (default = 999).
- **Max. number of lines per log file:** The maximum number of lines allowed within each log file, from 200 ~ 999 (default = 999).
- **Log: API:** Enabled by default, records API-related logs.
- **Log: Recognition:** Disabled by default, records recognition-related logs.
- **Log: Recognition upon I/O trigger:** Disabled by default, records logs related to recognition triggered by I/O.
- **Log: Video input:** Disabled by default, records video input-related logs.
- **Log: Result export:** Disabled by default, records result export-related logs.
- **Log: FPS:** Disabled by default, records FPS-related logs.
- **Saving image: Unidentifiable image:** Enabled by default, saves images captured containing unidentifiable license plates.
- **Saving image: Identifiable image:** Enabled by default, saves images captured containing identifiable license plates.
- **Saving image: Min. free space (MB):** The minimum hard disk space that must be kept for saving images, from 2048 ~ 9999 (default = 2048).
- **Saving image: Number of images per folder:** The number of images that can be stored within a folder, from 1000 ~ 9999 (default = 1000).

[Deep Learning] Settings for deep-learning LPR engine.

- **LPD Confidence:** The value of license plate detection sensitivity, from 1 ~ 5, with 1 being the most sensitive (default = 3).
- **Hardware Acceleration:** Enabled by default, utilizes GPU decoding for enhanced performance and reduced CPU loading.
- **Max. / Min. license plate height (pixels):** Set the maximum, from 12 ~ 999 (default = 200), or minimum, from 1 ~ 999 (default = 40), height of license plate images to activate the recognition process. If the image height exceeds the maximum or is under the minimum, the system will not start recognition.

Note: When the resolution of images sent to the system exceeds 2 MP, it is necessary to change **Min. license plate height (pixels)**. The setting rule is that the image height in pixels must be greater than [image resolution x 20]. For example, set the **Min. license plate height (pixels)** to 60 pixels for 3 MP and 80 pixels for 4 MP.



[Machine Learning] Settings for machine-learning LPR engine.

- **Recognition loop number:** Repeat recognition for the number of times specified, from 1 ~ 20 (default = 10).
- **Max. / Min. characters:** Set the maximum, from 3 ~ 16, or minimum, from 2 ~ 16, number of characters on the license plate to activate the recognition process. If the number of characters exceeds the maximum or is under the minimum, the system will not start the recognition. The default values of max. and min. are dependent on the country of recognition engine.
- **Max. / Min. character height:** You can set the maximum, from 12 ~ 999 (default = 120), and minimum, from 1 ~ 999 (default = 16), height of characters on the license plate in pixels to activate the recognition process.
- **Enable rotation detection:** Enabled by default, License plates tilted horizontally can be detected.
- **Enable fast rotation detection:** Disabled by default, this option can increase the recognition speed by 10 % but decrease the accuracy by 3%.

- **Max. / Min. rotation detection angle:** Set the maximum, from 10 ~ 90 (default = 10) and minimum, from -90 ~ -1 (default = -10), tilt angle to be allowed to activate the recognition process.
- **Enable Slant Detection:** Enabled by default, License plates tilted vertically can be detected.
- **Max. / Min. slant detection angle:** Set the maximum, from 1 ~ 90 (default = 10) and minimum, from -90 ~ -1 (default = -10), tilt angle to activate the recognition process.
- **Detect 2 line license plate:** Disabled by default, recognize two rows of characters on license plates. Note this option is only available on engine versions of V5000 or later.
- **Detection number of license plates:** Set the maximum number of plates to be recognized simultaneously, from 1 ~ 8 (default = 1).
- **Default plate background color:** **Light** by default, to only recognize plates with white characters on dark background, or select **Dark** to only recognize plates with dark characters on white background. This function is only supported when **Global** or **China** is selected for Country.
- **Invert plate background color:** Enabled by default, to invert plate color when the license plate cannot be recognized. This function is only supported when **Global** or **China** is selected for Country.
- **Replace I with 1:** Disabled by default, always identify the character “I” as “1” (one).
- **Replace zero with O:** Disabled by default, always identify the character “0” as “O” (letter O).
- **Replace Q with zero:** Disabled by default, always identify the character “Q” as “0” (zero). Note this option is only available on engine versions of V5000 or later.
- **License Plate Rule:** None set by default, you can customize up to six plate number formats and the recognized plates will be converted to similar characters to follow the format. The format must use 4 and 9 characters and consists of “A” (Alphabets), “D” (Numeric digits) and “X” (Any). For example, if you set up a format “AA-DDDD”, a license plate detected as XY-123A will be converted to XY-1234. If the detected plate number does not fit in the format, the rule won’t be applied.

Note:

1. The total number of recognition cameras and overview cameras connected per GV-DVR / NVR / VMS cannot exceed 16 cameras.
 2. The Overview Cameras need to be set to round-the-clock recording on GV-DVR / NVR / VMS.
-

3. To ensure optimal performance, the total number of Overview Cameras supported in a GV-DVR / NVR / VMS is limited based on the resolution of the overview cameras:
 - Overview camera: D1 = maximum 16 overview cameras
 - Overview camera: 1 MP = maximum 8 overview cameras
 - Overview camera: 2 MP = maximum 4 overview cameras
 - Overview camera: 3 MP = maximum 3 overview cameras
 - Overview camera: 4 MP = maximum 2 overview cameras
 - Overview camera: 5 MP = maximum 1 overview camera
4. To open a gate when the detected license plate is recognized as a registered vehicle:
 - A. Set up I/O devices on GV-DVR LPR / GV-VMS LPR (**Configure** button > **Accessories** > **I/O Device** > **I/O Device Setup**). Refer to *6.1 Setting up I/O Devices* in GV-DVR or GV-VMS User's Manual to see how to set the gate as the output device.
 - B. Select the output device under **Barrier Control**.

13.2.4 Exporting LPR Data

You can export LPR data to other machines, such as a parking lot ticket machine. There are two ways to export the data, through RS-232 connection or export into a file that can be imported into a third-party program. The Export Setting also allows you to customize a storage path to store captured license plates.

In GV-DVR LPR, click the **Configure** button > **Video Analysis** > **License Plate Recognition** > **Configure** > **Export Setting**.

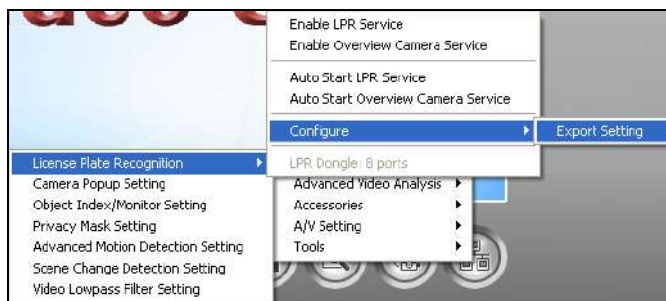





Figure 13-11

In GV-VMS LPR, click the **Home** button  > **Toolbar**  > **Tools**  > **License Plate Recognition** > **Configure** > **Export Setting**.

Export through RS-232

1. To connect the PC LPR system to a machine using RS-232 connection, click the **Export Through RS232** tab and select **Enable Export through RS232**.

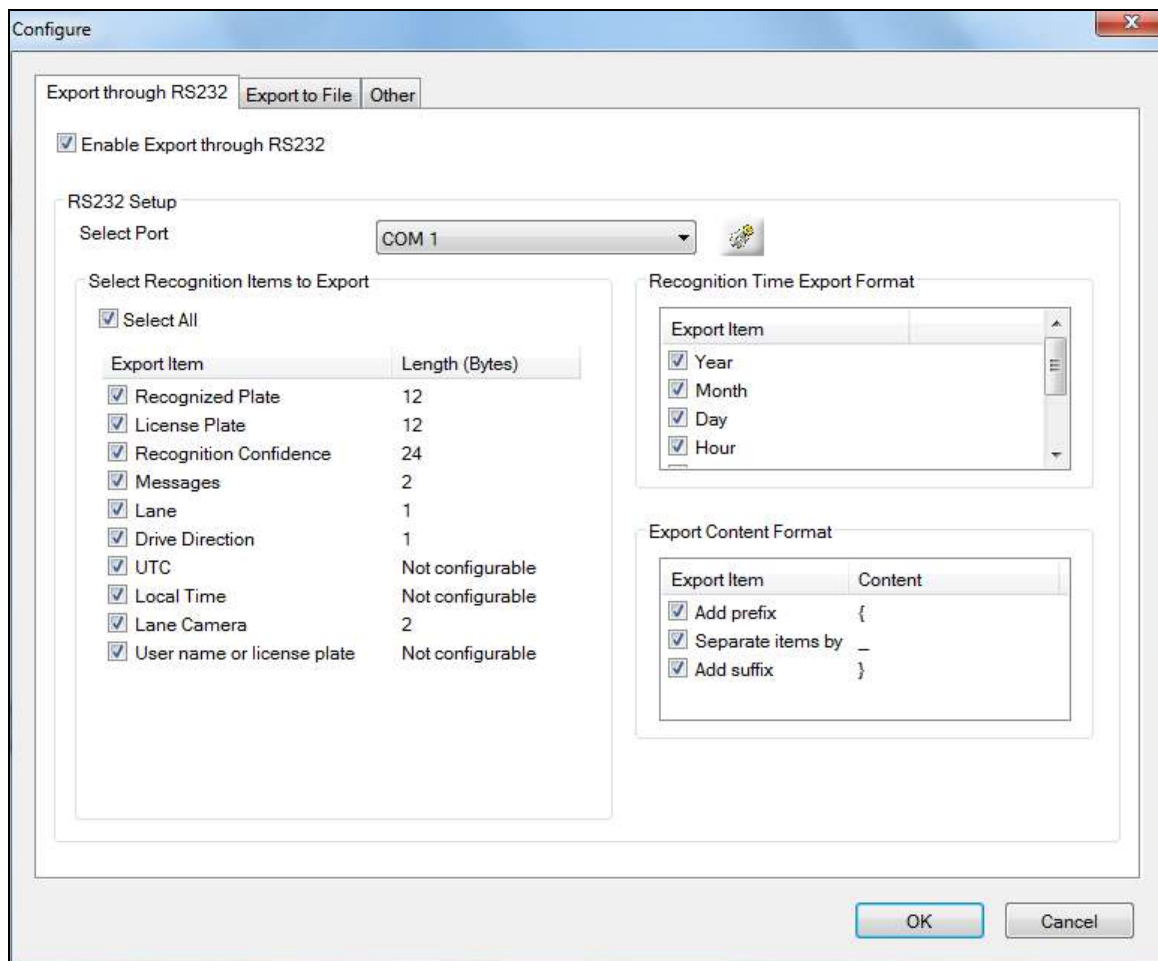


Figure 13-12

2. Next to **Select Port**, select the COM port that is used for connection.
3. Under **Select Recognition Items to Export**, select the LPR data you want to export.
4. Under **Length (Bytes)**, you can click the number to specify the length of the data you want to display.
5. Under **Recognition Time Export Format**, select how detailed you want the time information to be.
6. Under **Export Content Format**, you can add text or symbols to the beginning or the end of the LPR data. You can also separate each item with the text or symbol specified.
7. Click **OK**.

Export into a File

1. To export a TXT file to the machine, click the **Export to File** tab and select **Enable File Export**.

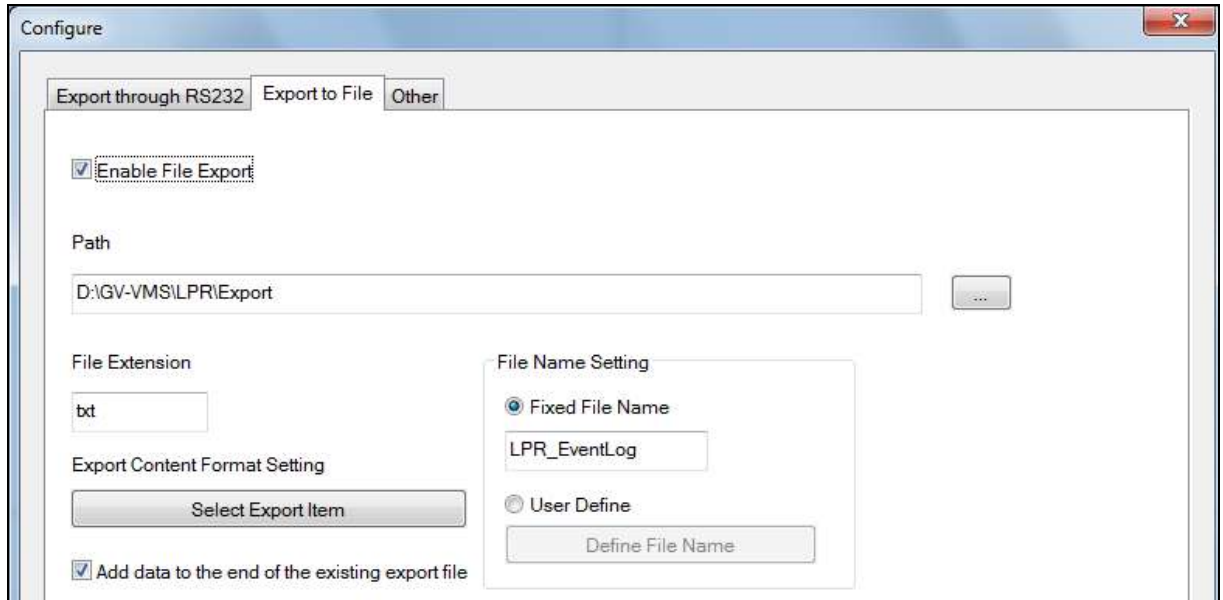


Figure 13-13

2. Select a storage **Path** to store the exported file by clicking the ... button.
3. Under **File Extension**, you can change the default **txt** file extension if needed.
4. To select what items to export, click **Select Export Item** button.

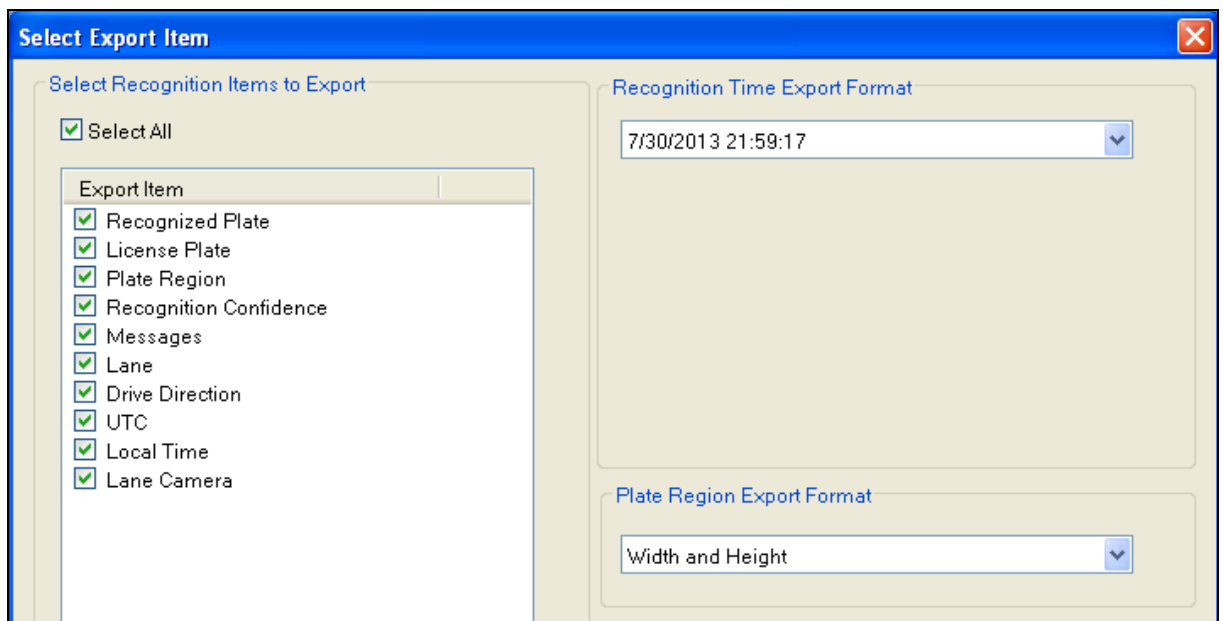


Figure 13-14

- a. Select the items you want to export.

- b. Use the **Recognition Time Export Format** to select how you want to display the recognition time.
 - c. Use the **Plate Region Export Format** drop-down list to specify how you want to display the position of the license plate detected.
 - d. Click **OK**.
5. Under File Name Setting,
- You can use a **Fixed File Name**.
 - To define your own file name, select **User Define** and click the **Define File Name** button. Next, select the data you want listed in the file name.

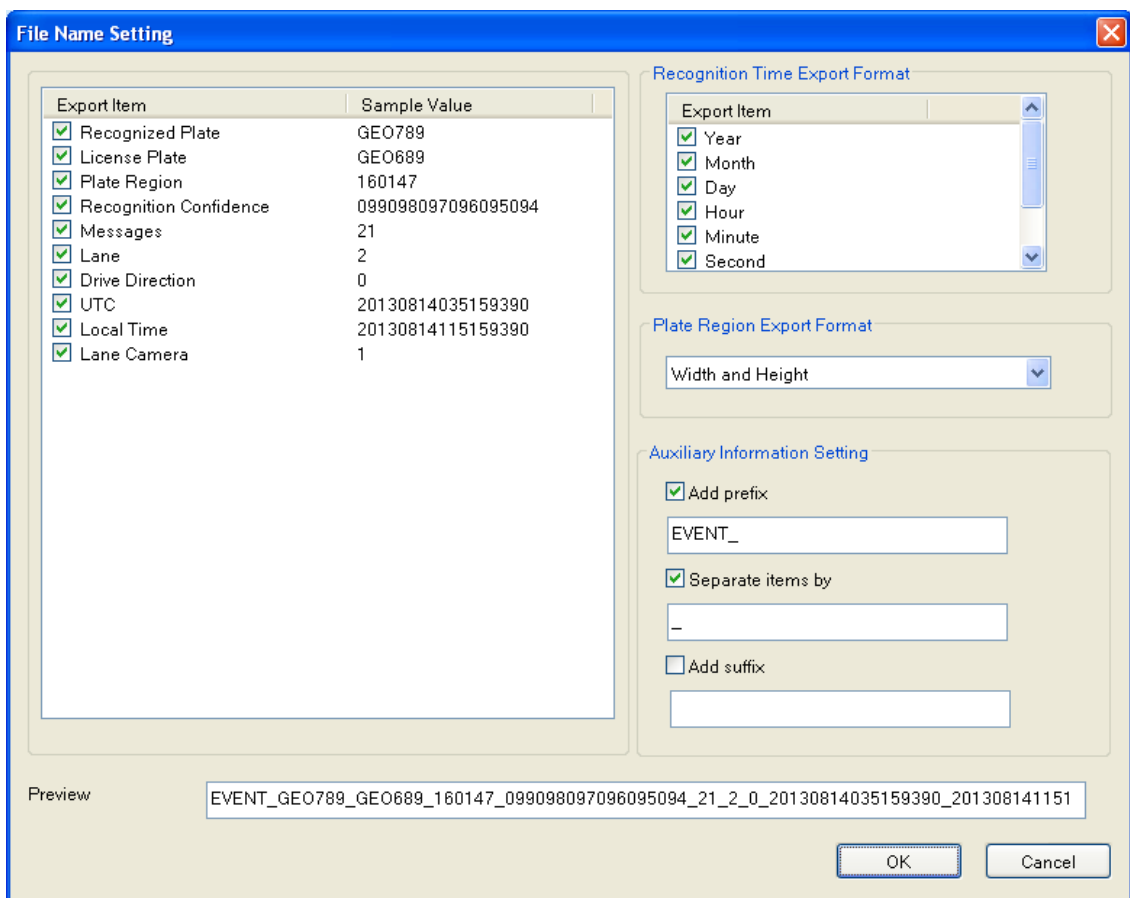


Figure 13-15

6. To add the new export data to the end of the existing export file, click **Add data to the end of the existing export file**. If this option is not selected, the old data will be overwritten.
7. Click **OK**.

Customize a Storage Path for Captured License Plates

1. Click the **Other** tab.

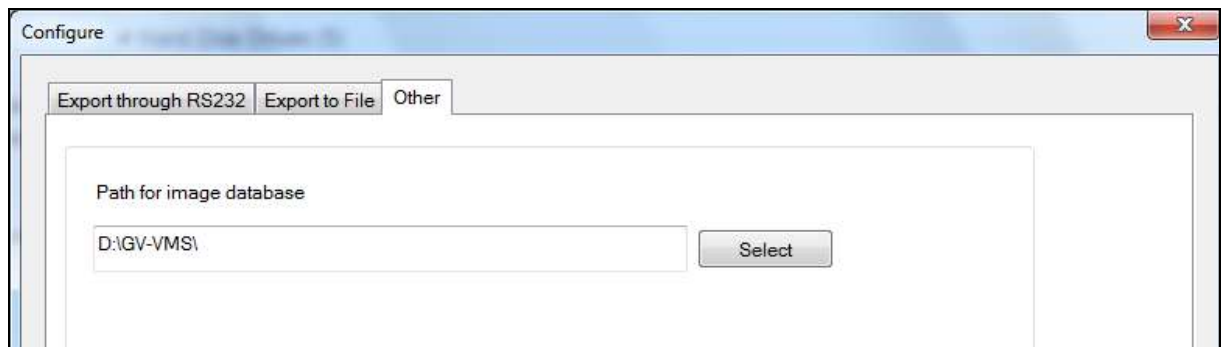


Figure 13-16

2. Click **Select** to select a folder for storing captured license plates.
3. Click **OK**.

13.3 Adding Standalone LPR

To add standalone LPR devices to GV-ASManager, follow the steps below.

- **Step 1 Enabling Connection with GV-ASManager**
Enable connection with GV-ASManager, exemplified using GV-DSP LPR / GV-LPR1200.
- **Step 2 Adding a Standalone LPR to GV-ASManager**
Establish the communication between a standalone LPR and GV-ASManager.
- **Step 3 Configuring a Channel**
Configure the recognition conditions of a camera channel.

13.3.1 Step 1: Enabling Connection with GV-ASManager

To enable connection with GV-ASManager on GV-DSP LPR / GV-LPR1200, first make sure a SD card is inserted to the standalone LPR and formatted. Next, go to the Web interface of the standalone LPR and follow the steps below.

1. In the left menu under Events and Alerts, select **Registry Database**. This dialog box appears.

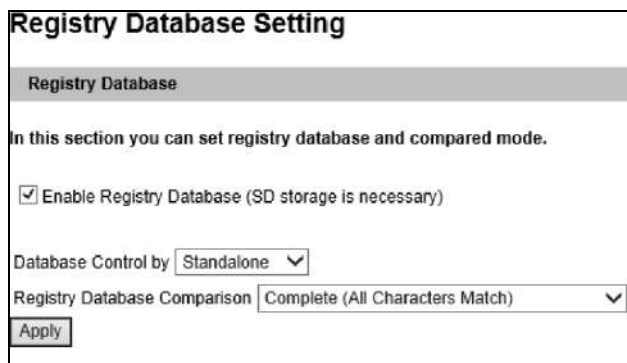


Figure 13-17

2. Select **Enable Registry Database**.
3. Select **AS Manager** for Database Control to allow the vehicle database transmitted from GV-ASManager and save on the memory card.
4. Use the **Registry Database Comparison** drop-down list to select one of these options:
 - **Complete (All Characters Match):** License plates are only considered as recognized when all characters are matched.
 - **Like (One Character Mismatch):** Recognition results can tolerate 1 mismatched character not being the first or the last character.
 - **Somewhat Like (Two Characters Mismatch):** Recognition results can tolerate 2 mismatched characters not being the first and the last character.
5. Click **Apply**.

To set the Recognition Engine and recognition conditions, recognition sensitivity for example, refer to the *Detection Mode* and *Recognition Engine Settings* in Chapter 4 of the *GV-DSP LPR User Manual*, and Chapter 4 of the *GV-IP LPR Camera User Manual*.

To open a gate when the detected license plate is recognized as a registered vehicle, refer to *Output Setting* in the *GV-DSP LPR User Manual* and the *GV-IP LPR Camera User Manual* to see how to set the gate as the output device.

13.3.2 Step 2: Adding Standalone LPR to GV-ASManager

1. On the menu bar, click **Setup > Devices**. The Devices dialog box appears.
2. Under **Device Group**, define a group for the controller to be added. Otherwise, use the **Default** group.

Note: The devices (Controller, LPR, I/O Box and Camera) under the same Device Group will be applied with the identical settings of Time Zones, Weekly Schedules, Access Groups, Holidays, Door Groups and Parking Lots.

3. Right-click **LPR > New LPR**.

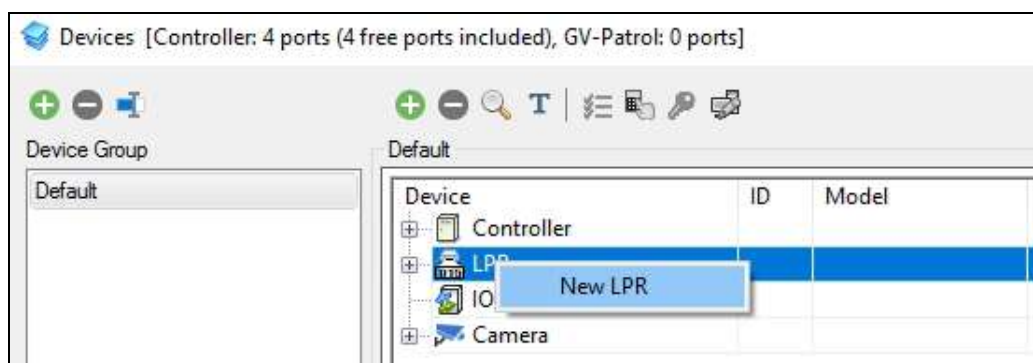


Figure 13-18

4. Type **ID** and **Name** of the LPR device, select **Standalone LPR** and click **OK**.

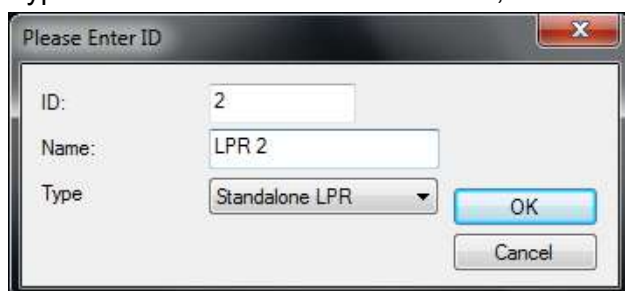


Figure 13-19

5. Set up the following connection information.

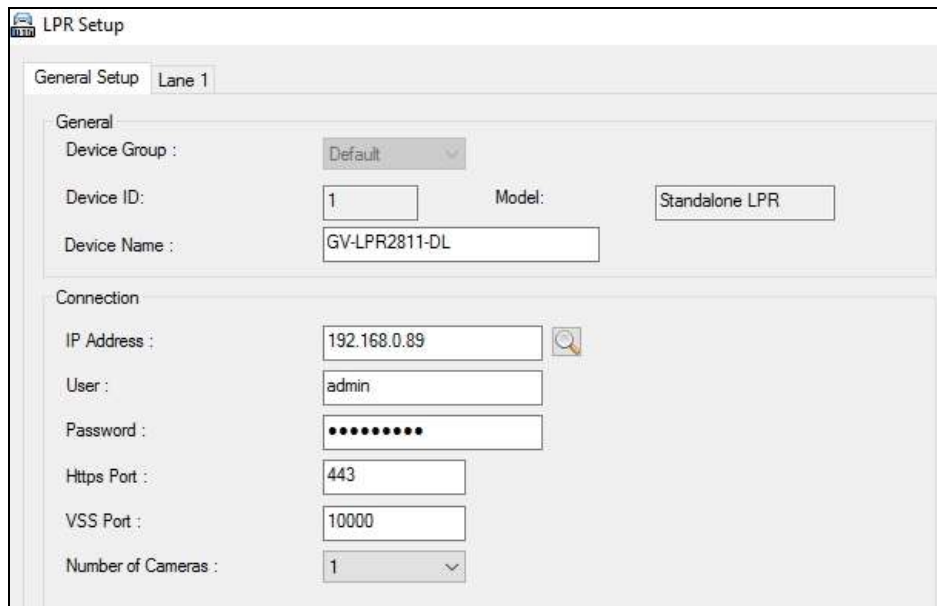



Figure 13-20

[Connection] Type the **IP Address**, **User Name** and **Password** of the standalone LPR. You can also click the **Search** button  to search for standalone LPR in the same LAN.

- **Https Port:** The default value is 443.
- **VSS Port:** The default value is 10000.

13.3.3 Step 3: Configuring a Channel

1. To configure a channel, select the **Lane 1** tab. This dialog box appears.

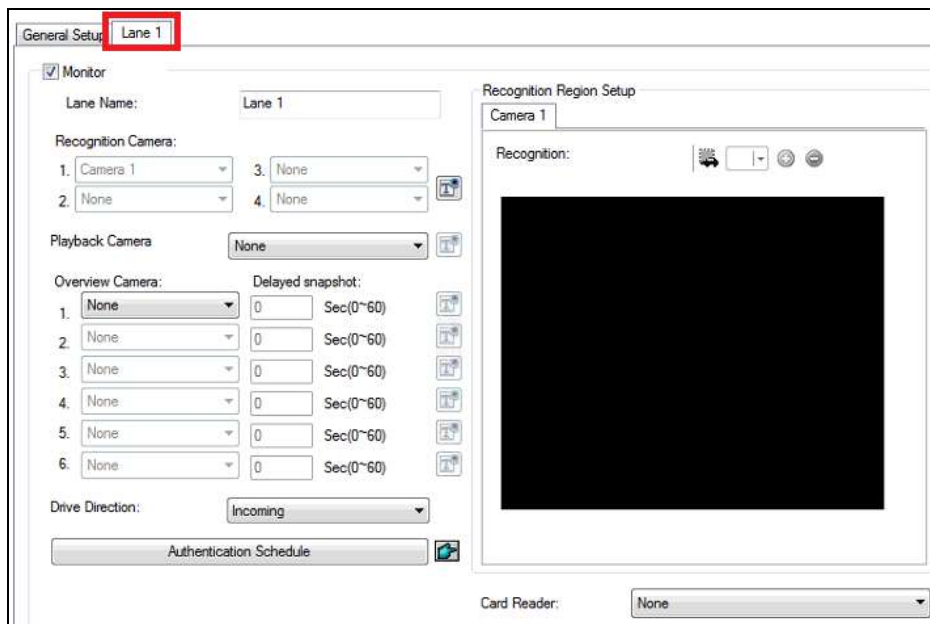


Figure 13-21

2. Select **Monitor** to enable the following settings.

[Playback Camera] The playback camera needs to be from GV-DVR / NVR / VMS and GV-DVR / NVR / VMS needs to be added to the camera list in GV-ASManager. When you select an event in the monitoring window, GV-ASManager can play back the camera view recorded at the time of the event. See *5.5 Retrieving Recording Video* for details.

[Overview Camera] Select up to six **Overview Cameras** to capture the overall appearance of a vehicle. The overview cameras must be from GV-DVR / NVR / VMS with GV-LPR Plugin installed and the **Enable Overview Camera Service** function enabled (see Figure 13-5).

[Drive Direction] Select **Incoming** to assign the lane as the entrance of the parking lot or select **Outgoing** to set the lane as the exit of the parking lot.

[Authentication Schedule] Optionally, set up the schedule for different access modes at different time periods. By default, it is **License Plate Mode** that requires vehicles with authorized plate numbers to be recognized for access granted. See the same function in *13.2.3 Step 3: Configuring a Channel*.

[Recognition Region Setup] Define the recognition area for the camera if needed.

[Card Reader] See the same function in *13.2.3 Step 3: Configuring a Channel*.

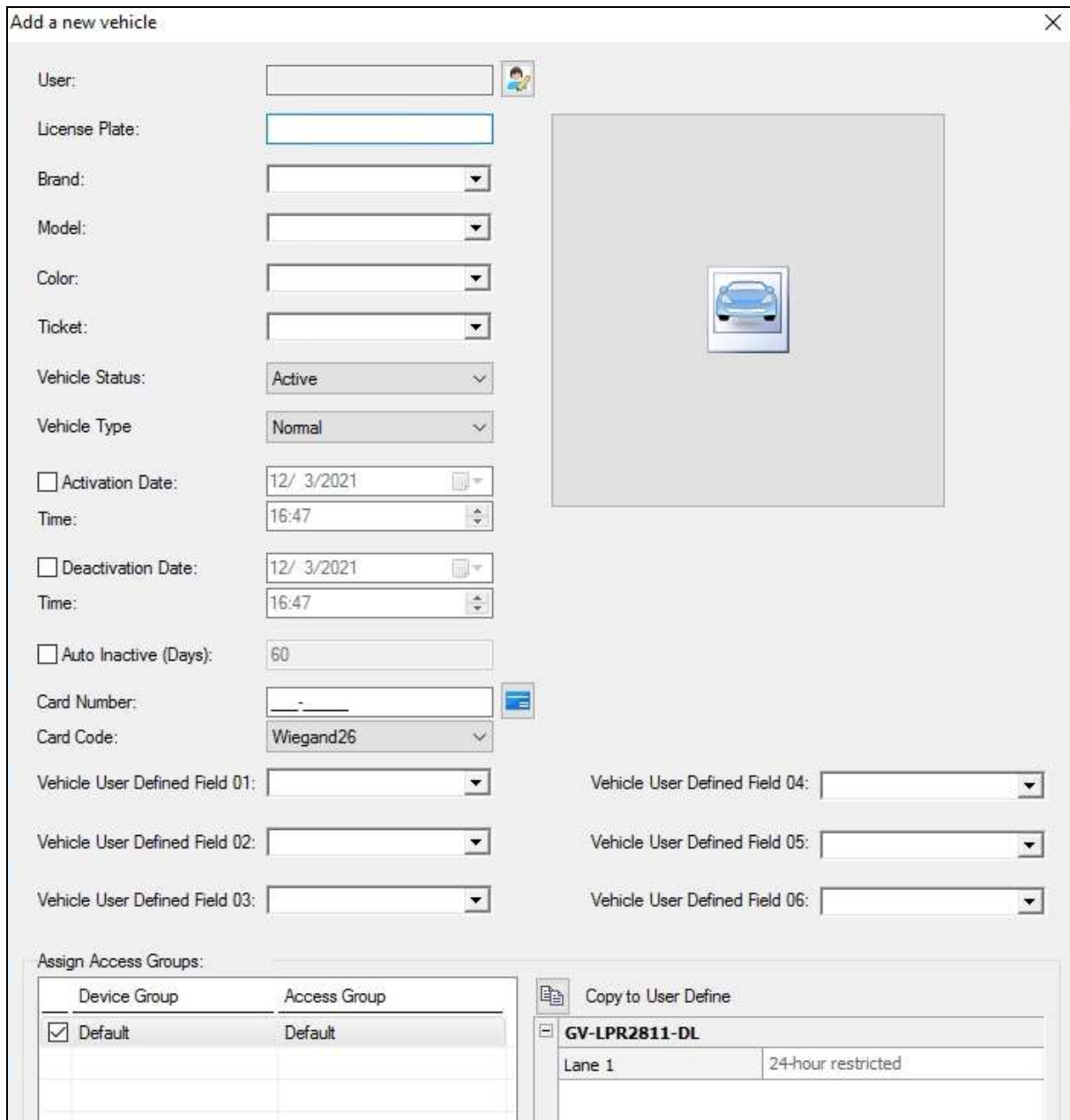
3. Click **OK**.

Recognition conditions, area, and associated output device can be set up on the Web interface of the standalone LPR. Refer to the *Recognition Engine Settings* section in Chapter 4 of the *GV-DSP LPR User Manual* and Chapter 4 of the *GV-IP LPR Camera User Manual*.


Note:

1. The Playback Cameras need to be set to recording in GV-DVR / NVR / VMS in either round-the-clock mode or upon motion detection.
 2. The Overview Cameras need to be set to round-the-clock recording in GV-DVR / NVR / VMS.
 3. To ensure optimal performance, the total number of Overview Cameras supported in a GV-DVR / NVR / VMS is limited based on the resolution of the cameras:
 - Overview camera: D1 = maximum 16 overview cameras
 - Overview camera: 1 MP = maximum 8 overview cameras
 - Overview camera: 2 MP = maximum 4 overview cameras
 - Overview camera: 3 MP = maximum 3 overview cameras
 - Overview camera: 4 MP = maximum 2 overview cameras
 - Overview camera: 5 MP = maximum 1 overview camera
-

2. Click the **New** button on the toolbar. This dialog box appears.



Add a new vehicle

User: 

License Plate:

Brand:


Model:

Color:


Ticket:

Vehicle Status:

Vehicle Type:


Activation Date: 

Time:

Deactivation Date: 

Time:

Auto Inactive (Days):

Card Number: 

Card Code:

Vehicle User Defined Field 01:

Vehicle User Defined Field 02:

Vehicle User Defined Field 03:


Vehicle User Defined Field 04:

Vehicle User Defined Field 05:

Vehicle User Defined Field 06:

Assign Access Groups:


Device Group	Access Group
<input checked="" type="checkbox"/> Default	Default


 Copy to User Define

GV-LPR2811-DL	
Lane 1	24-hour restricted

Figure 13-23

3. These settings are available:

- **User:** Click the **Assign User** button  to assign the vehicle to a user.
- **License Plate:** Type the license plate number of the vehicle.
- **Brand / Model / Color:** Specify the brand, model and color of the vehicle if needed.
- **Ticket:** Type a note for your own reference.
- **Vehicle Status:** Set the vehicle status to be **Active** or **Inactive**. The Deactivation Date, if enabled, will override the selection here.

- **Vehicle Type:** Set the vehicle type. If the vehicle belongs to a visitor for temporary access, select **Visitor**.
- **Activation / Deactivation Date:** Specify the date to activate or deactivate the vehicle access.
- **Auto Inactive (Days):** When the vehicle access has not been recognized for the specified days, it will be deactivated.
- **Card Number:** Type or select a card number. If you have the GV-PCR1251 / 1352 Enrollment Reader installed, click  to detect cards.
- **Card Code:** Select the code format of the card.
- **Vehicle User Defined Field:** For details, see *4.6.2 Customizing a Data Field*.
- **Assign Access Group:** Select **Device Group** and then click its **Access Group** drop-down list to assign one predefined access group. For details, see *4.5 Adding Access Groups*.
- **Lane:** The Lane box displays the associated lanes with Access Groups.

Tip: For first-time users of GV-ASManager, you can click the **Copy to User Define** button and select **24-hour access** for each Lane for test run.

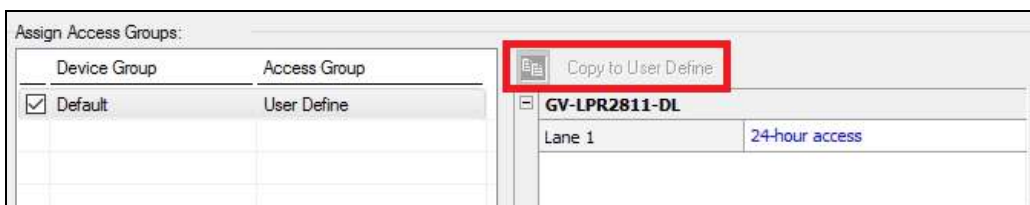


Figure 13-24

To assign multiple vehicles to a user, on the menu bar, click **Personnel > Users**. Next to Vehicle List, click the **Add** button to assign vehicles to the user.

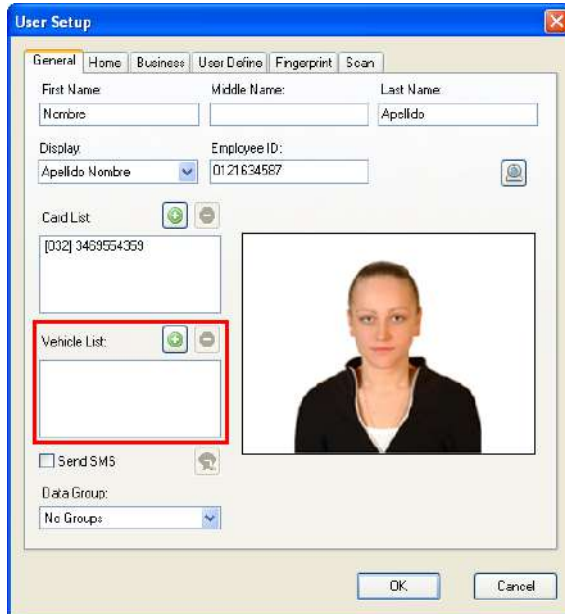


Figure 13-25

You can also import and export vehicle data in mdb, xls or xlsx format. Refer to 4.3.4 *Importing / Exporting Card Data* for similar settings.

13.5 Monitoring LPR Activities

13.5.1 LPR View Window

The LPR view window displays the connection status of the connected LPRs. To open the LPR Device View, click **View > LPRs**.

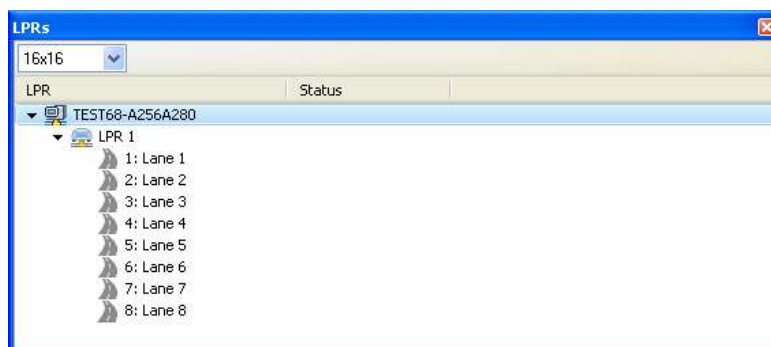


Figure 13-26

Right-click a **LPR** to access the following options:

Name	Function
Reconnect	Reconnect to the LPR device.
Sync LPR	Sync the settings between the LPR device and GV-ASManager immediately.
Settings	Access the LPR setup dialog box.

Right-click a **Lane** to access the following options:

Name	Function
Unlock Lane	Open the gate barrier. To assign an output device to be the gate barrier for the PC LPR, see [Barrier Control], 13.2.3 Step 3: <i>Configuring a Channel</i> . For standalone LPR, see the <i>Output Settings</i> section in Chapter 4 of the <i>GV-DSP LPR User Manual</i> and <i>GV-IP LPR Camera User Manual</i> .
Recognize	Force license plate recognition.
Settings	Access the LPR settings.

13.5.2 Monitoring Windows

To monitor LPR activities, click **Monitoring > New LPR Monitor**.

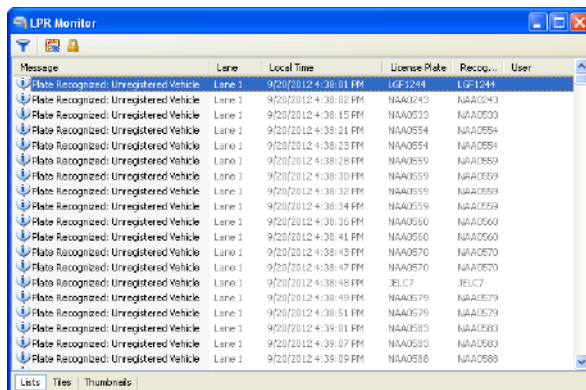


Figure 13-27

For details on the Monitoring Windows, see 3.3 *Monitoring Windows*.

For details on various LPR events, see “LPR” events, *Appendix A*

13.6 Receiving Notifications for LPR Activities

When alarm conditions occur, the system can automatically activate a variety of notifications to alert the operators: e-mail, SMS, trigger recording, push notification, popup message and more.

To set up the notifications for LPR events, click **Tools > Notifications**. For details, see 8.2.3 *Setting up Notifications*.

13.7 Setting up Vehicle Hotlist

The vehicle hotlist is a list of stolen vehicles or vehicles of interest. When any vehicles on the hotlist are recognized, the system can trigger various notifications to alert the operators.

There are two ways to add vehicles to the hotlist: manually add vehicles or import from an external database. Up to 2-million vehicles can be added to the vehicle hotlist.

13.7.1 Setting up the Hotlist Database

To import from an external database, you need to complete the steps below first.

1. Run **ASDBManager.exe** from the GV-ASManager program folder at :\\Access Control\\ASManager\\.

2. Select **Settings from Source to ASManager Database > Set the mapping relations for vehicle hotlist**. This dialog box appears.

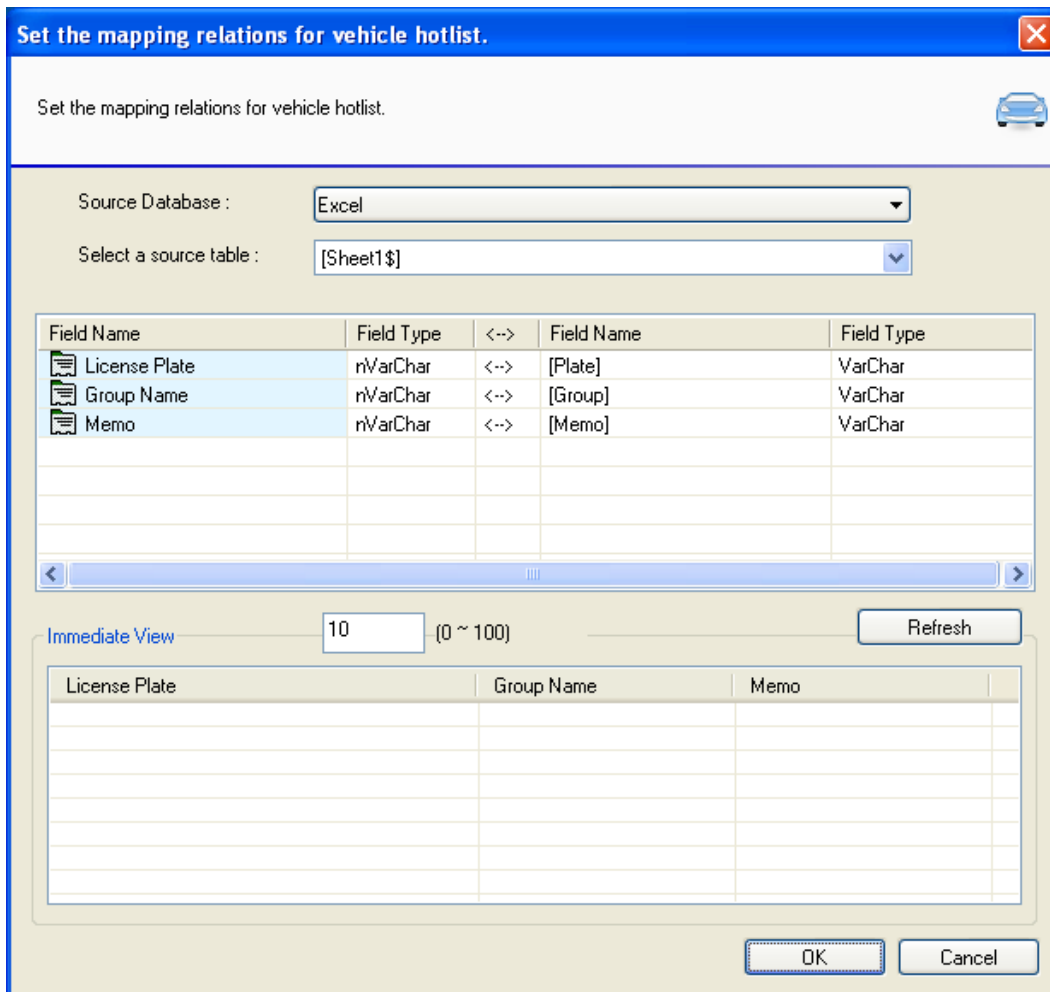


Figure 13-28

3. Use the **Source Database** drop-down list to select an excel database or another type of database.
4. Next to **Select a source table**, select the appropriate tab in the database.
5. Match the License Plate, Group Name and Memo to the appropriate fields.
6. Click **OK** to import.

13.7.2 Adding License Plates to the Hotlist

On the menu bar of GV-ASManager, click **Tools > Hotlist**. This dialog box appears.

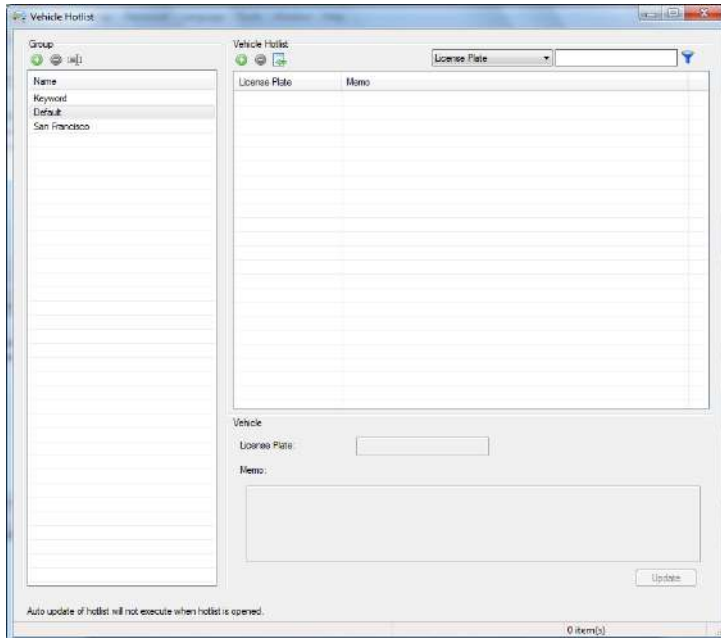




Figure 13-29

If you have imported data from an external database using ASDBManager, you will see these vehicles are listed under the **Default** group. You can also add license plates manually, import existing license plates from the vehicle list or create keywords (for partial license plate numbers).

Adding License Plates Manually

1. Under **Group** on the left pane, click **Add**  to create a group first if needed.
2. Under **Vehicle Hotlist** on the right pane, click **Add** , type a **License Plate**, and add a **Memo**, for example, to note the stolen time and location.

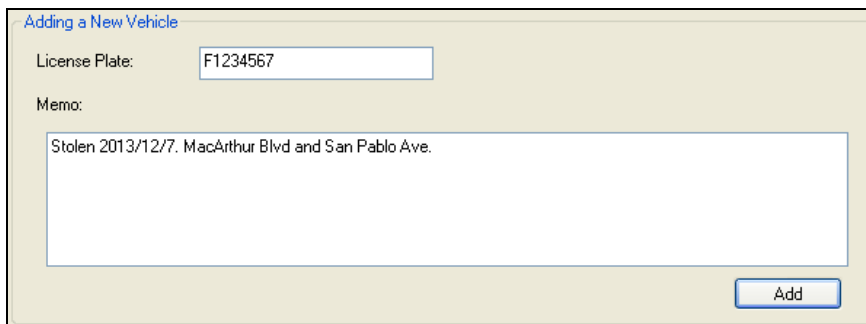



Figure 13-30

3. Click **Add**.

Importing License Plates from Vehicle List

1. To import an existing license plate from the vehicle list, under **Vehicle Hotlist** on the right pane, click the **Import** button . This dialog box appears.

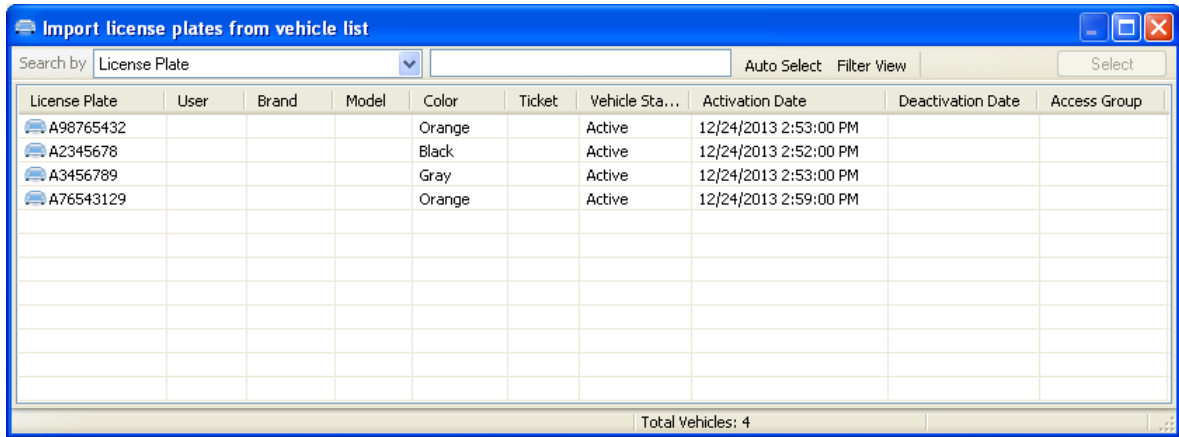



Figure 13-31

2. Select the vehicles you want to add, and click the **Select** button to add.

Setting Keywords for Partial Match

You can create keywords, which are partial license plate numbers.

1. Select **Keyword** under **Group** on the left pane, and click **Add**  under **Vehicle Hotlist** on the right pane.

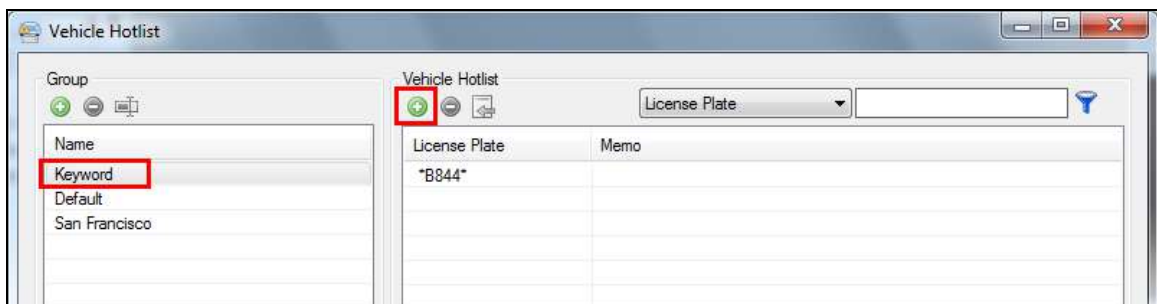


Figure 13-32

2. Under **Add a New Keyword**, type a partial license plate number to be **Keyword**.

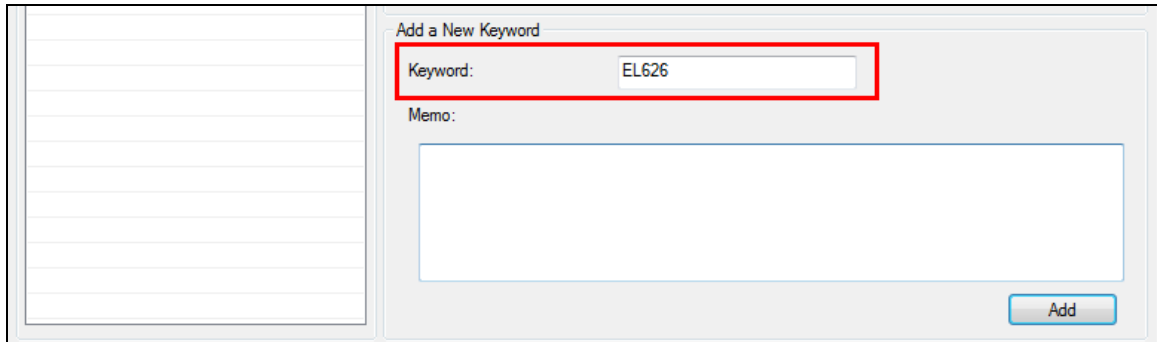


Figure 13-33

3. Click **Add**. License plates that contain the keyword will be highlighted on the screen of GV-ASManager.

When GV-ASManager recognizes a license plate that matches a license plate or a keyword in the hotlist, the vehicle will be highlighted in red in the LPR Monitor window as shown below.



Figure 13-34

To trigger notifications when any vehicles on the hotlist are recognized, on the menu bar, click **Tools > Notifications** to create an alert approach, and select **Hotlist** from **Event Type**. For details, see 8.2.3 *Setting up Notifications*.


13.8 Managing Parking Lots

With the parking lots management, you can regulate which vehicles have the permission to enter the parking lot, parking space availability, parking duration allowed, anti-passback, and parking spaces shared by more than one user.

Note: For the parking lot functions to work properly:

1. GV LPR device must remain connected to GV-ASManager.
 2. The time of GV-ASManager and GV IP device must be synchronized to the same NTP server.
 3. The function is only supported by the following versions and devices:
 - GV-ASManager V4.3 or later
 - GV-DVR LPR with GV-LPR Plugin for GV-DVR / NVR V8.6.0.0 or later
 - GV-VMS LPR with GV-LPR Plugin for GV-VMS V15.10.0.0 or later
 - GV-DSP LPR firmware V2.1 or later
 - GV-LPR1200 firmware V1.12 or later
 - GV-LPR2800-DL firmware V1.0 or later; GV-LPR2811-DL firmware V1.1 or later
-

13.8.1 Setting up a Parking Lot

1. On the menu bar, click **Setup > Devices**, and select a **Device Group**. The devices under the Device Group will be applied with identical Parking Lots settings.
2. Select **Parking Lots** on the left of the Devices dialog box. The Parking Lot List dialog box appears.
3. Click **Add** . The Please Enter ID dialog box appears.

4. Type a Parking Lot ID and name the Parking Lot, and click **OK**. This dialog box appears.

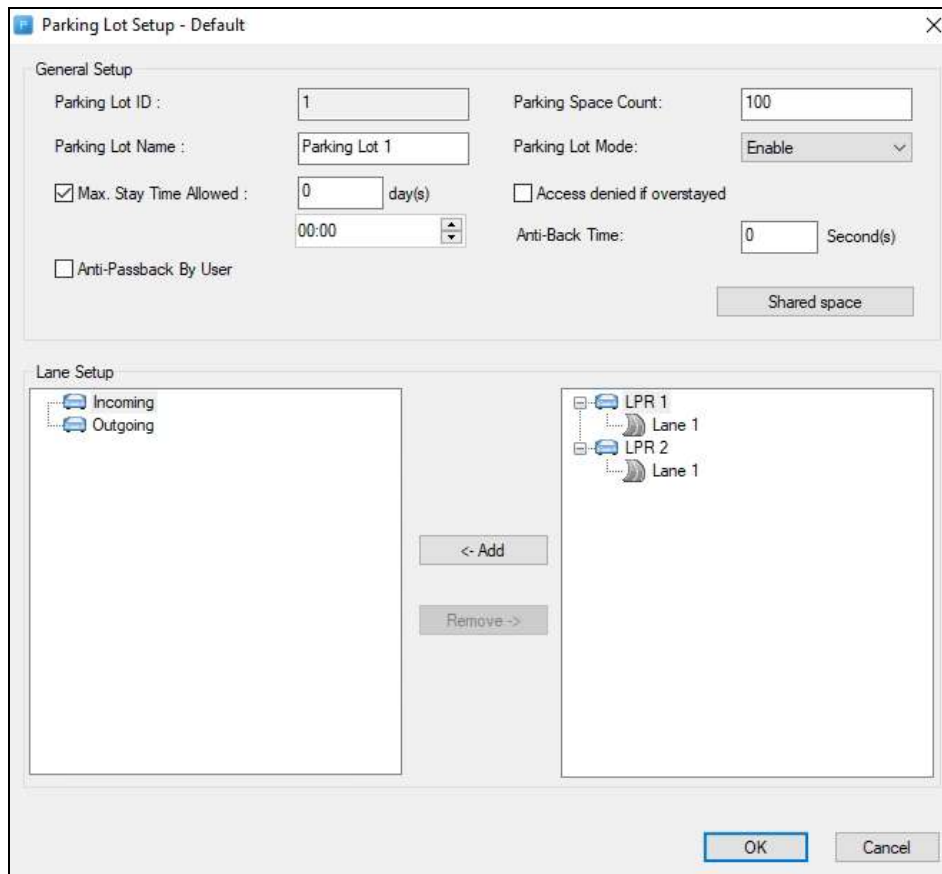



Figure 13-35

5. Under **General Setup**, the following settings are available.

- **Parking Lot Name:** Rename the parking lot if needed.
- **Parking Space Count:** Define the total number of parking spaces available in the parking lot. When the parking lot is full, entry to the parking lot will be denied unless you manually open the gate from Parking Lot Monitor.
- **Parking Lot Mode:** By default, the Parking Lot Mode is enabled. When **No Incoming** is selected, no vehicles can enter the parking lot but outgoing vehicles will be allowed. When **Disable** is selected, no vehicles can enter and exit the parking lot.
- **Max. Stay Time Allowed:** When enabled, vehicles that stay in the parking lot beyond the maximum stay time will be highlighted as “Overstayed Vehicle” in Parking Lot Monitor.
- **Access Defined if Overstayed:** Only works with GV-LPR Plugin V6.0.2 or later. When enabled, unregistered vehicles that overstay in the parking lot are unable to exit.

- **Anti-Back Time:** Specify the time interval in seconds the same license number is prohibited from entering or exiting the parking lot.
- **Anti-Passback by User:** Only allow one vehicle of a user entering the parking lot when the user has more than one registered vehicle.
- **Share Space:** Set up Share Space if multiple vehicles are sharing the same set of parking spaces.
 - a. Under **Share Group**, click **Add**  to create a group.

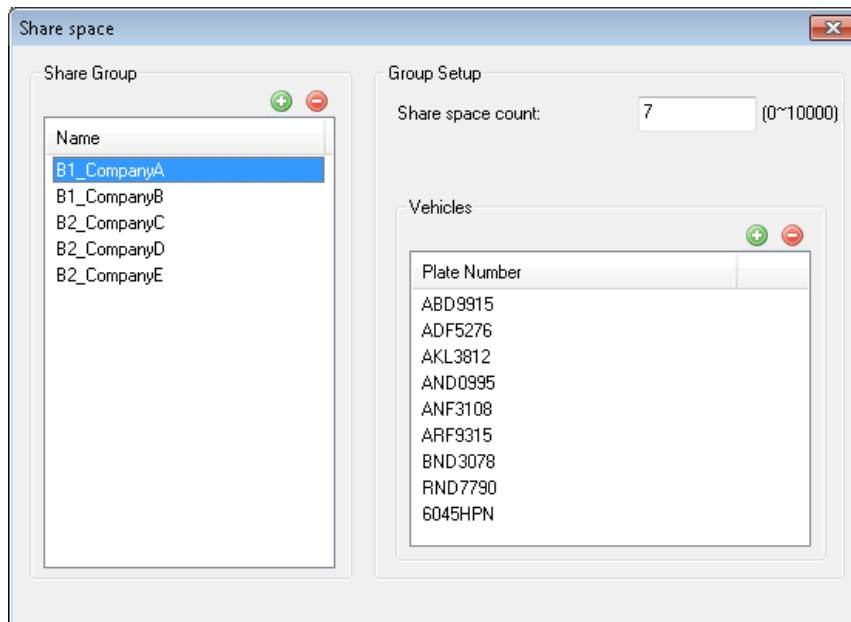



Figure 13-36

- b. For **Share space count**, type the number of parking spaces shared by that group.
- c. Under Vehicles, click **Add**  to select the license plate numbers that share the set of parking spaces.

In the figure above, company A has 7 allocated spaces in the parking lot that are shared by 9 employees, each with a registered vehicle. The first 7 vehicles in the list will be able to enter the parking lot, while the remaining 2 vehicles will be denied access even if there are other empty spaces available in the parking lot.

- To assign an LPR lane as the entrance of the parking lot, select **Incoming** on the left pane, select an LPR lane on the right pane, and click the **Add** button.



Figure 13-37

- For exit, select **Outgoing**, select another LPR lane, and click the **Add** button.
- To set multiple incoming and outgoing lanes, follow the steps above.
- Click **OK**.

To trigger notifications upon Parking Lot events, on the menu bar, click **Tools > Notifications** to create an alert approach, and select Parking Lot events from **Event Type**. For details, see *8.2.3 Setting up Notifications*.

13.8.2 Monitoring Parking Lots

Using the Parking Lot Monitor, you can see a list of vehicles that have entered and exited the parking lot, along with their snapshots and information. You can also manually add or remove a vehicle, and manually open the parking gate.

- On the menu bar, click **Monitoring > New Parking Monitor**.
- Select a parking lot and click **OK**. This window appears.

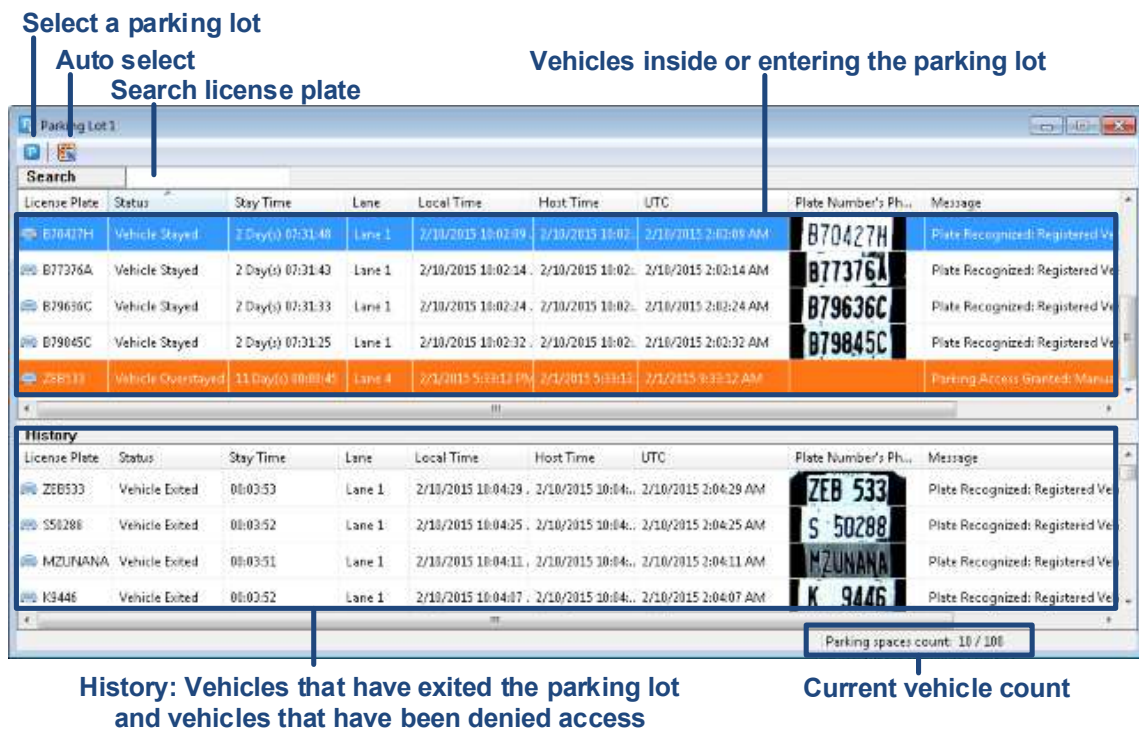


Figure 13-38

Vehicles inside the parking lot are listed in the top half of the Parking Lot Monitor. Vehicles that have exited the parking lot or have been denied access are listed under **History** in the lower half of the window. You can also use the **Search** function to search for license plates.

- To add a vehicle to the vehicle list,
 - a. Right-click the top half of the Parking Lot Monitor.
 - b. To add a vehicle already inside the parking lot to the vehicle list, select **Add**. If a vehicle is unable to enter the parking lot due to incorrect license plate recognition, you can select **Add and Open Gate** to add to the vehicle list and open the gate for the vehicle at the same time.

B70427H	Vehicle Stayed	2 Day(s) 07:31:48	Lane 1	2/10/2015 10:02:09	2/10/2015 10:02:09	2/10/2015 2:02:09
B77376A	Vehicle Stayed	2 Day(s) 07:31:43	Lane 1	2/10/2015		
B79636C	Vehicle Stayed	2 Day(s) 07:31:33	Lane 1	2/10/2015		
B79845C	Vehicle Stayed	2 Day(s) 07:31:25	Lane 1	2/10/2015		
ZEB533	Vehicle Overstayed	11 Day(s) 00:00:45	Lane 4	2/1/2015		

New/Edit Vehicle...
 Modify Plate Number...
 Add >
 Add and Open Gate >
 Remove >
 Remove and Open Gate >

Figure 13-39

- c. Select the entrance lane, type the license plate number, and select the entrance date and time.

Add Parking Vehicle

Plate Number:

Date:

Time:

Figure 13-40

Note:

1. If the vehicle had to be manually added because its license plate is not in the GV-ASManager database, make sure to click **New/Edit Vehicle** to add the vehicle to the database, or else the vehicle will be unable to exit the parking lot.
2. If the license plate is incorrectly recognized, you can click **Modify Plate Number** to edit the plate number.

- To remove a vehicle from the vehicle list,
 - a. Right-click the top half of the Parking Lot Monitor.
 - b. To remove a vehicle that is no longer inside the parking lot, right-click the vehicle in the list, and select **Remove**. If a vehicle is unable to exit the parking lot due to incorrect license plate recognition, select **Remove and Open Gate**.
 - c. Select the exit lane, and select the exit date and time.

You can click **View** on the menu bar, and select **Info** to see information and snapshots of the selected vehicle.

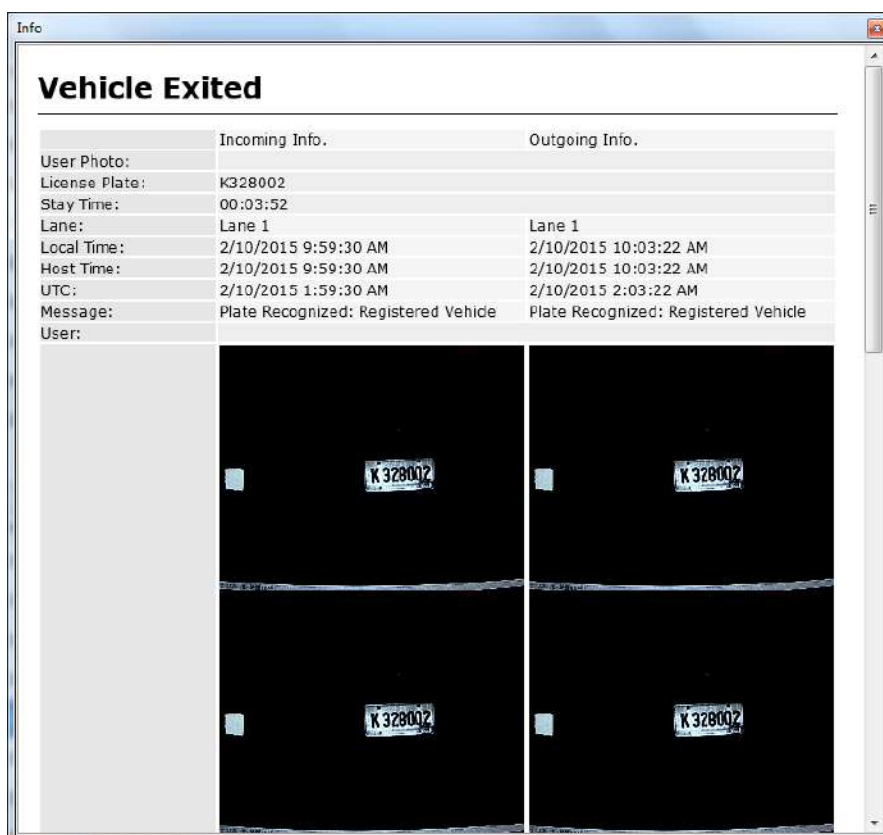


Figure 13-41

13.9 Calculating Average Speed

You can get a vehicle's average speed between two set points on a road, measured by two LPR devices at each point.

1. On the menu bar, click **Setup > Devices**. The Devices dialog box appears.
2. To set a lane as the end lane, right-click a LPR device > **Settings**. The LPR Setup dialog box appears.
3. Under Speed Calculation, configure the following settings.



Speed Calculation:

Starting Lane: None

Interval Distance: 100 m

Speed Limit: 0 km/h

- **Starting Lane:** Select the lane from where the travel starts.
- **Interval Distance:** Specify the distance in meter between the starting and end lanes.
- **Speed Limit:** Specify the speed limit in km/h.

13.10 LPR Functions on GV-ASWeb

Using GV-ASWeb, you can connect to GV-ASManager over a network and remotely access the following LPR functions:

- **LPR List:** Add and delete an LPR device to and from GV-ASManager.
- **Vehicle List:** Add, delete, edit and search for vehicles.
- **LPR Log:** Search the records of license plates recognized and play back recordings.
- **Parking Lot:** Set up parking lots. See *13.8 Managing Parking Lots* for details.

See *10.1 Connecting to GV-ASManager* for how to log into GV-ASWeb.

13.10.1 LPR List

You can use the LPR List to remotely add and delete an LPR device to and from GV-ASManager.

4. On GV-ASWeb, click **LPR List**. This window appears.

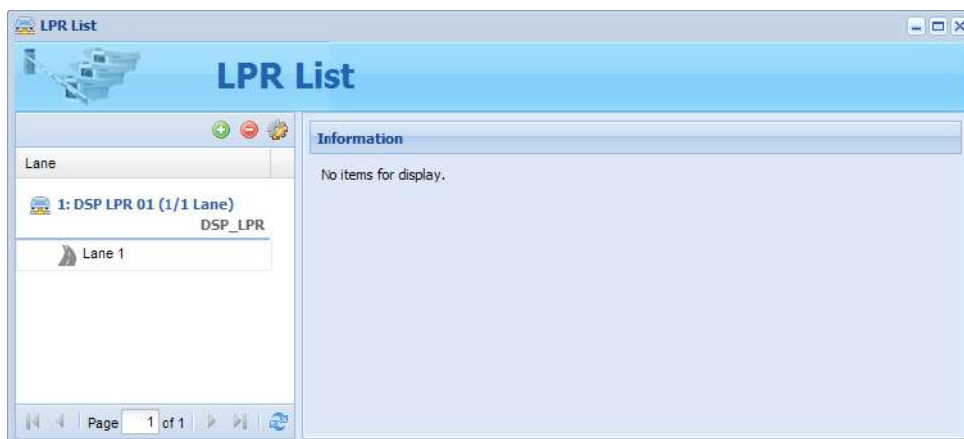






Figure 13-42

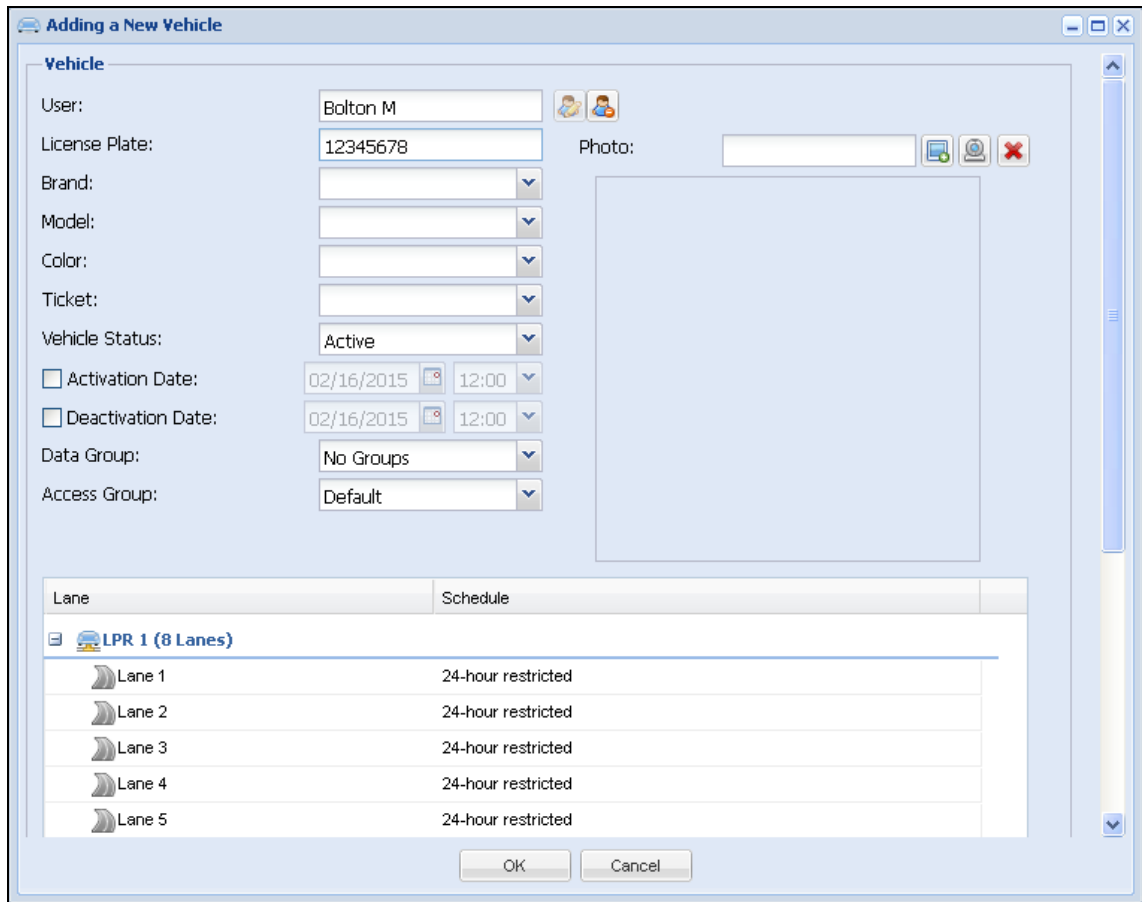
5. Click **Add**  to add an LPR device. For details, see *13.2.2 Adding PC LPR to GV-ASManager* and *13.3.2 Adding Standalone LPR to GV-ASManager*.
6. To set up individual channels, click **Edit**  and select a channel. For details, see *13.2.3* and *13.3.3 Configuring a Channel*.
7. To delete an LPR, select an LPR and click **Delete** .

Note: Any changes made on GV-ASWeb will be reflected in GV-ASManager.

13.10.2 Vehicle List


Vehicle List allows you to remotely add, search, edit and delete vehicles.

1. On GV-ASWeb, click **Vehicle List**.
2. Click **New** . This dialog box appears.



Lane	Schedule
LPR 1 (8 Lanes)	
Lane 1	24-hour restricted
Lane 2	24-hour restricted
Lane 3	24-hour restricted
Lane 4	24-hour restricted
Lane 5	24-hour restricted

Figure 13-43

3. Fill out the required information. See *13.4 Adding Vehicles* for details.
4. Click **OK** to save the settings.
5. To delete a vehicle, select the vehicle and click **Delete** .

Note: Any changes made on GV-ASWeb will be reflected in GV-ASManager.

13.10.3 LPR Log

Using LPR Log, you can look up a record, see snapshots of recognized license plates, track the locations of vehicles and play back recorded videos.

Defining Search Criteria

You can narrow down the search results by setting search criteria such as LPR lanes, date, parking lots, and license plates.

Under **Filter** on the left, set the search criteria and click the **Search** button. For example, we want to search for the records that match the conditions of “Unregistered Vehicle”, license plate number “FM-0505”, and detected by LPR 1. The resulting filter window may look like this.

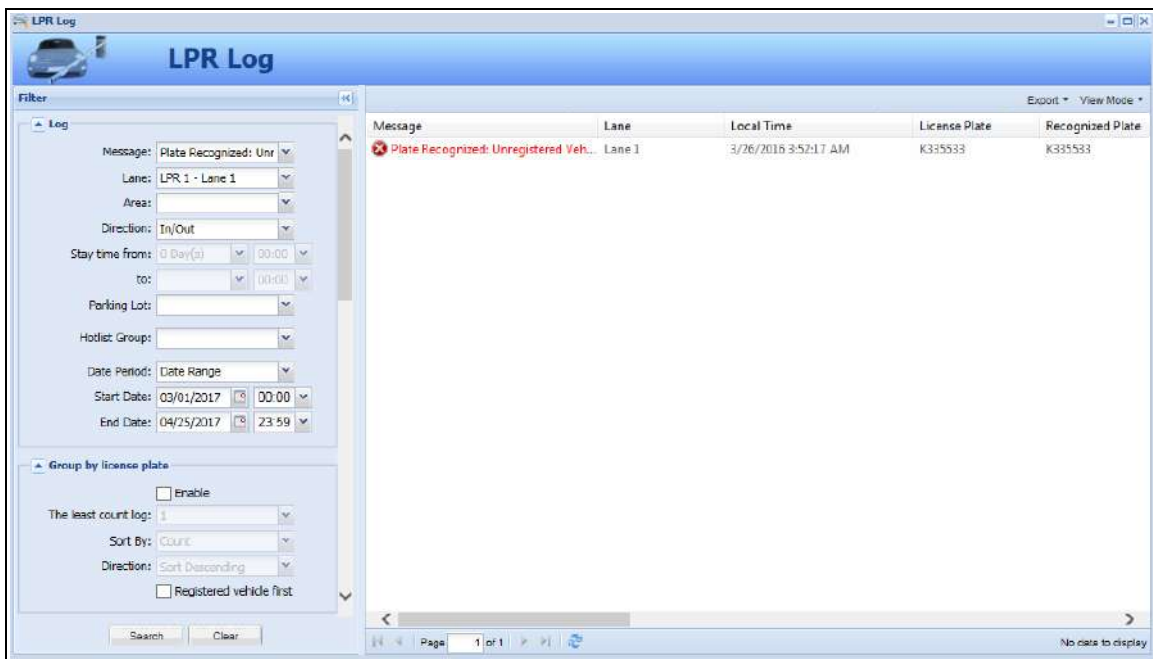


Figure 13-44

If **Fuzzy Matching** is selected, the letters below will be recognized as numbers:

- Letter B will become 8
- Letter Z will become 2
- Letter O and D will become 0 (Zero)
- Letter I will become 1
- Letter S will become 5
- Letter G will become 6

When a license plate number is typed in the **Recognized Plate** field, you can apply Fuzzy Matching and the Matching Mode you set will be applied as well (e.g. Allow 1 mismatched character). When a license plate number is typed in the **License Plate** field, only the license plate that matches completely will be displayed in the search results.

Tip: When searching license plates,

1. You can include question marks in a license plate, for example OP98?5, to represent any character or number.
2. You can add an asterisk at the end of a partial license plate, for example OP98*, and any plates that start with OP98 will be displayed.

The Search Results Window

Below is an example of the search results window.

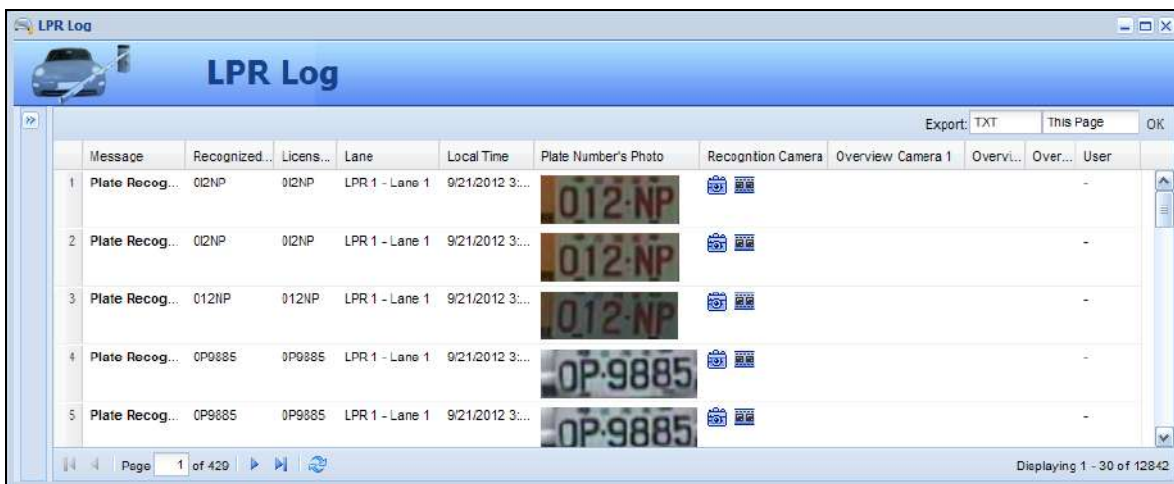





Figure 13-45

A snapshot of the recognized license plate will be displayed.

: Indicate the availability of the recorded video.

: Indicate the availability of the video image.

You can right-click each search result to access more information such as vehicle information , user information  or log information (for parking lot).

For how to export logs, see *10.6 Setting up Export Schedule for Lists and Logs* for details. For how to define the displayed columns of the search results window, see *10.4.4 Defining Columns* for details.

Note: For remote playback to work on the PC LPR, you need to enable **Remote ViewLog Service** on it.

Obtaining the Locations

If the license plates of vehicles that have entered and exited the monitored areas are recognized in the connected LPR cameras, their driving routes can be displayed on the map. To track the locations of those vehicles, click **View Mode** in the top-right corner and select **Map Mode**. For details on pinning the locations of the LPR cameras on the map see *10.12 Creating Maps*.

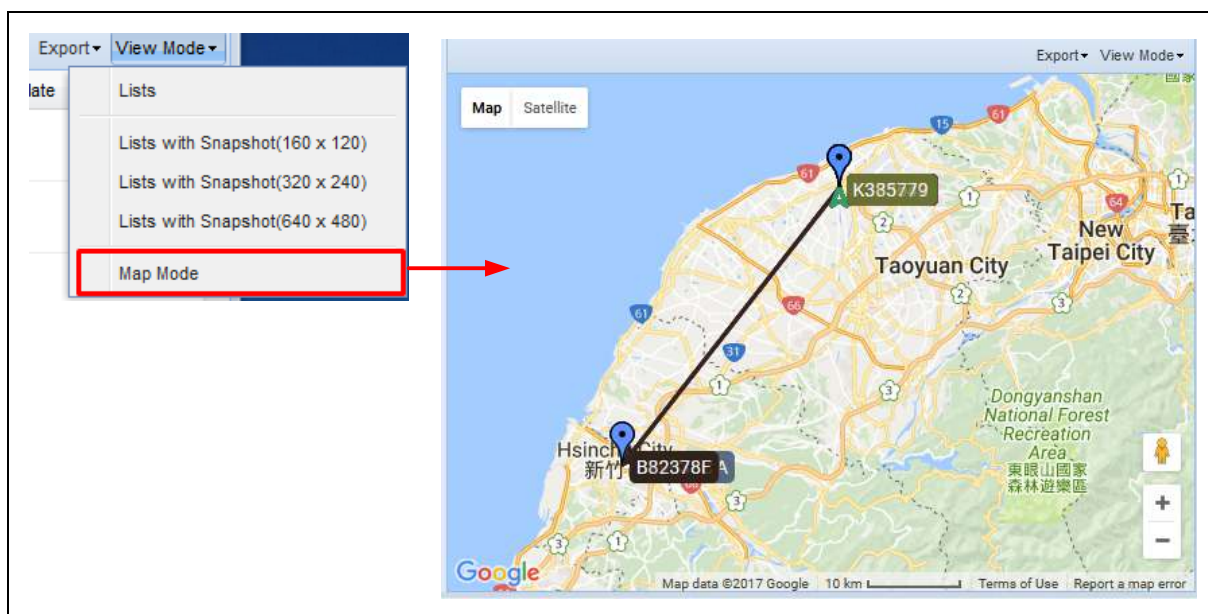


Figure 13-46

Chapter 14 Face Recognition

The Face Recognition function allows GV-Face Recognition Camera and GV-AI FR software to connect to controllers, acting as extended readers, to grant access when the faces recognized and their paired access data match the users registered in GV-ASManager's database.

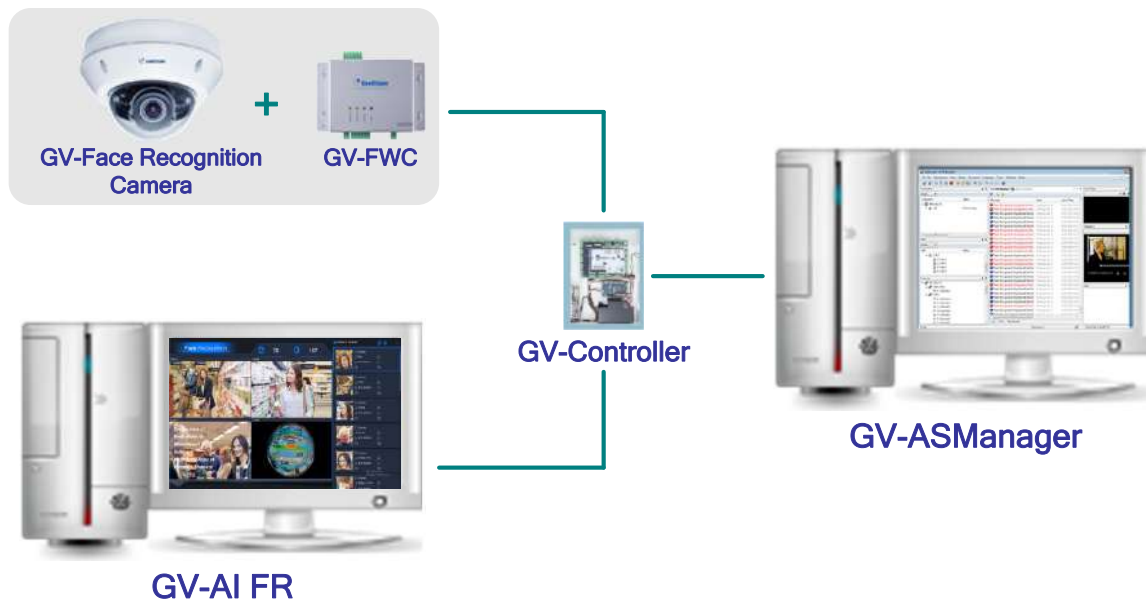


Figure 14-1

- For integrating face recognition using GV-Face Recognition Camera, see *14.1 GV-Face Recognition Camera*.
- For integrating face recognition using GV-AI FR software, see *14.2 GV-AI FR*.

Note:

1. Before integrating the face recognition feature, make sure you have a controller capable of connecting to extended readers properly set. See *4.2 Adding Controllers*.
 2. GV-FR Panel (reader) also supports access control with face recognition. For details, see [GV-FR Panel User's Manual](#).
-

14.1 GV-Face Recognition Camera

When integrating GV-Face Recognition Cameras to GV-ASManager, a **GV-FWC** is required, which receives and converts face recognition into access card data to be sent to the controller upon recognition. To set up GV-Face Recognition Camera, follow the steps below:

- **Step 1 Configuring GV-FWC**

Configure GV-FWC for communication. See 2.3 *Accessing GV-FWC* and 3.1 *Configuring for Communication on GV-FWC* in [GV-FWC Installation Guide](#).

- **Step 2 Connecting GV-Face Recognition Camera to GV-FWC**

Connect GV-Face Recognition Camera to GV-FWC. See 3.2 *Sending Face IDs from Camera* in [GV-FWC Installation Guide](#).

- **Step 3 Connecting GV-FWC to GV-AS Controller**

Connect GV-FWC to the controller. See 3.3 *Receiving Access Card Data by Controller* in [GV-FWC Installation Guide](#).

- **Step 4 Adding GV-Face Recognition Camera to GV-ASManager**

Add GV-Face Recognition Camera to GV-ASManager. See 14.1.1 *Adding GV-Face Recognition Camera*.

Note: To add users into the necessary databases for face-recognition-based access management, see 14.3 *Managing Face Recognition Access Data*.

14.1.1 Adding GV-Face Recognition Camera

In the **Devices** dialog box (**Setup > Devices**), double-click the controller that GV-FWC is connected to and select a **Door**. The following window appears.

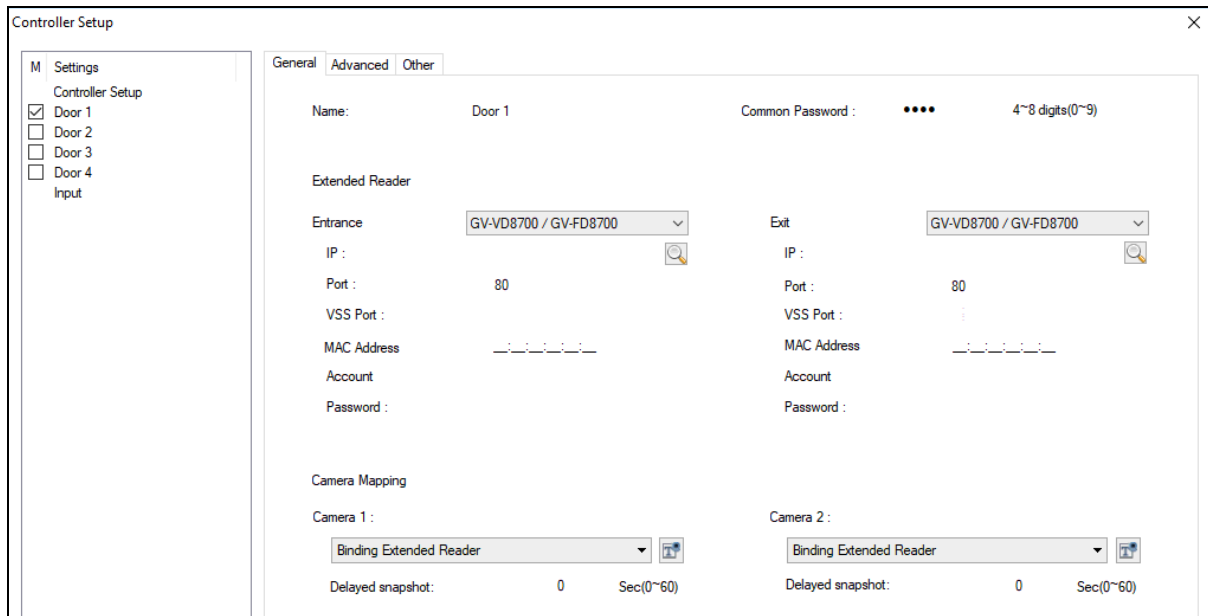


Figure 14-2

1. Under **Extended Reader**, select **GV-VD8700 / FD8700-FR** from **Entrance** or **Exit** drop-down list, according to the access scenario.
2. Under the drop-down list used, type the connection information of the face recognition camera, such as IP and login credentials.
3. Under **Camera Mapping**, select **Binding Extended Reader** from **Camera 1** or **Camera 2** drop-down list.
4. Click **OK**.
5. To create face recognition data and transfer it back to the camera, see *14.3 Managing Face Recognition Access Data*.

Note: For other Door settings, see *4.2.2 Step 2: Configuring Doors or Elevator Floors* for details.

14.2 GV-AI FR

GV-AI FR is video analytic software designed to provide face recognition for up to 8 camera channels. To integrate GV-AI FR into GV-ASManager for face-recognition-based access control, follow the steps below:

Note: The following procedures are only applied to GV-AI FR V1.2.0 or later.

1. In the **Device List** dialog box (**Setup > Devices**), double-click the controller that GV-AI FR is to be connected to and select a **Door**. This dialog box appears.

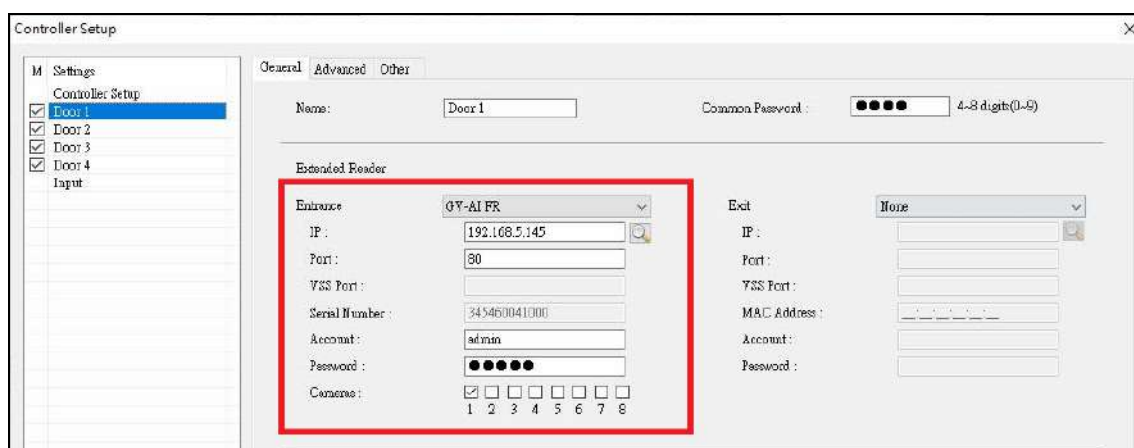


Figure 14-3

2. Under **Extended Reader**, select **GV-AI FR** from **Entrance** and **Exit** drop-down lists, according to the access scenario.
3. Type the connection information of GV-AI FR, such as IP and login credentials.
4. For **Camera**, select the cameras of GV-AI FR used in the access scenario.
5. Click **OK**. GV-AI FR is connected to the controller and GV-ASManager.
6. To create face data and transfer it back to GV-AI FR, see *14.3 Managing Face Recognition Access Data*.

To verify the connection on GV-AI FR:

- On the GV-FWC / Controller Setting page (**Dashboard > Notify Settings > GV-FWC / Controller**), you should find an entry, for example, *[ASManager] Door 1 (In)*, written back from GV-ASManager to indicate which controller IP and door are connected to.



Figure 14-4

- On the Event Trigger page (**Event Trigger > Notify Settings**), you should also find an entry of face recognition. No matter which types of FR events, recognized or unknown faces, all will trigger GV-AI FR to send the access data to GV-ASManager.

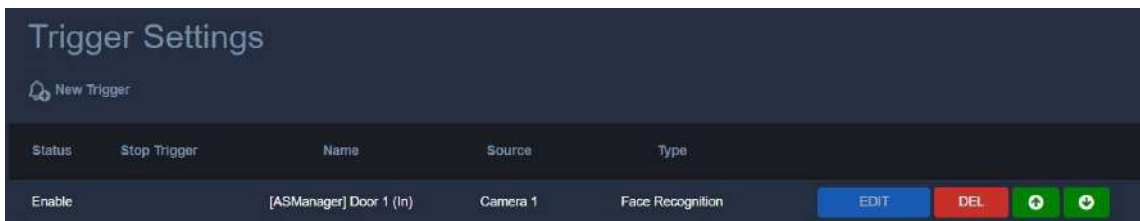



Figure 14-5

Note: You can map the cameras of GV-AI FR to the corresponding entrance or exit for live view display. To add a camera, see [5.1 Mapping Cameras](#) for details.

14.3 Managing Face Recognition Access Data

Once GV-Face Recognition Camera / GV-AI FR is properly set, you need to create a user database with the required face images and access data.

1. There are two methods of adding face recognition data:
 - When an unregistered face recognition event occurs, the message *Access Denied: Invalid Card* is displayed. Right-click the message and select **Assign Image to a New User** to create a new user to the database.
 - On the menu bar, click **Personnel > Users**. The User List window appears.
2. Click the **New** button on the toolbar. The User Setup dialog box appears.
3. Type a **Display Name** for the user, which is also the name of the Face ID in the GV-Face Recognition Camera / GV-AI FR database.
4. To assign a card to the user, click **Add**  next to **Cards**.
5. To add a face photo of the user from the PC, which will be used for face recognition on GV-Face Recognition Camera / GV-AI FR, click on the image column under **GV-VD8700 / GV-FD8700-FR / GV-AI FR** in the **Features** tab and select the access card number of the user in the drop-down list next to the photo added.

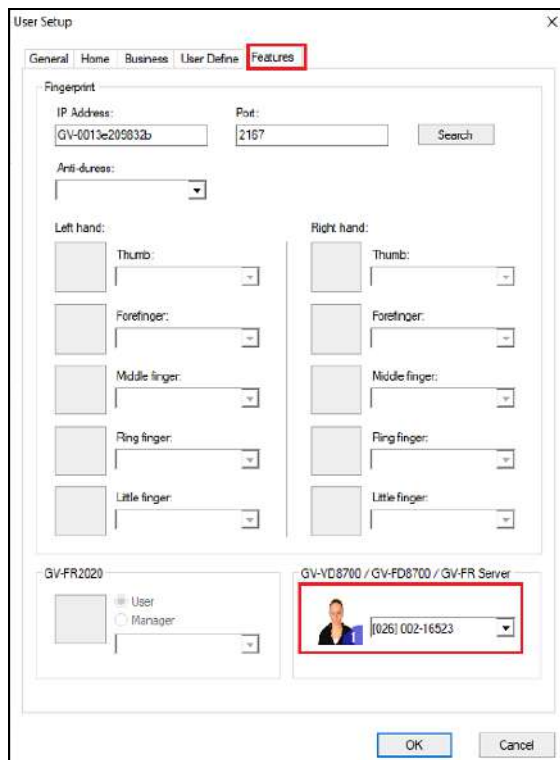


Figure 14-6

6. Click **OK**.

- After adding the users, click **Setup > Feature Access** and select the **Door** the GV-Face Recognition Camera / GV-AI FR is connected to.

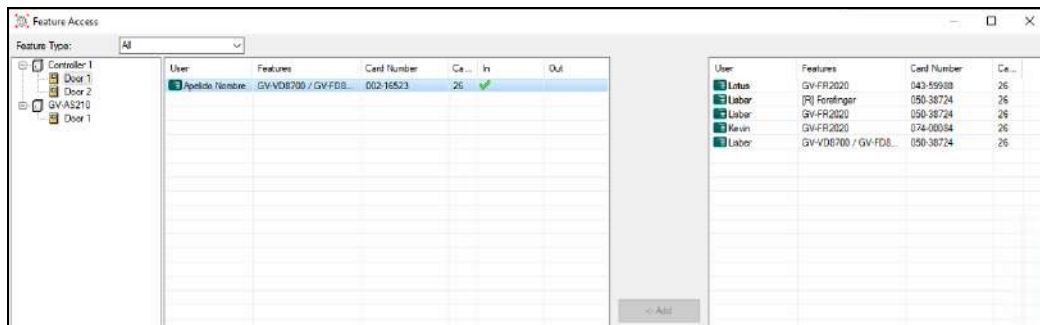


Figure 14-7

- From the right column, select the users to be added to the database of GV-Face Recognition Camera / GV-AI FR and click **Add**. Once the users are successfully uploaded to GV-Face Recognition Camera / GV-AI FR, a green tick ✓ is displayed next to the user data.

IMPORTANT: For GV-AI FR, all of its camera channels, to which separate Doors may be connected to, share the same face database, therefore whenever a User is uploaded to or removed from any of its channels, the same changes will be made to all of its other channels simultaneously. **To prevent confusion, you must upload and remove face data using a designed door.**

Note:

- If you are unable to upload User data in Step 7 due to an unstable network, you can optionally reupload the same data while replacing the current database of GV-Face Recognition Camera / GV-AI FR by right-clicking the Door it is connected to and select **Sync GV-VD8700 / GV-FD8700-FR** or **Sync GV-AI FR**, see 3.2.1 Controls on the Window.
 - For detailed instructions on how to add or batch enroll face photos to GV-ASManager to be uploaded to GV-Face Recognition Cameras / GV-AI FR, see [How to Enroll GV-FR Device Faces with GV-ASManager](#).
 - For additional User settings, see 4.6 Adding Users.
-

Note: For GV-ASManager to receive unknown face recognition events, make sure the GV-Face Recognition Camera is set to send unknown events:

1. Access the **Event Manager** page (**System Settings > Events and Alert > Event Manager**).
2. In the **Settings** tab, enable **HTTP Event**, select **Yes** under **Send events when faces are unknown** and click **Apply**.

Settings | Http Event | GV-FWC

Send face events to

Http Event Enable Disable

GV-FWC Enable Disable

Send events when faces in the selected group(s) detected

Authorized

Unauthorized

New Group

Send events when faces are unknown

Yes

No

Figure 14-8

3. In the **Http Event** tab, select **POST** as **Http Method**, select **JSON** as **Post Content Type** and type the IP address and Port of the connected GV-FWC in the form of “http://<IP of GV-FWC>:<HTTP Event Port of GV-FWC>” (for example: **http://192.168.4.9:8080**) under **URL**

Settings | Http Event | GV-FWC

Http Method

POST

Post Content Type

Form (multipart/form-data)

JSON (application/json)

URL

http://192.168.4.9:8080

Figure 14-9

4. Under **Face Recognition Data**, click **+** to add the parameters *Note2*, *Group*, *Snapshot*, *Name*, *MAC* and *Note1*, exactly as illustrated by Figure 14-9.

Face Recognition Data

Parameter Name	Note2	Face Data	Note2	+
Parameter Name	Group	Face Data	Group Name	+
Parameter Name	Snapshot	Face Data	Face Snapshot	+
Parameter Name	Name	Face Data	Name	+
Parameter Name	MAC	Face Data	MAC Address	+
Parameter Name	Note1	Face Data	Note1	+

+

Figure 14-10

5. Optionally click **Test** for testing the connection.
6. Click **Apply**.

Chapter 15 GV-Access Mobile App

GV-Access app allows you to access up to 5 GV-ASManager systems through iOS or Android devices. You can watch camera live view, check door status, unlock doors and open an LPR gate.


For details on the mobile app, visit our [website](#).

Chapter 16 GV-ASNotify

GV-ASNotify is an application designed to watch live video and communicate with visitors at the access control site, as well as unlocking doors remotely. For the application to work, the GV-IP Camera supporting two-way audio or the GV-CS1320 controller connected to GV-ASManager is required.

If the GV-CS1320 controller is applied, snapshots, messages, alarms can be triggered to alert the operators when the bell button (touch pad) on GV-CS1320 is activated.

16.1 Installing GV-ASNotify

To download and install GV-ASNotify, go to the [Download Page](#) of GV-ASManager and click the **Download** icon  of **GV-ASNotify**.

Note: If you do not have **Microsoft DirectX End-User Runtimes (November 2008)** installed, download and install from [here](#).

16.2 Connecting to GV-ASManager

Before GV-ASNotify connects to GV-ASManager, you must enable GV-ASManager to allow remote access:

- On the menu bar of GV-ASManager, click **Tools > Servers > Remote Monitor Server**. When the server is started, the icon  appears at the bottom-right of the main screen.

1. Run **GV-ASNotify.exe**.
2. To connect to GV-ASManager, click the **Add Host** button. This dialog box appears.

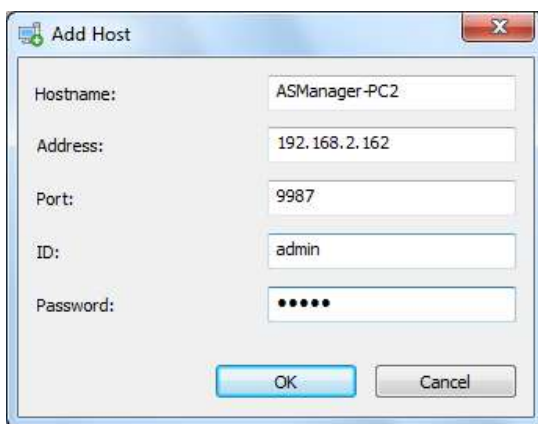


Figure 16-1

3. Type the connection information of GV-ASManager, such as IP and login credentials.
4. Click **OK**. GV-ASManager is added to the host list.

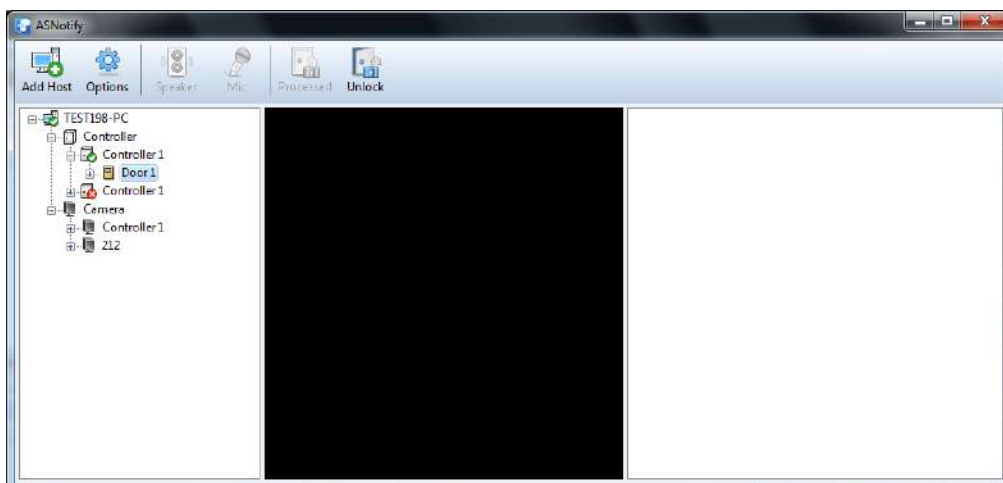


Figure 16-2

16.3 Utilizing GV-ASNotify

1. In the host list, select a camera or GV-CS1320 connected to GV-ASManager to access its live view.

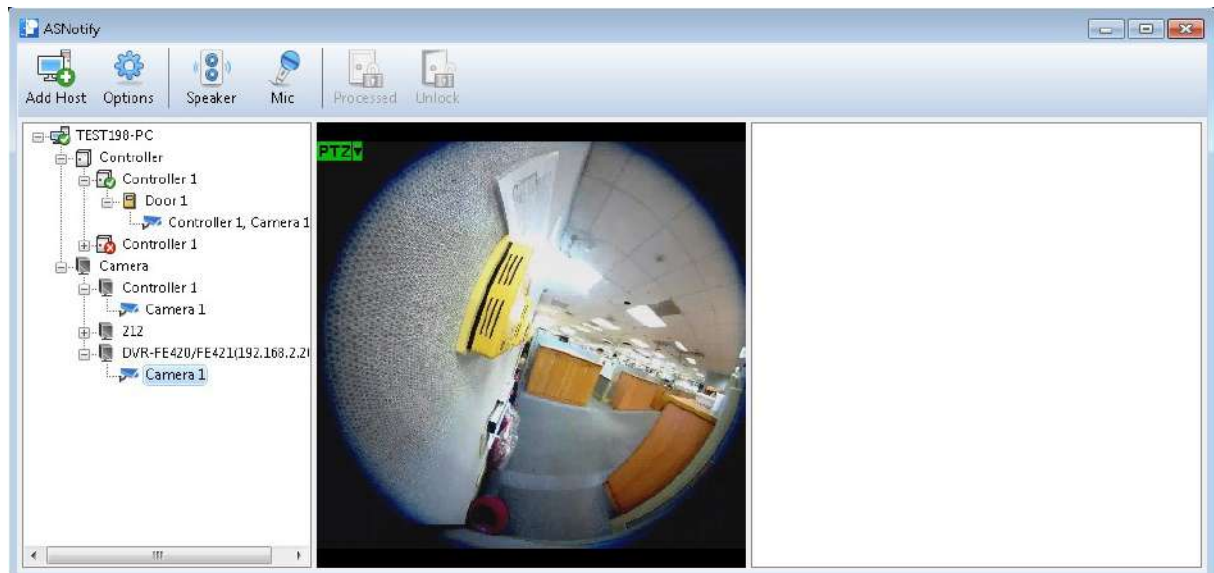


Figure 16-3

2. To speak to the access control site, click the **Mic** button.
3. To listen to audio from the access control site, click the **Speaker** button.

Note: To use the two-way audio function:

- The device must be GV-CS1320 or GV-IP Camera with two-way audio functions.
 - GV-ASManager must be connected to GV-CS1320 or GV-IP Camera directly. Audio is not supported when GV-ASManager is connected to the camera through other hosts, such as GV-DVR / NVR / VMS.
-

GV-CS1320 Functions

The snapshots and event messages will appear on the right of the GV-ASNotify window when the bell button on GV-CS1320 is activated.

1. Use the **Speaker** and **Mic** buttons to communicate with visitors, or use the **Unlock** button to grant access.
2. After handling the event, mark the notification as “Processed” by selecting the event and then clicking the **Processed** button. Events marked as Processed are grayed out.

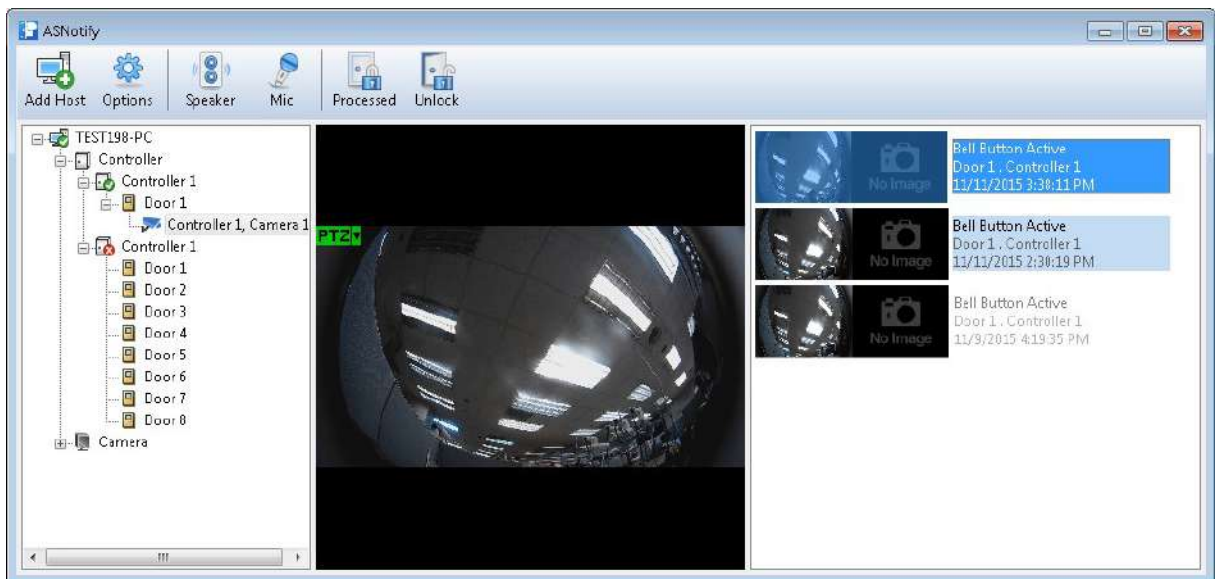


Figure 16-4

3. To trigger computer alarms or popup messages for alert when GV-ASNotify is minimized in the Windows taskbar, click **Options** to enable the related settings.

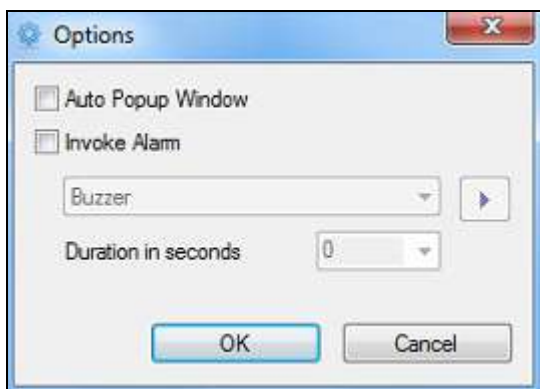


Figure 16-5

Chapter 17 Database Settings

Before you can run GV-ASManager, it is required to create a database or to upgrade your old database to fit the latest version of GV-ASManager. You can select either a **Microsoft Office Access** or **Microsoft SQL Server** to be the database of GV-ASManager.

If a database already exists, you can use **Source Database** function to convert various database formats into GV-ASManager's Microsoft Access or SQL Server formats.

Note: GV-ASManager has a size limit of 2 GB for its database. To get additional data allowance, you can install and create the Microsoft SQL Server.

17.1 Starting the Database Tools

To start the Database Tools, run **ASDBManager.exe** from the program folder to access it.

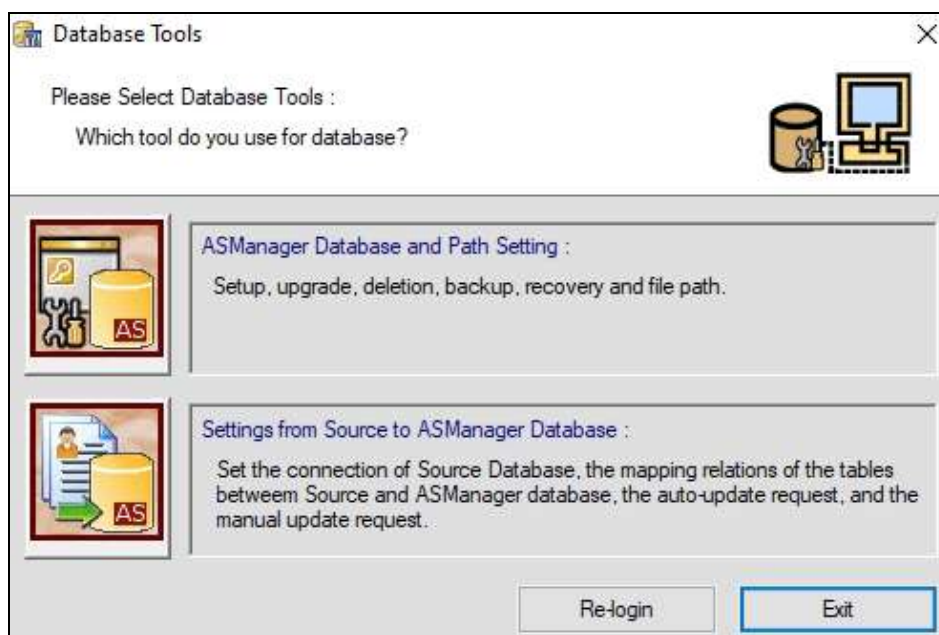


Figure 17-1

17.2 Creating a Database

You can select either Microsoft Office Access or Microsoft SQL Server as the database of GV-ASManager.

1. On the Database Tools dialog box (Figure 17-1), click **ASManager Database and Path Setting > Setup MDB / MSSQL Database for ASManager**. This dialog box appears.

Figure 17-2






2. To use Access as the database, select **Microsoft Office Access Database > OK**. The database is created in the local computer.
3. To use the SQL Server as the database, select **Microsoft SQL Server**.
 - a. Under **SQL Database Setting**, type IP address or domain name of the SQL Server in the **Data Source** field, and select its authentication way.

- b. Optionally select **Expand Data Size** to increase the maximum number of log files stored on the SQL Server.
 - c. Under **Database**, name the databases for Configuration, Log, LPR and Patrol files that will be created on the SQL Server separately.
 - d. Click **Test Connection** to test the connection to the SQL Server.
 - e. Click **OK**. The databases are created in the SQL Server.
4. Define **Keep Days** for how long to keep log data. The log data passed the Keep Days will be deleted from the database.

Note: To install Microsoft SQL Server for the first time, select **Install New SQL Server Express**. To use this function, connect your server to the Internet.

17.3 Other Database Settings

You can upgrade, delete, back up, restore, and compact the database of GV-ASManager. Select **ASManager Database Setting** on the Database Tools dialog box (Figure 17-1) to have the following functions.

Icon	Function
	[Upgrade to the latest database version] Upgrade the database to the latest version.
	[Delete ASManager Database] Remove the database from the local computer or the Microsoft SQL Server.
	[Backup Database] Specify the backup storage path and select the types of files you want to back up: Configurations, Logs, Photos and Account Profiles. You can also set up a Schedule to automatically back up the database.
	[Recovery Database] Restore the files you backed up previously to the current computer or import them to another computer.
	[Compact Database] Compact and reduce the size of the database. You can also set up a Schedule to automatically compact the database.

**[File Path Setting]**

- **Daily Auto Backup:** Specify a path to automatically save another copy of log and image data. The function is performed at 24:00 A.M every day. The default path is at C:\Access Control\ASManager\ASBackup
- **Export to File:** For third-party integration. Access data is exported to a specified storage path. Every access record will create a file and up to 5000 files can be exported.
- **Photo:** The path to save user profile photos. The default path is at C:\Access Control\ASManager\Photo
- **Folder Path:** The path to save images captured by the cameras. When **Recycle** is enabled, the oldest images will be deleted when the free hard disk space falls below a specified **Threshold**. If recycling is enabled, avoid using the same folder path for images captured and for **Daily Auto Backup**.
- **System Other Settings:** For third-party integration. The path to store the files for syncing with third-party database.
- **Base Path Setting:** Replace all the root paths of Daily Auto Backup, Export to file, Photo, Folder Path to a specified one.

Note: The log data backed up by **Daily Auto Backup** will not be affected by the **Keep Days** function (Figure 17-2).

17.4 Mapping Source Database

The Source Database function can convert **OLE DB, Active Directory** database and **excel** files into GV-ASManager (Microsoft Access or SQL Server) database. Click the **Setting from Source to ASManager Database** button on the Database Tools dialog box (Figure 17-1). This dialog box appears.



Figure 17-3

Under the **Setting** Menu:

[Set Connection] Configures the connection to an active directory or an OLEDB provider.

[Set Mapping] Maps the user, cards, vehicle or hotlist fields between the GV-ASManager database and the source database.

[Input/Modify the auto-update time setting] Specify a time to update the database automatically.

Under the **Update** Menu:

[Update User Data manually] Update the user data manually.

[Update Card Data manually] Update the card data manually.

[Update Vehicle Data Manually] Update the vehicle data manually.

[Update Vehicle Hotlist Manually] Update the vehicle hotlist manually.

17.4.1 Converting Data from the Active Directory Database

If you are using the latest version of GV-ASManager, see this [technical notice](#) for instructions on how to sync data from Windows Active Directory.

1. Click the **Set Connection** button on the Options dialog box (Figure 17-3). The Source Database dialog box appears.
2. Select **Active Directory**. This dialog box appears.

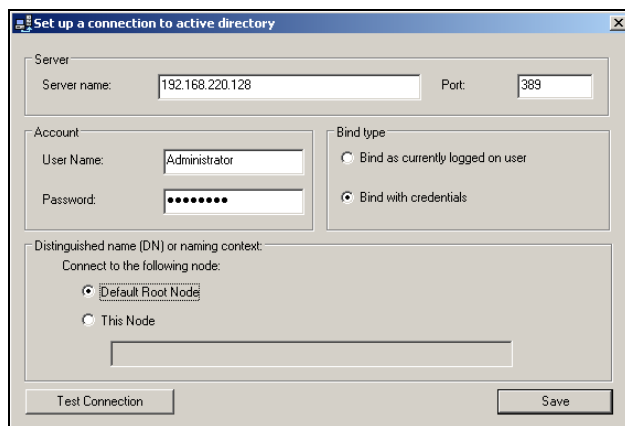


Figure 17-4

3. If you log in the local computer with the authorized username and password from the source database server, select **Bind as currently logged on user** and type the IP address or domain name of the server. If not, select **Bind with credentials**, type the IP address or domain name of the server and its login username and password.
4. Ensure the **Port** number matches that of the source database server.
5. Select **Default Root Node** to connect to the root node of the source database. Otherwise, select **This Node** and specify the node path.
6. Click **Test Connection** to connect to the source database server.
7. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 17-3) to convert the cardholder data from the source database to the GV-ASManager database immediately.
8. Click the **Update Card Data manually** button in the Options dialog box (Figure 17-3) to convert the card data from the source database to the GV-ASManager database immediately.
9. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 17-3) and specify the time in minutes.

17.4.2 Converting Data from the OLE Database

To convert data from the OLE database, you need to go through these instructions:

- **Step 1: Connect an OLE Database**
- **Step 2: Map the User Data**
- **Step 3: Map the Card / Vehicle Data**
- **Step 4: Convert the Data from the Source Database**

Step1: Connect an OLE Database:

1. Click the **Set Connection** button on the Options dialog box (Figure 17-3). The Source Database dialog box appears.
2. Select **Other Database**. This dialog box appears.

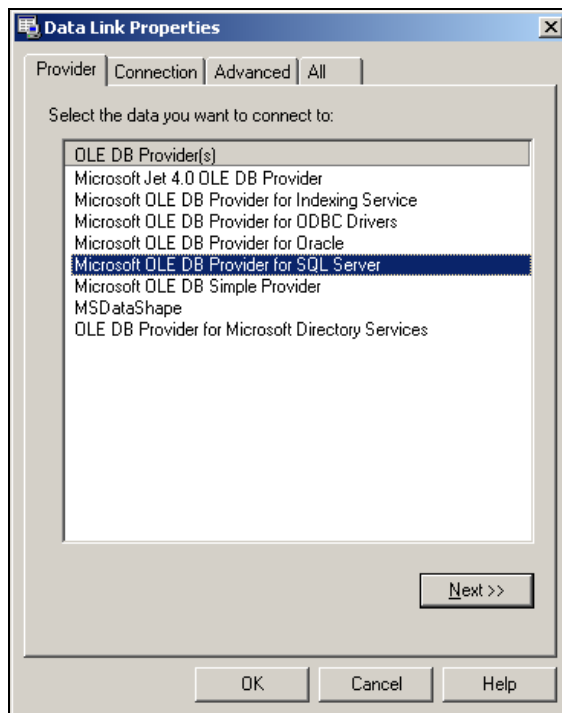


Figure 17-5

3. Select the OLE DB provider that you wish to connect to, and click **OK**. The connection dialog box appears. The dialog box varies depending on the OLE DB provider you choose. Here we select **Microsoft OLE DB Provider for SQL Server** as example.

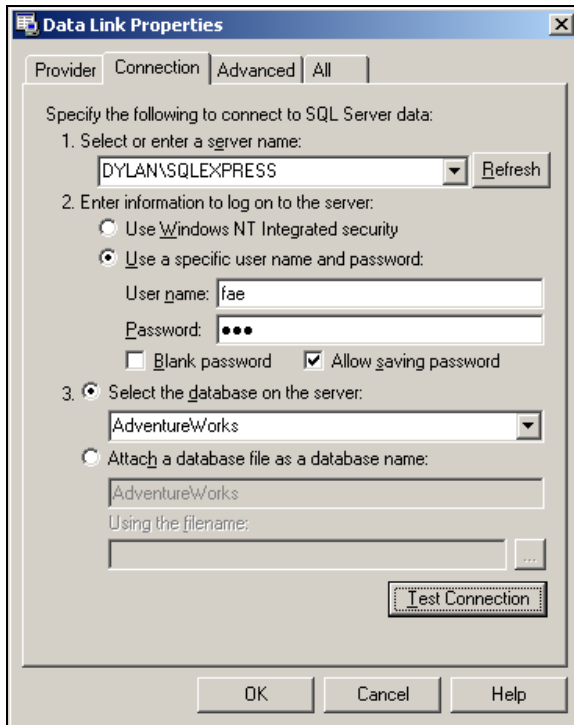


Figure 17-6

4. Type the IP address or domain name of the source database server, select its login authentication method, and select a specific database on the server. Click **Test Connection** to connect to the source database server.

Step 2: Map the User Data:

1. Click the **Set the mapping relations for user** button in the Options dialog box (Figure 17-3). This window appears.

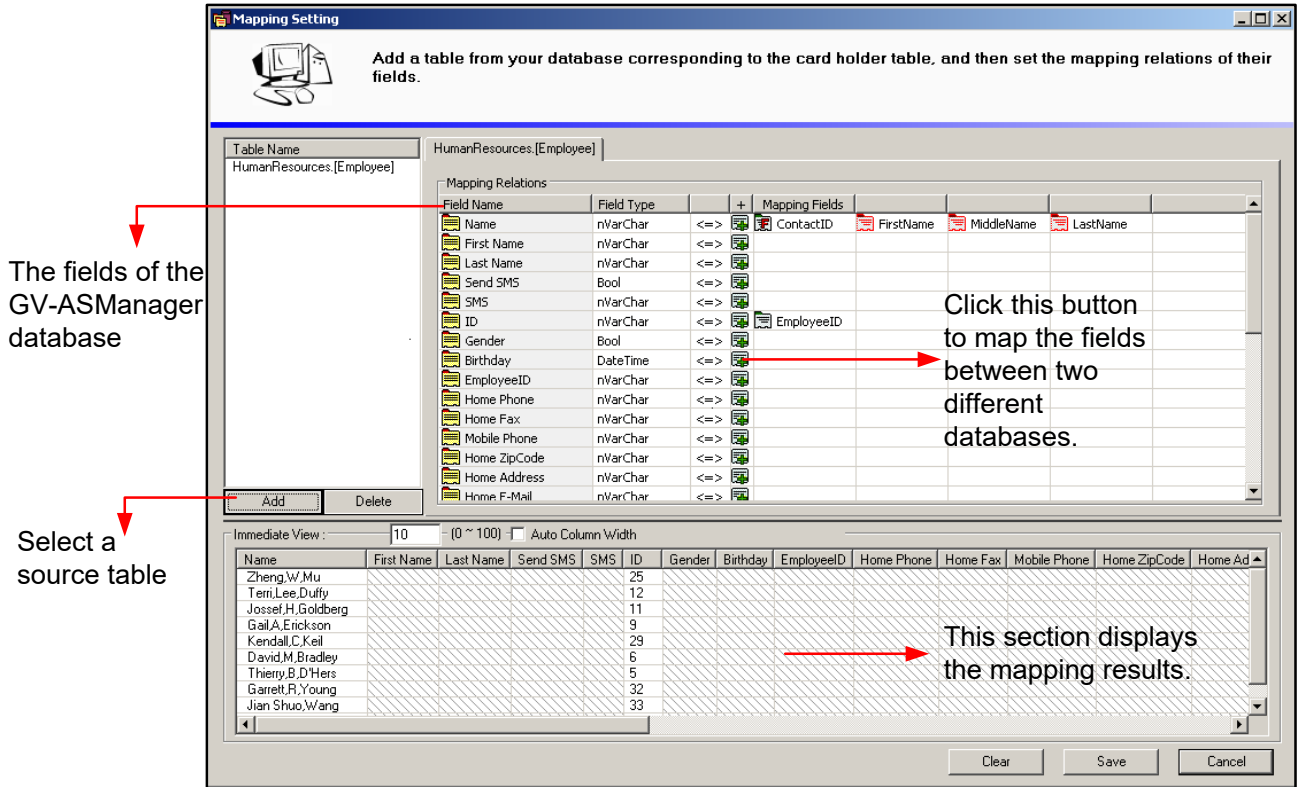


Figure 17-7

2. Click the **Add** button to select a related table on the source database.
3. Click the buttons to map each field of GV-ASManager database to a corresponding field of the source database.
4. In the following steps, we demonstrate how to map the **Name** field as example. Click the button in the Name field. This dialog box appears.

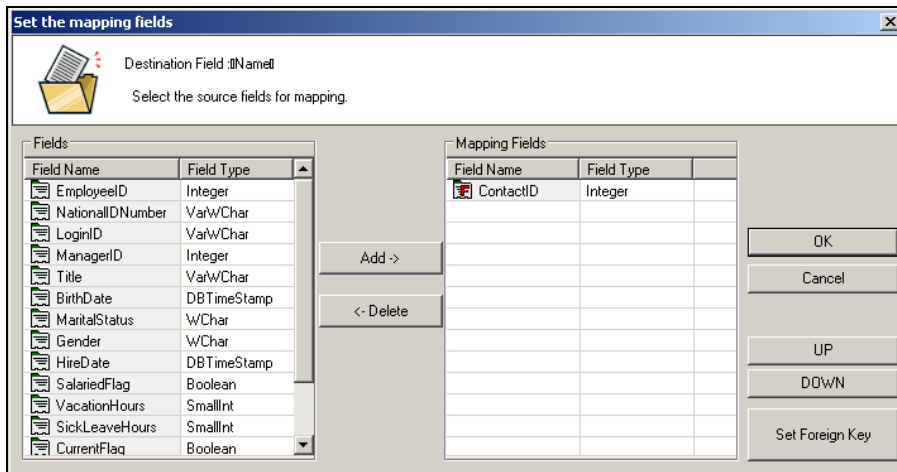


Figure 17-8

5. In the left pane of the mapping field dialog box, select the field(s) of the source database corresponding to the Name field of the GV-ASManager database. Then click **Add**. In this example (Figure 17-8), the **Contact ID** field of the source database corresponds to the **Name** field of the GV-ASManager database.
6. If the field of the source database, without having the data entered, is linked to an index or another table, click the **Set Foreign Key** button. This dialog box appears.

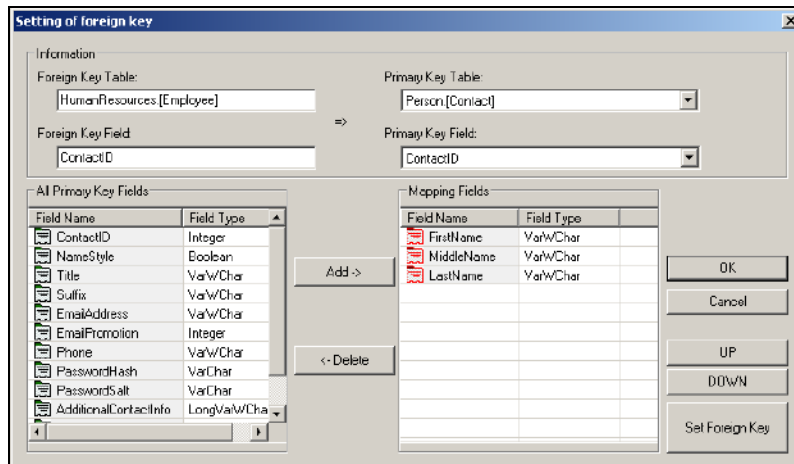


Figure 17-9

7. When the foreign key dialog box is open, the linked **Primary Key Table** and **Primary Key Field** should be displayed if the connection of the Foreign Key Table and Primary Key Table has been created. Otherwise, use the drop-down lists to select the Primary Key Table and Field.
8. In the left pane of the foreign key dialog box, select the field(s) of the Primary Key Table corresponding to the field of the Foreign Key Table. In this example (Figure 17-9), the **Contact ID** field of “Human Resource (Employee)” Foreign Key Table is linked to the **First Name, Middle Name and Last Name** fields of “Person (Contact)” Primary Key Table.
9. Click **OK**. In the Mapping Setting window, you can see the mapping results. In the example (Figure 17-9), the **Name** field of the GV-ASManager database is mapped to the **Contact ID** field of the source database which includes **First Name, Middle Name and Last Name** (which are linked from the Primary Key Table).

Note: To map the **Photo** field,

1. Click the  button and select the corresponding **Source Field**.

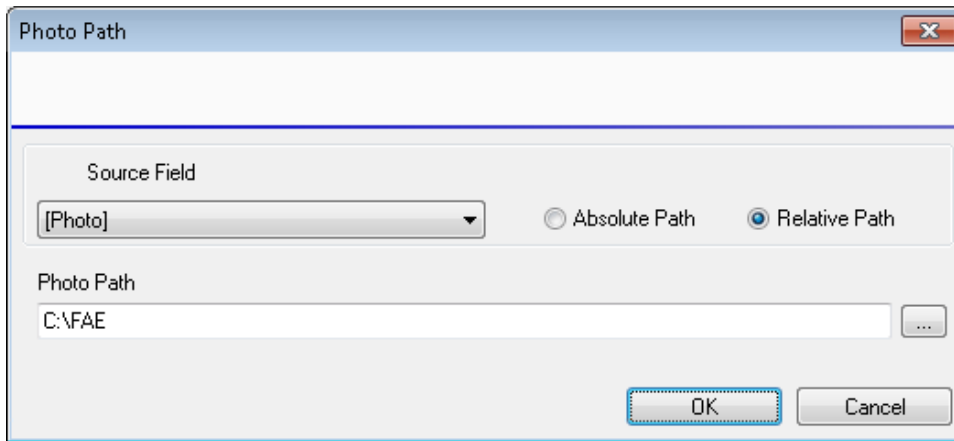


Figure 17-10

2. Select **Absolute Path** if the source field contains complete storage paths of the photos.

	A	B	C	D	E	F	G	H	I	J
1	Cardholder Name	FirstName	LastName	SendSMS	SMSMessID			Gender	BirthDay	Photo
2										
3	1	Abel Carte	Abel Carter	FALSE				TRUE	1983/11/20	C:\FAE\abel.jpg
4	2	Edwin Wa	Edwin Wang	FALSE				TRUE	1980/12/1	C:\FAE\edwin.jpg
5	4	Jesse Bol	Jesse Bolton	FALSE				TRUE	1979/1/16	C:\FAE\jesse.jpg
6	5	Jackie Lav	Jackie Lawson	FALSE				TRUE	1975/6/30	C:\FAE\jackie.jpg

Figure 17-11

3. Select **Relative Path** and appoint a folder if all photos are stored under the same folder and the source field only contains the relative path under the appointed folder.

	A	B	C	D	E	F	G	H	I	J
1	Cardholder Name	FirstName	LastName	SendSMS	SMSMessID			Gender	BirthDay	Photo
2										
3	1	Abel Carte	Abel Carter	FALSE				TRUE	1983/11/20	abel.jpg
4	2	Edwin Wa	Edwin Wang	FALSE				TRUE	1980/12/1	edwin.jpg
5	4	Jesse Bol	Jesse Bolton	FALSE				TRUE	1979/1/16	jesse.jpg
6	5	Jackie Lav	Jackie Lawson	FALSE				TRUE	1975/6/30	jackie.jpg

Figure 17-12

Step 3: Map the Card / Vehicle Data:

1. Click the **Set the mapping relations for cards / vehicles** button in the Options dialog box (Figure 17-3). This window appears.

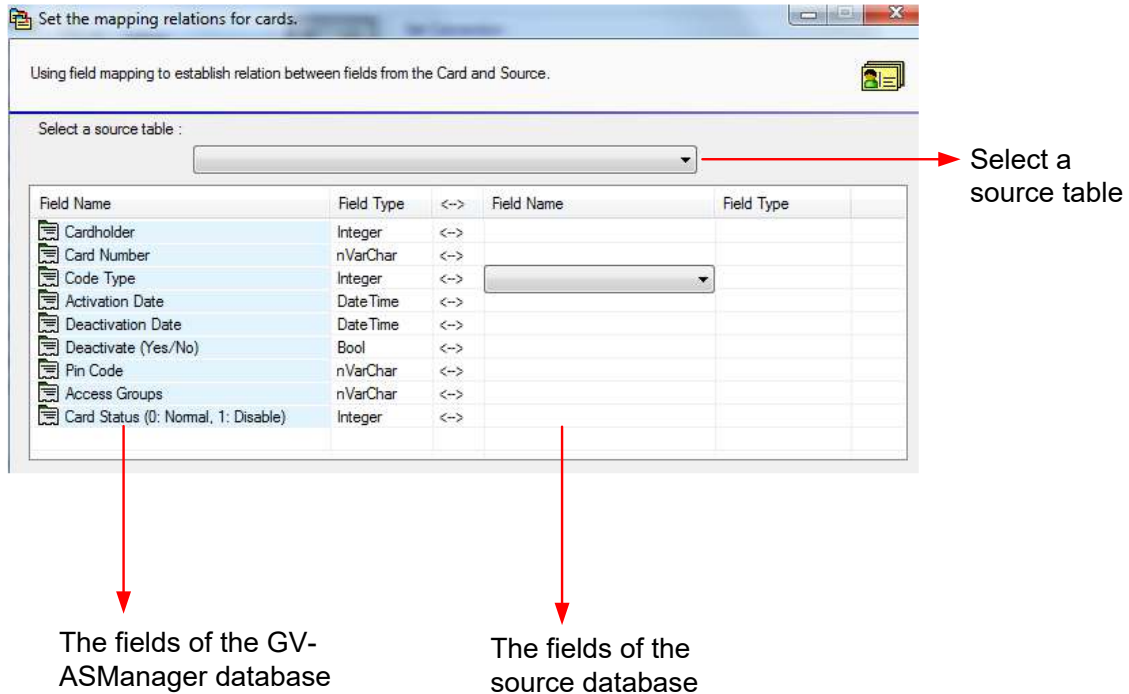


Figure 17-13

2. Select a related table on the source database.
3. Click the **Field Name** column on the right pane to map each field of the GV-ASManager database and the source database.

Step 4: Convert the Data from the Source Database:

1. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 17-3) to convert the cardholder data from the source database to the GV-ASManager database immediately.
2. Click the **Update Card Data manually** button in the Options dialog box (Figure 17-3) to convert the card data from the source database to the GV-ASManager database immediately.
3. To update the database automatically later, click the **Input/Modify the Auto-update time setting** button in the Options dialog box (Figure 17-3) and specify the update time.

17.4.3 Converting Data from an Excel File

To convert data from an excel file, follow the steps below:

1. Click the **Set Connection** button on the Options dialog box (Figure 17-3). The Source Database dialog box appears.
2. Select **Other Database**, select **Excel File**, and click **OK**.

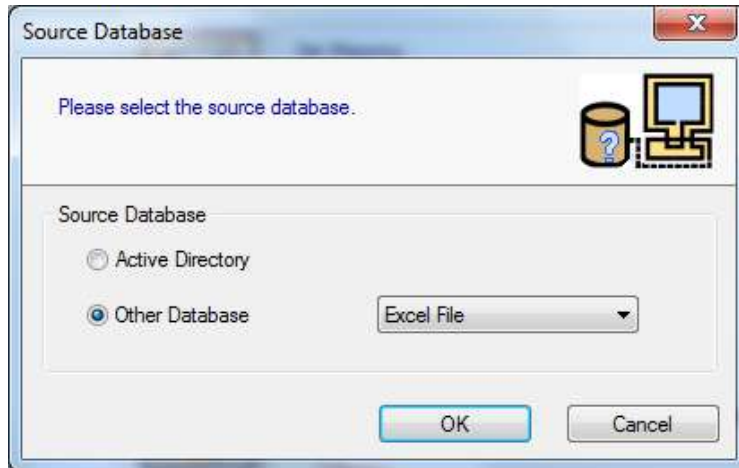


Figure 17-14

3. Locate the storage path of the excel file.
4. Follow the instructions in *Step 2: Map the User Data* and *Step 3: Map the Card / Vehicle Data* and in the previous section to match the columns of the excel files with the fields in GV-ASManager.

Chapter 18 Firmware Upgrade

For more information on how to upgrade your GV-AS Controllers, click [here](#).

Chapter 19 Troubleshooting

Q1: GV-ASManager cannot connect to GV-AS / GV-EV Controller over the Internet.

There are several causes for this problem such as IP address conflict, incorrect connection settings and network failure. The following solution is to assign a fixed IP to GV-ASManager and GV-AS / GV-EV Controller respectively. This way can determine if the problem is caused by the faulty devices or incorrect network settings.

1. Disconnect the hub or switch, which connects GV-ASManager and GV-AS / GV-EV Controller, from the network.
2. On the GV-ASManager system, specify a fixed IP address that is NOT used by another device, e.g. 192.168.0.154.

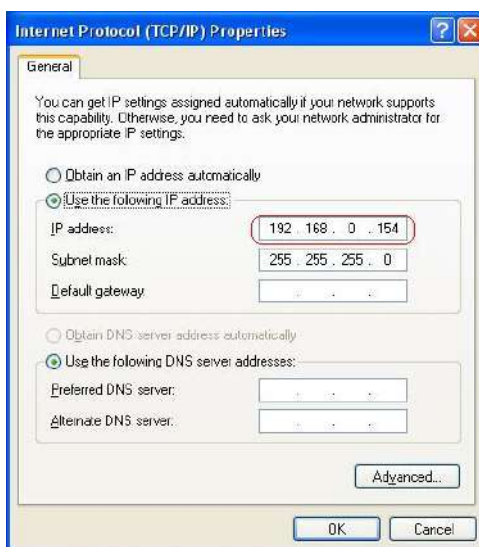


Figure 19-1

3. Reset GV-AS / GV-EV Controller to factory defaults.
 - a. Plug GV-ASKeypad to GV-AS / GV-EV Controller.
 - b. Remove the jumper cap from the 2-pin **Default** jumper.
 - c. Press the **Reset** button.
 - d. Replace the jumper cap back to the 2-pin **Default** jumper.
 - e. To reset the Ethernet Module, press and hold the **Default EN** button for 6 seconds.

- Open the browser and enter the default IP of GV-AS / GV-EV Controller:
<http://192.168.0.100>

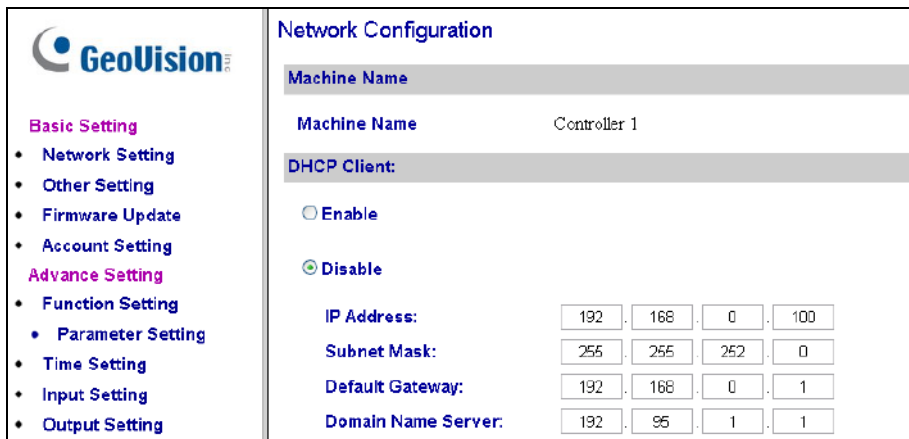


Figure 19-2

- In the IP address field, specify an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
- On the GV-ASManager system, enter the following settings:

Controller ID: 1

Network: TCP/IP

IP: 192.168.0.XXX

Port: 4000

User: admin / user-defined ID

Password: admin / user-defined password

Crypto key: 12345678

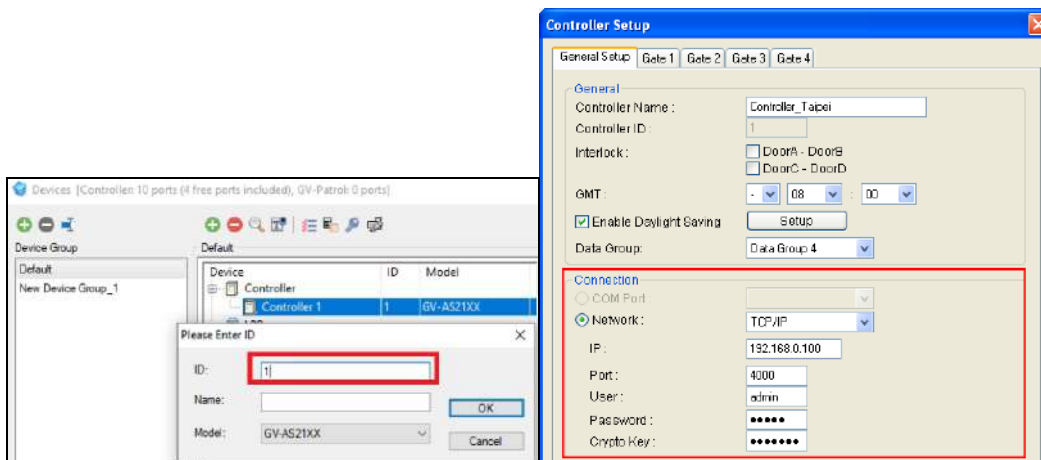



Figure 19-3

- The connection between GV-ASManager and the controller should be established, and the connection icon  should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

Q2: The connection established between GV-ASManager and GV-AS / GV-EV Controller is interrupted.

This may be due to IP address conflict. Follow these steps to troubleshoot the problem:

- Disconnect the hub or switch, which connects to GV-ASManager and GV-AS / GV-EV Controller, from the network.
- Run Windows **Command Prompt**. Take Classic Windows Start Menu for example, click **Start**, select **Accessories** and click **Command Prompt**.
- Type **arp -d** and press **Enter**.

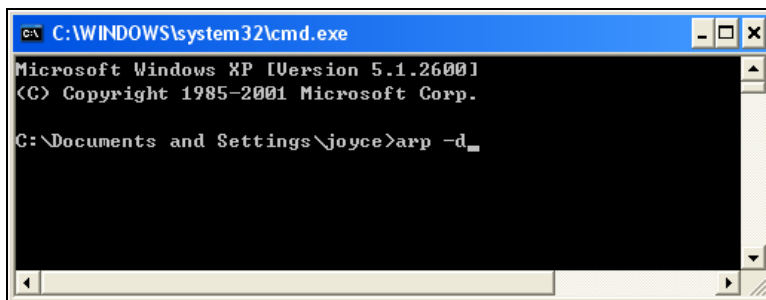


Figure 19-4

- Specify a fixed IP address that is NOT used by another device, to the GV-ASManager system. See Figure 17-1.
- Open the browser and enter the assigned IP address of the controller. The Network Configuration page appears. See Figure 19-2.
- In the IP address field, give the controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
- On the GV-ASManager system, enter the following settings. See Figure 19-3.

Controller ID: 1

Network: TCP/IP


IP: 192.168.0.XXX

Port: 4000

User: admin

Password: admin

Crypto key: 12345678

8. The connection between GV-ASManager and GV-AS / GV-EV Controller should be established, and the connection icon  should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

Q3: GV-ASManager cannot receive card messages but the reader accepts cards when the connection between GV-ASManager and GV-AS / GV-EV Controller is well established.

It may be due to memory failure in the controller. Reset both the controller module and the Ethernet module to factory default settings. Refer to Step 3 in Question 1.

Q4: GV-ASManager cannot retrieve the video from GV-DVR for playback.

1. Make sure the **Remote ViewLog Service** on **Control Center Server** is enabled on GV-DVR.
2. Make sure the time on GV-ASManager and GV-DVR is consistent.
3. Make sure the event file you want to play back has been created completely on GV-DVR. For example, the assigned time length of every recorded event on GV-DVR is 5 minutes. The desired event of 5 minutes must have been displayed on the ViewLog Event List, so you can access the event file for playback.

Q5: After I add a card by presenting to the reader, the message “Access Denied Invalid Card” still appears

(For details on adding a card, see Step 1 in *4.3.1 Adding a Single Card*.)

It may be the card format is not compatible with the controller. For GV-AS100, GV-AS110 and GV-AS120, ensure the format is 26~64 bits. Otherwise, send us the related information of your card format so that we can customize the format for you.

Q6: GV-ASManager cannot receive card messages from GV-Reader connected to GV-AS / GV-EV Controller through RS-485 interface.

1. Make sure GV-Reader is correctly wiring to the controller and Switch 4 on GV-Reader is set to OFF.
2. Make sure the correct GV-Reader ID is set on the controller.

Q7: I can't change the Advanced Settings on the Web interface of GV-AS / GV-EV Controller. The "Submit" button is missing.

To modify the Advanced Settings, make sure the **Web Setting Switch** on the controllers is set to ON. For the location of the Web Setting Switch, refer to the *Web Setting Switch* section of each controller or GV-ASNet / GV-ASBox.

Q8: After installing GV-ASManager, the message "d3dx9_40.dll cannot be found" appears.

Make sure DirectX End-User Runtimes is installed and restart the computer afterwards. To install DirectX End-User Runtimes, visit [Microsoft's website](#).

Q9: What ports should I open to enable external network access with GV-ASManager?

Devices	Ports
Controller	4000 (data and command transmission)
GV-CS1320	4000 (data and command transmission); 10000 (video transmission) To enable push notifications of 'door bell activated' events, certain ports are required to be opened in GV-ASManager's server: <ul style="list-style-type: none"> • For GV-ASManager V5.3.0 and earlier, open Port 2195 (for iOS) and 443 (for Android) • For GV-ASManager V5.3.1 and later, open Port 443 (for iOS and Android)
PC-LPR	3388, 5611, 5552
Standalone LPR	443, 10000 (video transmission)



Q10: How can I find more help?

Visit our website at <http://www.geovision.com.tw>

Write to us at support@geovision.com.tw

Appendix

A. Event Notifications

- “Alarm” events

Type	Description
Force Open	Door <name> is forcibly open.
Duress	Duress function is triggered. See “Duress” in <i>1.2 Concepts</i> .
Tamper	Tamper Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in GV-AS / GV-EV Controller User’s Manual . For software settings, see <i>4.2.2 Configuring Doors or Elevator Floors</i> .
Fire Alarm	Fire Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in GV-AS / EV Controller User’s Manual . For software settings, see <i>4.2.2 Configuring Doors and Elevator Floors</i> .
Held Open	Door <name> is held open over the specified time. See <i>4.2.2 Configuring Doors and Elevator Floors</i> .
Access Denied	The access is rejected.

- “Access” events

Type	Description
Access Granted	The access is granted because the access card is approved.
Access Granted: Card Entry	The access is granted because the door contact sensor is triggered and the Anti-Passback function is also enabled.
Access Denied: Invalid Card	The access is rejected because an unknown card is presented.
Access Denied: Card Suspended	The access is rejected because Card <Status> is inactive.
Access Denied: Wrong PIN	The access is rejected because the PIN number entered is wrong.
Access Denied: Card Expired	The access is rejected because <Deactivation Date> is expired.

Access Denied: Invalid schedule	The access is rejected because the user access is not on the programmed schedule.
Access Denied: Wrong Door	The access is rejected because the user has access to the wrong door.
Access Denied: APB (Double Entry)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded twice.
Access Denied: APB (No Entry)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as exit, without entry, to a secure area.
Access Denied: APB (No Exit)	The access is rejected because the Anti-Passback rule is violated. Card <Number> is recorded as entry, without exit, to a secure area.
Access Denied: Unknown Card	The access is rejected because the card format is not compatible.
Access Denied: Invalid Start Date	The access is rejected because Card <Number> is not enabled.
Access Denied: Previous Door Still Open (Interlock)	The access is rejected because the Interlock function is violated. The entry door is left unlocked/open. See “Interlock” at Step 5 in <i>4.2.1 Step 1: Configuring a Controller</i> .

- “Event” events

Type	Description
Force Open	Door <name> is forcibly open.
Duress	Duress function is triggered. See “Duress” in <i>1.2 Concepts</i> .
Tamper	Tamper Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in GV-AS / GV-EV Controller User’s Manual . For software settings, see <i>4.2.2 Configuring Doors or Elevator Floors</i> .
Fire Alarm	Fire Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in GV-AS / GV-EV Controller User’s Manual . For software settings, see <i>4.2.2 Configuring Doors or Elevator Floors</i> .
Held Open	Door <name> is held open over the specified time. See <i>4.2.2 Configuring Doors or Elevator Floors</i> .
Access Denied	The access is rejected.


















Alarm Restored	Alarm sounds are cleared.
Forced Open-Restored	Force Open alarm is cleared.
Duress Restored	Duress alarm is cleared.
Tamper Restored	Tamper alarm is cleared.
Fire Alarm Restored	Fire alarm is cleared.
Held Open Restored	Held Open alarm is cleared.
Restored Alarm Failed	Fail to clear alarm sounds.
Clear Forced Open Event Failed	Fail to clear Force Open alarm.
Clear Duress Event Failed	Fail to clear Duress alarm.
Clear Tamper Event Failed-No Event Present	Fail to clear Tamper alarm.
Clear Fire Alarm Event Failed-No Event Present	Fail to clear Fire alarm.
Clear Held Open Event Failed	Fail to clear Held Open alarm.
Clear Access Denied Failed	Fail to clear Access Denied alarm.
Clear Tamper Event Failed-I/O Still Unclear	Fail to clear Tamper alarm because Tamper Inputs remain triggering.
Clear Fire Event Failed-I/O Still Unclear	Fail to clear Fire alarm because Fire Inputs remain triggering.
Door Open	Door <name> is open.
Door Close	Door <name> is close.
Door Unlock	Door <name> is unlocked.
Door Lock	Door <name> is locked.
Two Person Rule-Active	Two-person A/B rule is active when Card <number> is presented.
Two Person Rule-Confirm	Two-person A/B rule is confirmed when Card <name> is presented after the other AB card.
Two Person Rule-Inactive	Two-person A/B rule is violated when Card <name> is presented successively or the other AB Card isn't presented within 20 seconds.
Keypad Code Confirm	On the Card or Common mode, the password entered is correct.
Wrong Keypad Code	On the Card or Common mode, the password entered is wrong.
Door Bell Activated	The doorbell of Door <name> is activated.
Release Mode	Door <name> is on the Release Mode.

	See 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Card or Common Mode	Door <name> is on the Card or Common Mode. See 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Card and PIN Code Mode	Door <name> is on the Card and PIN Code mode. See 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Card Mode	Door <name> is on the Card mode. See 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Fire Unlock Mode	Door <name> is unlocked after Fire Inputs are triggered. See “Fire Action” in 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Fire Lock Mode	Door <name> is locked after Fire Inputs are triggered. See “Fire Action” in 4.2.2 Step 2: <i>Configuring the Doors or Elevator Floors</i> .
Force Unlock Remotely	Door <name> is unlocked remotely from the control of GV-ASManager or GV-ASRemote server.
Force Lock Remotely	Door <name> is locked remotely from the control of GV-ASManager or GV-ASRemote server.
Disable Remote Door Lock Operation	The event of “Force Unlock Remotely” or “Force Lock Remotely” is cleared.
Force Unlock Locally	Door <name> is unlocked on the site of Door Controller.
Force Lock Locally	Door <name> is locked on the site of Door Controller.
Disable Local Door Lock Operation	The event of “Force Unlock Locally” or “Force Lock Locally” is cleared.
Reset	Door Controller <name> is reset.

- “LPR” events

Type	Description
Plate Recognized: Registered Vehicle	Access for a registered vehicle granted according to the Authentication Schedule
Plate Recognized: Registered Vehicle (Invalid Schedule)	Access for a registered vehicle denied according to the Authentication Schedule
Plate Recognized: Registered Vehicle (Vehicle plate and card number do not match)	Access denied for a registered vehicle due to unmatched access card, during LPR and Card Mode
Plate Recognized: Unregistered Vehicle	Access granted for a visitor vehicle
Plate Recognized: Unregistered Vehicle (Invalid Schedule)	Access denied for a visitor vehicle as according to the Authentication Schedule
Parking Access Granted: Vehicle Added Manually	Access of a vehicle to parking lot granted by manually typing its license plate
Parking Access Granted: Vehicle Added Manually and Gate Opened	Access of a vehicle to parking lot granted and gate opened by manually typing its license plate
Parking Access Granted: Vehicle Removed Manually	Access of a vehicle to parking lot granted and its license plate is removed manually
Parking Access Granted: Vehicle Removed Manually and Gate Opened	Access of a vehicle to parking lot granted, gate opened and its license plate is removed manually
Parking Access Denied: Gate Disabled	Access to parking lot denied and gate does not open
Parking Access Denied: Full	Access to parking lot denied due to reaching its maximum vehicle capacity
Parking Access Denied: Re-entry	Access to parking lot denied due to the vehicle has already entered with no exit record
Parking Access Denied: No entry record	Access to parking lot denied due to the vehicle has no enter record
Parking Access Denied: Share Space Full	Access to parking lot denied due to reaching its maximum public parking capacity
Parking Request Failed	Access to parking lot denied due to disconnecting between PC LPR (with GV-LPR Plugin) and GV-ASManager
Authentication Not Completed	Access denied due to failed authentication of either the license plate or access card under LPR and card mode
Plate Not Recognized	Access denied for unrecognizable license plate
SD Card Write Failed	SD card of GV-LPR1200 failed to write data
SD Card Full	SD card of GV-LPR1200 reached its maximum storage capacity

B. E-Mail and SMS Alert Symbols

Icon	Description
	%M (Message): include related alert message.
	%m (Device Group): include the name of triggered device group.
	%T (Controller): include the name of triggered controller.
	%D (Door): include the name of triggered door.
	%L (Local Time): include local time.
	%U (UTC): include UTC time.
	%S (Snapshot): include snapshot.
	%Q (Direction): include the direction of triggered LPR lane.
	%N (Card Number): include card number.
	%H (User Name): include user name.
	%G (Gender): include user's gender.
	%E (Employee ID): include employee ID.
	%Y (Company): include company name.
	%K (Division): include division name.
	%P (Department): include department name.
	%F (Office): include office name.
	%C (Photo): include user's photo.

C. Controller Status

Status	Description
Disconnected (Login Failed)	The username, password or crypto key (3DES) entered is wrong.
Disconnected (Duplicate Connection)	Another GV-ASManager is connecting with the controller.
Disconnected (Hardware Error)	The Controller ID entered is wrong. Or controller errors occur.

D. Supported ML Engines of PC LPR

The latest GV-DVR LPR / GV-VMS LPR only supports the following versions of *Machine Learning (ML)* recognition engines:

No.	Country	Engine Version	No.	Country	Engine Version
1	Argentina	6.0.2.0	20	Israel	3.1.2.2
2	Australia	4.2.1.1	21	Italy	6.0.2.1
3	Austria	6.0.2.0	22	Mexico	4.5.5.6
4	Belgium	6.0.2.0	23	Morocco	6.0.2.7
5	Brazil	6.0.2.0	23	Netherlands	6.0.2.0
6	Bulgaria	6.0.2.0	24	New Zealand	6.0.2.0
7	Canada	6.0.2.0	25	Norway	6.0.2.0
8	Chile	3.2.0.9	26	Poland	6.0.2.0
9	China	4.2.1.3	27	Portugal	6.0.2.6
10	Columbia	4.2.1.5	28	Qatar	3.1.2.2
11	Croatia	6.0.2.0	29	Russia	6.0.2.0
12	Czech	6.0.2.0	30	Slovakia	6.0.2.0
13	France	6.0.2.0	31	South Africa	6.0.0.9
14	Germany	6.0.2.4	32	Spain	6.0.2.0
15	Global	6.0.2.0	33	Taiwan	4.5.5.9
16	Hong Kong	6.0.1.2	34	UK	6.0.2.0
17	Hungary	6.0.2.0	35	USA	4.2.1.4
18	India	4.2.1.1	36	Vietnam	4.2.1.1
19	Ireland	6.0.2.0			

E. Supported Number of Connections

The following is the maximum number of applications and devices that a GV-ASManager system can establish connections with.

Application / Device	Number of Connections to a GV-ASManager
GV-ASRemote	Unlimited
GV-ASNotify	Unlimited
GV-ASWeb	128 connections
GV-Access app	128 apps
GV-I/O Box	16 sets of GV-I/O Boxes