



# GV-ASManager

## *User's Manual*





© 2018 GeoVision, Inc. All rights reserved.

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

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

**Note:** No memory card slot or local storage function for Argentina.

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

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

January 2018

## Contents

<b>Note for Users Upgrading GV-ASManager .....</b>	<b>vi</b>
<b>Firmware and Software Compatibility .....</b>	<b>viii</b>
<b>Naming and Definition.....</b>	<b>xi</b>
<b>Chapter 1 Introduction.....</b>	<b>1</b>
1.1 Main Features .....	2
1.2 Concepts.....	5
1.3 Optional Devices .....	7
<b>Chapter 2 Installation.....</b>	<b>8</b>
2.1 System Requirements .....	8
2.2 Installing the GV-ASManager .....	9
2.3 Logging in .....	11
<b>Chapter 3 The Main Screen of GV-ASManager.....</b>	<b>13</b>
3.1 Main Screen.....	13
3.1.1 Toolbar .....	15
3.2 Controllers / LPRs View .....	17
3.2.1 Controls on the Window .....	17
3.3 Monitoring Windows .....	19
3.3.1 Controls on the Window .....	19
3.3.2 Customizing a Monitoring Window .....	21
3.3.3 Arranging Monitoring Windows.....	22
<b>Chapter 4 Settings .....</b>	<b>23</b>
4.1 Setup Flowchart .....	23
4.2 Adding Controllers.....	24
4.2.1 Step 1: Configuring a Controller .....	24
4.2.2 Step 2: Configuring the Doors or Elevator Floors .....	27
4.3 Setting Cards .....	35
4.3.1 Adding a Single Card .....	35
4.3.2 Adding a Group of Cards.....	40
4.3.3 Adding a Passcode .....	41
4.3.4 Importing/Exporting Card Data .....	43
4.3.5 Customizing a Card Data Field.....	45
4.4 Setting Weekly Schedules.....	46
4.4.1 Step 1: Setting Time Zones.....	47
4.4.2 Step 2: Setting Weekly Schedules.....	49
4.4.3 Step 3: Setting Holidays .....	51
4.5 Setting Access Groups.....	52
4.6 Setting Users .....	55

4.6.1	Adding a User .....	55
4.6.2	Customizing a User Data Field .....	58
4.6.3	Importing/Exporting User Data .....	59
4.7	Adding IO Boxes .....	60
4.7.1	Step 1: Configuring GV-I/O Box to GV-ASManager .....	60
4.7.2	Step 2: Configuring the input and output functions .....	62
<b>Chapter 5</b>	<b>Video Integration .....</b>	<b>64</b>
5.1	Mapping Cameras .....	65
5.2	Accessing a Live View .....	67
5.2.1	Live Video Window .....	68
5.3	Accessing a Video Image .....	69
5.4	The MultiView Window .....	69
5.4.1	Adding a Matrix View .....	71
5.5	Retrieving Recorded Video .....	72
5.6	Using Text Overlay .....	74
<b>Chapter 6</b>	<b>Anti-Passback .....</b>	<b>76</b>
6.1	Anti-Passback .....	77
6.2	Local Anti-Passback .....	78
6.3	Global Anti-Passback .....	80
6.3.1	Step 1: Enabling Global Anti-Passback .....	80
6.3.2	Step 2: Configuring Areas .....	81
6.3.3	Step 3: Configuring Readers .....	82
6.3.4	Step 4: Configuring Door Contacts .....	82
6.3.5	Step 5: Monitoring Areas .....	84
6.3.6	Step 6: Locating Users .....	85
<b>Chapter 7</b>	<b>Patrol Tour .....</b>	<b>86</b>
7.1	Creating Patrol Tour .....	86
7.2	Activating the Patrol Tour .....	89
7.3	Monitoring Patrol Activities .....	91
7.4	Accessing Patrol Log .....	92
<b>Chapter 8</b>	<b>Other Functions .....</b>	<b>93</b>
8.1	Setting Up System User .....	93
8.2	Setting Up Alert Notification .....	96
8.2.1	Setting SMS Server .....	96
8.2.2	Setting E-Mail Server .....	97
8.2.3	Setting Notification .....	99
8.3	Startup, Backup and Export Setup .....	102
8.4	Setting Up GV-GF Fingerprint Readers .....	104
8.5	Setting Up GV-FR Face Recognition Readers .....	105



8.6	Scanning Driver's Licenses and Business Card .....	106
8.7	Setting Hot Keys .....	109
8.8	Using Remote Lock Down App.....	110
8.9	Defining New Card Formats .....	115
8.10	Monitoring Emergency Exits with Input Sensors.....	117
8.11	Designing and Printing Access Card Template.....	119
8.12	Utilizing Job Codes .....	124
<b>Chapter 9</b>	<b>GV-ASRemote .....</b>	<b>127</b>
9.1	Installing GV-ASRemote .....	127
9.2	The GV-ASRemote Window .....	128
9.2.1	Windows Toolbar .....	130
9.3	Connecting to GV-ASManager .....	131
9.4	GV-ASRemoteWeb .....	133
<b>Chapter 10</b>	<b>GV-ASWeb.....</b>	<b>134</b>
10.1	Connecting to GV-ASManager .....	134
10.2	Accessing Live Video .....	137
10.3	Monitoring GV-ASManager .....	138
10.4	Accessing Logs .....	140
10.4.1	Setting Search Criteria .....	140
10.4.2	Log Window Icons .....	141
10.4.3	Exporting Logs .....	141
10.4.4	Defining Columns .....	142
10.5	Adding and Deleting Controllers / LPR .....	144
10.6	Adding and Deleting Cards and Users .....	146
10.7	Searching, Adding and Deleting IP Cameras .....	150
10.8	Setting Schedule .....	152
10.8.1	Setting Daily Schedule .....	152
10.8.2	Setting Weekly Schedule.....	153
10.8.3	Specifying Holiday .....	154
10.9	Setting Access Groups.....	154
10.10	Setting Door Groups.....	155
10.11	Configuring Areas for Anti-Passback .....	156
10.12	Creating Maps .....	157
10.13	Setting Export Schedule for Lists and Logs .....	160
10.14	Setting Up Other Functions .....	162
10.15	Creating Accounts to Manage GV-ASWeb .....	163
10.16	Accessing GV-ASWeb using Mobile Devices .....	165
<b>Chapter 11</b>	<b>GV-TAWeb for Workforce Schedule and Payroll .....</b>	<b>168</b>
11.1	Connecting to GV-ASManager .....	169

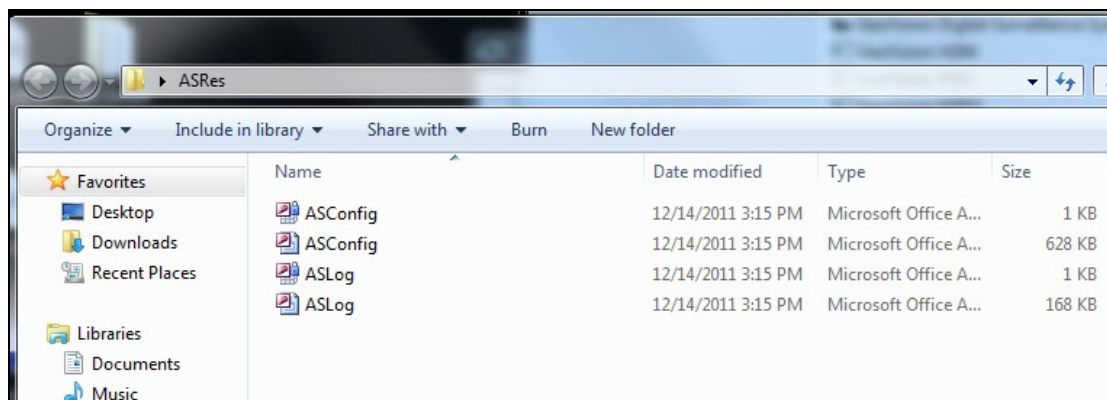
11.2	Setting Up Workforce Schedule .....	172
11.2.1	TA Shift: Setting Up a Daily Schedule .....	172
11.2.2	TA Template: Setting Up a Schedule Template .....	174
11.2.3	TA Holidays: Setting Certain Dates as Holidays .....	175
11.2.4	TA Schedule: Assigning Schedules to Employees.....	176
11.3	TA User: Specifying Hourly Pay .....	180
11.4	TA Report: Looking Up Records.....	181
11.5	Creating Accounts to Manage GV-TAWeb .....	187
<b>Chapter 12</b>	<b>GV-VMWeb for Visitor Management .....</b>	<b>188</b>
12.1	Connecting to GV-ASManager .....	188
12.2	Creating Accounts to Manage GV-VMWeb .....	190
12.3	Creating Visitor Profile.....	192
12.4	Granting Visitor Access .....	193
12.5	Searching GV-VMWeb Database .....	195
12.6	Visitor Self Registration .....	195
12.6.1	Setting Up Mail Server in GV-VMWeb .....	196
12.6.2	Creating a Visitor Account .....	198
12.6.3	Creating a Visit Request.....	199
<b>Chapter 13</b>	<b>License Plate Recognition .....</b>	<b>201</b>
13.1	Installing PC LPR .....	203
13.1.1	System Requirements .....	203
13.1.2	Installing LPR Plugin .....	206
13.1.3	Inserting LPR Dongle .....	206
13.1.4	Accessing Recognition Results on PC LPR.....	207
13.2	Setting Up PC LPR .....	208
13.2.1	Step 1: Enabling LPR Functions on PC LPR .....	209
13.2.2	Step 2: Adding PC LPR to GV-ASManager .....	211
13.2.3	Step 3: Configuring a Channel .....	213
13.2.4	Exporting LPR Data.....	218
13.3	Setting Up Standalone LPR.....	224
13.3.1	Step 1: Enabling Connection with GV-ASManager .....	225
13.3.2	Step 2: Adding Standalone LPR to GV-ASManager .....	226
13.3.3	Step 3: Configuring a Channel .....	228
13.4	Adding Vehicles .....	230
13.5	Monitoring LPR Activities .....	233
13.5.1	LPR Device View .....	233
13.5.2	Monitoring Windows .....	234
13.6	Receiving Notifications for LPR Activities .....	235
13.7	Setting Up Vehicle Hotlist.....	236

13.7.1	Setting Up the Hotlist Database.....	236
13.7.2	Adding License Plates to the Hotlist .....	237
13.8	Managing Parking Lots.....	240
13.8.1	Setting Up a Parking Lot.....	240
13.8.2	Monitoring Parking Lots.....	244
13.9	LPR Functions in GV-ASWeb.....	247
13.9.1	LPR List .....	248
13.9.2	Vehicle List.....	249
13.9.3	LPR Log .....	250
13.9.4	Access Group Setup .....	253
<b>Chapter 14</b>	<b>GV-Access Mobile Applications .....</b>	<b>254</b>
<b>Chapter 15</b>	<b>GV-ASNotify .....</b>	<b>255</b>
15.1	Installing GV-ASNotify .....	255
15.2	Connecting to GV-ASManager .....	256
15.3	Utilizing GV-ASNotify .....	257
<b>Chapter 16</b>	<b>Database Settings .....</b>	<b>259</b>
16.1	Starting the Database Tools .....	259
16.2	Creating a Database .....	260
16.3	Other Database Settings .....	261
16.4	Mapping Source Database .....	263
16.4.1	Converting Data from the Active Directory Database.....	265
16.4.2	Converting Data from the OLE Database .....	266
16.4.3	Converting Data from an Excel File .....	272
<b>Chapter 17</b>	<b>Net Module Utility .....</b>	<b>273</b>
<b>Chapter 18</b>	<b>Troubleshooting .....</b>	<b>274</b>
<b>Appendix 280</b>		
A.	Compatible IP Devices.....	280
B.	Event Notifications .....	281
C.	E-Mail and SMS Alert Symbols.....	285
D.	Controller Status.....	286
E.	Supported Recognition Engines of PC LPR.....	287

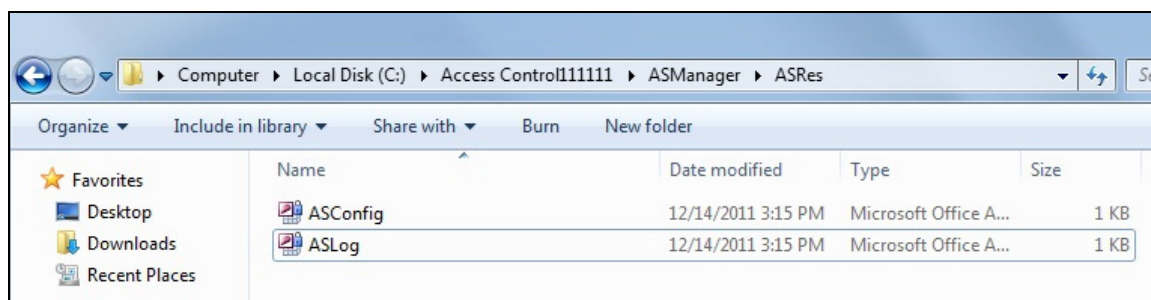
## Note for Users Upgrading GV-ASManager

You can keep your current database when upgrading GV-ASManager to the latest version. Follow the steps below to back up the current database and restore it to the GV-ASManager after upgrading to the latest version.

1. Go to **:\Access Control\ASManager\ASRes\** and there should be four files.

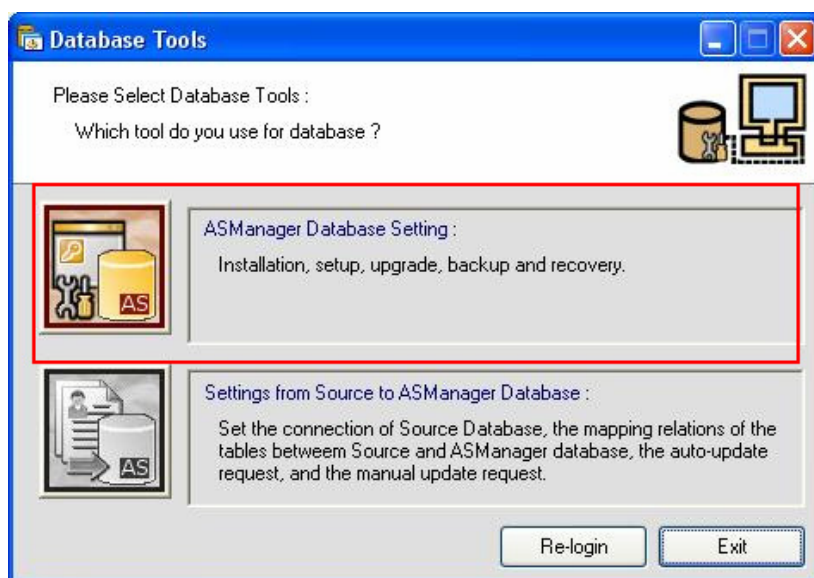


2. Back up the four files in the folder.
3. Uninstall the old **GV-ASManager**. After uninstalling, only two files remain in the ASRes folder.

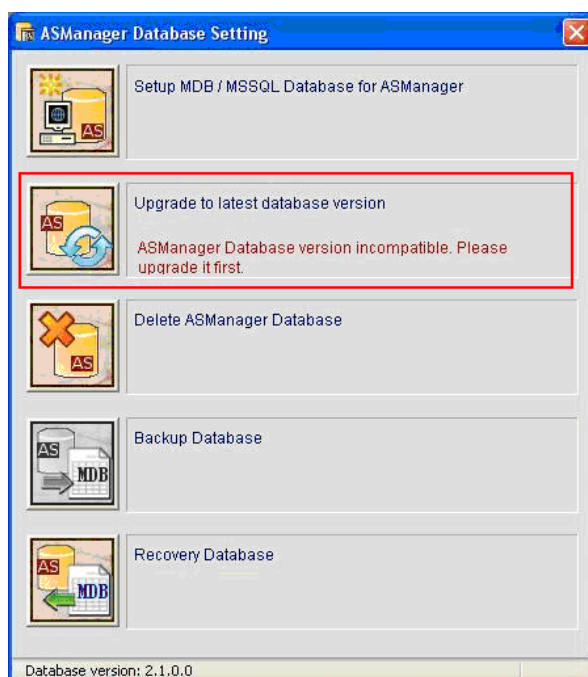


4. Install the latest **GV-ASManager**.
5. Copy and paste the four files you backed up back to **:\Access Control\ASManager\ASRes**.
6. Run **ASDBManager.exe** from the GV-ASManager program folder at **:\Access Control\ASManager**.

7. Select **ASManager Database Setting**.



8. Select **Upgrade to latest database version**.



9. The GV-ASManager starts upgrading the database. When the upgrade is complete and the message "Upgrade database successfully" appears, click **OK**.

---

**Note:** After you upgrade GV-ASManager, it is recommended to also upgrade the GV-AS / GV-EV Controller firmware. To upgrade the controller firmware, use the **Update to the latest firmware version** function in the Net Module Utility. See *Chapter 17*.

---

## Firmware and Software Compatibility

The GV-DVR / NVR / VMS versions compatible with GV-ASManager V4.2.3 - V5.0.2.0 are listed below.

GV-ASManager Version	GV-DVR / NVR Version	GV-VMS Version
<b>GV-ASManager V5.0.1.0 – V5.0.2.0</b>	GV-DVR / NVR V8.7.3.0	GV-VMS V16.11.0.0
<b>GV-ASManager V5.0</b>	GV-DVR / NVR V8.7.1.0	GV-VMS V16.11.0.0
<b>GV-ASManager V4.4.3</b>	GV-DVR / NVR V8.7.1.0	GV-VMS V15.11.3
<b>GV-ASManager V4.4.2</b>	GV-DVR / NVR V8.7.0.0 / V8.7.1.0	GV-VMS V15.10 / V15.11
<b>GV-ASManager V4.4.1</b>	GV-DVR / NVR V8.6.2.0 / V8.7.0.0	GV-VMS V15.10
<b>GV-ASManager V4.3.5 – V4.4</b>	GV-DVR / NVR V8.6.2.0	GV-VMS V15.10
<b>GV-ASManager V4.3</b>	GV-DVR / NVR V8.6.0.0	Not supported
<b>GV-ASManager V4.2.3</b>	GV-DVR / NVR V8.5.9.0	Not supported

The GV-AS / GV-EV Controller firmware versions compatible with GV-ASManager V4.2.3 - V5.0.2.0 are listed below.

	GV-ASManager				
Models	V4.2.3	V4.3	V4.35	V4.4	V4.4.1
GV-AS100	V1.08				
GV-AS110 / 120	V1.07				
GV-AS200	V2.02				N/A
GV-AS200 Ethernet Module	V2.01				N/A
GV-AS400	V1.06				
GV-AS1010	V1.0	V1.1	V1.2		V1.3
GV-AS1110	V1.0	V1.1	V1.2		
GV-AS1520	N/A				
GV-AS410	V1.23	V1.3		V1.4	
GV-AS210 / 810	V1.23	V1.3		V1.4	
GV-AS2110 / 4110 / 8110	V1.23	V1.3		V1.4	
GV-AS4111 / 81111	V1.23	V1.3		V1.4	
GV-AS2120	N/A	V1.35		V1.4	
GV-CS1320	N/A		V1.0	V1.10	
GV-EV48	V1.12	V1.3		V1.4	
GV-ASBox / GV-ASNet (Optional devices)	V1.07				



	GV-ASManager				
Models	V4.4.2	V4.4.3	V5.0	V5.0.1.0	V5.0.2.0
GV-AS100	V1.08	N/A			
GV-AS110 / 120	V1.07	N/A			
GV-AS200	N/A				
GV-AS200 Ethernet Module	N/A				
GV-AS400	V1.06				
GV-AS1010	V1.31		V1.32		
GV-AS1110	V1.21				
GV-AS1520	N/A		V2.00		
GV-AS410	V1.4	V1.41	V2.00	V2.11	V2.11 / V2.12
GV-AS210 / 810	V1.4	V1.41	V2.00	V2.11	
GV-AS2110 / 4110 / 8110	V1.4	V1.41	V2.00	V2.11	
GV-AS4111 / 8111	V1.4	V1.41	V2.00	V2.11	
GV-AS2120	V1.4	V1.41	V2.00	V2.11	
GV-CS1320	V1.10	V1.11	V2.00	V2.11	V2.11 / V2.20
GV-EV48	V1.4	V1.41			
GV-ASBox / GV-ASNet (Optional devices)	V1.07				
<b>Note:</b> The coming firmware V2.12 of GV-AS21 / 41 / 81 series Controller and V2.20 of CS1320 support the Auto Sync function.					

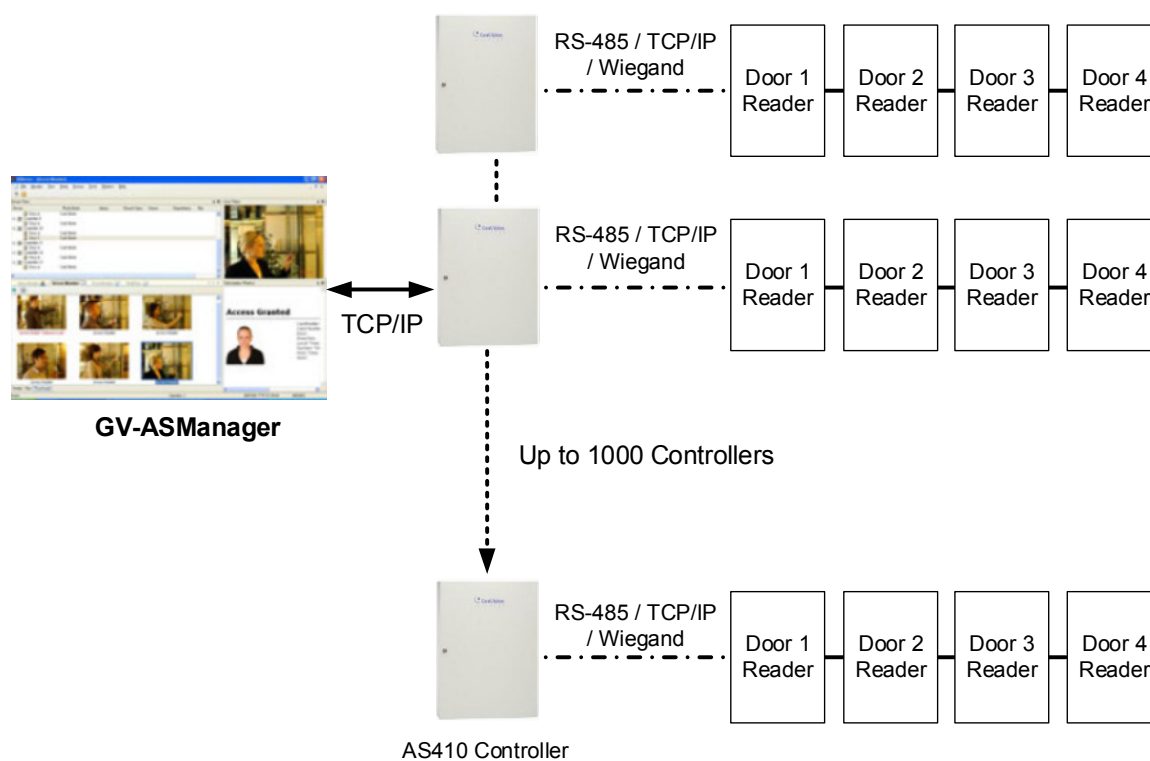
## Naming and Definition

<b>GV-DVR / NVR</b>	GeoVision Analog and Digital Video Recording Software. The GV-DVR / NVR also refers to <b>Multicam System</b> , <b>GV-NVR System</b> , <b>GV-Hybrid DVR System</b> and <b>GV-DVR System</b> at the same time.
<b>GV-VMS</b>	GeoVision Video Management System for IP cameras.
<b>PC LPR</b>	PC LPR refers to GV-DVR LPR and GV-VMS LPR. A GV-DVR / NVR or GV-VMS can be turned into a GV-DVR LPR / GV-VMS LPR simply by installing the LPR Plugin and inserting an LPR Dongle. PC LPRs are capable of comparing captured license plates with the database from GV-ASManager.
<b>Standalone LPR</b>	Standalone LPR refers to GV-DSP LPR and GV-LPR1200. Both 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 and GV-AS / GV-EV Controller offers full control of the entrances of your premise. Up to 1000 units of GV-AS / GV-EV Controllers can be monitored and controlled by one GV-ASManager.

The following diagram is an example of how the GV-ASManager and GV-AS / GV-EV Controller can be set up.



*Figure 1-1*

## **1.1 Main Features**

### **GV-ASManager**

- Control up to 1000 GV-AS / GV-EV Controllers
- Up to 256 time zones and weekly schedules
- Up to 100,000 cards for GV-AS21 / 41 / 81 Series Controllers and 40,000 cards for other GV-Controllers
- Up to 1,000 system users
- Holiday planning for 14 months
- Multiple cards per user
- Four (4) access mode options: Card only mode, Card and PIN Code mode, Card or Common mode, Release mode
- Enroll cards in batch mode
- Door alarms: door held open, door forced entry, tamper, access denied
- 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 matrix of 16-channel multi-views
- User-defined screen layout and dual monitor display support
- SMS or E-Mail notification with user-defined content, video snapshot and user photo
- Video integration with GeoVision IP devices (GV-Video Server, GV-Compact DVR, GV-IP Camera) and third-party IP cameras
- Support for connecting to third-party IP devices using ONVIF, PSIA and RTSP protocols
- Support Microsoft Access, SQL database and Active Directory database
- Patrol Tour that requires security personnel to check in at the specified locations
- User interface in English, French, Hebrew, Japanese, Portuguese, Russian, Serbian, Spanish, Traditional Chinese, Turkish

### **GV-ASRemote**

- Monitor unlimited GV-ASManagers over the 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**

- Control up to 255 GV-DVR LPR / GV-VMS LPR / GV-DSP LPR / GV-LPR1200
- Up to 100,000 vehicles
- Multiple vehicles per user
- Import / export of vehicle data in Access or Excel file format
- Vehicle hotlist to help locate stolen vehicles or other vehicles of interest
- Parking lot management to control vehicle access, maximum stay time allowed and number of vehicles allowed
- GV-ASWeb: Remotely enroll vehicles and set up GV-DVR LPR / GV-VMS LPR / GV-DSP LPR / GV-LPR1200
- GV-ASWeb: Remotely search detected vehicles, see license plate snapshots, watch recordings from connected GV-DVR LPR / GV-VMS LPR / GV-DSP LPR / GV-LPR1200

### **GV-Access Mobile Applications**

- Access up to 5 GV-ASManagers from iOS and Android mobile devices
- Watch live view from cameras associated with a door or lane
- Lock or unlock a door
- Check door status to see if any alarm events have occurred at a door
- Open LPR lanes

## 1.2 Concepts

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

<b>Weekly Schedule</b>	<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 Setting Weekly Schedule</i>.</p>
<b>Access Group</b>	<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 Setting Access Group</i>.</p>
<b>Alarm Condition</b>	<p>An alarm condition is a condition monitored through sensors, and alarms can be activated when the condition is detected by the sensors. For example, the AS210 Controller can monitor up to 8 sensors, such as door status sensor, smoke detector and tamper detector. The AS210 Controller also provides output relays for activating and deactivating electric lock, siren and emergency door release when the alarm condition occurs.</p> <p>Note that 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, the tampering alarm sensor needs to be installed separately and the triggering conditions depend on the type of sensor installed.</p> <p>For settings of alarm conditions see Step 4 of <i>4.2.2 Step 2: Configuring the Doors</i>. For configuring inputs and outputs see <i>GV-AS / GV-EV Controller User's Manual</i>.</p>
<b>Anti-Duress</b>	<p>If a person is forced to open the door under threat, he or she can enter his or her PIN plus 1 to activate an alarm and send a signal to 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 in the system.</p>
<b>Anti-Passback</b>	<p>The feature is designed to prevent card sharing and to enforce use of entry and exit readers. If a card was used at an entry reader, it must be used at an exit reader before it will be valid at an entry reader again. For settings, see <i>4.2.2 Step 2: Configuring the Doors</i>.</p>



<b>Interlock</b>	<p>The feature is also called “mantrap” or interlocking”. The feature interlocks the selected 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 opened. When either of Door B or C is opened, Door A will not unlock.</p> <p>For settings, see <i>4.2.1 Step 1: Configuring a Controller</i>.</p>
<b>Two-person A/B rule</b>	<p>The door unlock only when two assigned cards are presented together. Two Person Card A must be presented before Two Person Card B.</p> <p>For settings, see <i>4.3.1 Adding a Single Card</i>.</p>
<b>IP device</b>	<p>The video device is connected to the ASManager through the network. The ASManager enables you to access the live video from not only GeoVision IP devices (GV-DVR / NVR / GV-VMS, GV-Video Server, GV-Compact DVR and GV-IP Camera) but also certain third-party IP cameras. Connections to IP devices through ONVIF, PSIA and RTSP protocols are also supported.</p> <p>For details, see <i>Chapter 5 Video Integration</i>.</p>
<b>Data Group</b>	<p>This feature allows the 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 data group. For example, the administrator can create a data group for the sales department and assign sales department-related cards and controllers under that data 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>8.1.1 Adding a New User</i>.</p>
<b>Door Group</b>	<p>When a large number of GV-AS / GV-EV Controllers are connected to the GV-ASManager, the doors of different controllers can be organized into different door groups. The door group allows you to quickly upload fingerprints and user data to the doors installed with fingerprint and face recognition readers respectively.</p> <p>For details, see <i>Uploading Fingerprints to Controllers Using Door Groups</i> section in Chapter 3 of <i>GV-GF Fingerprint Reader User's Manual</i>.</p>

### 1.3 Optional Devices

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

<b>GV-FR2020 Face Recognition Reader</b>	Faces can be enrolled through a GV-FR2020 Face Recognition Reader and GV-ASManager will synchronize the face data using TCP/IP connection.
<b>GV-GF1911 Fingerprint Reader</b>	Fingerprints can be enrolled through a GV-GF1911 Fingerprint Reader installed on the computer of the GV-ASManager. The fingerprint data are distributed through GV-ASManager to the assigned fingerprint readers installed on GV-AS / GV-EV Controllers for access control.
<b>GV-GF1921 / 1922 Fingerprint Reader</b>	Fingerprints can be enrolled locally or remotely using a GV-GF1921 / 1922 Fingerprint Reader through TCP/IP connection with GV-ASManager.  For <b>local fingerprint enrollment</b> , the user needs to register his or her fingerprints onsite using a reader connected with GV-ASManager. For <b>remote fingerprint enrollment</b> , empty fingerprints can be created on the GV-ASManager first, and the user can register his or her fingerprints later at a GV-GF1921 / 1922 with the assigned card.
<b>GV-IO Box</b>	The GV-IO Box provides 4, 8 or 16 inputs and relay outputs. It supports both DC and AC output voltages, and provides a USB port for PC connection.
<b>GV-PCR310 Enrollment Reader</b>	The GV-PCR310 is a USB card reader designed to assist with card enrollment to GV-ASManager / GV-ASWeb. It reads and transfers the identification data of a detected card to GV-ASManager / GV-ASWeb. The user can conveniently establish user accounts on GV-ASManager / GV-ASWeb by inserting the cards in the GV-PCR310 Enrollment Reader. Starting from GV-ASManager V4.3.5, GV-PCR310 supports both 26 and 34-bit Wiegand card formats (13.56 MHz).

## Chapter 2 Installation

### 2.1 System Requirements

For GV-ASManager version 4.2.1 or later, the minimum hardware and software requirements are:

OS	32-bit	Windows 7 / 8 / 8.1 / 10 / Server 2008
	64-bit	Windows 7 / 8 / 8.1 / 10 / Server 2008 R2 / Server 2012 R2
CPU		Core 2 Duo E8400, 3.0 GHz
Memory		2 x 1 GB Dual Channels
Hard Disk		500 GB
VGA		PCI-Express, 1280 x 1024, 32-bit color and support DirectX 10
DirectX		End-User Runtimes (November 2008)
Software		.NET Framework 3.5
		SQL Server 2005 Express (optional)
Browser		Internet Explorer 9.0 or later
<b>Note:</b> The software programs End-User Runtimes (November 2008) and .NET Framework 3.5 are required to run the GV-ASManager. The software programs can be found on the Download Guide.		

## 2.2 Installing the GV-ASManager

Starting from version 4.2.1, the GV-ASManager software supplied with GV-AS / GV-EV Controller can connect with up to 4 controllers for free. If you need to manage more than 4 controllers, a **USB dongle** is required. GV-ASManager can support connection with up to 1000 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 the GV-ASManager from the GeoVision Website.

### Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:  
<http://www.geovision.com.tw/download/product/>
2. Insert the USB Dongle to your computer.
3. To install USB driver, select **Driver & F/W** from the drop-down list.
4. Click the **Download** icon  of **GV-Series Card Driver / USB Devices Driver**.

Type	Title	Ver.	Size	Download
	GV-Series Card Driver / GV-USB Device Driver	V8570	5.9MB	

Figure 2-1

5. To install GV-ASManager, visit  
<http://www.geovision.com.tw/download/product/GV-ASManager>
6. Click the **Download** icon  of **GV-ASManager**.



Type	Title	Ver.	Size	Download
	GV-ASManager	V4.4.3.0	390MB	

Figure 2-2

7. If you don't have **Microsoft DirectX 9.0c** installed in your computer, download and install from: <http://www.microsoft.com/en-US/download/details.aspx?id=34429>

8. To download and install **Microsoft DirectX End-User Runtimes (November 2008)**, go to: <http://www.microsoft.com/en-us/download/details.aspx?id=15805>
9. To download and install **.Net Framework 3.5**, go to:  
<http://www.microsoft.com/en-us/download/details.aspx?id=21>

## 2.3 Logging in

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

1. Click **Start**, point to **Programs**, 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.

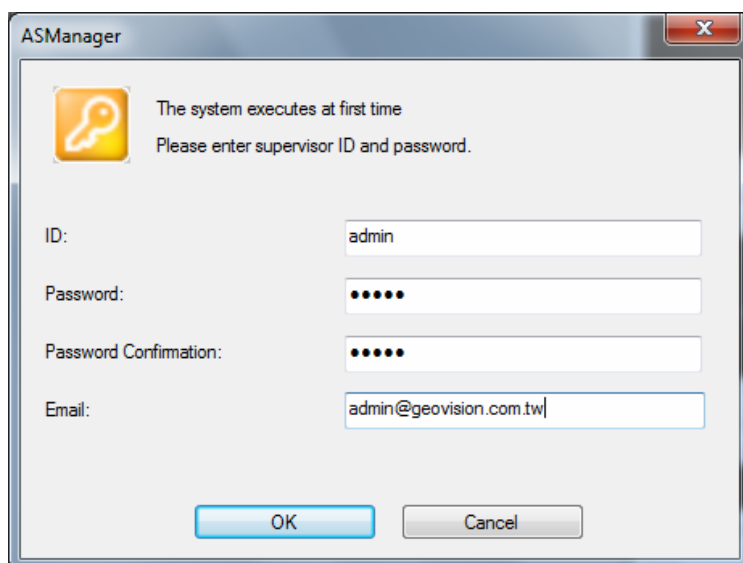


Figure 2-3

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 *Setting E-Mail Server* in Chapter 8 for details.
3. Type a name you wish to be the Supervisor in the ID field and type the password. This dialog box appears.

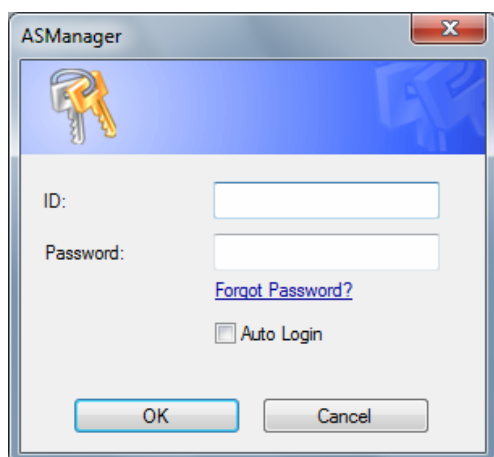


Figure 2-4

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.

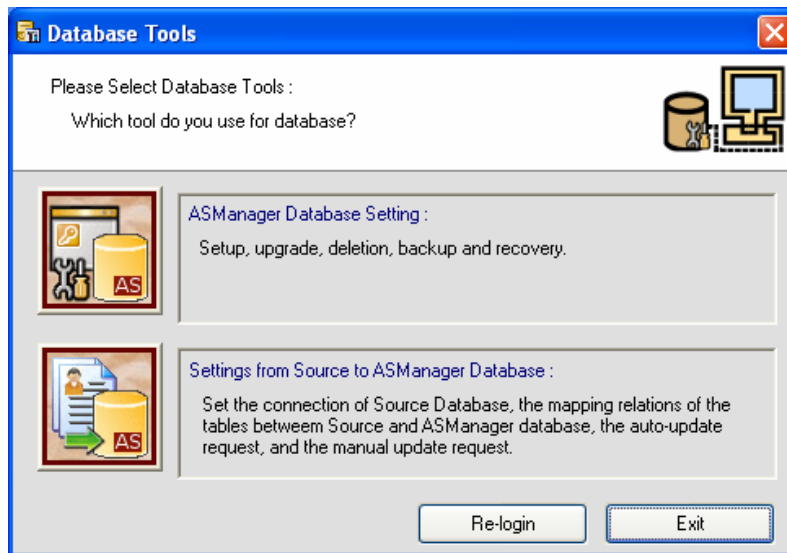


Figure 2-5

7. Select **ASManager Database 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 15 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 the 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 the GV-ASManager, the following main screen will appear. Get yourself familiar with the main screen, as it will help you when you read further in the following sections.

### 3.1 Main Screen

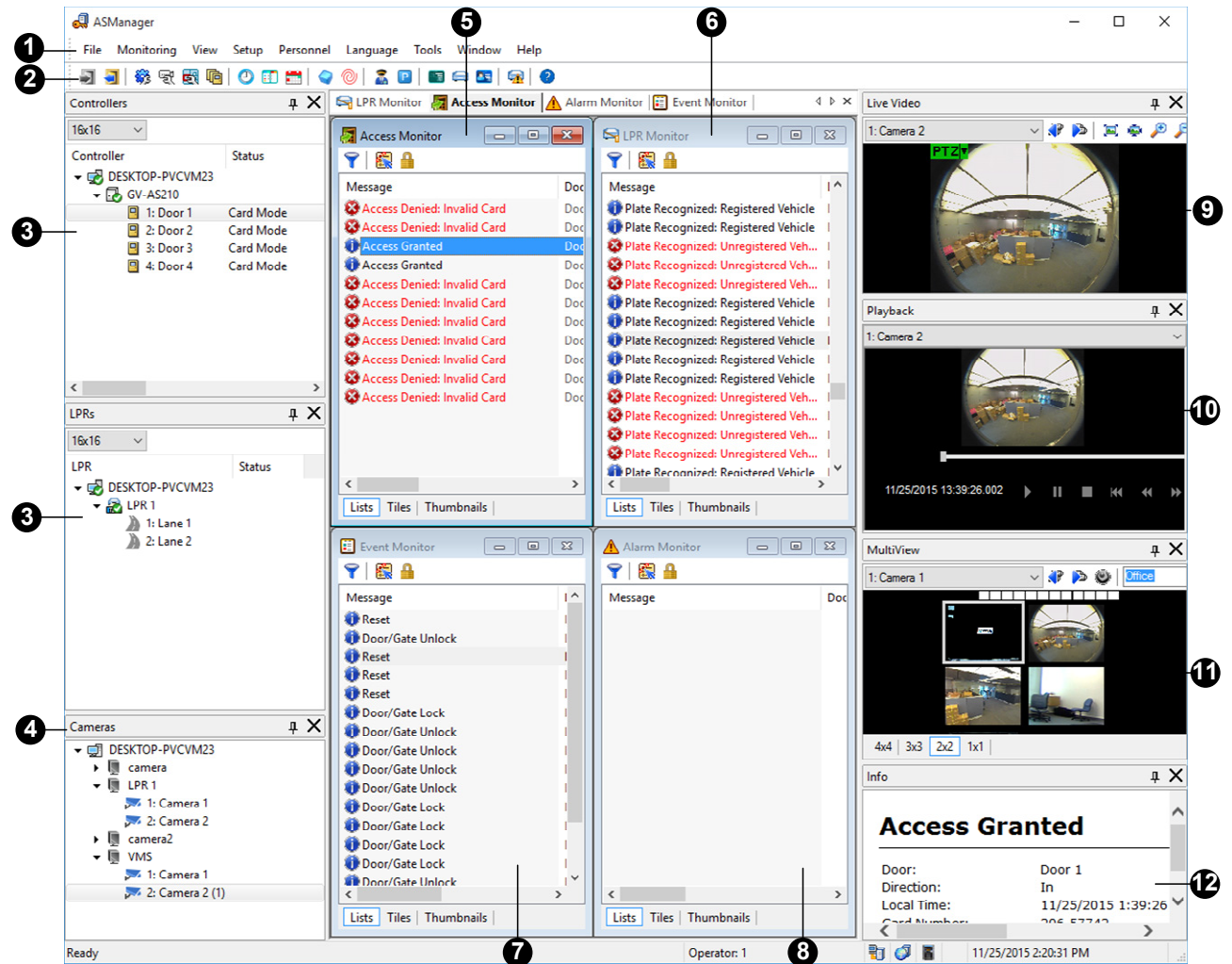


Figure 3-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of <b>File</b> (log in / out the GV-ASManager), <b>Monitoring</b> (display monitoring windows), <b>View</b> (display the function windows), <b>Setup</b> (set up connected devices and schedules), <b>Personnel</b> (set up the users' accounts), <b>Language</b> (select language of user interface), <b>Tools</b> (set up notification and log) and <b>Window</b> (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	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 drop-down list.
4	Camera List	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 connected cameras from multiple IP devices. For details, see <i>5.4 The MultiView Window</i> .
12	Information Window	Displays the information of doors, card readers and monitored events.

---

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

---

### 3.1.1 Toolbar



Figure 3-2

The buttons on the Toolbar of GV-ASManager:

No.	Name	Function
1	Login	Logs in the GV-ASManager.
2	Logout	Logs out the GV-ASManager.
3	Devices	Defines controllers, doors, LPR devices and lanes.
4	Cameras	Searches the GV IP devices on the same network. For details, see <i>Chapter 5 Video Integration</i> .
5	Areas	Configures Global Anti-Passback. For details, see <i>6.3 Global Anti-Passback</i> .
6	Door Groups	Assigns the doors of different controllers into door groups to be able to quickly upload fingerprints and user data to the doors installed with the fingerprint and face recognition readers respectively. For details, see <i>Uploading Fingerprints to Controllers Using Door Groups</i> section in Chapter 3 of <i>GV-GF Fingerprint Reader User's Manual</i> .
7	Time Zones	Defines the minutes and hours of the day when a user is granted access to a secure site. For details, see <i>4.4.1 Step 1: Setting Time Zones</i> .
8	Weekly Schedules	Defines the days of the week when a user is granted access to a secure site. For details, see <i>4.4.2 Step 2: Setting Weekly Schedules</i> .
9	Holidays	Defines the specific dates as holidays. For details, see <i>4.4.3 Step 3: Setting Holidays</i> .
10	Access Groups	Sets up different groups to define who can access what door at what time of a day. For details, see <i>4.5 Setting Access Groups</i> .
11	Feature Access	Uploads the enrolled fingerprints and user data to the controllers and face recognition readers respectively. For details, see <i>Chapter 3 Fingerprint Only Mode</i> in the <i>GV-GF Fingerprint Reader User's</i>

		<i>Manual</i> or Uploading to the Face Recognition Reader in Chapter 5 of <i>GV-FR Face Recognition Reader User's Manual</i> .
12	Patrol Tours	Creates patrol tours to require security staff to check in at the specified locations. For details, see <i>Chapter 7 Patrol Tour</i> .
13	Parking Lots	Assigns LPR lanes to be the entry or exit of a parking lot. For details, see <i>13.8 Managing Parking Lots</i> .
14	Cards	Creates and edits a database of card information. For details, see <i>4.3 Setting Cards</i> .
15	Vehicles	Creates and edits a database of vehicle information. For details, see <i>Chapter 13 License Plate Recognition</i> .
16	Users	Creates and edits a database of user information. For details, see <i>4.6 Setting Users</i> .
17	Hotlist	Sets up vehicle hotlist to identify stolen vehicles or other vehicles of interest. See <i>13.7 Setting Up Vehicle Hotlist</i> .
18	About	Displays the version of GV-ASManager.

## 3.2 Controllers / LPRs View

To see the activity and status of the connected controllers and LPRs, click **View** on the menu bar and select **Controllers** or **LPRs**.

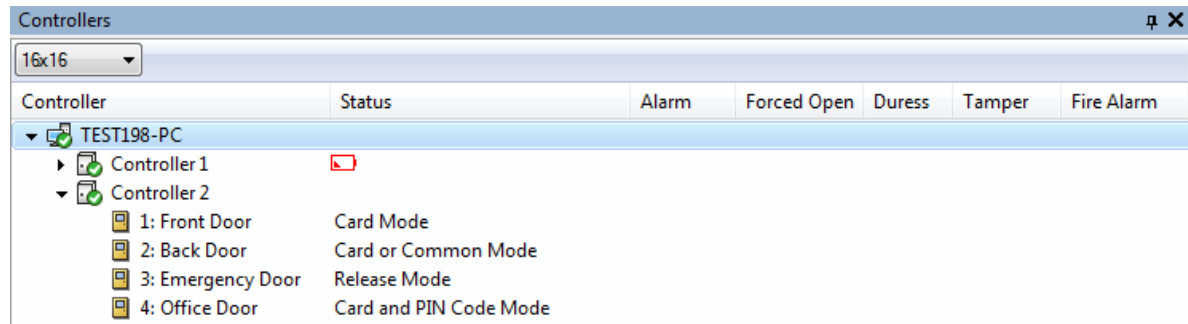


Figure 3-3

### 3.2.1 Controls on the Window

You can control the connected controllers or doors by right-clicking it in the Controller window. The following control options are available when right-clicking the GV-ASManager PC, the doors and / or the controllers:

Name	Function	Available For
Unlock Door, Lock Down, Force Unlock, Force Lock, Disable Door Lock Operation	<p>Controls the selected door or all doors associated with the selected controller.</p> <p>The options of <b>Force Unlock</b> and <b>Force Lock</b> will let the door stay open or locked until you select <b>Disable Door Lock Operation</b>.</p> <p>The <b>Unlock Door</b> option will let the door open temporarily until the specified time is expired. See “Lock Reset Time” at Step 2 in 4.2.2 Step 2: <i>Configuring the Doors</i>.</p> <p>The <b>Lock Down</b> function is only supported by GV-AS1010 / 1110 / 210 / 2110 / 2120 / 410 / 4110 / 810 / 8110. 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>	ASManager Controller Door

Clear all events	Clears the GV-ASManager / door / controller of all alarm events.	ASManager Controller Door
Reset Anti-Passback	Clicking this option enables a user to re-access the entry or exit reader. <i>See Chapter 6 Anti-Passback.</i>	ASManager Controller
Sync Controller	After the controller settings are modified, clicking <b>Sync Controller</b> can immediately renew the settings.	ASManager Controller
Reconnect	Reconnects with the controller.	Controller
Settings	Accesses the setting page of the selected controller or door.	Controller Door
ASWeb	Links to GV-ASWeb.	ASManager
Stop Alarm, Clear Forced Open, Clear Duress, Clear Tamper, Clear Fire Alarm, Clear Held Open, Clear Access Denied	Clears the alarm conditions. For alarm settings, see Step 5 in 4.2.2 <i>Step 2: Configuring the Doors</i> .	Door
Sync GeoFinger	If fingerprint data failed to upload to the controllers, click <b>Sync GeoFinger</b> to re-upload the selected fingerprint data.	Door
Sync GeoFace	Click <b>Sync GeoFace</b> to upload the selected user data to the assigned GV-FR2020 face recognition reader.	Door

### 3.3 Monitoring Windows

The monitoring windows allow you to oversee various activities.

- To open these windows, click **Monitoring** on the menu bar, and select the desired windows.

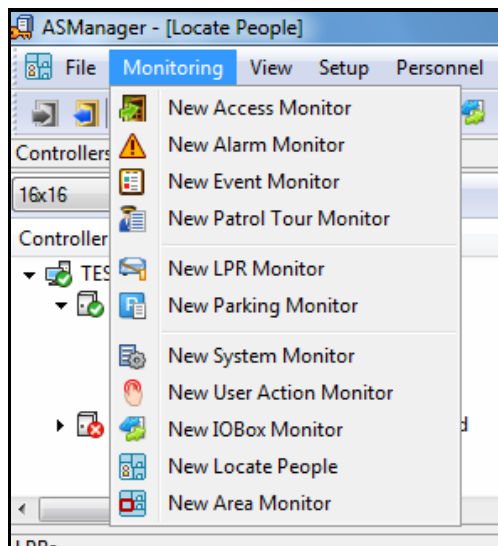


Figure 3-4

#### 3.3.1 Controls on the Window

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

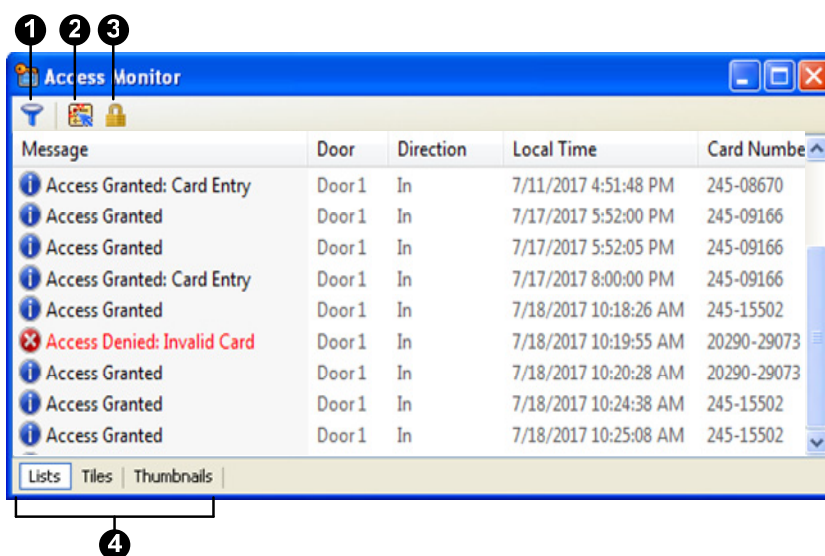


Figure 3-5



No.	Name	Function
1	Filter	Sets up criteria to only display the desired activity information.
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. Under Tiles and Thumbnails views, user profile photo and snapshots captured will be displayed if available.

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

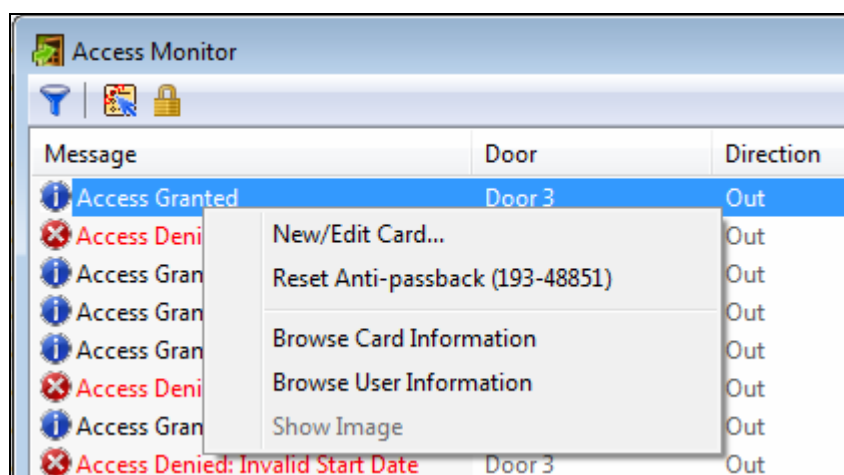


Figure 3-6

### 3.3.2 Customizing a Monitoring Window

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

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

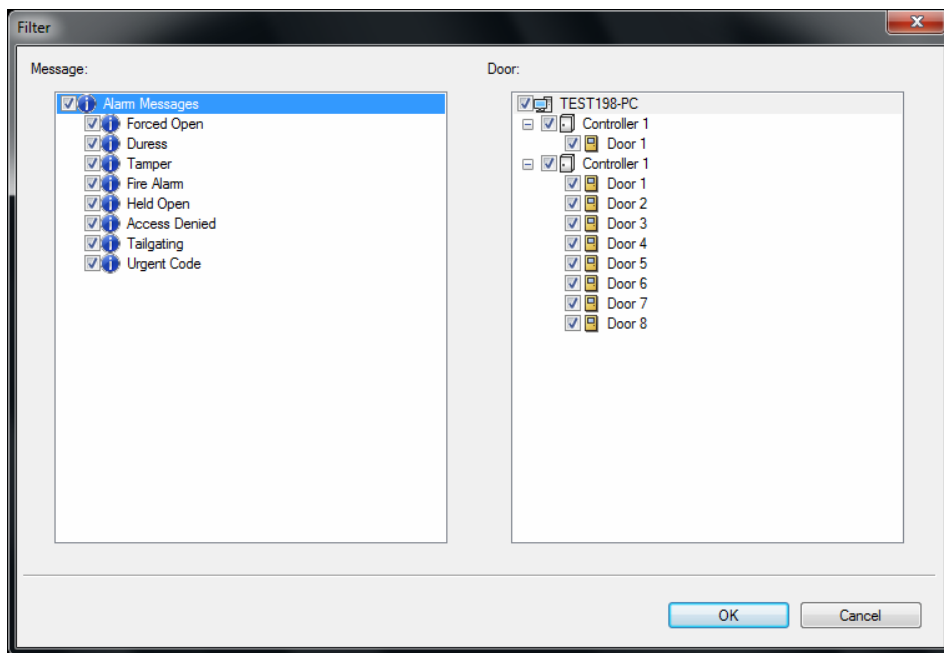


Figure 3-7

3. Select the desired messages and devices for monitoring, and click **OK**. The monitoring 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 new monitoring window.

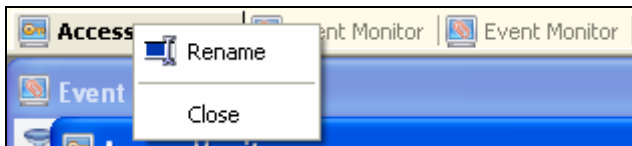


Figure 3-8

---

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

---

### 3.3.3 Arranging Monitoring Windows

The monitoring windows can be arranged on screen in several ways.

On the menu bar, click **Window**, and select one of the following options to arrange the windows:

- **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 open the monitoring windows in separate windows and place the monitoring windows on different monitors. On the menu bar, click **Window** and select **New Window**. On the menu bar of the new window, click **Monitoring** to open different monitoring windows and click **Window** to arrange them.

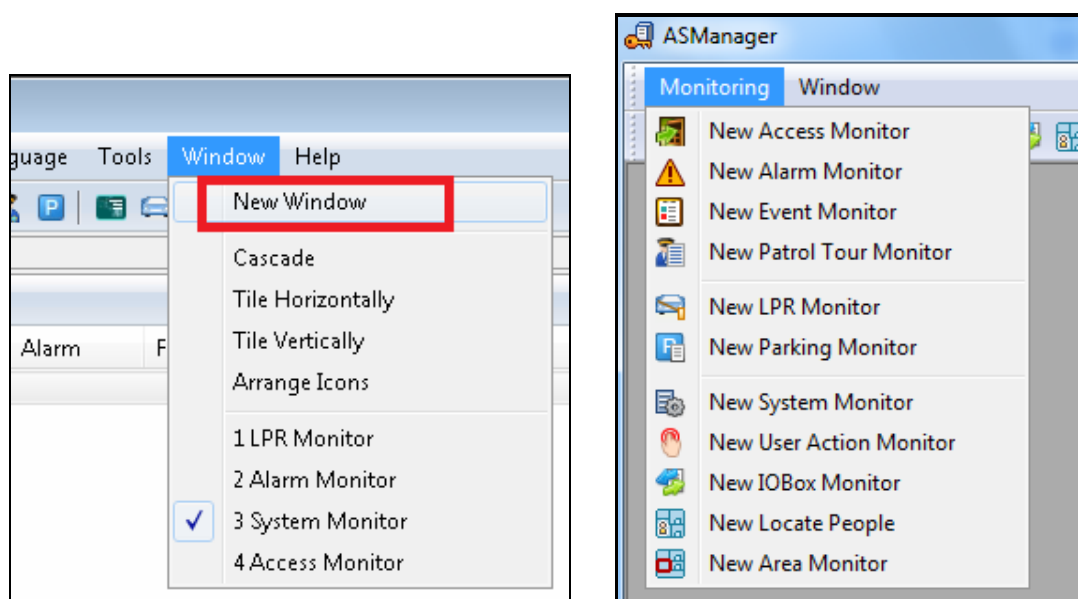


Figure 3-9

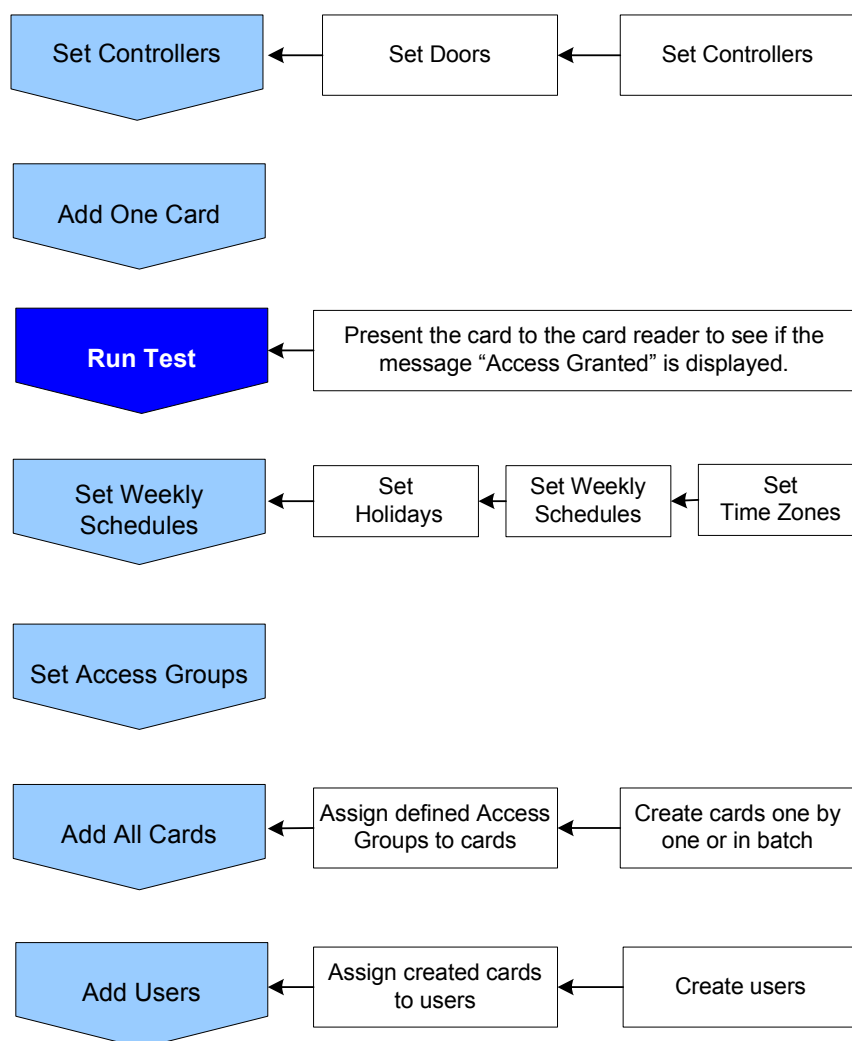
## Chapter 4 Settings

This section describes the following settings:

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

### 4.1 Setup Flowchart

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



## 4.2 Adding Controllers

To add the GV-AS / EV Controller to the GV-ASManager, follow these steps:

- **Step 1 Configuring a Controller**

Establish the communication between the controller and GV-ASManager.

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

Define the doors on a door controller or the elevator floors on an elevator controller.

### 4.2.1 Step 1: Configuring a Controller

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

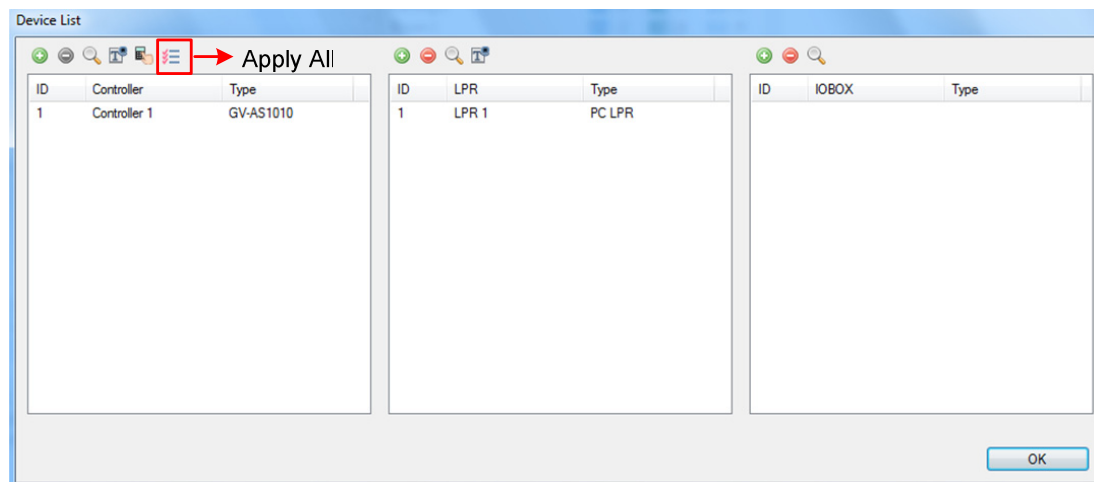



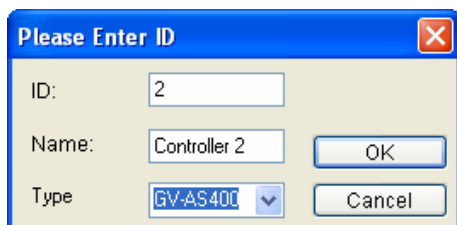
Figure 4-1

---

**Tip:** You can also click the **Search** button  to search for controllers detected in the same LAN.

---

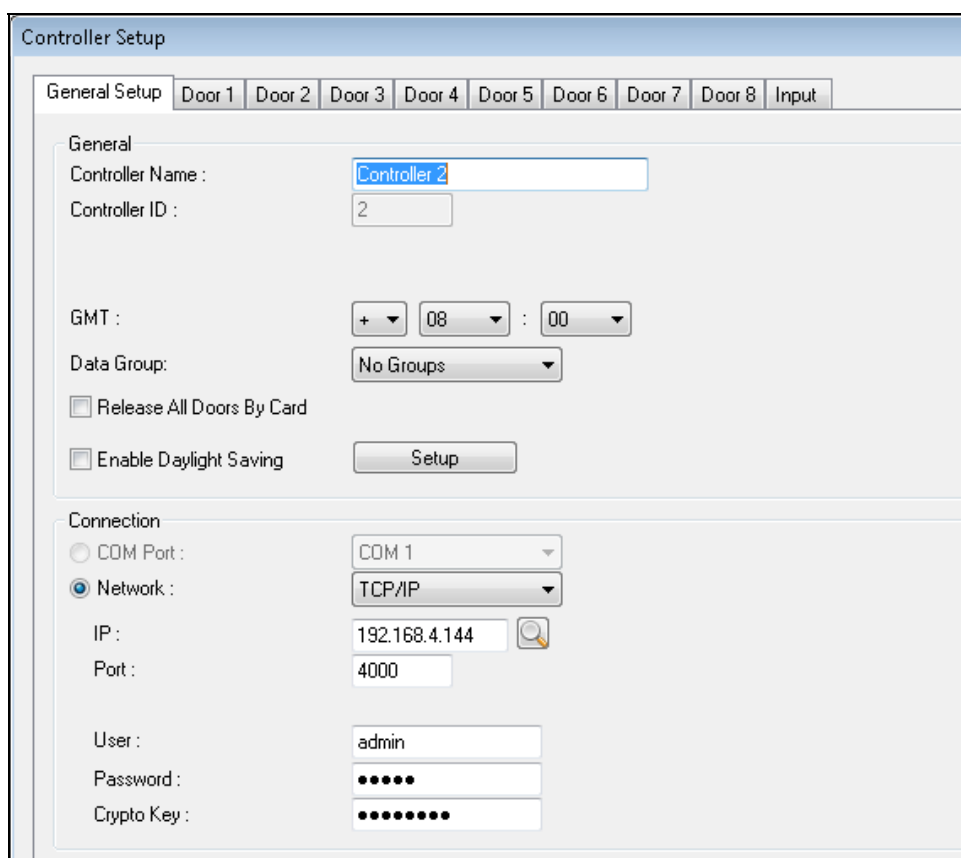
- Click the **Add** icon on the top left corner. This dialog box appears.



A small dialog box titled "Please Enter ID" with a close button (X) in the top right corner. It contains three input fields: "ID:" with the value "2", "Name:" with the value "Controller 2", and "Type:" with a dropdown menu showing "GV-AS400". There are "OK" and "Cancel" buttons at the bottom right.

Figure 4-2

- Enter **ID** and **Name** of the Controller, select **Type** of the Controller and click **OK**. This dialog box appears.



A larger dialog box titled "Controller Setup" with a tabbed interface. The "General Setup" tab is selected. It contains two main sections: "General" and "Connection".  
 In the "General" section, there are fields for "Controller Name:" (set to "Controller 2"), "Controller ID:" (set to "2"), "GMT:" (set to "+ 08 : 00"), "Data Group:" (set to "No Groups"), and checkboxes for "Release All Doors By Card" and "Enable Daylight Saving". A "Setup" button is located below these options.  
 In the "Connection" section, there are radio buttons for "COM Port:" and "Network:". The "Network:" option is selected. Below it, there are fields for "IP:" (set to "192.168.4.144"), "Port:" (set to "4000"), "User:" (set to "admin"), "Password:" (masked with dots), and "Crypto Key:" (masked with dots). A search icon is next to the IP field.


Figure 4-3

---

**Note:** The Controller ID must match the Controller ID set ahead on the Web interface of the controller. Refer to *GV-AS / GV-EV Controller User's Manual*.

---


- In Connection section, select the communication mode between the GV-AS / GV-EV Controller and GV-ASManager.
  - If using RS-485 connection, select **COM Port** that is used for connection.

- If using Ethernet, select **Network** and select **TCP / IP** or **LocalDDNS**. Type the IP address, device name (if LocalDDNS is selected), port number, login user, login password and Crypto key (3DES code) of the controller. You can also click the **Search** button  to search for controllers detected in the same LAN.

---

**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**.

---

5. To check if the above connection settings are correct, you can click **OK** at this step and back to the main screen. The icon  appearing on the Controller window indicates the connection is established.

---

**Note:** For the disconnection messages displayed on the Status column (Figure 4-9), see *D. Controller Status* in *Appendix*.

---

6. OPTIONAL settings in the General section:

- **GMT:** The current time at the host computer.
- **Data Group:** Assign the controller to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read / write / execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.
- **Release All Doors by Card:** When a card is presented, all doors set to **Release by Card** mode will open and will remain 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 function by selecting your time zone. The system will automatically adjust for daylight saving time.

---

**Note:** The **Release All Doors by Card** function is not available for GV-EV48.

---

## 4.2.2 Step 2: Configuring the Doors or Elevator Floors

### A. GV-AS Controller: Doors

1. To define the doors on the controller, click the **Door** tab. This dialog box appears.

The screenshot shows the 'Controller Setup' dialog box with the 'Door 1' tab selected. The dialog is divided into several sections:

- General Setup:** Includes fields for Name (Door 1), Common Password (4~8 digits), Urgent Code (4~8 digits), Lock Reset Time (5 Sec), Held Open Time (10 Sec), Lock Card Time (Entrance: 0 Sec, Exit: 0 Sec), Fire Action (Unchange), Reader's Keypad (Entrance and Exit checked), GeoFinger (Entrance and Exit with IP addresses), GeoFace (Entrance and Exit with IP addresses), Anti-Passback (By Card - Global selected), Auto Check Out (Entrance and Exit), Two-Person Rule (Entrance and Exit), Interlock, and Time Clock (checked).
- Alarm Event:** Includes checkboxes for Held Open, Forced Open, Tamper, Fire Alarm, Access Denied, Tailgating, and Urgent Code.
- Camera Mapping:** Includes Camera 1 and Camera 2 settings, each with a dropdown menu and a delayed snapshot field.
- Buttons:** Authentication Schedule, Exit Button Schedule, OK, and Cancel.


Figure 4-4

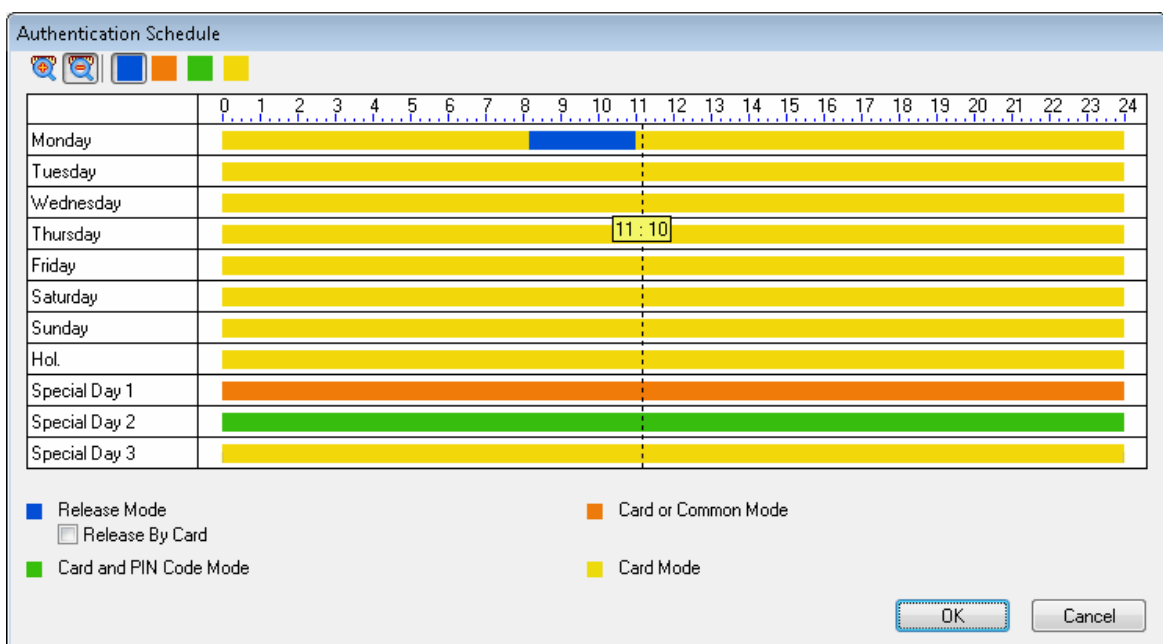
2. In the General section, select **Enable** to define the general settings for the door:
  - **Name:** Give a name to the door.
  - **Common Password:** Set a password for the door. When under **Card or Common Mode**, the user can gain access by entering this password using a keypad. The default password is 1234. See Step 6 for details on Card or Common Mode.
  - **Urgent Code:** When the Urgent Code is entered at 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.

- **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.
  - **Fire Action:** Set the door to be locked or unlocked when fire alarm occurs.
3. The following settings are OPTIONAL and are only applicable when related settings are also configured:
- **Reader's Keypad:** When the Card and PIN Code Mode is applied, normally both the access card and PIN code are required. But if the **Entrance** or **Exit** option is not selected, only the access card is required to unlock the door. For example, if only the **Entrance** option is selected, the user will be required to both present the card and enter the PIN code to unlock the entry door, but only the card will be required to unlock the exit door. To apply Card and PIN Code mode, see step 6 below.
  - **Anti-Passback:** For detailed instructions, see *Chapter 6 Anti-Passback*.
  - **Auto Check Out:** Automatically checks out the Visitor Card when the visitor presents the card at the exit door. To set a card as Visitor Card, see *Adding a Single Card* section later in this chapter.
  - **Two Person Rule:** Select **Entrance** to require presenting Two Person A Card and then Two Person B Card before the entry door is unlocked. Select **Exit** to require presenting both cards in the right order before the exit door is unlocked. To set a card as Two Person A/B Card, see *Adding a Single Card* section later in this chapter.
  - **GeoFinger:** Allow GV-ASManager to upload enrolled fingerprints to the specified fingerprint reader. Refer to *Chapter 3 Fingerprint Only Mode* in the *GV-GF Fingerprint Reader User's Manual* for details.

- **GeoFace:** Allow GV-ASManager to synchronize the enrolled face data from the specified face recognition reader. Refer to *Chapter 4 Access Control Configurations* in the *GV-FR Face Recognition Reader User's Manual* for details.
  - **Interlock:** Enable Interlock function on the selected doors. Doors that are interlocked cannot be open at the same time. The door only unlocks when the other door is closed. Using Figure 4-4 as an example, Door 1 will not unlock if either of Doors 3 and 4 is open, and when Door 1 is open, Doors 3 and 4 will not unlock. The Interlock function is not available for GV-EV48.
  - **Time Clock:** This option must be selected to enable GV-TAWeb. See *Chapter 11 GV-TAWeb for Workforce Schedule* for more details.
4. The settings in the Alarm Event section are OPTIONAL unless an alarm device is installed on the GV-AS Controller. Enable the desired alarm conditions that will cause the alarm to occur: **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.
  5. The settings in the Camera Mapping section are OPTIONAL unless a camera is installed at the secure site. For details, see *Chapter 5 Video Integration*.
  6. The **Authentication Schedule** is an OPTIONAL setting for specifying different access modes at different periods of time. The default access mode is **Card Mode** that requires users to present the card only to be granted access. You can click the finger button  to apply the settings to all doors of this controller.



The Authentication Schedule window displays a 24-hour timeline for each day of the week. The timeline is divided into segments representing different access modes. The legend indicates the following modes:

- Release Mode:** Blue square
- Release By Card:** Grey square
- Card and PIN Code Mode:** Green square
- Card or Common Mode:** Orange square
- Card Mode:** Yellow square

The schedule shows the following access modes for each day:

- Monday:** Card Mode (0-8), Release Mode (8-11), Card Mode (11-24)
- Tuesday:** Card Mode (0-24)
- Wednesday:** Card Mode (0-24)
- Thursday:** Card Mode (0-11), Card or Common Mode (11-12), Card Mode (12-24)
- Friday:** Card Mode (0-24)
- Saturday:** Card Mode (0-24)
- Sunday:** Card Mode (0-24)
- Hol.:** Card Mode (0-24)
- Special Day 1:** Card or Common Mode (0-24)
- Special Day 2:** Card and PIN Code Mode (0-24)
- Special Day 3:** Card Mode (0-24)

The window includes an OK button and a Cancel button at the bottom right.

Figure 4-5

To define which kind of access mode should be applied at specific day and time, select one access mode on the toolbar and drag the mouse over the timelines. Four (4) access modes are available in the system:

- **Card Mode:** This is the default mode. 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 with the reader.
  - **Release by Card:** The door will unlock only after a card is presented and will remain unlocked during the time specified for Release Mode. This option is designed to prevent unattended doors from opening during the Release Mode.
- **Card and PIN Code Mode:** This mode requires the user to present the card AND enter the card's PIN code on the keypad. To set up a PIN code, see 4.3.1 *Adding a Single Card*.

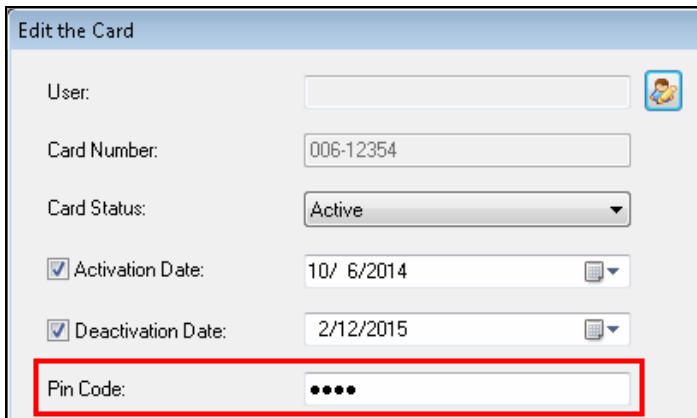


Figure 4-6

- **Card or Common Mode:** This mode requires the user to present his or her card **OR** enter the door's common password using the keypad.

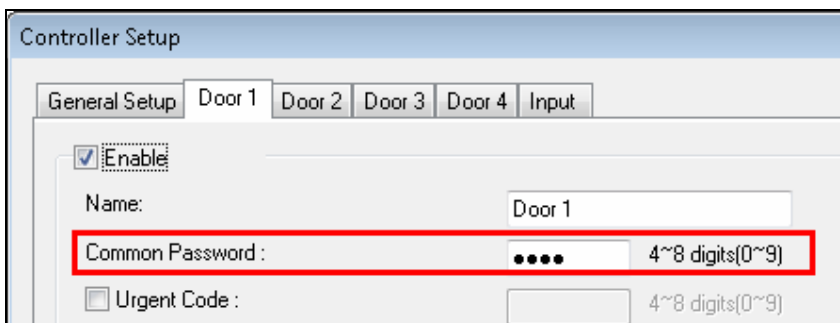




Figure 4-7

7. The **Exit Button Schedule** is an OPTIONAL setting to specify when to allow access to the exit button. By default, access to the exit button is granted at all times. To set a schedule, click the **Delete Access Time** button  and drag the mouse over the time periods when you want the exit button to be locked. You can click the finger button  to apply the settings to all doors of this controller. The Exit Button Schedule function is only supported by GV-AS1010 / 1110 / 210 / 2110 / 2120 / 410 / 4110 / 810 / 8110.

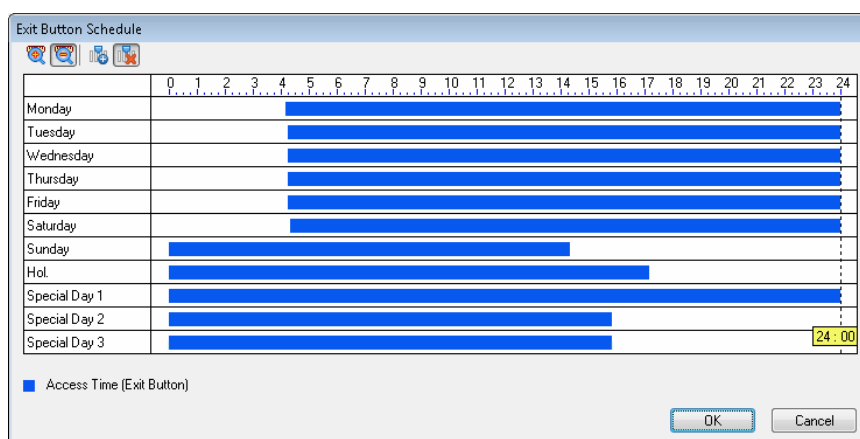




Figure 4-8

**Tip:** After finishing setting up a door, you can click the **Apply All** button  (Figure 4.1) to apply the Authentication Schedule and/or Exit Button Schedule of that door to the doors of all controllers.

8. Click **OK** several times and return to the main screen. A controller folder tree will be displayed on the Device View window as example below.

If the icon  appears, 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.

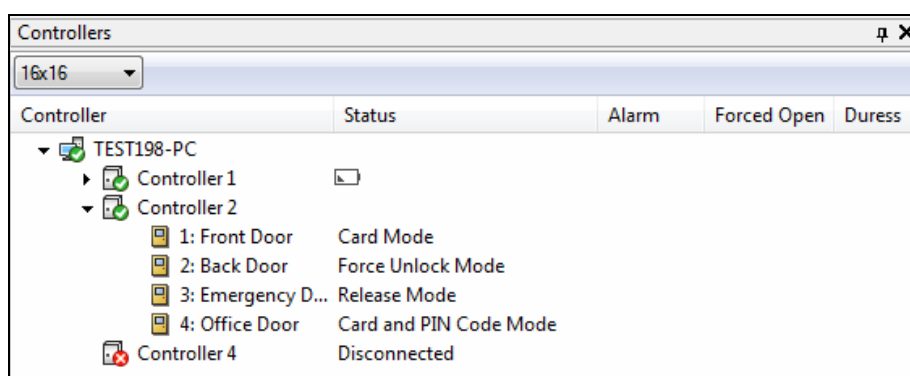


Figure 4-9

## B. GV-EV Controller: Floors

1. To define the elevator floors on GV-EV48, click the **Floors** tab. This dialog box appears.

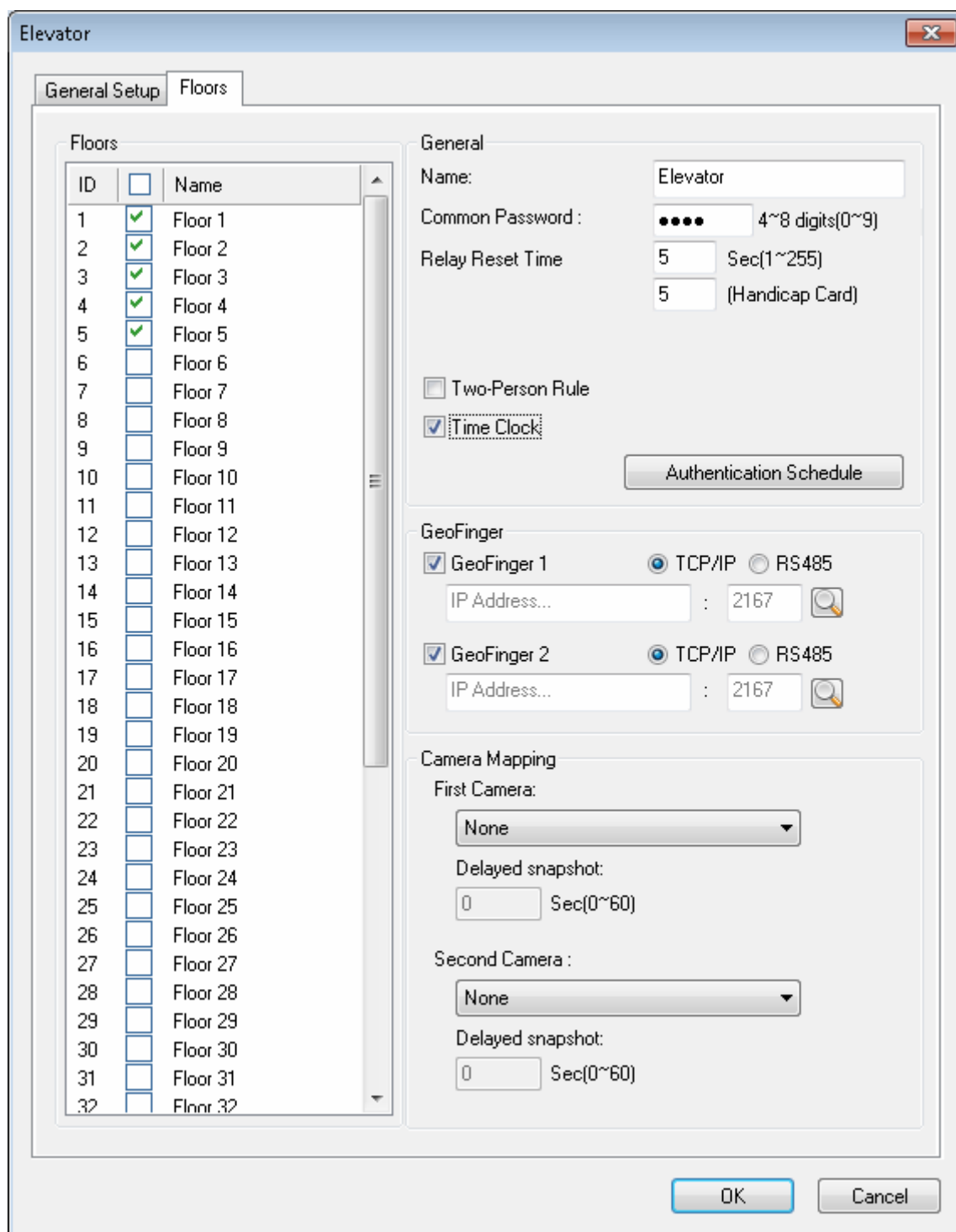


Figure 4-10

2. To enable elevator floors, select the floors on the left. For example, if your elevator only has 40 floors, you can clear the selection for floors 41 to 48.

3. In the General section, define the general settings for the elevator:
  - **Name:** Name the elevator.
  - **Common Password:** Set a password for the elevator. When under **Card or Common Mode**, the user can gain access by entering this password using a keypad. The default password is 1234.
  - **Relay Reset Time:** If the elevator access is restricted, type the number of seconds the buttons will remain accessible after card is presented. After the specified time expired, the elevator buttons will automatically be locked. Next to **Handicap Card**, type the number of seconds the elevator button will remain accessible when a Handicap Card is swiped.
4. The following settings are OPTIONAL and are only applicable when related settings are also configured:
  - **Two Person Rule:** Select to require presenting Two Person A Card and then Two Person B Card before the elevator floor is unlocked. If Two Person A Card and Two Person B Card have access to different floors, access will only be granted if both cards have access to that particular floor. To set a card as Two Person A/B 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 more details.
  - **GeoFinger:** Allow GV-ASManager to upload enrolled fingerprints to the specified fingerprint reader. Refer to *Chapter 3 Fingerprint Only Mode* in the *GV-GF Fingerprint Reader User's Manual* for details.
5. The **Authentication Schedule** is an OPTIONAL setting for specifying different access modes at different periods of time; otherwise the default access mode is **Card Mode** that requires users to present the card only to be granted access.

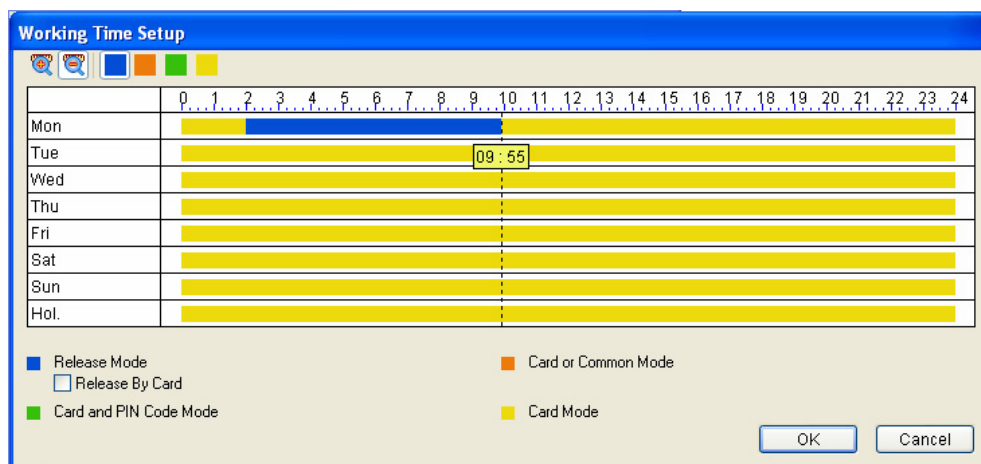



Figure 4-11

To define which kind of access mode should be applied at specific day and time, select one access mode on the toolbar and drag the mouse over the timelines. Four (4) access modes are available in the system:



- **Card Mode:** This is the default mode. 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 with the reader.
  - **Release by Card:** The floor will unlock only after a card is presented and will remain unlocked during the time specified for Release Mode. This option is designed to prevent unattended floors from opening during the Release Mode time.
- **Card and PIN Code Mode:** This mode requires the user to present his or her card and then enter the card's PIN code on the keypad. To set up a PIN code, see 4.3.1 *Adding a Single Card*.
- **Card or Common Mode:** This mode requires the user to present his or her card to gain access **OR** enter the door's password using the keypad to gain access.

---

**Tip:** After finishing setting up a elevator you can click the **Apply All** button  (Figure 4.1) to apply the Authentication Schedule of that door to the doors of all controllers.

---

6. The settings in the Camera Mapping section are OPTIONAL unless a camera is installed at the secure site. For details see *Chapter 5 Video Integration*.
7. Click **OK** several times and return to the main screen. A controller folder tree will be displayed on the Device View window.

If the icon  appears, 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.

### 4.3 Setting Cards

Once you have configured the controller, you may start enrolling cards. All new cards must be enrolled into the GV-ASManager before access is allowed. Depending on the controller models, up to 40,000 cards or 100,000 cards can be stored. If a card that was not enrolled is presented to the reader, the message *Access Denied: Invalid Card* will be displayed.

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.

#### 4.3.1 Adding a Single Card

1. To add one card, use one of these ways:
  - Present the 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 with card number and code type entered (Figure 4-13). Then follow Step 3 to complete other settings.
  - On the menu bar, click **Personnel** and select **Cards**. This window appears.

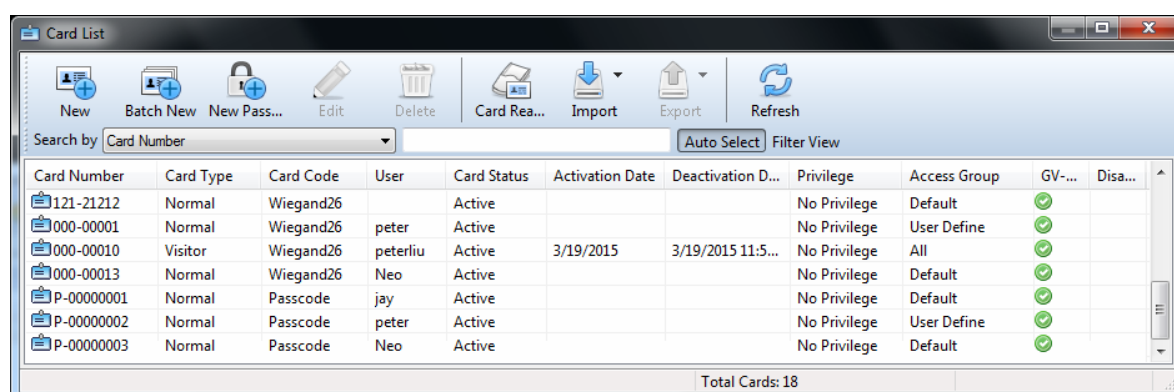
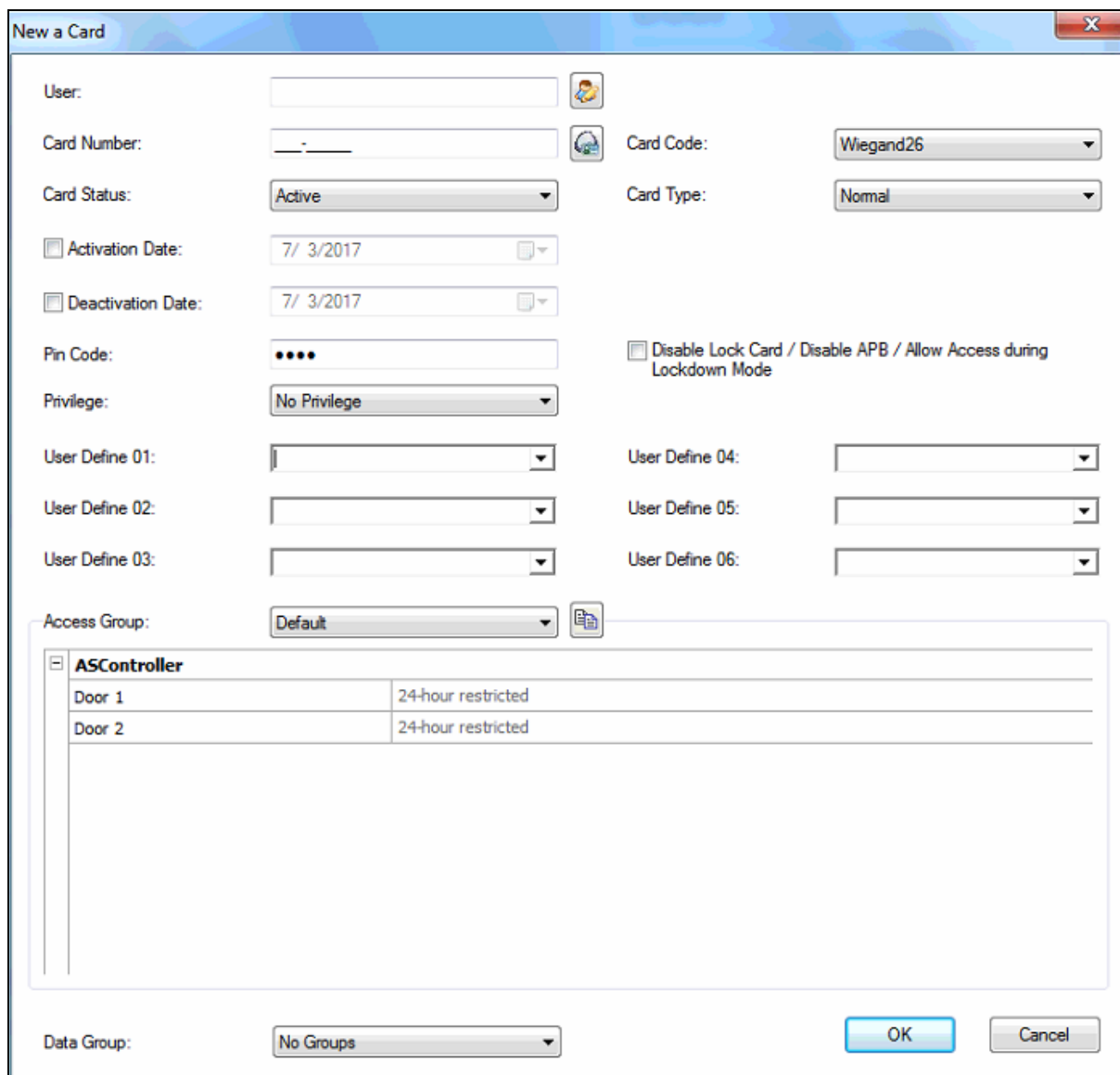


Figure 4-12

**Note:** You can also enroll cards by installing the optional device GV-PCR310 Enrollment Reader to the PC running GV-ASManager. Refer to *GV-PCR310 Enrollment Reader's Installation Guide* for details.



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





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

- User:** Text field with an 'Assign User' icon.
- Card Number:** Text field with a 'USB Card Reader' icon.
- Card Status:** Dropdown menu (Active).
- Card Code:** Dropdown menu (Wiegand26).
- Card Type:** Dropdown menu (Normal).
- Activation Date:** Date field (7/ 3/2017) with a calendar icon.
- Deactivation Date:** Date field (7/ 3/2017) with a calendar icon.
- Pin Code:** Text field (\*\*\*\*).
- Privilege:** Dropdown menu (No Privilege).
- Disable Lock Card / Disable APB / Allow Access during Lockdown Mode:** Check box.
- User Define 01-06:** Six dropdown menus for user-defined settings.
- Access Group:** Dropdown menu (Default) with a 'View Access Groups' icon.
- Access Groups Table:**

ASController	
Door 1	24-hour restricted
Door 2	24-hour restricted
- Data Group:** Dropdown menu (No Groups).
- Buttons:** OK and Cancel.

Figure 4-13

3. The settings are available for the card:

- **User:** Click the **Assign User** button  to assign the card to a user.
- **Card Number:** Enter the card number. If you have a GV-PCR310 Enrollment Reader installed, click the **USB Card Reader** button  to detect cards.
- **Code Type:** 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 NOT unlock. The feature may be set together with **Privilege** below. The patrol card user may have the privilege to stop alarm sounds 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 can be managed using GV-VMWeb.
  - **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 for handicap card. To see how to set prolonged Lock Reset Time and Held Open Time for handicap card users, refer to *4.2.2 Step 2: Configuring the Doors or Elevator Floors*.
- **Activation/Deactivate Date:** Specify the date to activate or deactivate the card.
  - **PIN Code:** Enter a four-digit PIN code for the card. When authentication mode is set to Card and PIN Code Mode, the user needs to present the card and enter the PIN code. The default setting is 1234.

For the controllers below, users can also gain access by manually entering the card number and 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 Example: 123456780000
GV-AS1010	V1.0 only	
GV-AS110	V1.04 or later	*Card Number + Pin Code # Example: *123456780000#
GV-AS1110	V1.0 only	
GV-AS210 / 410 / 810	V1.0 - V1.23	Pin Code + Card Number Example: 000012345678
GV-EV48	V1.0 – V1.12	

- **Privilege:** Assign one of these privileges to the user:
  - **Stop Alarm:** The user can stop alarm sounds by presenting the card.

- **Clear Event:** The user can clear alarm events by presenting the card. All alarms in the Device View window are erased. A record of these alarms is still 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 the Lock Card Time setting and the APB setting. In addition, this card will be allowed access to doors when Lockdown Mode is activated.

For details on Lock Card Time, refer to *Step 2: Configuring the Doors or Elevator Floors* in Chapter 4. For details on Lockdown Mode, refer to the *Device View* section in Chapter 3.

---

**Note:** The Allow Access during Lockdown Mode function 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
- 

- **Access Group:** Access Groups control which personnel can access which door and at what time. For details, see *4.5 Setting Access Groups*.

For first-time user of the GV-ASManager, the access group is not yet established. Select **User Define** for test run.

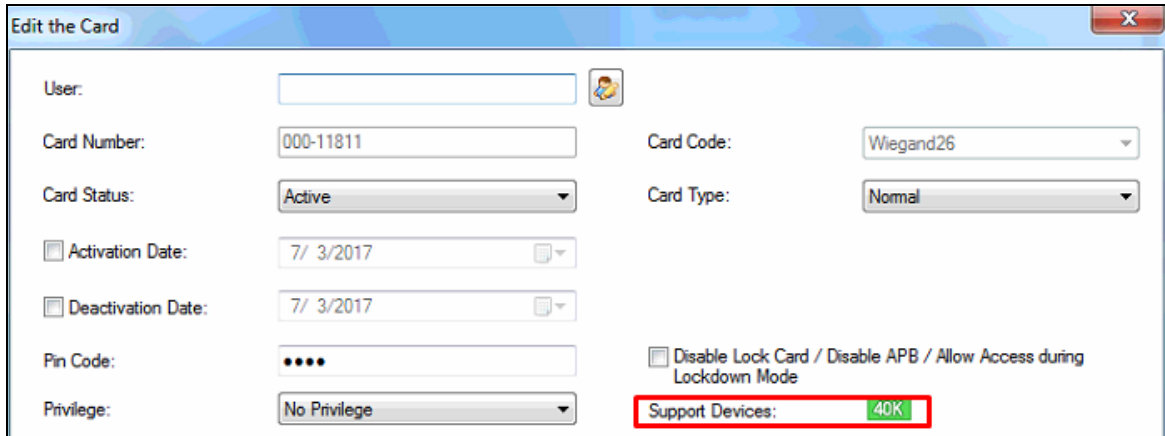
- **Controller:** The Controller column displays the associated doors. The selection for each door will be automatically brought up when one access group was entered.

For first-time user of the GV-ASManager, select **24-hour access** for each door for test run.

- **Data Group:** Assign the card to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions listed under the data group. Refer to *Adding a New User* in Chapter 8 for more details.

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

**Note:** Depending on the controller models, up to 40,000 or 100,000 cards can be supported. The first 40,000 cards created will be labeled as **40K** and cards 40,001 ~ 100,000 will be labeled as **100K**.



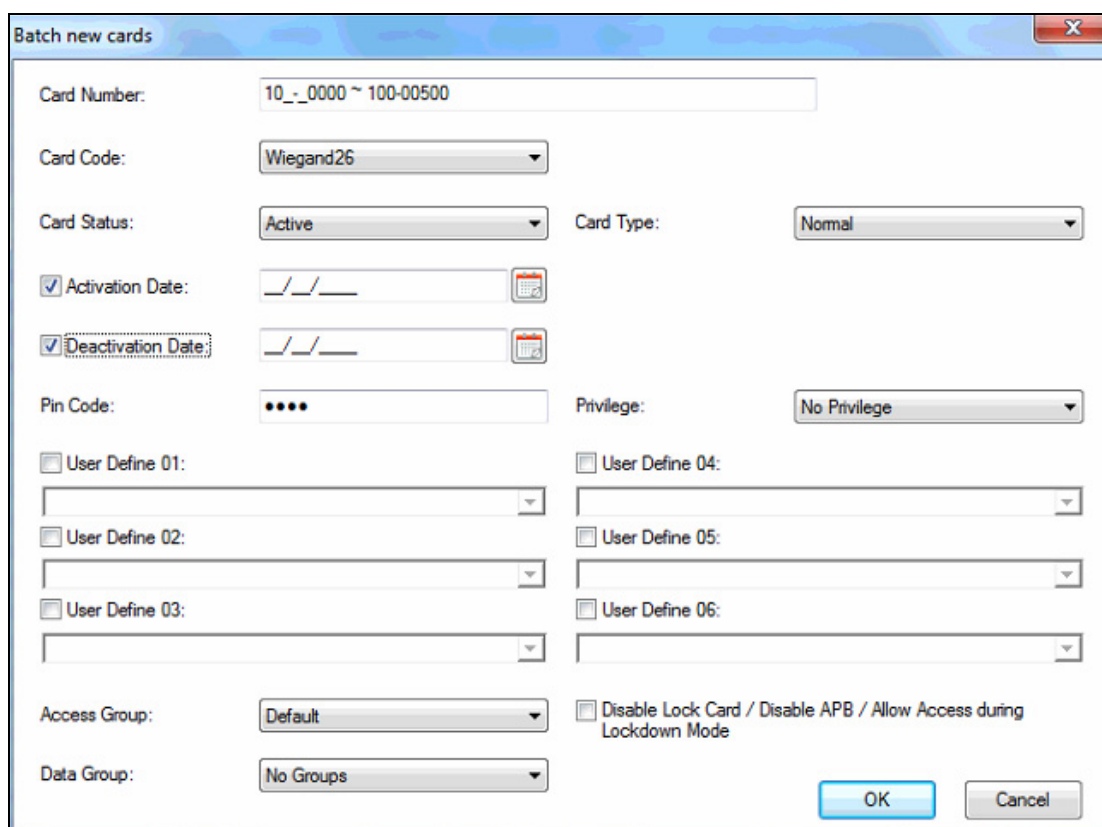
The screenshot shows a window titled "Edit the Card" with a close button (X) in the top right corner. The window contains the following fields and options:

- User:** A text input field.
- Card Number:** A text input field containing "000-11811".
- Card Status:** A dropdown menu set to "Active".
- Activation Date:** A date input field set to "7/ 3/2017" with a calendar icon.
- Deactivation Date:** A date input field set to "7/ 3/2017" with a calendar icon.
- Pin Code:** A text input field containing four dots "••••".
- Privilege:** A dropdown menu set to "No Privilege".
- Card Code:** A dropdown menu set to "Wiegand26".
- Card Type:** A dropdown menu set to "Normal".
- Support Devices:** A dropdown menu set to "40K", which is highlighted with a red rectangular box.
- Disable Lock Card / Disable APB / Allow Access during Lockdown Mode:** An unchecked checkbox.

### 4.3.2 Adding a Group of Cards

Before you use the Batch function to enroll new cards, please note that the group of cards must be numbered sequentially.

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



The dialog box titled "Batch new cards" contains the following fields and controls:

- Card Number:** Text field with value "10\_-0000 ~ 100-00500".
- Card Code:** Dropdown menu with value "Wiegand26".
- Card Status:** Dropdown menu with value "Active".
- Card Type:** Dropdown menu with value "Normal".
- Activation Date:** Checked checkbox, followed by a date field (///) and a calendar icon.
- Deactivation Date:** Checked checkbox, followed by a date field (///) and a calendar icon.
- Pin Code:** Text field with four dots (\*\*\*\*).
- Privilege:** Dropdown menu with value "No Privilege".
- User Define 01:** Unchecked checkbox, followed by a dropdown menu.
- User Define 02:** Unchecked checkbox, followed by a dropdown menu.
- User Define 03:** Unchecked checkbox, followed by a dropdown menu.
- User Define 04:** Unchecked checkbox, followed by a dropdown menu.
- User Define 05:** Unchecked checkbox, followed by a dropdown menu.
- User Define 06:** Unchecked checkbox, followed by a dropdown menu.
- Access Group:** Dropdown menu with value "Default".
- Data Group:** Dropdown menu with value "No Groups".
- Disable Lock Card / Disable APB / Allow Access during Lockdown Mode:** Unchecked checkbox.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 4-14

3. The settings in the dialog box are the same as those of adding a single card. See Step 3 in 4.3.1 *Adding a Single Card*.

---

**Note:** Cards that were enrolled using the Batch function will have the same PIN. If you want to change the PINs of certain cards, you have to enter the PIN using the **Edit** function on the Card List dialog box.

---

### 4.3.3 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.

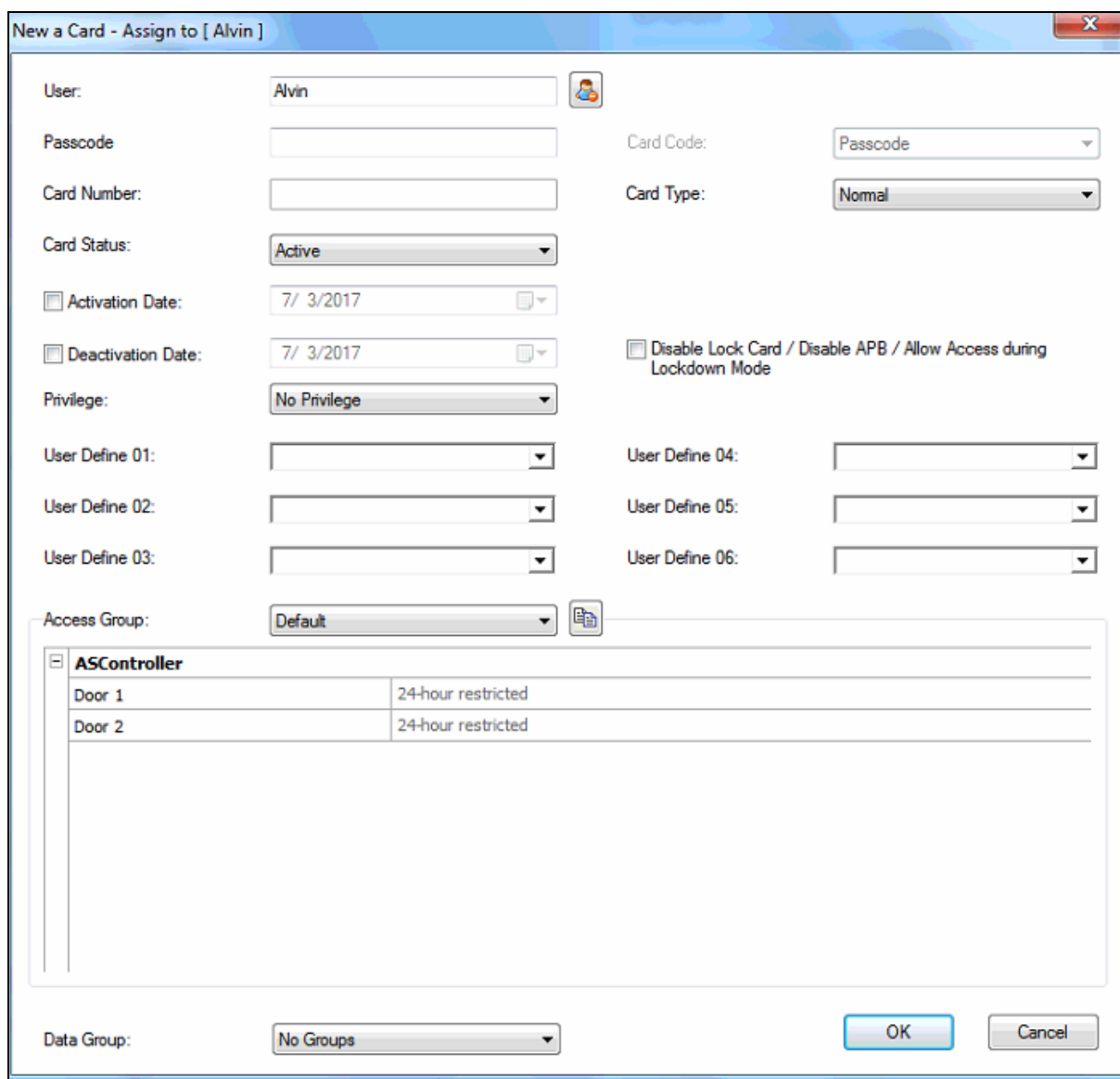
---

**Note:**

1. 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
  2. Passcode is not supported when exporting or importing card data.
- 

1. On the menu bar, click **Personnel** and select **Cards**.

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



The dialog box titled "New a Card - Assign to [ Alvin ]" contains the following fields and options:

- User:** Alvin (with a user icon)
- Passcode:** (empty text field)
- Card Number:** (empty text field)
- Card Status:** Active (dropdown menu)
- Card Code:** Passcode (dropdown menu)
- Card Type:** Normal (dropdown menu)
- Activation Date:** 7/ 3/2017 (calendar icon)
- Deactivation Date:** 7/ 3/2017 (calendar icon)
- Privilege:** No Privilege (dropdown menu)
- Disable Lock Card / Disable APB / Allow Access during Lockdown Mode:** (checkbox)
- User Define 01:** (empty dropdown)
- User Define 02:** (empty dropdown)
- User Define 03:** (empty dropdown)
- User Define 04:** (empty dropdown)
- User Define 05:** (empty dropdown)
- User Define 06:** (empty dropdown)
- Access Group:** Default (dropdown menu with a document icon)
- Table:**

ASController	
Door 1	24-hour restricted
Door 2	24-hour restricted
- Data Group:** No Groups (dropdown menu)
- Buttons:** OK, Cancel

Figure 4-15

- Type a **Passcode** consisting of 4 to 8 numbers.
- The rest of the settings in the dialog box are similar 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.

### 4.3.4 Importing/Exporting Card Data

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

#### To export card data:

1. On the Card List window (Figure 4-12), select desired cards using Ctrl + left click.
2. Click the **Export** button and select **Export to Access** or **Export to Excel**.
3. Assign the file path, and optionally enter password to export card data.

---

**Note:** The Excel file format does not support the password protection.

---

#### To import card data:

1. On the Card List window (Figure 4-12), click the **Import** button and select one of these options: **Import from Access**, **Import from Excel**, **Import from CSV**, or **Import from Others**.
2. Assign the file path and type the **Password** if necessary. Click **OK**. This dialog box appears.

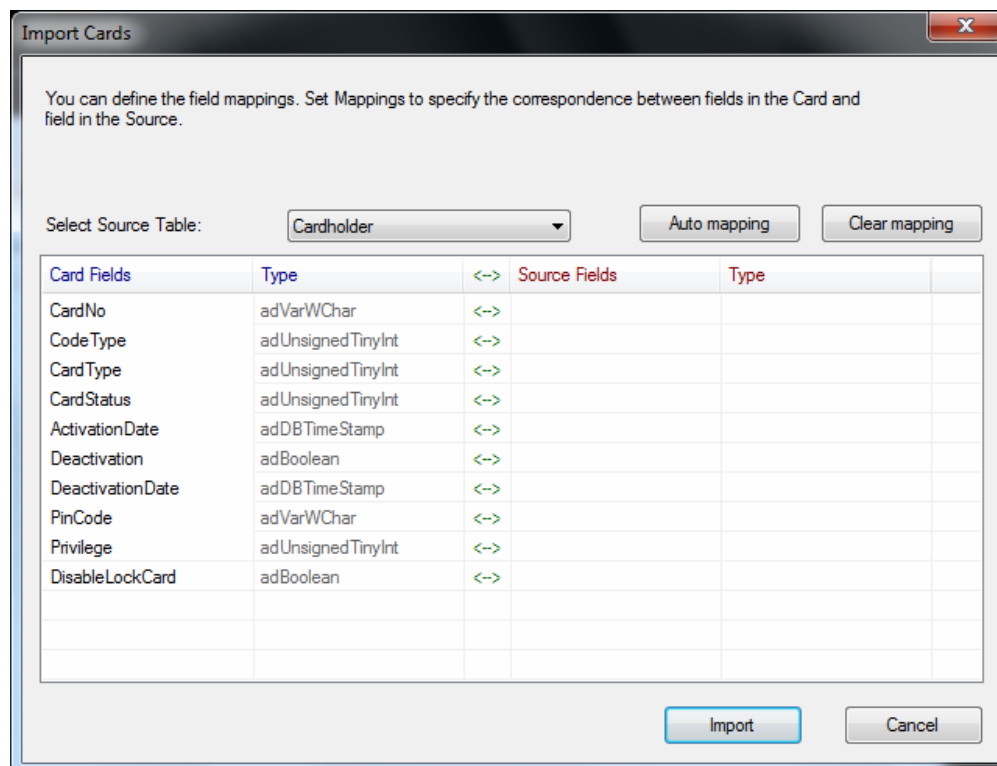


Figure 4-16



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.

### 4.3.5 Customizing a Card Data Field

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

When a custom field is created for cards, the field label will be displayed on the Edit the Card / New a Card dialog box where you type the actual data for each card.

#### To customize a card data field:

1. On the Card List window, click **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 Department field was created.

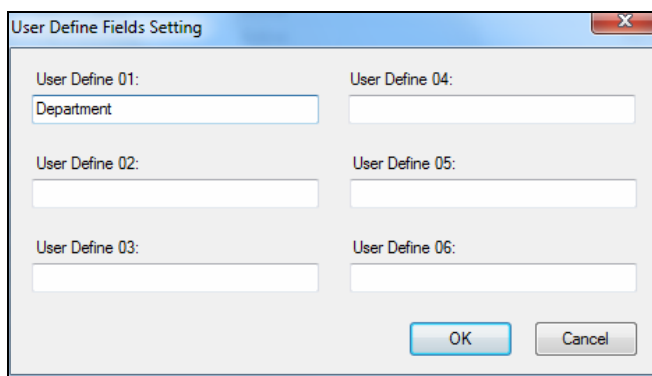


Figure 4-17

#### To enter card data:

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

Figure 4-18

## 4.4 Setting Weekly Schedules

This section will help you define the daily and holiday access times. Up to 254 weekly schedules may be defined with two default weekly 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 Setting 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 Setting Weekly Schedules**

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

- **Step 3 Setting Holidays**

Define specific dates as holidays and special days.

#### 4.4.1 Step 1: Setting Time Zones

This section provides examples of setting the following time zones:

- Day shift – 09:00 to 19:00 hours
- Night shift – 19:00 to 9:00 hours (cross midnight)
- Supervisor – 07:00 to 24:00 hours

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

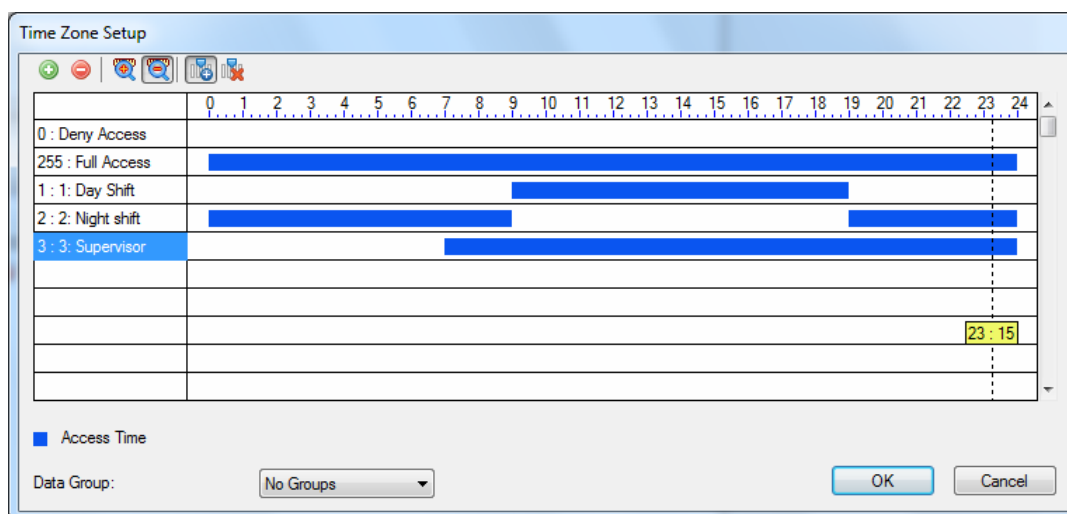


Figure 4-17

2. Click the **Add** button . This dialog box appears.

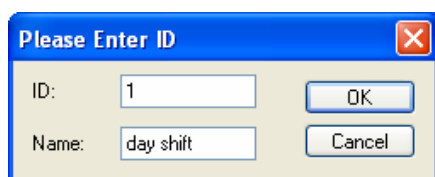



Figure 4-18

3. The **ID** is the number of the time zone. The system will automatically create the ID based on how many time zones have been added. Give a **Name** to the time zone you are going to define. Click **OK**.

For example, name the Time Zone 1 as **day shift**.

4. Click the **Add Access Time** button . Then drag the mouse on the timeline to define a period of access time.

For example, the time of day shift is **from 09:00 to 19:00**.

5. To create the second time zone, click the **Add** button and name it as **night shift**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 19:00 to 24:00** and **from 00:00 to 09:00**.
6. To create the third time zone, click the **Add** button and name it as **Supervisor**. Then click the **Add Access Time** button. Drag the mouse on the timeline to set the time **from 07:00 to 24:00**.
7. You can use the **Data Group** drop-down list to assign the time zone to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.
8. Click **OK**. The three time zones have been defined.

### 4.4.2 Step 2: Setting Weekly Schedules

This section provides examples of setting 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
- Schedule-Supervisor – Monday through Sunday and Holidays, 07:00 to 24:00 hours

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

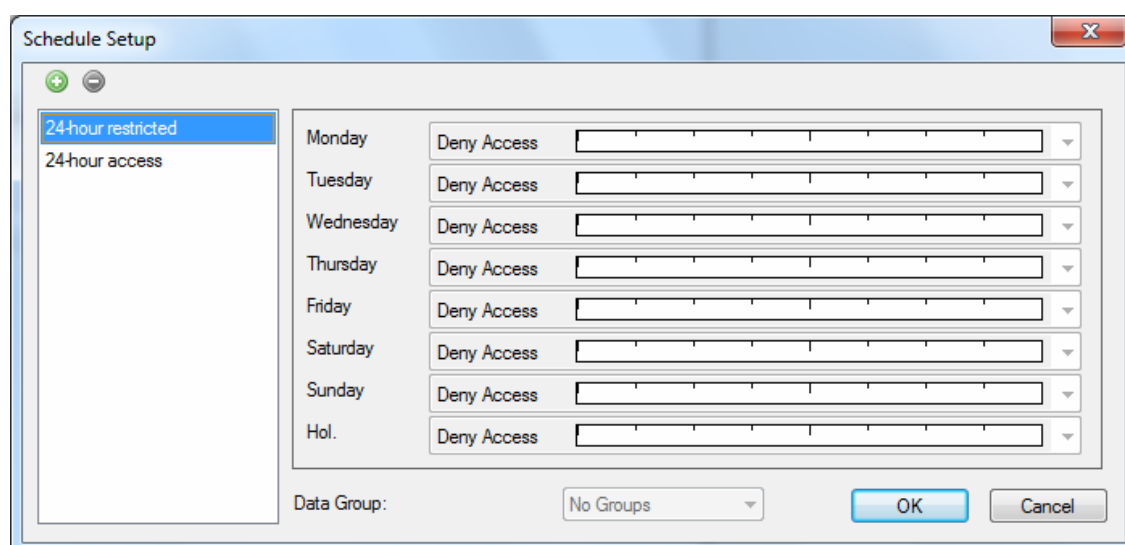


Figure 4-19

2. Click the **Add** button. This dialog box appears.

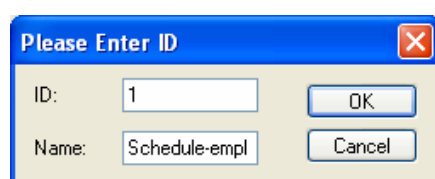


Figure 4-20

3. The **ID** is the number of the weekly schedule. The system will automatically create the ID based on how many time schedules have been added. Give a **Name** to the weekly schedule you are going to define. Click **OK**.

For example, name the Weekly Schedule 1 as **Schedule-Day shift**.

4. From the drop-down lists of **Monday** to **Friday**, select the **Day shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.

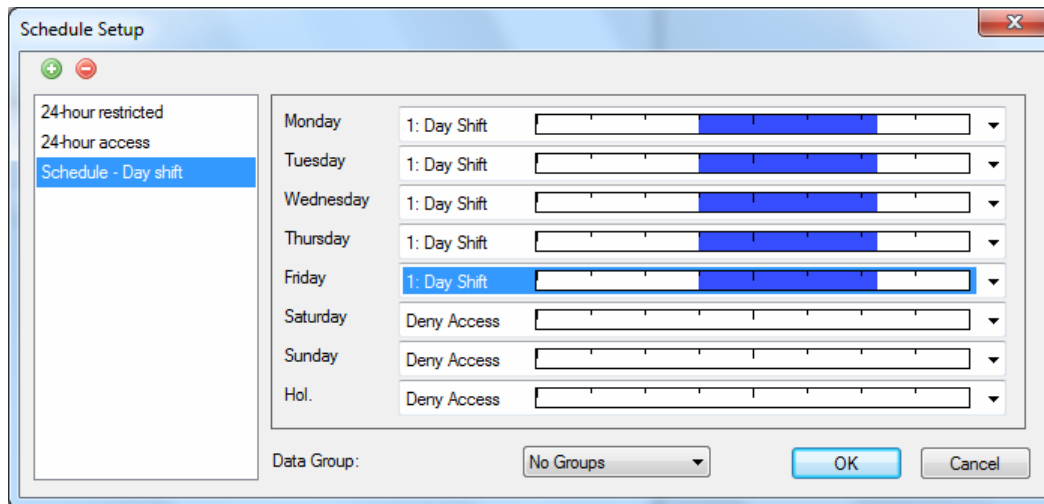


Figure 4-21

5. To create the second time schedule, click the **Add** button and name it as **Schedule-Night shift**. From the drop-down list of **Monday** to **Friday**, select the **Night shift** time zone we have created. No access is allowed on Saturday, Sunday and Holiday.
6. To create the third time schedule, click the **Add** button and name it as **Schedule-Supervisor**. From the drop-down lists of **Monday** to **Hol**, select the **Supervisor** time zone we have created.

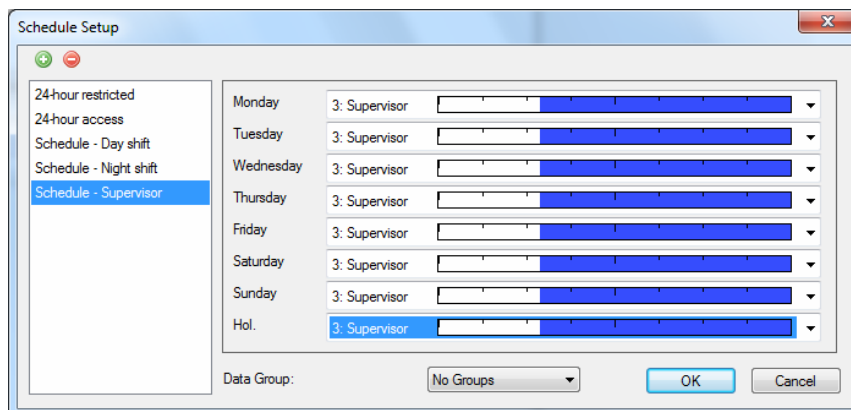


Figure 4-22

7. You can select a time schedule and use the **Data Group** drop-down list to assign the time schedule to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.
8. Click **OK**. The three weekly schedules have been defined.

### 4.4.3 Step 3: Setting Holidays

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

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

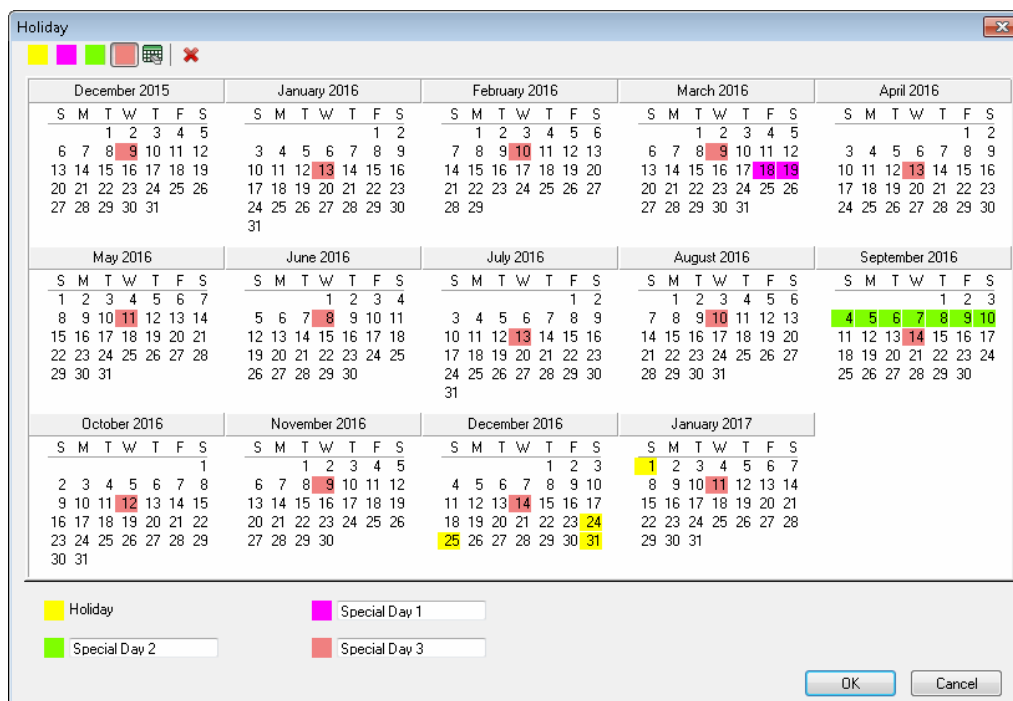


Figure 4-23

2. Click the **Holiday** icon and click the dates you want to set as holidays. For example,
  - Dec 24, 2016 – Christmas Eve
  - Dec 25, 2016 – Christmas Day
  - Dec 31, 2016 – New Year's Eve
  - Jan 01, 2017 – New Year's Day
3. You can designate up to 3 other types of special days for Authentication Schedule and Exit Button Schedule by clicking the color blocks and clicking the dates.
4. To delete holidays or special days, click the **Remove Holiday** icon and click the date you want to delete.

---

**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 setting prior to the beginning of a new year to ensure proper holiday coverage.

---



## 4.5 Setting 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. In the example below, an access group was created to give office staff access to all 4 doors of Controller 1 during daytime shift.

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

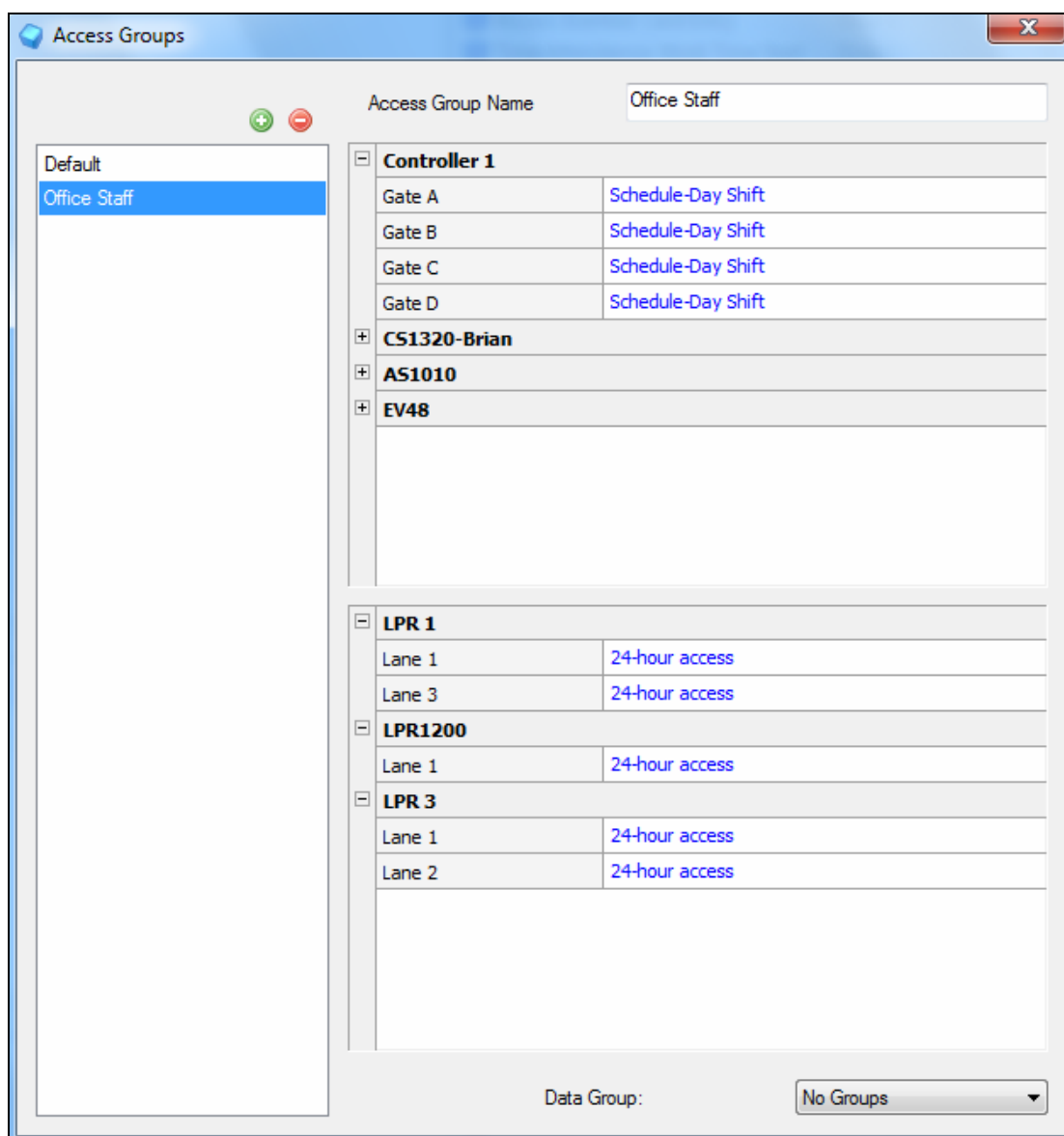

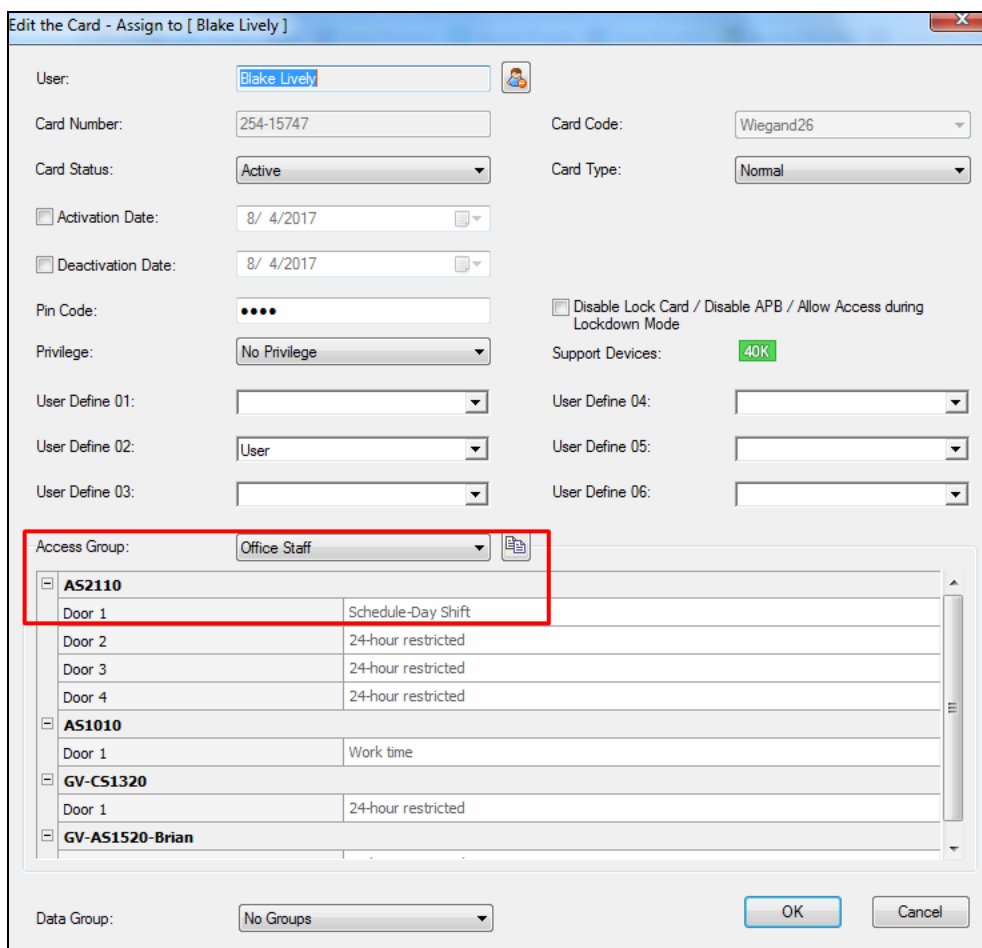



Figure 4-24

2. Click the **New** button , and give a **Name** to the new access group. For example, name the access group **Office Staff**.
3. To define door access for the access group, click the drop-down list next to each door and select one of pre-defined Weekly Schedules. For example, click the blue text next to **Door 1**, and then select **Schedule-Day Shift**.
4. You can use the **Data Group** drop-down list to assign the access group to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.
5. Click **OK**. The access group for office staff has been created.
6. To assign the criteria of the access group to a single card, click **Personnel** on the menu bar and select **Cards**. The Card List dialog box appears.
7. Double-click one listed card. The Edit Card dialog box appears.
8. From the **Access Group** drop-down list, select one pre-defined access group, e.g. **Office Staff**. The assigned Weekly Schedule will be displayed on the associated door's field.





Edit the Card - Assign to [ Blake Lively ]

User:  

Card Number:  Card Code:

Card Status:  Card Type:

☐ Activation Date:  

☐ Deactivation Date:  


Pin Code:  ☐ Disable Lock Card / Disable APB / Allow Access during Lockdown Mode

Privilege:  Support Devices:

User Define 01:  User Define 04:

User Define 02:  User Define 05:

User Define 03:  User Define 06:

Access Group:  


<input type="checkbox"/> AS2110	Door 1	Schedule-Day Shift
	Door 2	24-hour restricted
	Door 3	24-hour restricted
	Door 4	24-hour restricted
<input type="checkbox"/> AS1010	Door 1	Work time
<input type="checkbox"/> GV-CS1320	Door 1	24-hour restricted
<input type="checkbox"/> GV-AS1520-Brian		

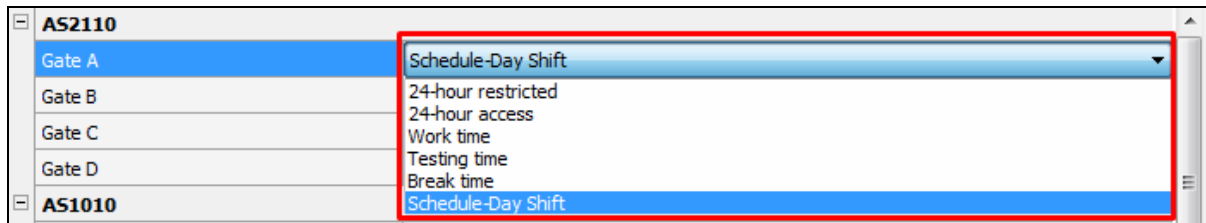
Data Group:

Figure 4-25

---

**Tip:** To customize a particular weekly schedule, select one pre-defined schedule from the

Door / Floor drop-down list, click the **Copy** button  to duplicate the current access group settings to the user-defined access group.



*Figure 4-26*

---

## 4.6 Setting 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** and select **Users**. The User List window appears.
2. Click the **New** button on the toolbar. This dialog box appears.



The **User Setup** dialog box is shown with the **General** tab selected. It contains the following fields and controls:

- First Name:** Nombree
- Middle Name:** (empty)
- Last Name:** Apellido
- Display:** Apellido Nombree (dropdown menu)
- Employee ID:** 0123456789
- Cards:** [026] 237-63838 (with add, delete, and edit icons)
- Vehicles:** (empty list with add, delete, and edit icons)
- ☐ **Send SMS** (with a speech bubble icon)
- Data Group:** No Groups (dropdown menu)
- Photo:** A portrait photo of a woman with blonde hair tied back, wearing a dark jacket over a white shirt.
- Buttons:** OK and Cancel at the bottom right.

Figure 4-27

3. Type a name under **Display**, which is a required field. Other user information such as Employee ID, Photo, Home information and Company information are optional entries.
4. To assign a card or a vehicle to the user,
  - Click **Add a new card / vehicle**  to create a new card / vehicle for the user, or
  - Click **Add**  and double-click one listed card / vehicle to assign an existing card / vehicle to the user.
5. To send SMS alerts whenever the card(s) assigned to the user is presented to the reader, select **Send SMS**.

---

**Note:** To send SMS alerts, see [8.2.1 Setting SMS Server](#) to configure the SMS server. For how to set up SMS alerts, refer to the same settings “Send SMS Alert” at Step 3 in [8.2.3 Setting Notification](#).

---

6. You can use the **Data Group** drop-down list to assign the user to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.

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**.

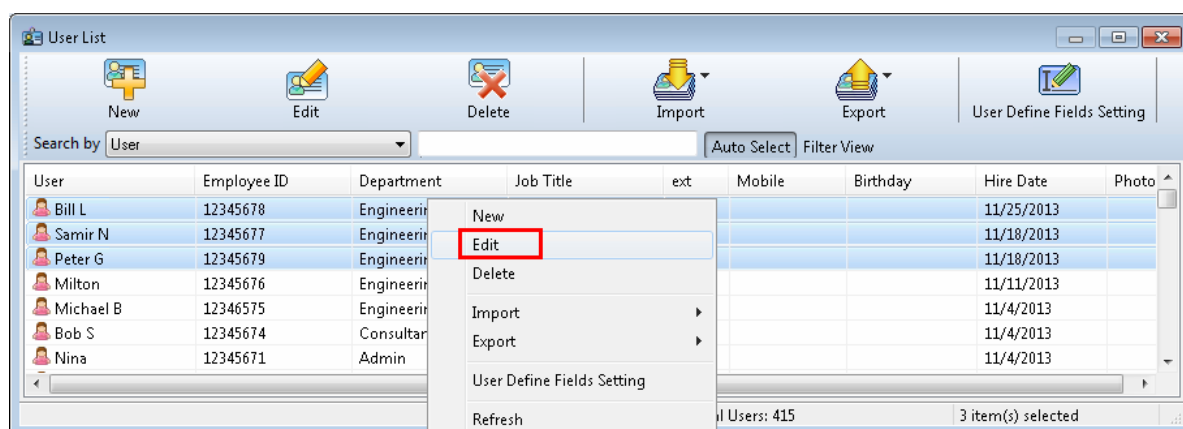


Figure 4-28

You can enroll fingerprints in the **Fingerprint** tab using GV-GF1911 / 1921 / 1922. For details, refer to *Chapter 3 Fingerprint Only Mode* in the *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.

When a custom data field is created, the field label will be displayed in the User Define tab on the User Setup dialog box. The actual personal data for each user is entered in the User Define tab.

### To customize a data field:

1. On the menu bar, click **Personnel** and select **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.

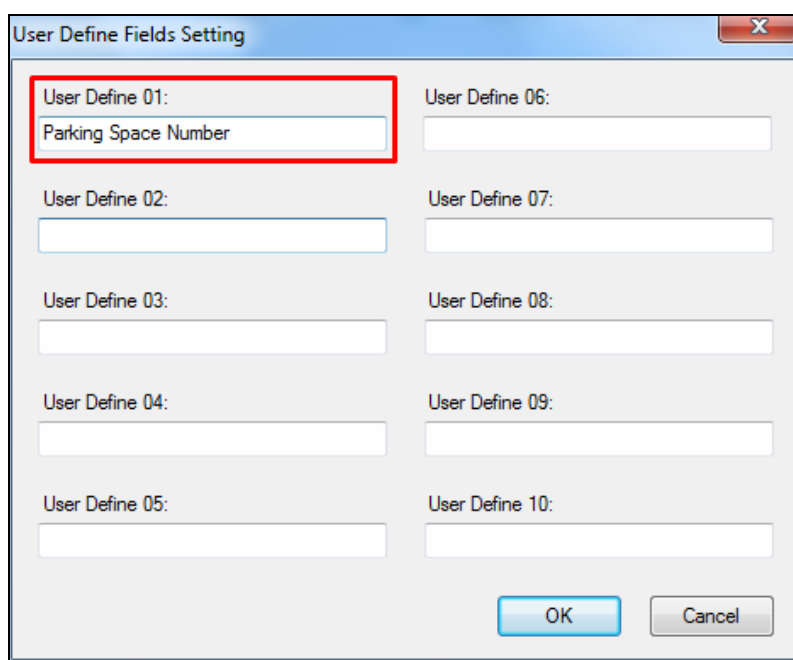
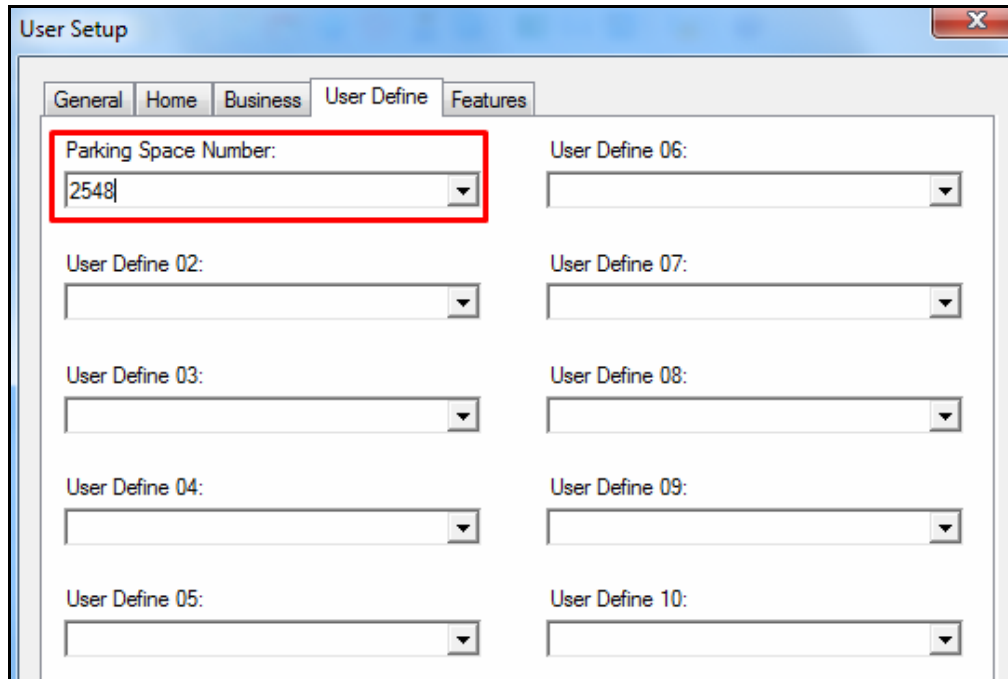


Figure 4-29

### To enter personal data:

1. On the menu bar, click **Personnel** and select **User**. The User List window appears.
2. Double-click one listed user to whom personal data should be entered. The User Setup dialog box appears.
3. Click the **User Define** tab. The custom data field you have created now is displayed.

- Click in the custom data field and enter the appropriate information. In this example, a number is entered in the created Parking Space Number field:



The screenshot shows a 'User Setup' dialog box with a 'User Define' tab selected. The 'Parking Space Number' field is highlighted with a red box and contains the value '2548'. Below it are fields for 'User Define 02' through 'User Define 10', all of which are currently empty. The dialog box has a standard Windows-style title bar and a close button in the top right corner.

Figure 4-30

#### 4.6.3 Importing/Exporting User Data

From the User List window, you can import and export user data in mdb or xls format. For this function, refer to *4.3.3 Importing / Exporting Card Data*.



## 4.7 Adding IO Boxes

To add the GV-I/O Box 4E/8/16 Ports to GV-ASManager over networks for I/O management, follow these steps:

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

Establish the communication between the GV-I/O Box and GV-ASManager.

- **Step 2 Configuring the input and output functions**

Define the input and output pins to be used by the GV-I/O Box

### 4.7.1 Step 1: Configuring GV-I/O Box to GV-ASManager

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

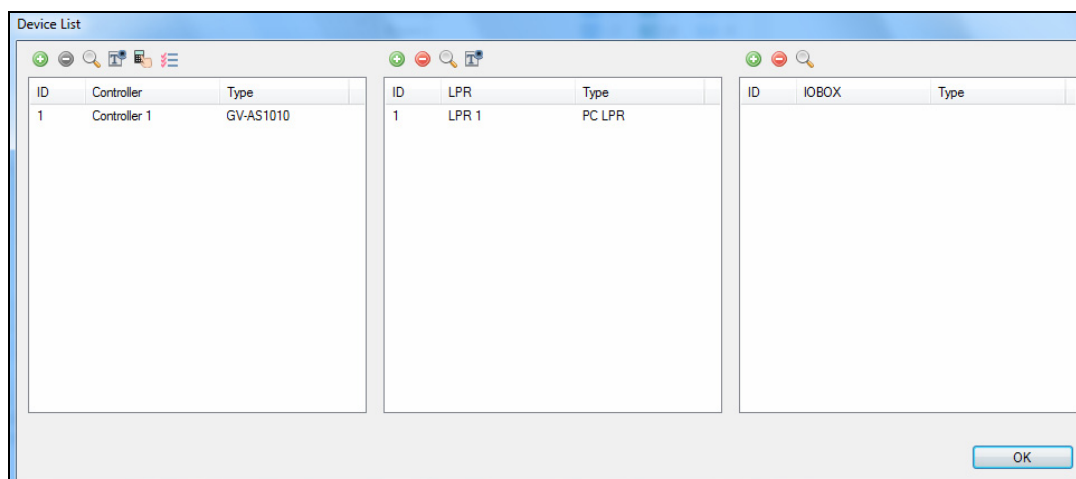


Figure 4-31

2. On the top-right side, click the **Add**  button. This dialog box appears.

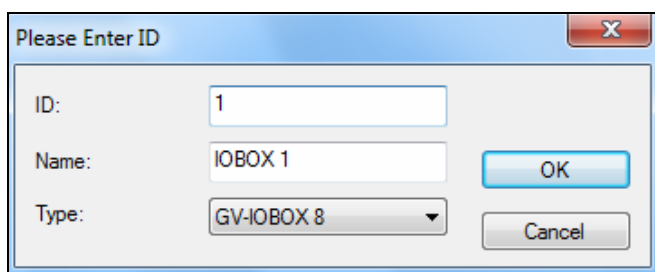


Figure 4-32

3. Type an **ID** number and **Name** for the GV-I/O Box, select Type of the **GV-I/O Box** and click **OK**. The IOBOX Setup dialog box appears.



The image shows the IOBOX Setup dialog box with two tabs: 'General Setup' and 'I/O'. The 'General' section contains the following fields:

- IOBOX Name:** IOBOX1
- IOBOX ID:** 1
- Data Group:** No Groups (dropdown menu)
- GMT:** + 08 : 00 (time zone selection)
- ☐ **Enable Daylight Saving**
- Setup** button

The **Connection** section contains the following fields:

- Network:** TCP/IP (dropdown menu)
- IP:** 192.168.5.43 (with a search icon)
- Port:** 10000
- User:** admin1
- Password:** (masked with dots)

Figure 4-33

4. Under Connection, select the communication mode between the GV-I/O Box and GV-ASManager.
  - If selecting **TCP / IP**, type the IP address, port number, login user and login password. You can also click the **Search** button  to search for GV-I/O Boxes detected in the same LAN.
  - If selecting **Local DDNS**, type the IP address of the LocalDDNS Service and the device name to match that of GV-I/O Box's Web interface registered from the LocalDDNS Server, the port number, login user and login password.
5. To check if the above connection settings are correct, you can click **OK** at this step and back to the main screen. The icon  appearing on the IOBox window indicates the connection is established.
6. OPTIONAL settings in the General section:
  - **Data Group:** Assign the I/O Box to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read / write / execute the functions assigned under the data group. Refer to *Adding a New User* in Chapter 8 for more details.
  - **GMT:** The current time at the host computer.

- **Enable Daylight Saving:** Enable the Daylight Saving Time function by selecting your time zone. The system will automatically adjust for daylight saving time.

#### 4.7.2 Step 2: Configuring the input and output functions

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

**IOBOX Setup**

General Setup | **I/O**

**Input**

Monitor	ID	Name
<input checked="" type="checkbox"/>	1	Input 1
<input type="checkbox"/>	2	Input 2
<input type="checkbox"/>	3	Input 3
<input type="checkbox"/>	4	Input 4
<input type="checkbox"/>	5	Input 5
<input type="checkbox"/>	6	Input 6
<input type="checkbox"/>	7	Input 7
<input type="checkbox"/>	8	Input 8

**Input 1**

☒ Enable

Input Mode : ☒ NO ☐ NC

☐ Latch Enable

Trigger Output: 03: Output 3

Camera 1 : LPR 3, Camera 9

Delayed snapshot: 0 Sec(0~60)

Camera 2 : LPR 1, Camera 8

Delayed snapshot: 0 Sec(0~60)

Trigger Device : ☒ Controller ☐ LPR

Device : AS1010, Door 1

Action : None

**Output**

Monitor	ID	Name
<input type="checkbox"/>	1	Output 1
<input type="checkbox"/>	2	Output 2
<input checked="" type="checkbox"/>	3	Output 3
<input type="checkbox"/>	4	Output 4
<input checked="" type="checkbox"/>	5	Output 5
<input type="checkbox"/>	6	Output 6
<input type="checkbox"/>	7	Output 7
<input type="checkbox"/>	8	Output 8

**Output 3**

☒ Enable

Output Mode : ☒ NO ☐ NC

Trigger Mode : ☒ Normal ☐ Toggle ☐ Pulse : 0 Sec(0~60)

Camera 1 : None

Delayed snapshot: 0 Sec(0~60)

Camera 2 : LPR 1, Camera 5

Delayed snapshot: 0 Sec(0~60)

OK Cancel

Figure 4-34

2. Click **Monitor** to select an input/output to be used by GV-I/O Box.

#### [Input]

- **Enable:** Click to 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 pin to trigger when the input is detected.
- **Camera 1 / 2:** Select a camera to take snapshots upon input trigger.
- **Delayed snapshot:** Type the number of seconds to delay capturing the snapshot after input is triggered.
- **Trigger Device:** Select a controller or LPR device to trigger door or lane operations.

### [Output]

- **Enable:** Select to 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 set in the **Sec** field.
- **Camera 1 / 2:** Select a camera to take snapshots upon output trigger.
- **Delayed snapshot:** Type the number of seconds to delay capturing the snapshot after output is triggered.

## Chapter 5 Video Integration

GeoVision IP devices and certain third-party IP cameras can be connected to the GV-ASManager through the network. Live video can then be accessed and snapshots will be captured when an event is triggered.

The GV-ASManager provides the following video features:

- Live view
- Video playback
- Monitor up to 16 cameras at one time
- Text Overlay

---

**Note:**

1. GeoVision IP devices include GV-DVR / NVR / GV-VMS, GV-Video Server, GV-Compact DVR and GV-IP Camera. For compatible third-party IP cameras, see *Appendix A*.
  2. To connect third-party IP cameras to GV-ASManager V2.3 and earlier versions, a NVR Dongle is required.
  3. The GV-ASManager only supports GV-DVR / NVR of version 8.120 or later.
  4. Dewarping of GV-Fisheye IP Camera is only supported when using MultiView, and the source image can only be dewarp into Single View mode.
-

## 5.1 Mapping Cameras

To map a camera from the GV-DVR / NVR / VMS to a door, you must first enable the following service for video access:

- Enable **Control Center Server (CCS)**

To map cameras to a door:

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

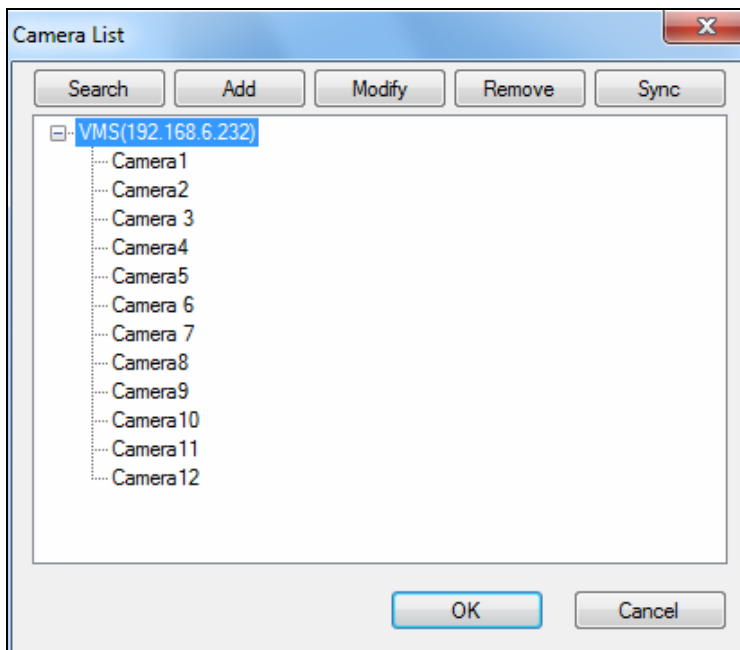


Figure 5-1

- Click **Add**, select the type of the IP device, and type its IP address and login information.
  - Click **Search** to detect all GV-IP Devices or GV-DVR / NVR / VMS on the same LAN. After the found device is added, click the **Modify** button to enter its login ID and password.
  - Click **Sync** to synchronize the camera names created from GV-VMS
2. Click **OK** and return to the main screen.
  3. On the menu bar, click **Setup** and select **Devices**. The Device List dialog box appears.
  4. Double-click one listed controller and click a **Door** tab in the Controller Setup dialog box.

5. In the Camera Mapping section, use the drop-down list under **First Camera** and **Second Camera** to select a camera you just added.

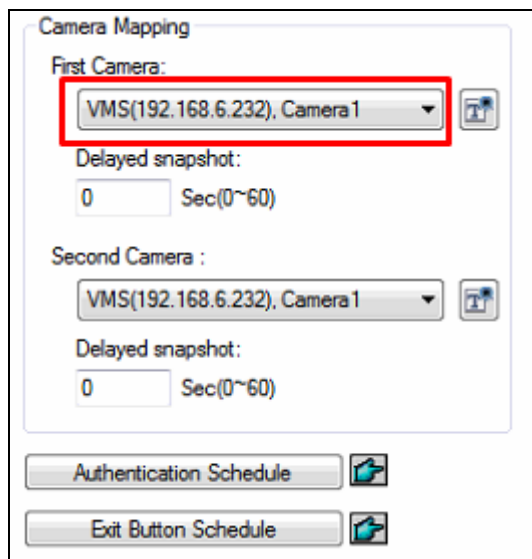


Figure 5-2

6. You can enable **Delayed snapshot** by typing the number of seconds to delay capturing the snapshot after an event is triggered. For example, if the camera is installed 10 meters away from the card reader and it takes 5 seconds for the user to walk pass the camera after presenting the access card, you can delay the snapshot for 5 seconds.
7. Click the specific door on the Device View window. The associated live view is displayed on the Live Video window.

---

**Tip:**

1. You can modify the host or camera name in the DVR List dialog box (Figure 5-1) by clicking the listed name directly.
  2. GV-ASManager is compatible with third-party IP devices using RTSP, ONVIF and PSIA protocols. To connect through RTSP, ONVIF and PSIA protocols, click the **Add** button, select **Add IPCam Mapping** and select **Protocol** in the **Brand** drop-down list to choose the type of protocol. For the RTSP commands, refer to the third-party IP camera's user manual.
-

## **5.2 Accessing a Live View**

After mapping cameras to doors, use one of the following methods to access a live view on the Live Video window:

- On the Controller / LPR window, click the desired door. Its associated live view will appear.
- On the Camera List window, click the desired camera. Its associated live view will appear.
- On the Alarm Monitor and Access Monitor windows, click the desired event. Its associated live view will appear.

To access live views from multiple IP devices, see *5.4 The MultiView Window* below.



## 5.2.1 Live Video Window

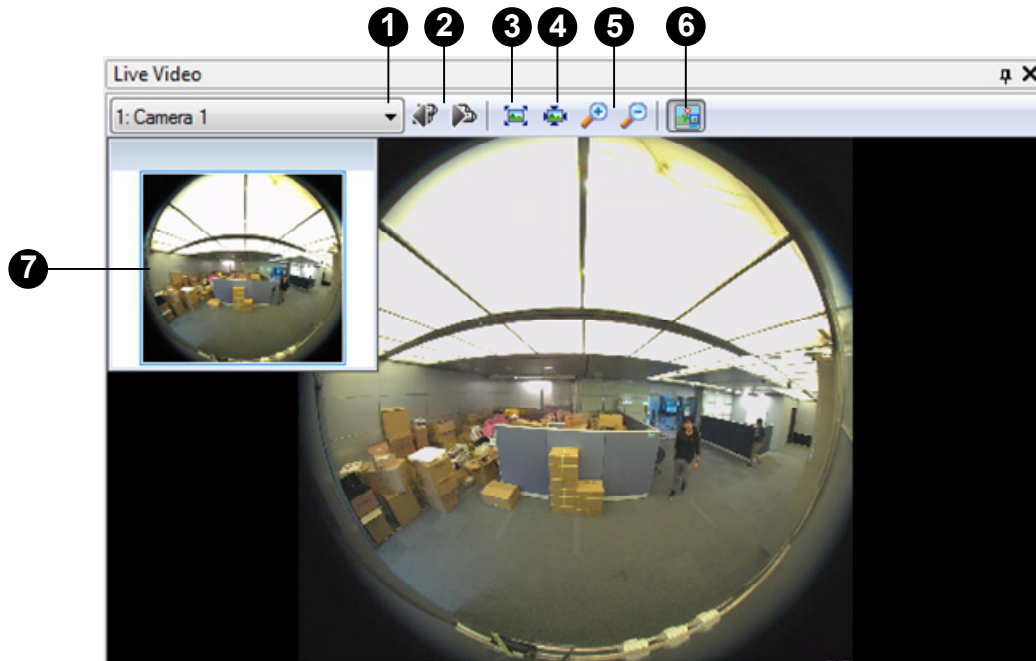


Figure 5-3

The controls on the Live Video window:

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 a Video Image

You can access the video image captured after the access and alarm triggered event.

- On the Access Monitor or Alarm Monitor window, double-click the desired event to display the image. Or, right-click the desired event and select **Show Image** to display the image. Notice if there is no image retrievable, the option will be grayed out.

### 5.4 The MultiView Window

The MultiView window provides a quick view of up to sixteen preset cameras on one screen. These cameras can be a mix of cameras from several IP devices.

To open and use MultiView:

- On the menu bar, click **View** and select **MultiView**. The MultiView window appears, similar to Figure 5-4.
- Drag the desired camera from the Camera List window, and drop it to a grid on MultiView.

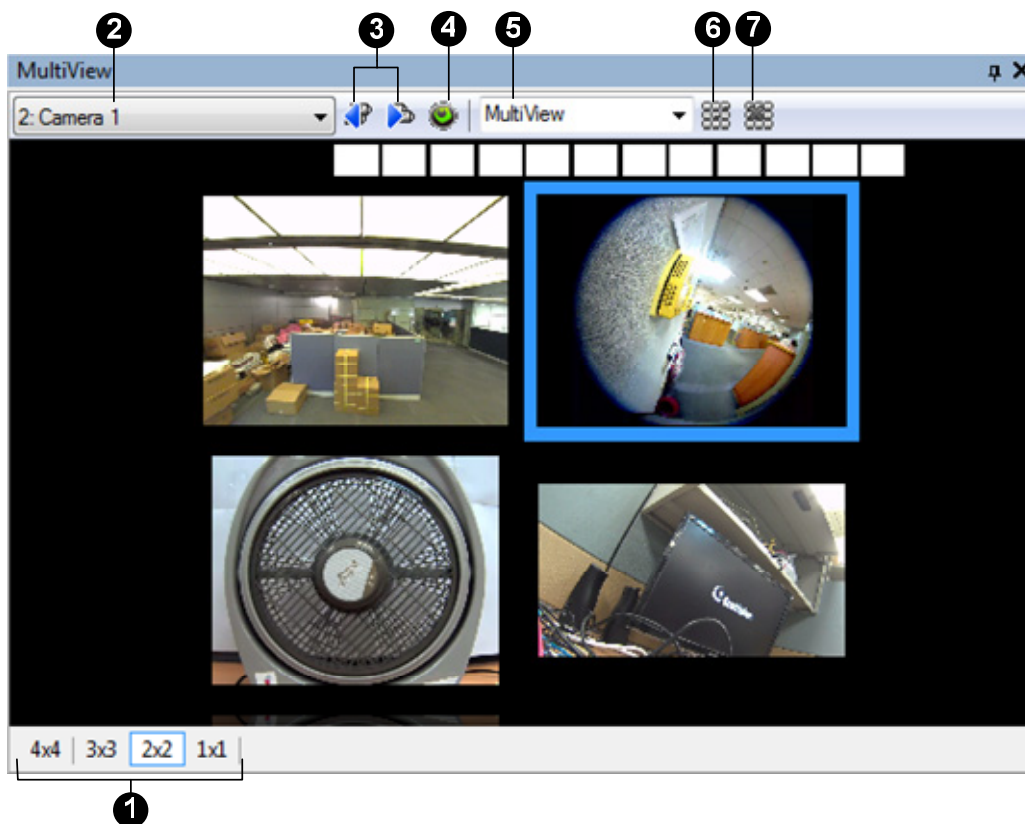


Figure 5-4

The controls on the MultiView window:

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	Matrix View	Select an existing Matrix View from the drop-down list. For details, see <i>5.4.1 Adding a Matrix View</i> .
6	Add Matrix	Add a Matrix View.
7	Delete Matrix	Delete a Matrix View.

---

**Note:** It is possible to drag the MultiView window out of the main screen and even drag the window to place at the second computer monitor.

---

### 5.4.1 Adding a Matrix View

A Matrix View, or a group of views, is a programmed arrangement of frames in the MultiView window that can present up to sixteen different camera views. Multiple Matrix Views can be added as required.

1. In the Matrix View drop-down list (No. 5, Figure 5-4), type a name for the Matrix View.
2. Click the **Add Matrix** button. The Matrix View name is created.
3. Drag the desired camera from the Camera List window to an available frame in the window. The video associated with the camera is displayed in the frame.
4. You can repeat Steps 1-3 to add more than one Matrix View. And use the drop-down list to change to a different Matrix View.

## 5.5 Retrieving Recorded Video

Recorded videos can be reviewed by retrieving the videos from the GV-DVR / NVR / VMS and playing it back. Before you can review videos recorded on the GV-DVR / NVR / VMS, the following function must be enabled to allow remote access:

- Enable **Remote ViewLog Service** on Control Center Server

To play back a video:

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

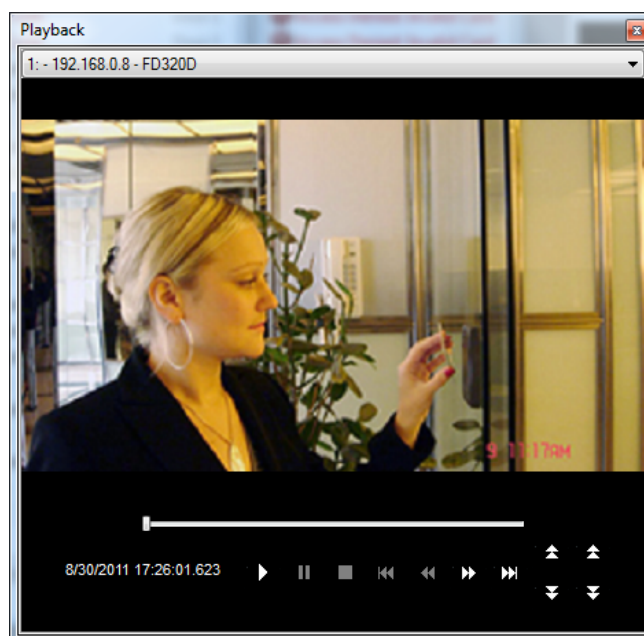


Figure 5-5

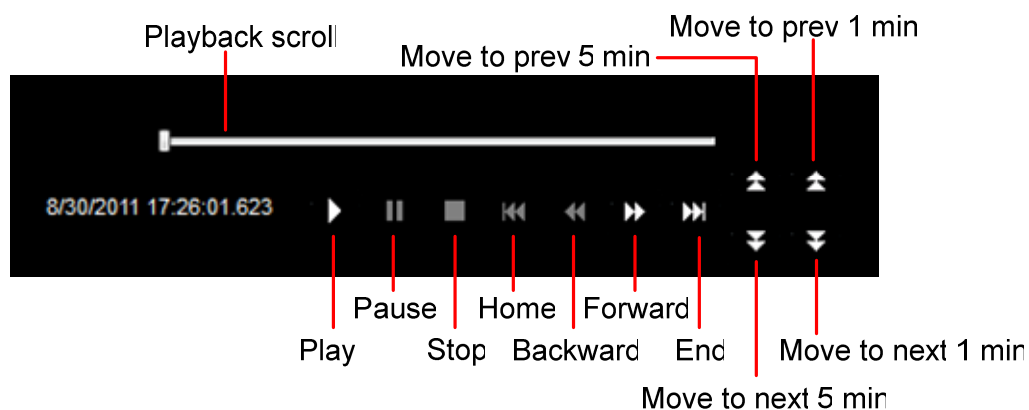


Figure 5-6

Right-click the window to have the following features:

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


## 5.6 Using Text Overlay

You can overlay GV-ASManager's data such as user information, company information and LPR data, on the camera view of your mapped cameras from GV-VMS. For details on mapping GV-IP cameras, see *5.1 Mapping Cameras*.

---

**Note:** This function only supports GV-VMS V16.10.3.0 or later.

---

1. After mapping cameras from GV-VMS, you need to enable the Text Overlay setting.
  - For GV-IP cameras, on the menu bar, click **Setup**, select **Devices**, double-click the **ASController**, and click the **Door** tab. In the Camera Mapping section, click the **Text Overlay** icon  besides the cameras.

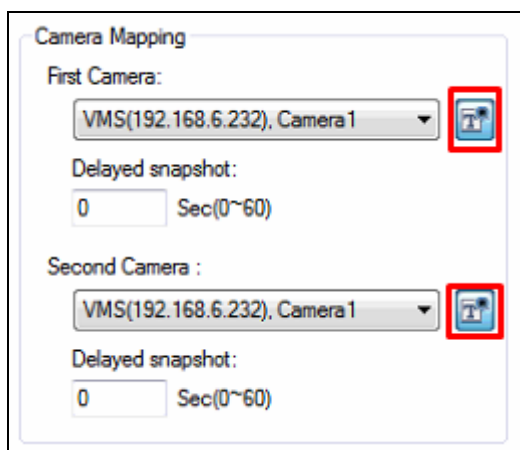



Figure 5-8

- For GV-LPR cameras, on the menu bar, click **Setup**, select **Devices**, double-click the **LPR camera**, and click the **Lane** tab. Select up to four cameras connected to GV-VMS to be **Recognition Cameras**. Click the **Text Overlay**  icon besides the cameras.

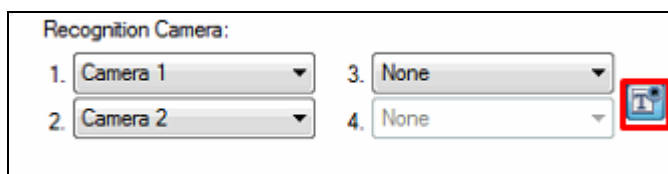


Figure 5-9

- Click **OK** to return to the Device List.

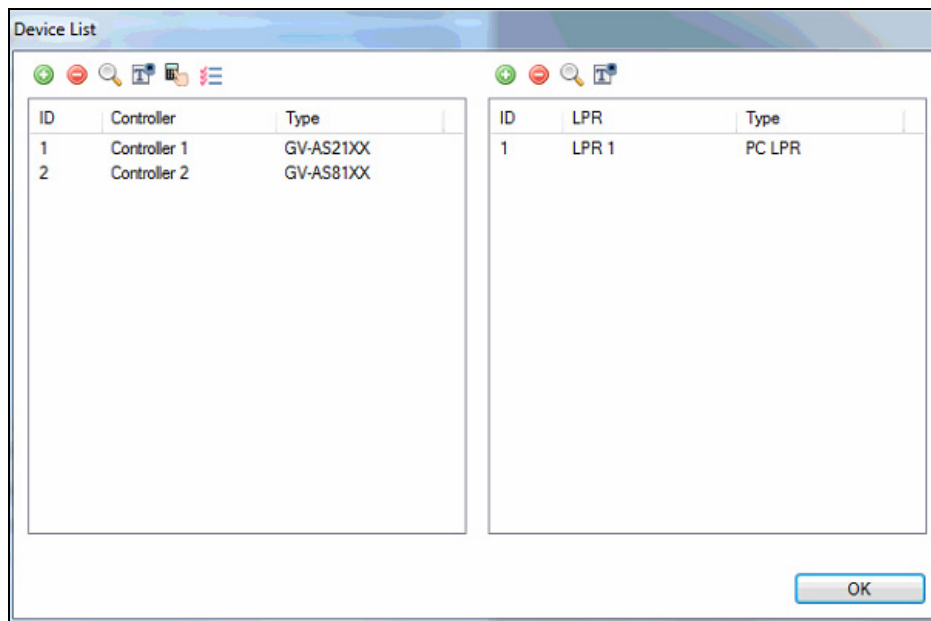




Figure 5-10

- Click the **Camera Text Overlay** icon . In this case, the icon above the LPR camera is selected.
- Select at least one icon from the list to display the text onto the camera view. For example, if you select the company's icon , the name of the company will be printed on the camera view.

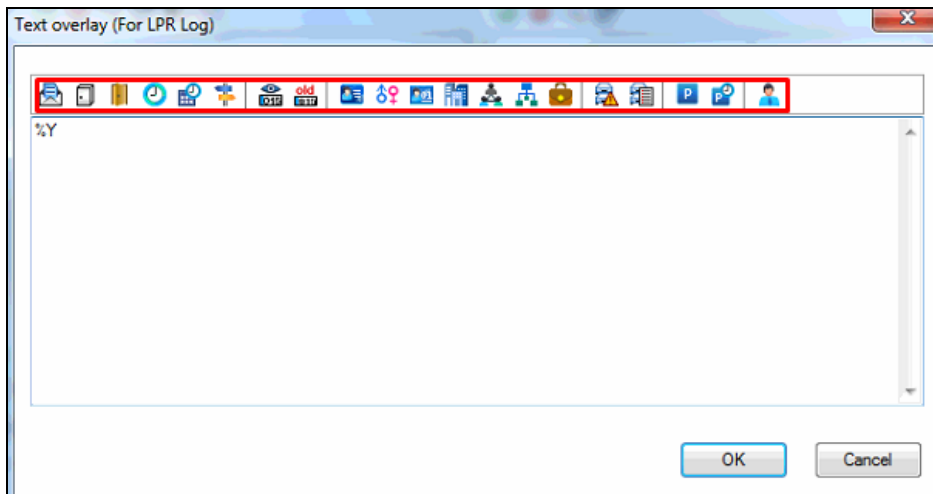


Figure 5-11

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



## 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**.

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

## 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.

The screenshot shows the 'Controller Setup' dialog box with the 'Door 1' tab selected. The 'Monitor' checkbox is checked. The 'Name' field is 'Door 1'. The 'Common Password' field is masked with dots, with a note '4~8 digits(0~9)'. The 'Urgent Code' field is also masked, with a note '4~8 digits(0~9)'. The 'Lock Reset Time' is set to 5 seconds, with a note 'Sec(1~255)'. The 'Held Open Time' is set to 10 seconds, with a note 'Sec(0~9999)'. The 'Lock Card Time' is set to 0 seconds for both 'Entrance' and 'Exit', with a note 'Sec(0~65535)'. The 'Fire Action' is set to 'Unchange'. The 'Reader's Keypad' section has 'Entrance' and 'Exit' checked. The 'GeoFinger' section has 'Entrance' checked. The 'Anti-Passback' section has three radio button options: 'None' (selected), 'By Card - Local' (highlighted with a red box), and 'By User - Local' (highlighted with a red box).

Figure 6-1

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

---

**Note:** The **By User – Local** option is supported only by GV-AS2 / 4 / 8 series Controllers and GV-AS1520 firmware version 2.0 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.

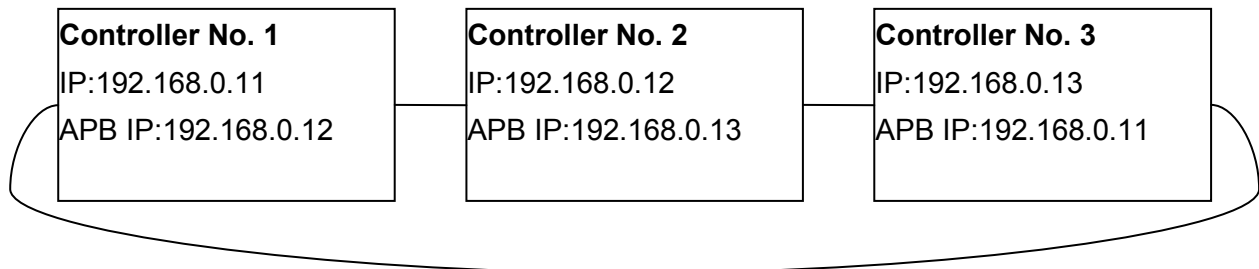
Here we will explain how to combine three controllers together to operate the Anti-Passback (APB) function. Since Anti-Passback is performed in a network connection, every controller has a unique IP address. When three controllers are connected for Anti-Passback, an APB IP address is then applied for interaction.

For example, Controller No. 1, No. 2 and No. 3 are combined in sequence, as illustrated 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:

1. Access the **Function Configuration** page of the Controller No. 1 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.

The screenshot shows the 'Door/Gate 4' configuration page. On the left is a sidebar with 'Basic Setting' and 'Advanced Setting' sections. Under 'Advanced Setting', 'Function Configuration' is highlighted with a red box. The main content area shows 'Function:' set to 'Door Control' and 'Authentication Mode:' set to 'Authentication Schedule Mode'. Below this, the 'Series Function(APB & Fire)' section is highlighted with a red box. It contains 'Enable/Disable:' set to 'Enable' and 'Info IP:' set to '192 . 168 . 0 . 12'. At the bottom are 'Submit' and 'Cancel' buttons.

Figure 6-2

2. Access the **Function Configuration** page of the Controller No. 2 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 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. On the 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 diagram below shows a typical site controlled by access control. The following sections will guide you through the steps you would need to go through to configure this site for Global Anti-Passback.

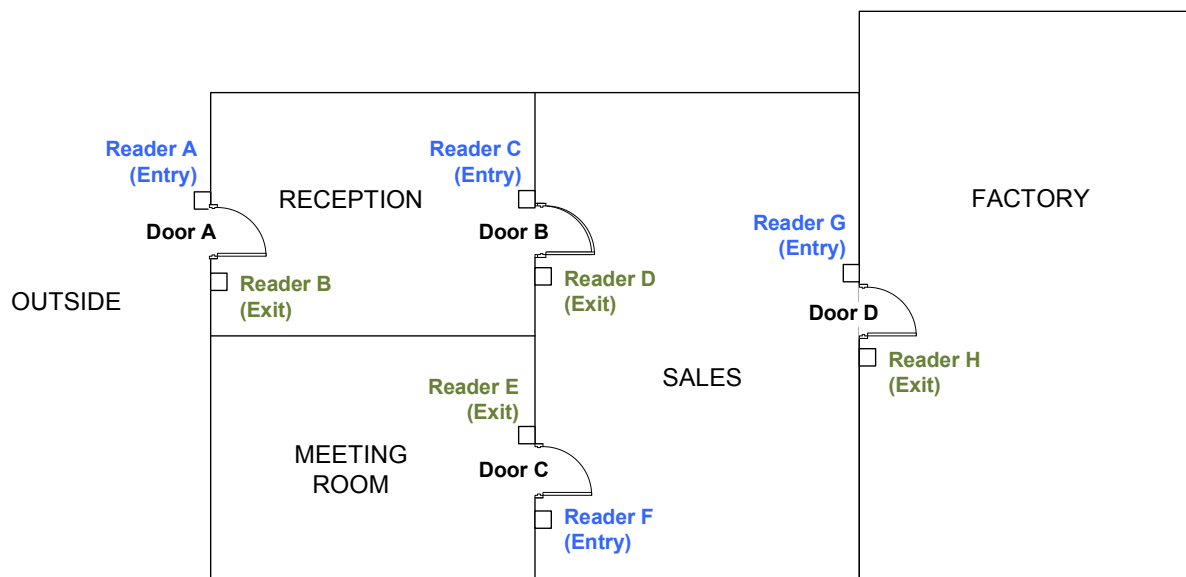


Figure 6-3

### 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 Entry and Exit areas for each door and name the areas properly.

- On the menu bar, click **Setup** and select **Areas**. This dialog box appears.

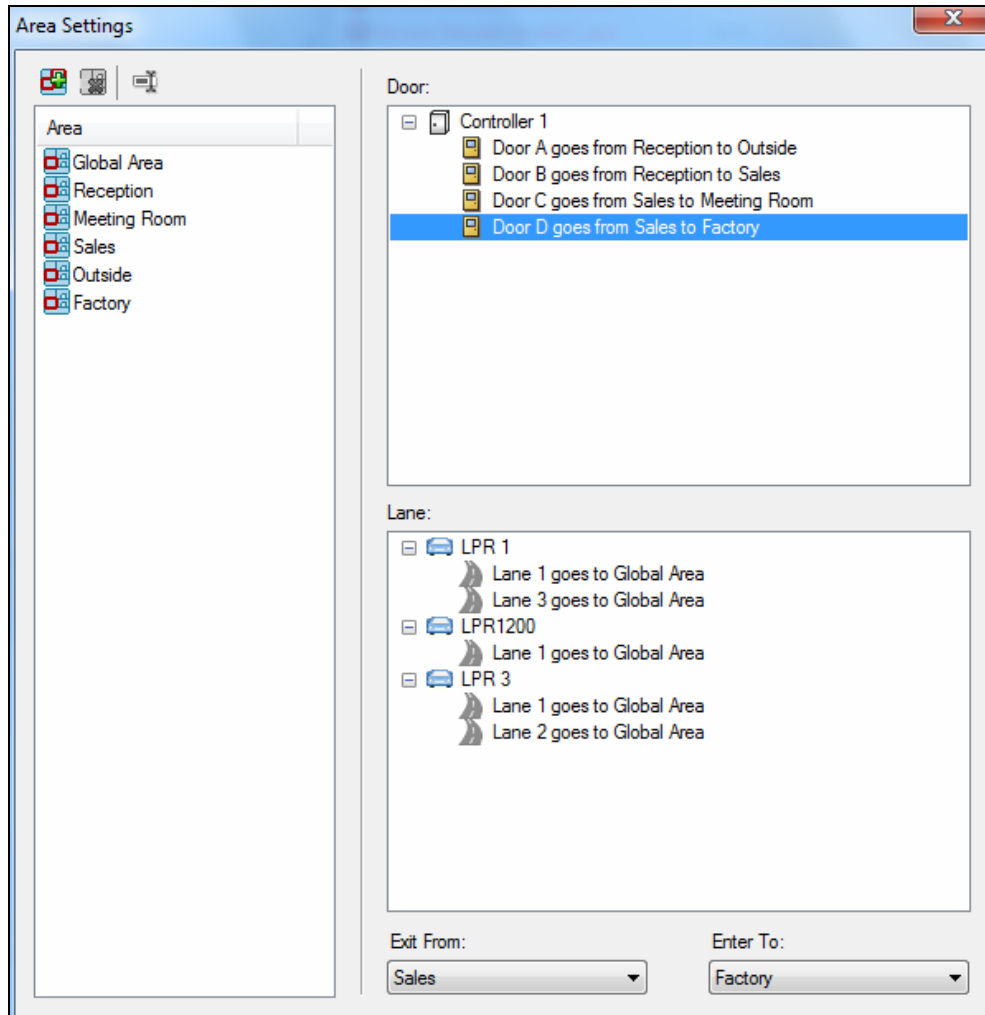


Figure 6-4

**Enter to** is the area where you enter by accessing the Entry reader. **Exit to** is the area where you exit to by accessing the Exit reader. In this case, we set up like this:

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

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

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

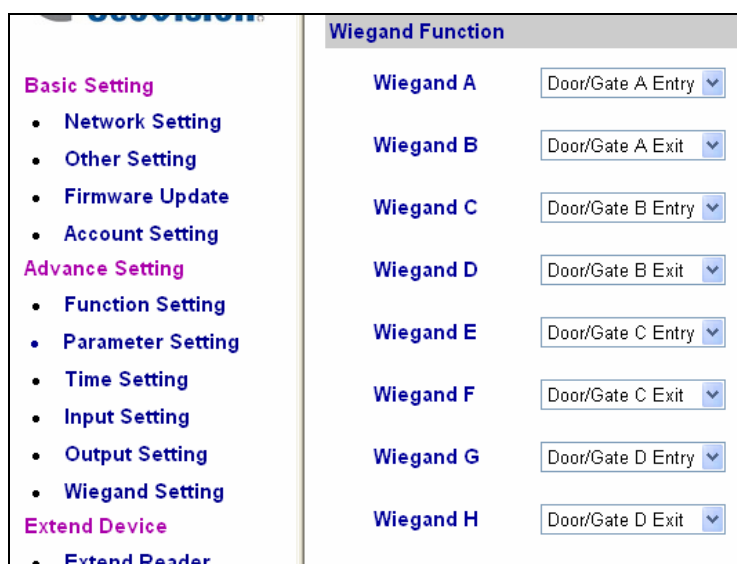
Door D: **Enter to** Factory; **Exit to** Sales

### 6.3.3 Step 3: Configuring Readers

This step is to define the Entry and Exit readers for each door. The reader definition tells the 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 the GV-AS / GV-EV Controller, and in the left menu, click **Wiegand Setting** for Wiegand readers or **Extended Reader** for RS-485 / TCP/IP readers. In the example below, 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 the door contact sensor is triggered and the door is unlocked, the GV-ASManager can tell the location of the user based on your area definition at Step 2.

To define door contact sensors, go to the Web interface of GV-AS / GV-EV Controller and click **Input Setting**. In the example below, Input 01 is set as Door Contact of Door A, Input 02 is set as Door Contact of Door B and etc.






















<ul style="list-style-type: none"><li>• Network Setting</li><li>• Other Setting</li><li>• Firmware Update</li><li>• Account Setting</li><li>• <b>Advanced Setting</b></li><li>• Function Setting</li><li>• Parameter Part1</li><li>• Parameter Part2</li><li>• Time Setting</li><li>• Input Setting</li></ul>	<h3>Input Configuration</h3> <table><thead><tr><th colspan="4">Input Function</th></tr></thead><tbody><tr><td>01</td><td>Input_01</td><td>NO ▾</td><td>Door A ▾ Door Contact ▾</td></tr><tr><td>02</td><td>Input_02</td><td>NO ▾</td><td>Door B ▾ Door Contact ▾</td></tr><tr><td>03</td><td>Input_03</td><td>NO ▾</td><td>Door C ▾ Door Contact ▾</td></tr><tr><td>04</td><td>Input_04</td><td>NO ▾</td><td>Door D ▾ Door Contact ▾</td></tr><tr><td>05</td><td>Input_05</td><td>NC ▾</td><td>Normal Input ▾ Latch Disable ▾</td></tr><tr><td>06</td><td>Input_06</td><td>NO ▾</td><td>Normal Input ▾ Latch Disable ▾</td></tr></tbody></table>	Input Function				01	Input_01	NO ▾	Door A ▾ Door Contact ▾	02	Input_02	NO ▾	Door B ▾ Door Contact ▾	03	Input_03	NO ▾	Door C ▾ Door Contact ▾	04	Input_04	NO ▾	Door D ▾ Door Contact ▾	05	Input_05	NC ▾	Normal Input ▾ Latch Disable ▾	06	Input_06	NO ▾	Normal Input ▾ Latch Disable ▾
Input Function																													
01	Input_01	NO ▾	Door A ▾ Door Contact ▾																										
02	Input_02	NO ▾	Door B ▾ Door Contact ▾																										
03	Input_03	NO ▾	Door C ▾ Door Contact ▾																										
04	Input_04	NO ▾	Door D ▾ Door Contact ▾																										
05	Input_05	NC ▾	Normal Input ▾ Latch Disable ▾																										
06	Input_06	NO ▾	Normal Input ▾ Latch Disable ▾																										

Figure 6-6



### 6.3.5 Step 5: Monitoring Areas

To monitor the areas for each door, select **Monitoring** on the menu bar and select **New Area Monitor**. After a card is swiped to enter an area, the GV-ASManager can distinguish which cardholders are granted access to which areas. In this case, the access from the card number 244-36572 is granted to the meeting room for the cardholder Ian Anston.

		Users Cards Vehicles		
Location	Status			
TEST198-PC (6)				
Global Area	 : 8  : 17  : 10			
Factory	 : 0  : 0  : 0			
Meeting Room	 : 0  : 1  : 0			
Outside	 : 0  : 0  : 0			
Reception	 : 2  : 8  : 0			
Sales	 : 0  : 0  : 0			



Card number	User
 244-36574	 Ian Anston

Figure 6-7

### 6.3.6 Step 6: Locating Users

To locate a user, select **Monitoring** on the menu bar and select **New Locate People**. When the Exit or Entry reader is triggered, the GV-ASManager can tell if users follow Anti-Passback rules and then grant or deny access. When the door contact sensor is triggered, the GV-ASManager can tell the location of the user. In this case, Christine Downes is granted access from the Entry reader of 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

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Controller window (Figure 3-3) 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** and select **Patrol Tours**. This dialog box appears.

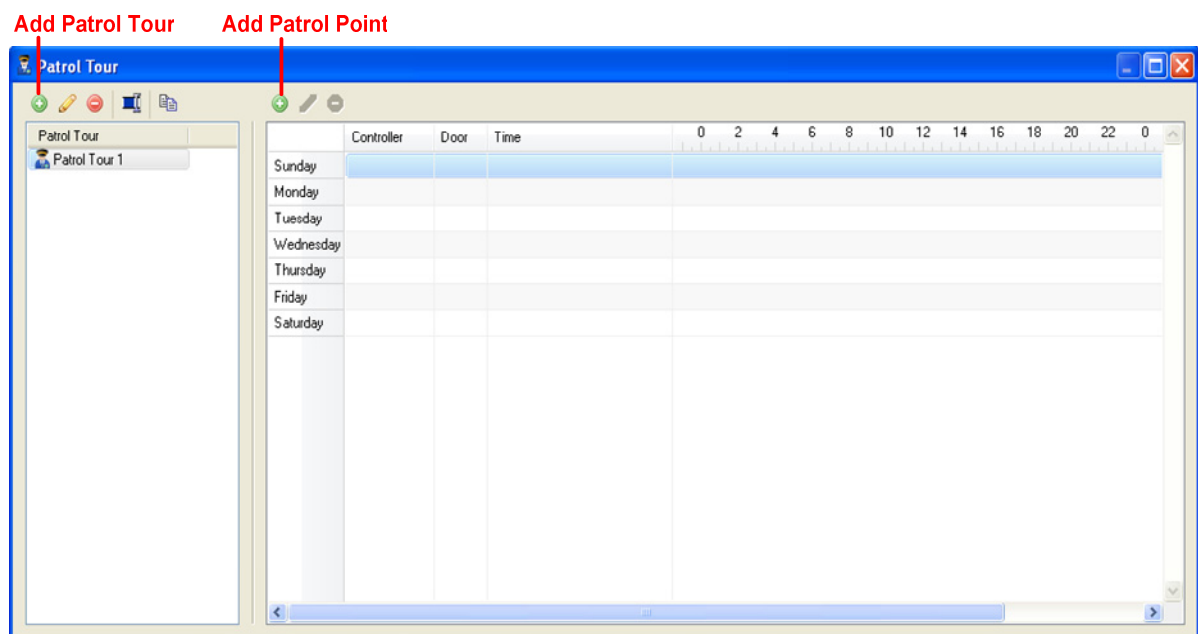
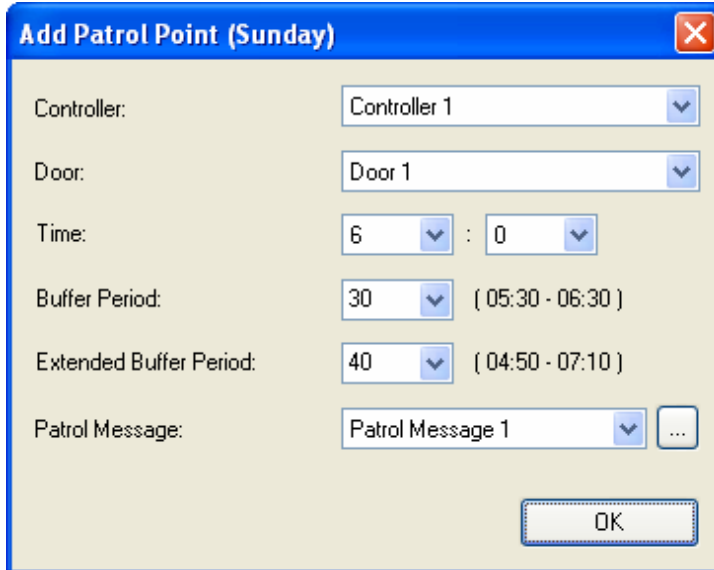


Figure 7-1

2. To create a new Patrol Tour, click the **Add Patrol Tour** button  on the left.

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



The dialog box titled "Add Patrol Point (Sunday)" contains the following fields:

- Controller:** A dropdown menu with "Controller 1" selected.
- Door:** A dropdown menu with "Door 1" selected.
- Time:** Two dropdown menus showing "6" and "0".
- Buffer Period:** A dropdown menu showing "30" and a text field showing "( 05:30 - 06:30 )".
- Extended Buffer Period:** A dropdown menu showing "40" and a text field showing "( 04:50 - 07:10 )".
- Patrol Message:** A dropdown menu with "Patrol Message 1" selected and a button with three dots "...".
- OK** button at the bottom right.

Figure 7-2

4. Select the location and check-in time of the Patrol Point:
- **Controller:** Select the controller of the door that the security staff needs to patrol.
  - **Door:** Select the door that the security staff needs to patrol.
  - **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 notification 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 to type an alert message that can be sent using e-mail or SMS when the security staff is on time, early, late or absent.

---

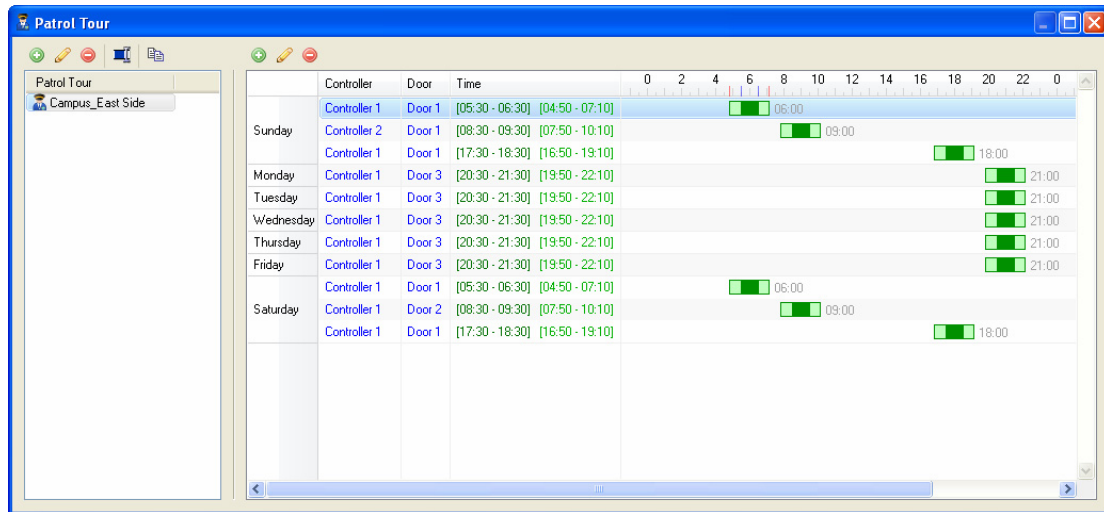
**Note:** Security staff checking in outside the Extended Buffer Period will be marked as absent.

---

5. Click **OK**.

6. To add more Patrol Points, select a day and click the **Add Patrol Point** button again to repeat the steps. You can also drag a Patrol Point to another day of week to create a copy.

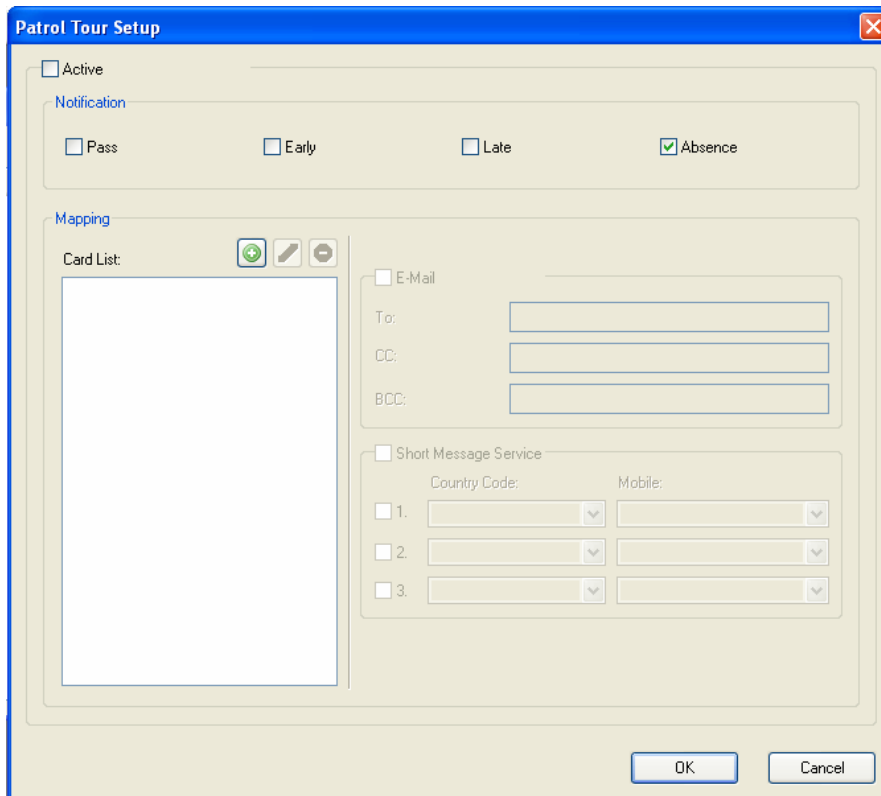
Below is an example of a completed Patrol Tour, where the dark green zone is when the security staff needs to check in and the light green zone is the extended buffer period.



*Figure 7-3*

## 7.2 Activating the Patrol Tour

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




The **Patrol Tour Setup** dialog box is shown. It has a blue title bar with a close button. The main area is divided into sections:

- Active:** A checkbox that is currently unchecked.
- Notification:** A section containing four checkboxes: **Pass** (unchecked), **Early** (unchecked), **Late** (unchecked), and **Absence** (checked).
- Mapping:** A section containing:
  - Card List:** A large empty rectangular box for listing cards. Above it are three small icons: a green plus in a square, a pencil, and a circular arrow.
  - E-Mail:** A section with an unchecked checkbox and three text input fields labeled **To:**, **CC:**, and **BCC:**.
  - Short Message Service:** A section with an unchecked checkbox. Below it are two columns of input fields: **Country Code:** and **Mobile:**. Each column has three rows, each starting with an unchecked checkbox and numbered 1, 2, and 3.

At the bottom right are **OK** and **Cancel** buttons.

Figure 7-4

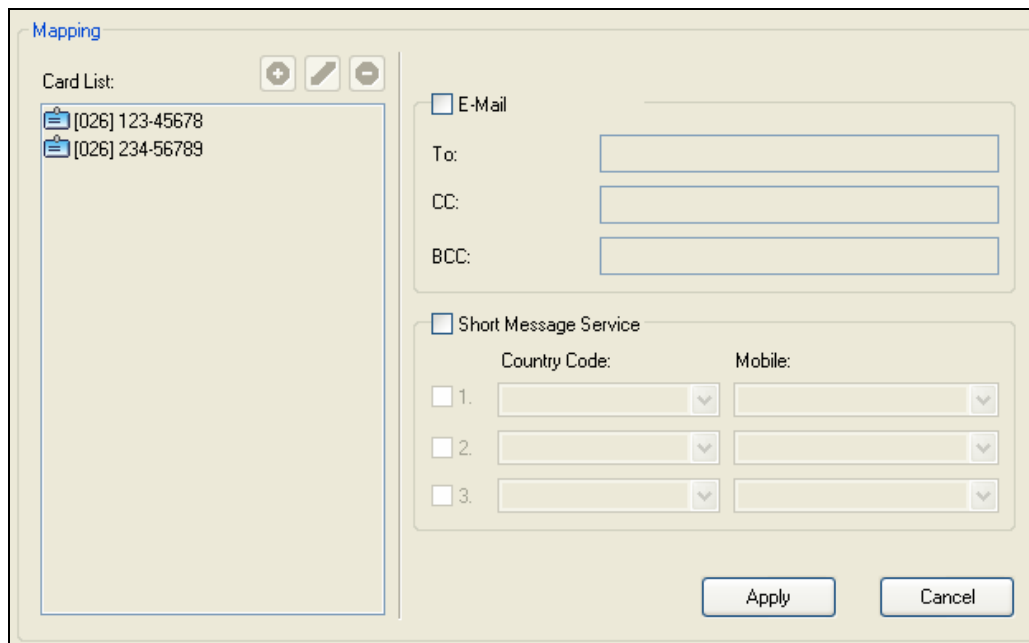
2. Click the **Add** button  and select a card. You can add multiple cards if needed and the security staff will be required to present one of the cards listed here.

---

**Note:** When the security staff presents the card, the controller may grant or deny door access according to the setting 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. Refer to 4.3 *Setting Cards* to see how to set the cards.

---

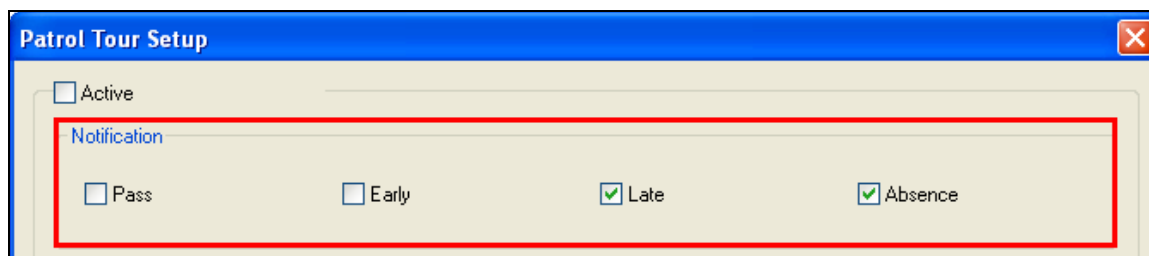
3. Double-click a card and select to notify by **E-Mail** and / or **Short Message Service**.



The 'Mapping' dialog box contains a 'Card List' on the left with two entries: '[026] 123-45678' and '[026] 234-56789'. On the right, there are two sections for notifications. The 'E-Mail' section has checkboxes for 'To:', 'CC:', and 'BCC:' followed by text input fields. The 'Short Message Service' section has a checkbox and three rows for 'Country Code' and 'Mobile' numbers, each with a dropdown menu. At the bottom right are 'Apply' and 'Cancel' buttons.

Figure 7-5

- **E-Mail:** Type the e-mail addresses that will receive the alert notifications.
  - **Short Message Service:** Type up to 3 mobile numbers and their country codes.
4. To set up alert notifications, select the notification conditions to send alert.




The 'Patrol Tour Setup' dialog box has a title bar with a close button. Below the title bar is an 'Active' checkbox. A red rectangle highlights the 'Notification' section, which contains four checkboxes: 'Pass', 'Early', 'Late' (checked), and 'Absence' (checked).

Figure 7-6

5. Click **Apply**.
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.
-

### 7.3 Monitoring Patrol Activities

To monitor Patrol activities, click **Monitoring** on the menu bar and select **New Patrol Tour Monitor**. This dialog box appears.

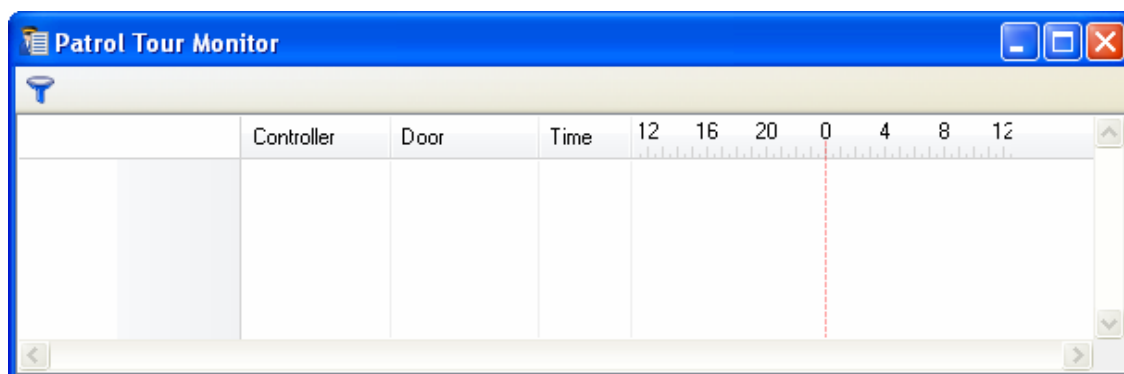



Figure 7-7

Next, click the **Filter** button  and 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.

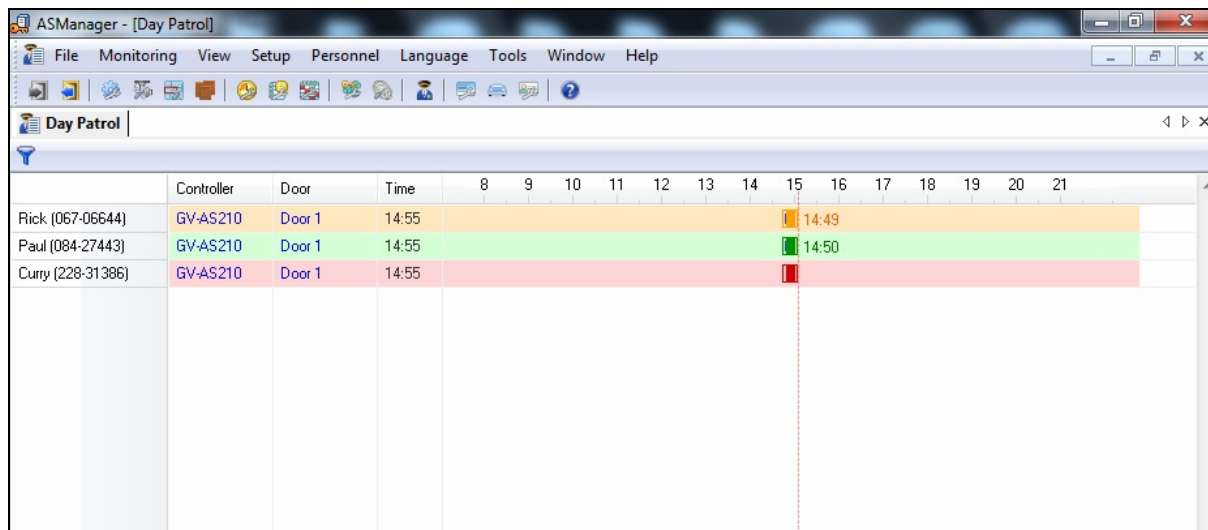
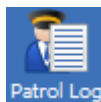


Figure 7-8



## 7.4 Accessing Patrol Log

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



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

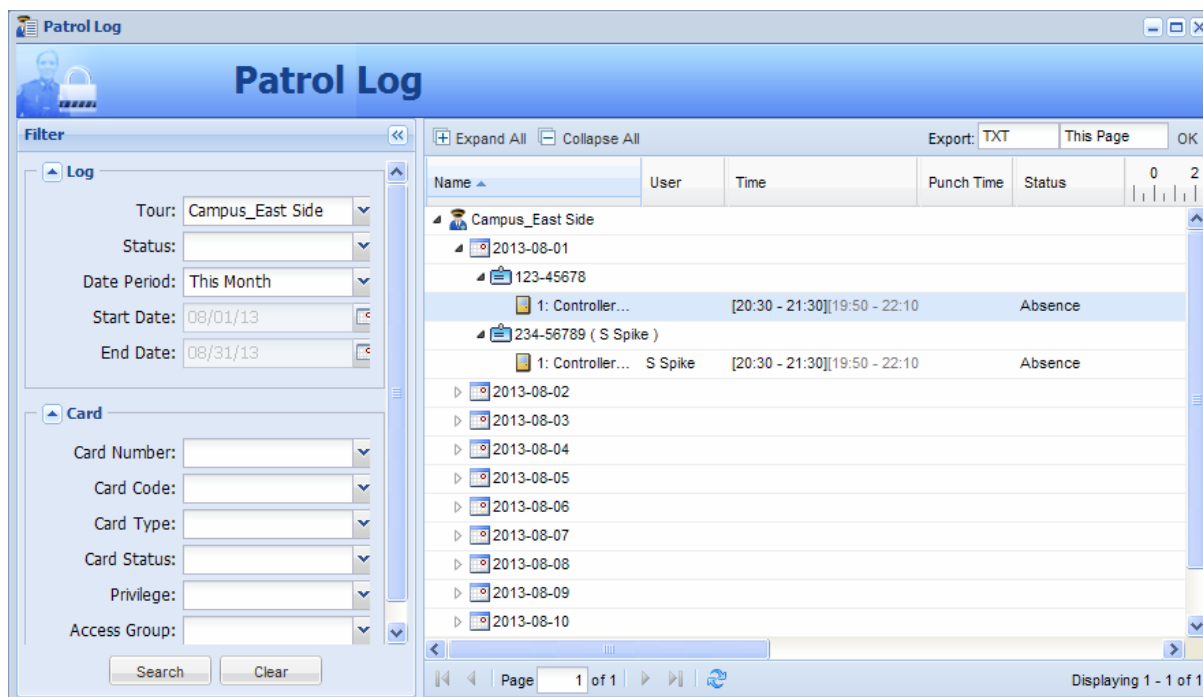


Figure 7-9

2. In the **Filter** section on the left, type or select 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 see how to export logs, refer to *10.3.3 Exporting Logs* for details. To see how to customize the search results columns, refer to *10.3.4 Defining Columns* for details.

## Chapter 8 Other Functions

### 8.1 Setting Up System User

A system user is a person using the GV-ASManager to monitor door controllers, enroll users or program the system. Using this function, the system supervisor 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** and select **Operators**. This dialog box appears.

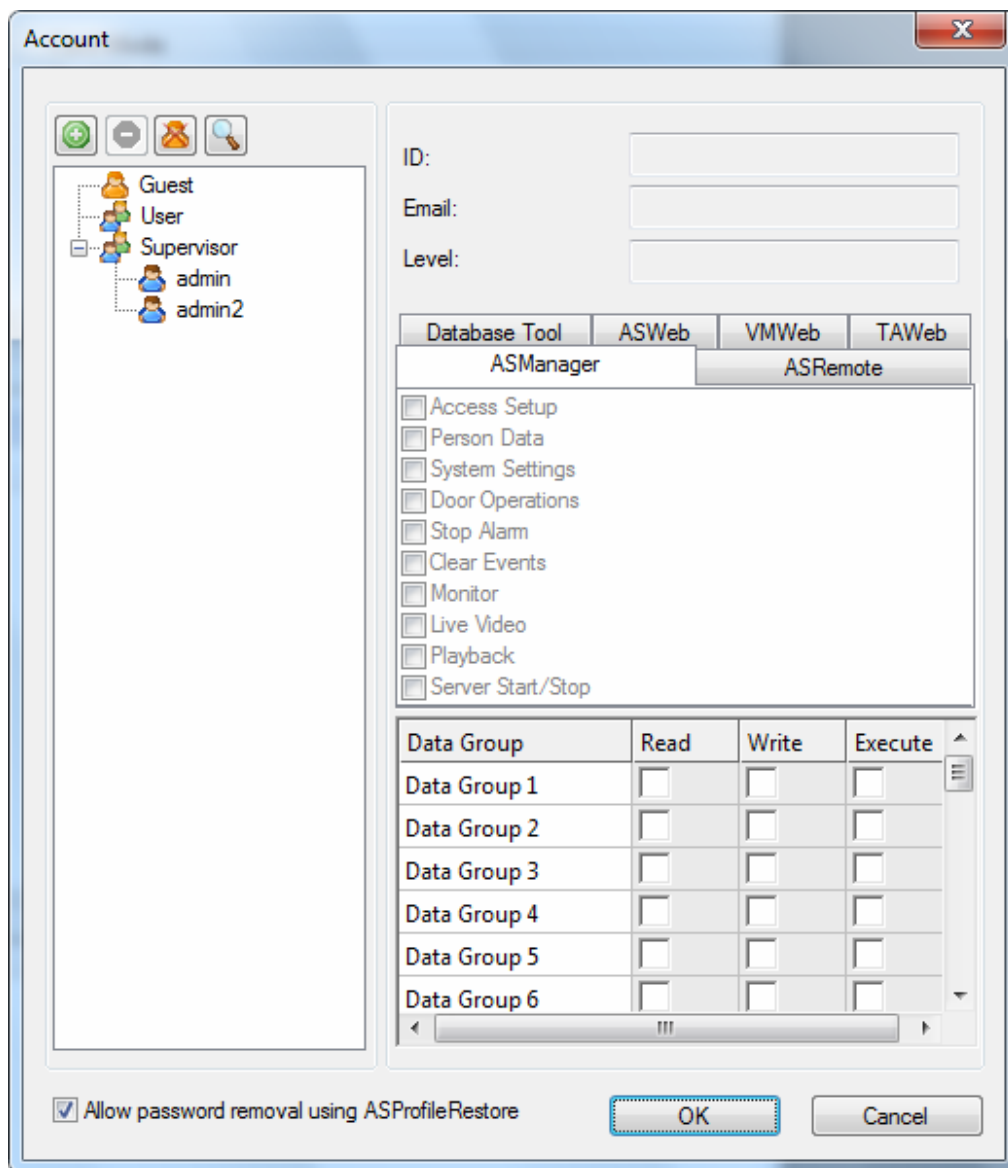
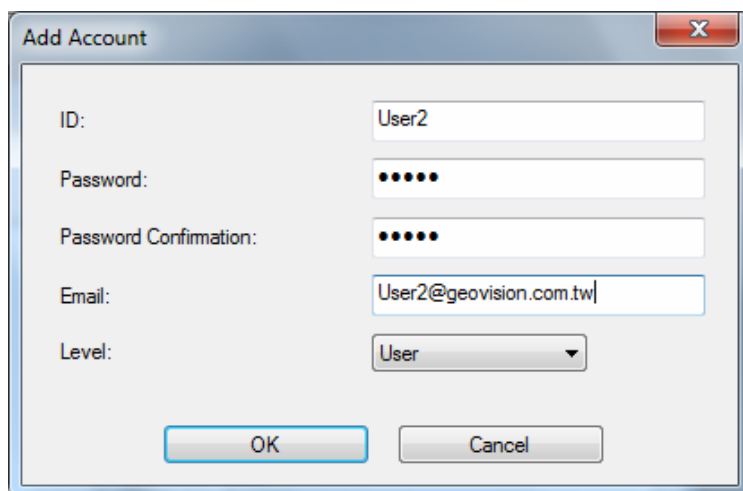


Figure 8-1

2. Click the **New** button  at the top left corner. This dialog box appears.



The image shows a Windows-style dialog box titled "Add Account". It contains the following fields and controls:


- ID:** A text input field containing "User2".
- Password:** A password input field with masked characters (dots).
- Password Confirmation:** A password input field with masked characters (dots).
- Email:** A text input field containing "User2@geovision.com.tw".
- Level:** A dropdown menu currently showing "User".
- At the bottom, there are two buttons: "OK" and "Cancel".

Figure 8-2

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 the tab **ASManager**, **ASRemote**, **ASWeb**, **Database Tool**, **VMWeb** or **TAWeb** in the middle of the window. Select the functions to grant access to the system user.
8. In the **Data Group** section, you can optionally select a data group and specify whether the user account will be able to read, write and execute the functions assigned under the data group. A data group may include controllers, cards, users, access groups, time zones and weekly schedules. Up to 32 data groups can be created. You can click the name of the data group to type a different name.
  - **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 Data 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 Data Group 4.

9. If you select **Allow Password Removal using ASProfileRestore**, you can erase all user and supervisor accounts by running **ASProfileRestore.exe** in the folder where the GV-ASManager program was installed.

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 are allowed to edit the information of a system user.

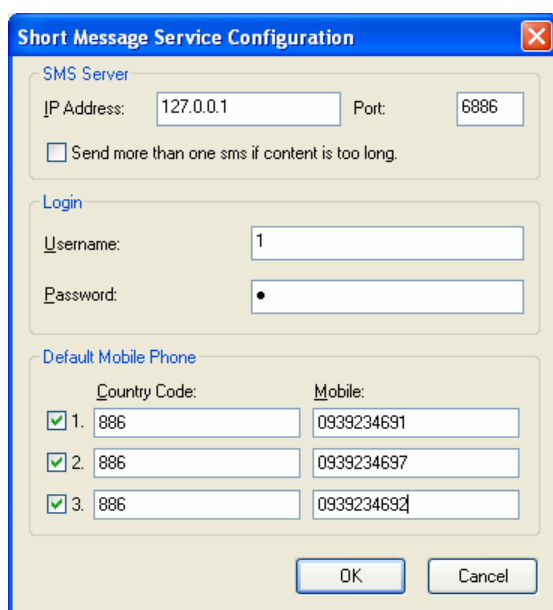
## 8.2 Setting Up Alert Notification

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

### 8.2.1 Setting SMS Server

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

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



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

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

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

At the bottom are **OK** and **Cancel** buttons.

Figure 8-3

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 and select **Connect to SMS Server**.

---

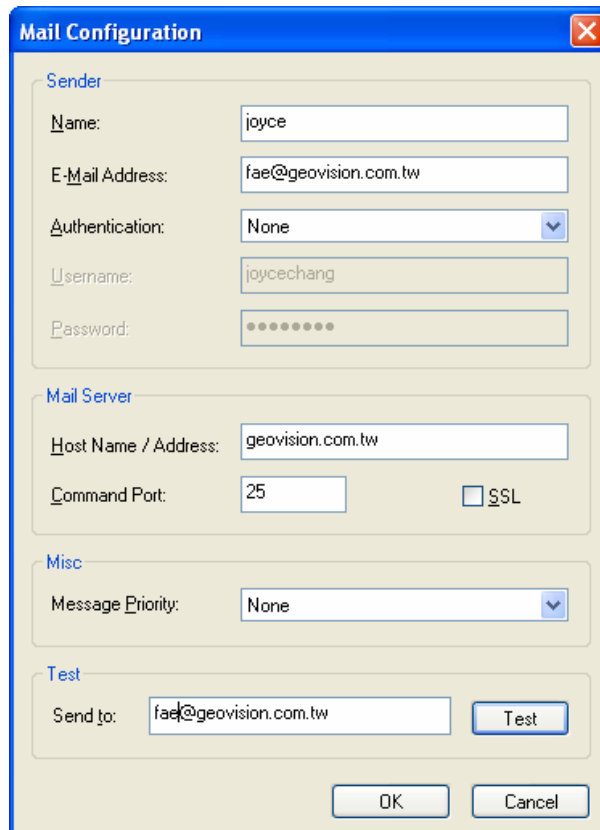
**Note:** For ASCII encoding (English language), SMS text messages are limited to 160 characters; for Unicode encoding (other languages), SMS text messages are limited to 70 characters. If you want to send longer text messages, select **Send more than one sms if content is too long**. The long messages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

---

### 8.2.2 Setting E-Mail Server

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

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



The image shows a 'Mail Configuration' dialog box with a blue title bar and a close button (X) in the top right corner. The dialog is divided into four sections: 'Sender', 'Mail Server', 'Misc', and 'Test'.  
 - **Sender section:** Contains five fields: 'Name' (text box with 'joyce'), 'E-Mail Address' (text box with 'fae@geovision.com.tw'), 'Authentication' (dropdown menu with 'None' selected), 'Username' (text box with 'joycechang'), and 'Password' (password field with 10 dots).  
 - **Mail Server section:** Contains three fields: 'Host Name / Address' (text box with 'geovision.com.tw'), 'Command Port' (text box with '25'), and an 'SSL' checkbox which is currently unchecked.  
 - **Misc section:** Contains one field: 'Message Priority' (dropdown menu with 'None' selected).  
 - **Test section:** Contains one field: 'Send to:' (text box with 'fae@geovision.com.tw') and a 'Test' button to its right.  
 At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Figure 8-4

2. Set up 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 Notification

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

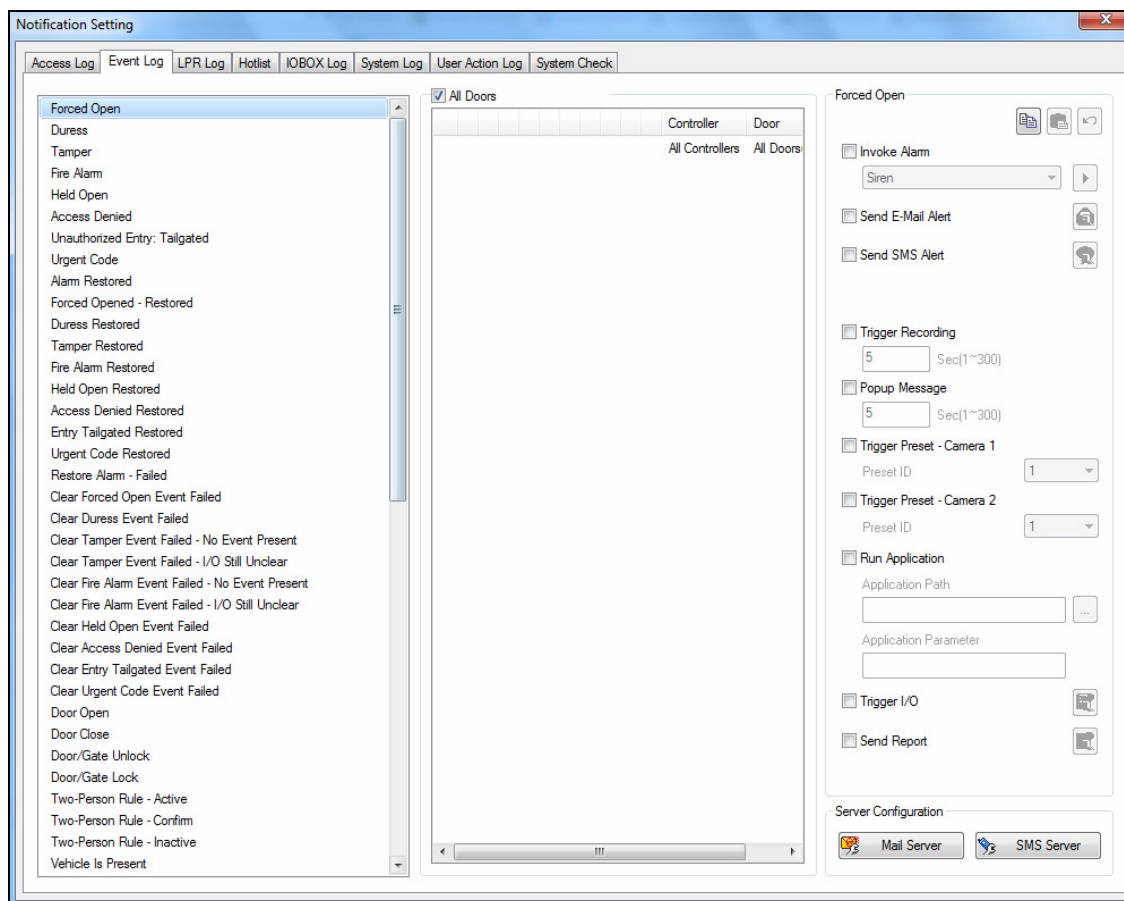



Figure 8-5

2. Click a tab to set the alert methods for different events: **Access Log**, **Event Log**, **LPR Log**, **Hotlist**, **IOBOX Log**, **System Log**, **User Action Log**, or **System Check**.
3. Select an event.
4. For **Access** and **LPR** tabs, you can clear the check mark for **All Access Groups** and select a specific access group. The alert will only be set off when specified event is triggered by members of that access group.



5. On the right, select the alert methods:

- **Invoke Alarm:** Enable the computer alarm when the selected event occurs.
- **Send E-Mail Alert:** When you select this option, an e-mail will pop up. Enter the recipient's e-mail address and alert subject. Then you can enter your own content, or use the buttons on the text window to send out the programmed information automatically.

For example, if you click the  button, the sent SMS alert will include the controller information. For details see *C. E-Mail and SMS Alert Symbols in Appendix*.

- **Send SMS Alert:** When you select this option, a dialog box will pop up. Ensure the preset mobile number(s). Select Text Code Type. Then type your messages; otherwise click the buttons on the text window to send out the programmed information automatically. See the above example in "Send E-Mail Alert".
- **Push Notification:** A push notification call with an associated live view will pop up on the GV-Access mobile App after you activate the doorbell alert in the Event Log. You can click a specific mobile device to enable or disable push notification. For details, see [http://pd.geovision.tw/datasheet/guide/GV-Access\\_Installation\\_Guide.pdf](http://pd.geovision.tw/datasheet/guide/GV-Access_Installation_Guide.pdf)
- **Trigger Recording:** Enable recording of DVR, Video Server or Compact DVR when the selected event occurs. You can specify the recording time between 1 and 300 seconds. For the function to work, you must activate monitoring on these IP devices ahead.
- **Popup Message:** An associated live view will pop up for alert when the selected event occurs. You can specify the duration of the live view remains on the screen between 1 and 300 seconds.
- **Trigger Preset:** Direct the camera(s) to a preset point when the selected event occurs.
- **Run Application:** Specify the **Application Path** and the designated application will run when the selected event occurs. You can also type a command in the **Application Parameter** field to execute a function of that application.
- **Trigger I/O:** Enable the trigger mode of an associated output when the selected event occurs.
- **Send Report:** Enable to send notifications of lists and logs upon the occurrence of the selected event. For the event of **Fire Status**, specify the time interval (1-60 minutes) between each fire alarm notification to avoid receiving repeated notifications. For the function to work, you must set up the E-mail server and the schedule in GV-ASWeb for lists and logs ahead. See *10.13 Setting Export Schedule for Lists and Logs*.

6. To define more than one event with the same alert configuration, first right-click the previously defined event on the list and select **Copy** to save its settings. Then use Ctrl + left click or Shift + left click to select several events. Right-click the selected events and select **Paste** to have the same settings.

---

**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, Backup and Export Setup

To access the Auto Startup, Auto Backup and Export to File functions, click **Tools** on the menu bar and select **Option**. This dialog box appears.

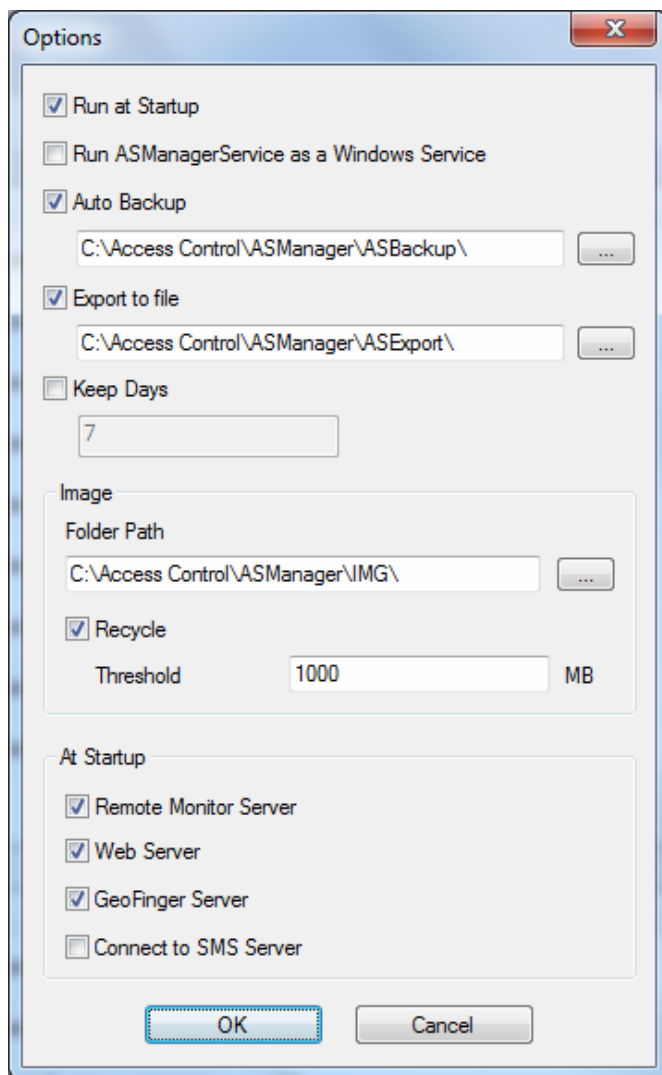


Figure 8-6

- **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.
- **Auto Backup:** You can also specify a path for the **Auto Backup** function to automatically save another copy of log and image files. The Auto Backup function performs backup at 24:00 A.M every day. By default, the log and image files are saved at **C:\Access Control\ASManager\ASBackup**.

- **Export to File:** Access data will be exported to text files at the specified storage path and can then be utilized by 3<sup>rd</sup> party programs. The access data will be listed in the file name of the text files. Up to 5000 files can be stored.
- **Keep Days:** Specify the number of days to keep log data. Note that log data passed the keep days will be deleted from GV-TAWeb.

---

**Note:** The copy of log data backed up by Auto Backup will not be affected by the Keep Days function.

---

#### [Image]

- **Folder Path:** You can change the storage path for images captured by the cameras connected to GV-ASManager.
- **Recycle:** When enabled, the oldest images will be deleted when the hard disk's free space falls below the **Threshold**. If recycling is enabled, avoid setting the **Folder Path** for images to the same hard disk used for **Auto Backup**.

#### [At Startup]

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

---

#### **Note:**

1. Web Server and GeoFinger Server options are selected by default.
  2. To back up the Configuration files, see *16.3 Other Database Settings*.
-

## 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 fingerprint must match the enrolled fingerprint.

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 the GV-ASManager.

For **remote fingerprint enrollment**, first enroll empty fingerprints for a user on the 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. The 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 the GV-ASManager for remote fingerprint enrollment.
- 

For details on how to enroll fingerprints and how to upload fingerprint data to GV-GF Fingerprint Reader, refer to *Chapter 3 Fingerprint Only Mode* in the *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 the 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 the GV-ASManager.
- 

For details on how to integrate with GV-ASManager for face enrollment, refer to *Chapter 4 Access Control Configurations* and *Chapter 5 User Management* in the *GV-FR Face Recognition Reader*.

## 8.6 Scanning Driver's Licenses and Business Card

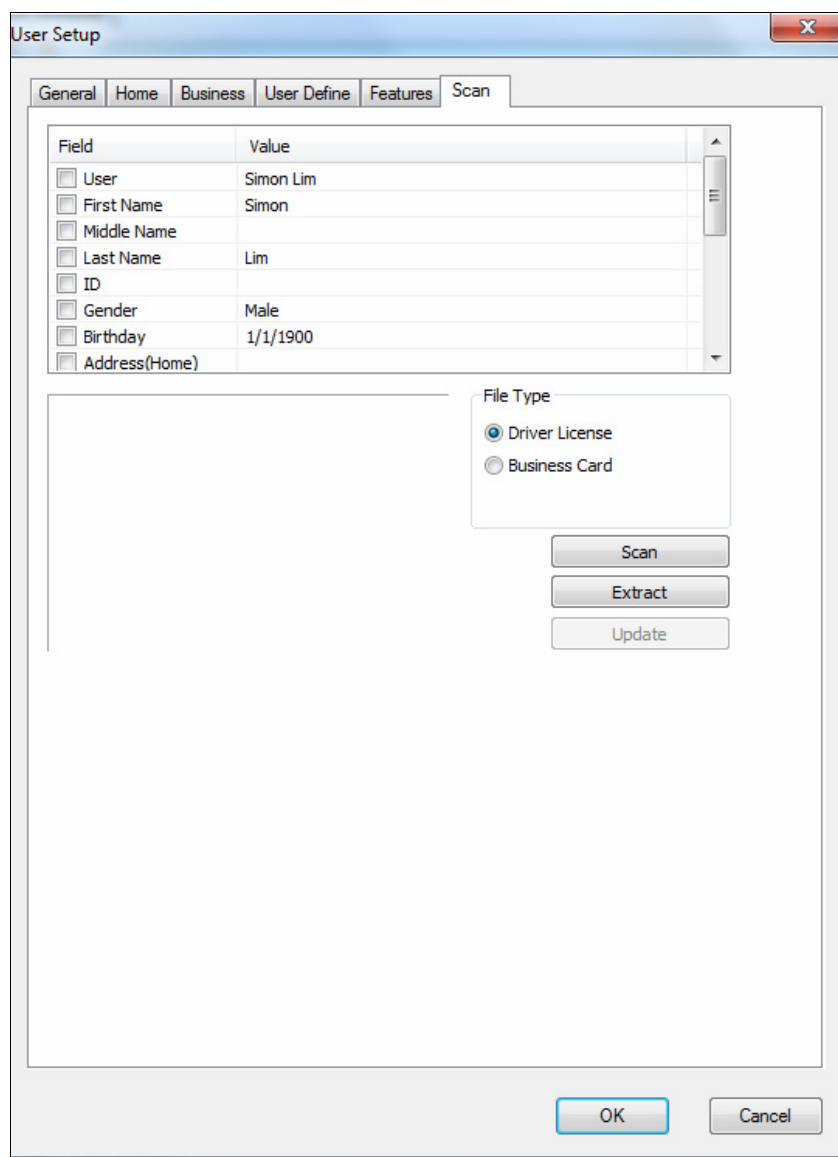
GV-ASManager can work with **SnapShell ID Scanner** to let you acquire and edit the personal data from driver's licenses and business cards.

---

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

---

1. Consult the Scanner's documentation to connect the Scanner with the GV-ASManager.
2. On the menu bar, click **Personnel** and select **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.



The User Setup dialog box is shown with the 'Scan' tab selected. It contains a table for user information and options for file type and actions.

Field	Value
<input type="checkbox"/> User	Simon Lim
<input type="checkbox"/> First Name	Simon
<input type="checkbox"/> Middle Name	
<input type="checkbox"/> Last Name	Lim
<input type="checkbox"/> ID	
<input type="checkbox"/> Gender	Male
<input type="checkbox"/> Birthday	1/1/1900
<input type="checkbox"/> Address(Home)	

File Type

☒ Driver License

☐ Business Card

Scan

Extract

Update

OK Cancel

Figure 8-7

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.



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

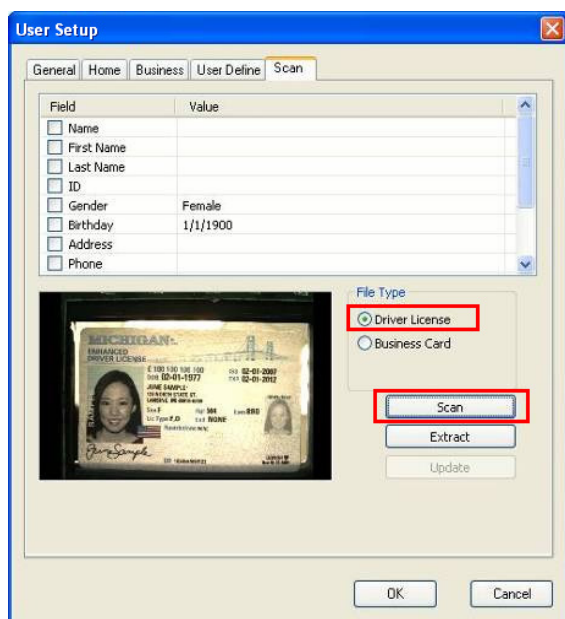


Figure 8-8

7. Click the **Extract** button to read the license data. The data is displayed in the **Value** column.
8. 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 8-9

9. Click the **Update** button. This driver's license is saved to the GV-ASManager's database.
10. 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 Setting Hot Keys

You can assign hot keys to quickly control individual, multiple doors, lanes and trigger outputs.

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

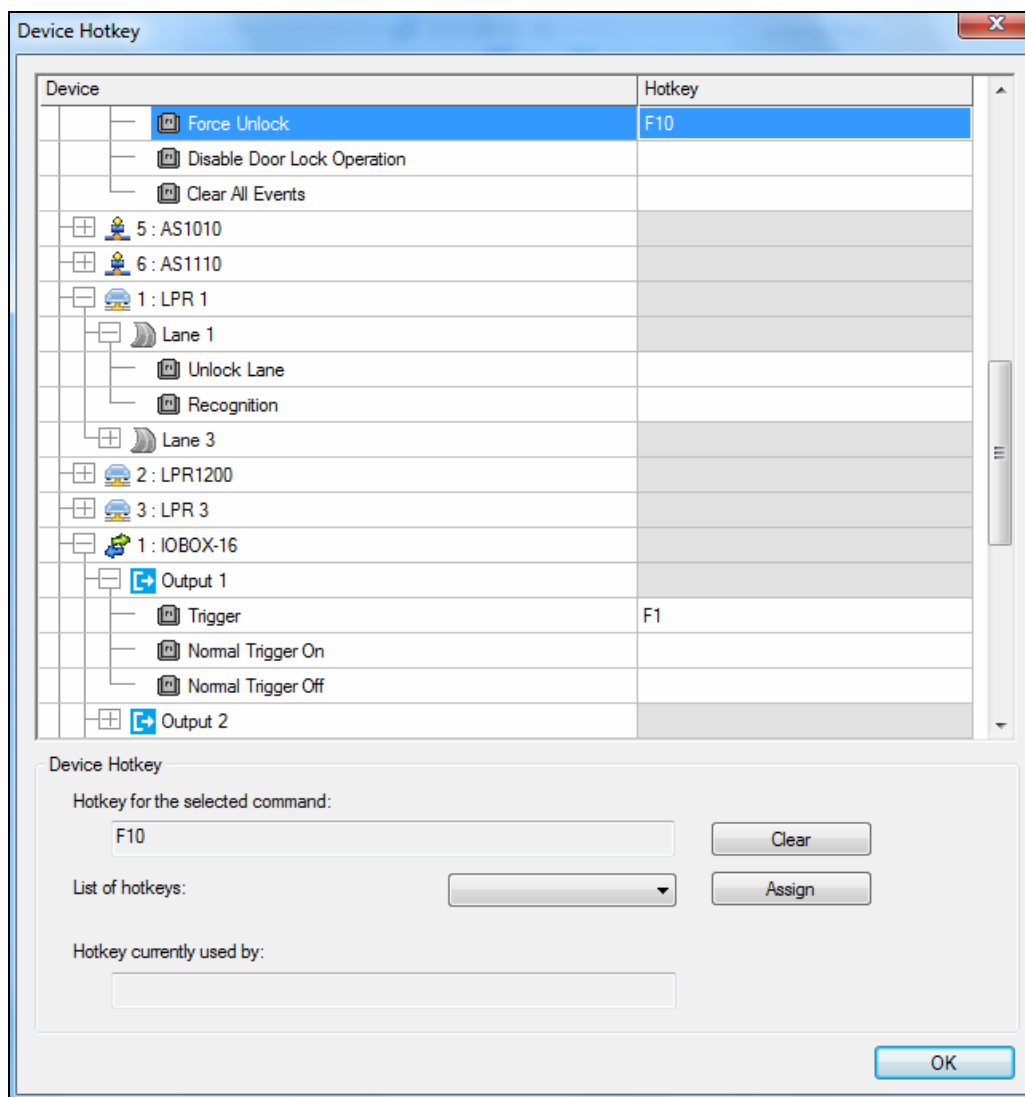


Figure 8-10

2. Under the Device list, select the GV-ASManager, a controller, a door, a lane, or an output and select the command you want to assign a hot key.
3. Next to **List of hotkeys**, select the hot key and click **Assign**. If the hot key is already assigned, the assigned command will be listed under **Hotkey currently used by**.
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 the doors of all GV-ASManager connected to the app. Up to 255 GV-ASManager can be connected to the app.

---


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

---


The Remote Lock Down App can be downloaded from the GeoVision website.

- **Downloading from GeoVision Website**

Go to <http://www.geovision.com.tw/download/product/GV-ASManager> Select

**Supplemental Utilities** in the drop-down list and click the **Download** icon  of **GV-LockDownApp**.

### Running Remote Lock Down APP

1. Click **Tools** on the menu bar of the GV-ASManager, select **Servers** and enable **Remote Monitor Server**. When the server is started, the icon  appears at the bottom of the main screen.
2. Run the **Remote Lock Down App**. This window appears.

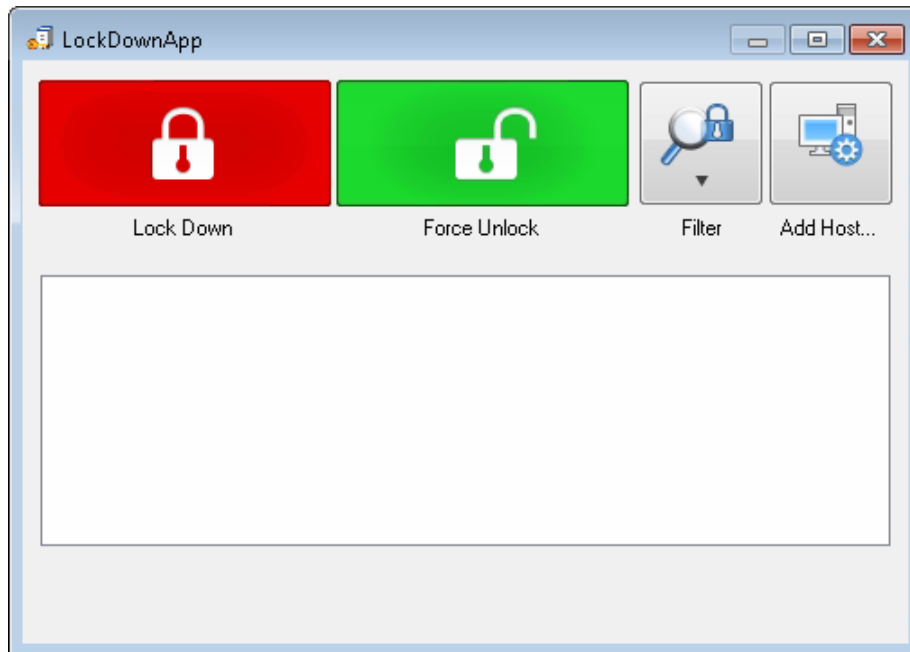



Figure 8-11

3. To connect to a GV-ASManager, click the **Add Host** button . This dialog box appears.

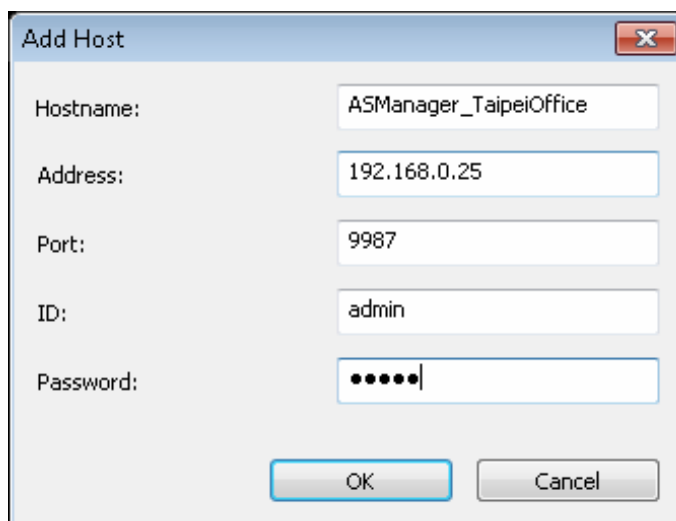
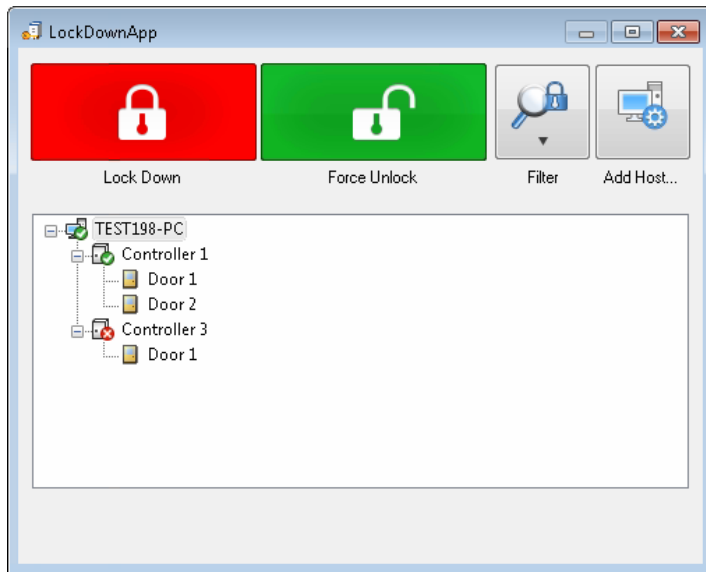



Figure 8-12

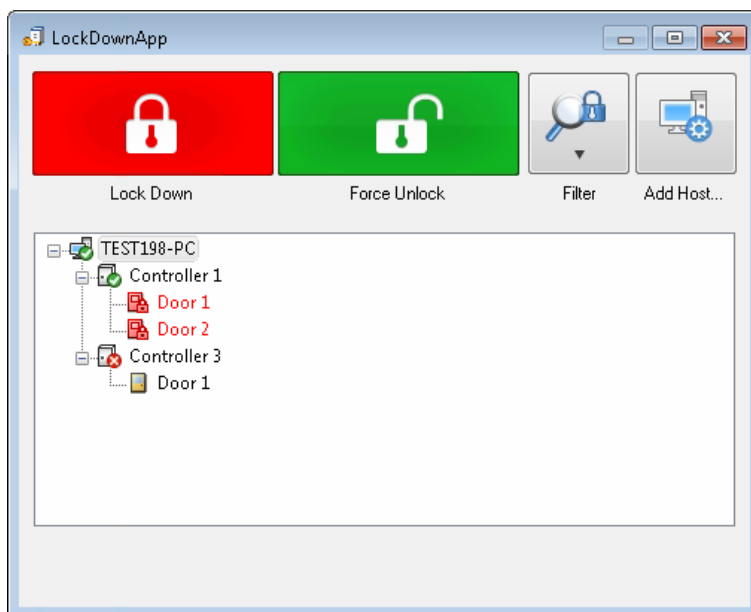
4. Type a **Hostname** to identify the GV-ASManager, and type the IP **Address**, **Port**, **ID** and **Password** of the GV-ASManager.

5. Click **OK**. The GV-ASManager and its controllers are now listed.




*Figure 8-13*

6. Repeat steps 3 – 5 for all other GV-ASManager.
7. To lock down the doors of all connected GV-ASManager, click the **Lock Down** button . All connected doors that are locked down are now highlighted in red.



*Figure 8-14*

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

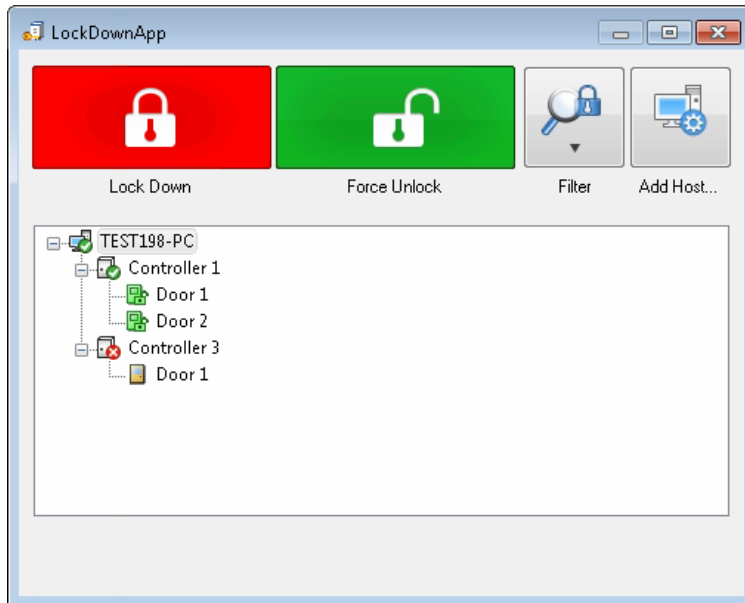



Figure 8-15

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

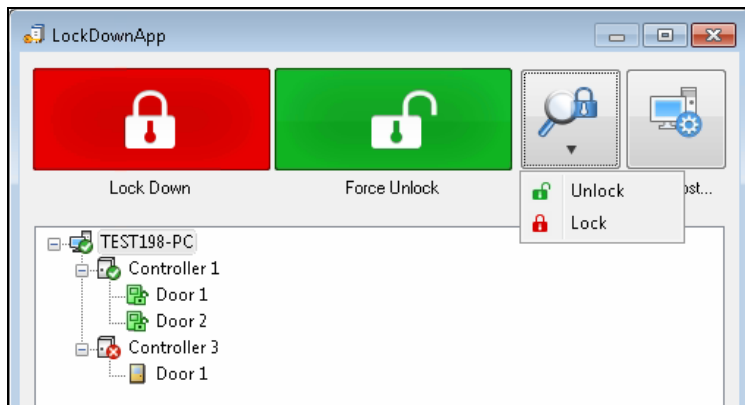


Figure 8-16

If you want to cancel lock down for all doors of a GV-ASManager, right-click the server in the Controller window of the GV-ASManager, and select **Disable Door Lock Operation**.

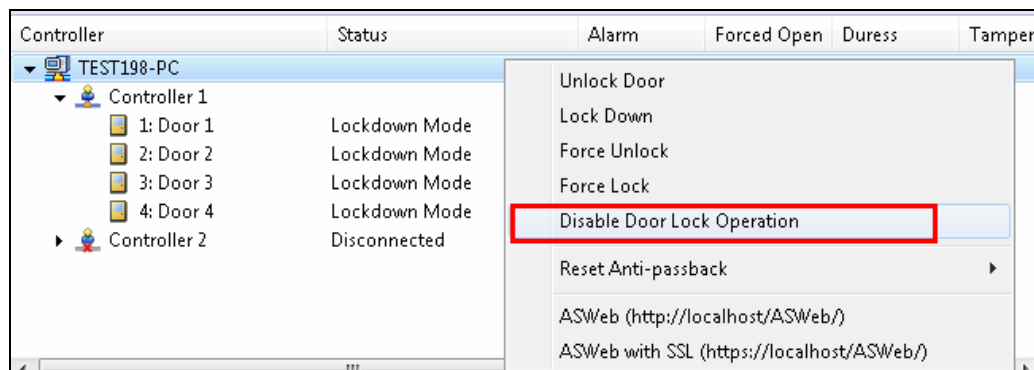


Figure 8-17

---

**Tip:** You can set a hot key for Disable Door Lock Operation to instantly restore the previous monitoring modes. Refer to *Setting Hot Keys to Quickly Control Doors* earlier in this chapter for details.

---

## 8.9 Defining New Card Formats

By default, GV-ASManager only recognizes identification 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 so that GV-ASManager can recognize it.

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

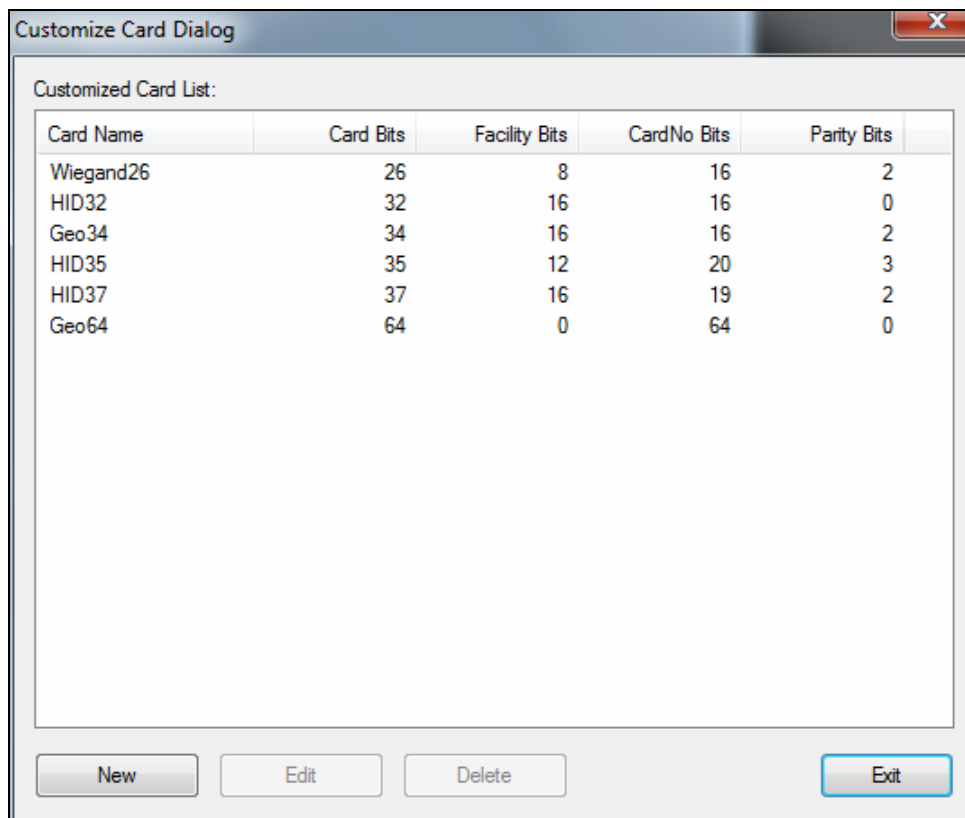
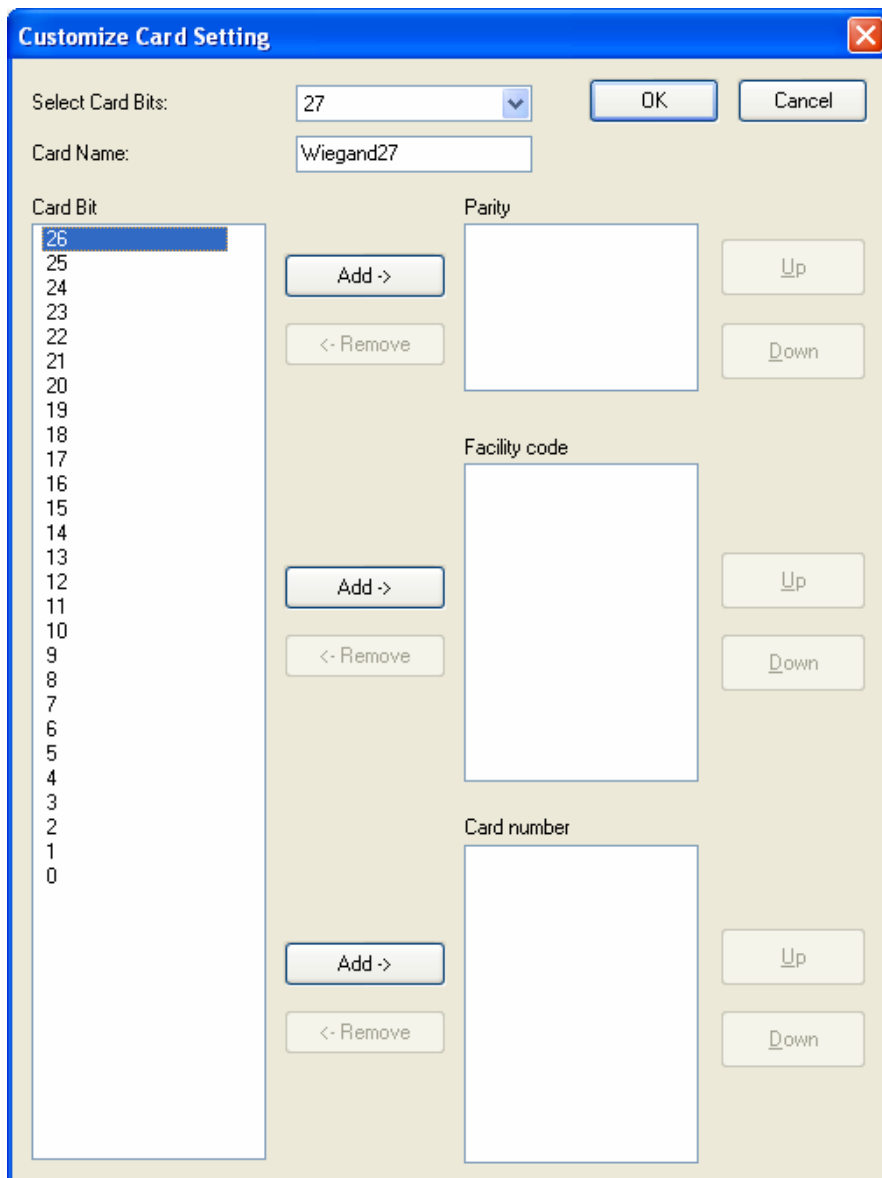


Figure 8-18



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



The dialog box is titled "Customize Card Setting" and has a close button (X) in the top right corner. It contains the following elements:

- Select Card Bits:** A dropdown menu showing "27".
- Card Name:** A text field containing "Wiegand27".
- OK** and **Cancel** buttons.
- Card Bit:** A list of bit numbers from 26 down to 0. Bit 26 is currently selected.
- Parity:** A large empty box for defining parity settings.
- Facility code:** A large empty box for defining facility code settings.
- Card number:** A large empty box for defining card number settings.
- Buttons:**
  - Between the Card Bit list and the Parity box: "Add ->" and "<- Remove".
  - Between the Card Bit list and the Facility code box: "Add ->" and "<- Remove".
  - Between the Card Bit list and the Card number box: "Add ->" and "<- Remove".
  - To the right of the Parity box: "Up" and "Down" buttons.
  - To the right of the Facility code box: "Up" and "Down" buttons.
  - To the right of the Card number box: "Up" and "Down" buttons.

*Figure 8-19*

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 the premise that must remain closed at all times, you can connect the exits to the input sensors on the GV-AS Controller and monitor them using the functions below.

- Monitor the input status in the Device View window
- Assign up to two cameras to the input 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. In the Web interface of the GV-AS Controller, make sure the input is set to **Normal Input**. You can modify the input name if needed.

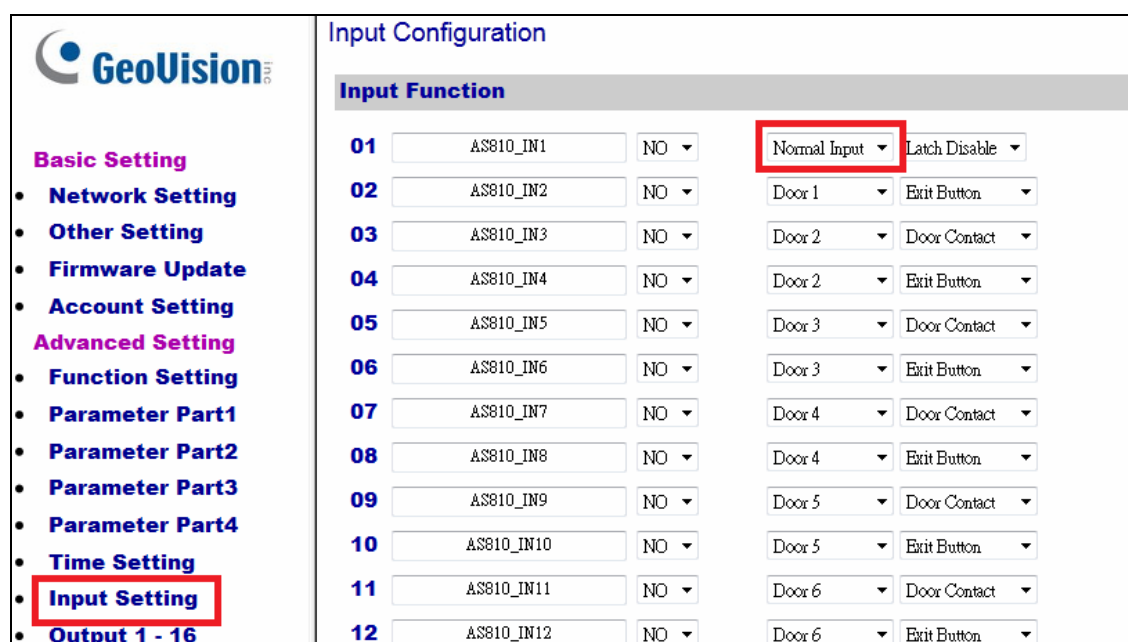


Figure 8-20

2. In GV-ASManager, right-click the GV-AS Controller in the Device View window and click **Settings**.

- Click the **Input** tab.

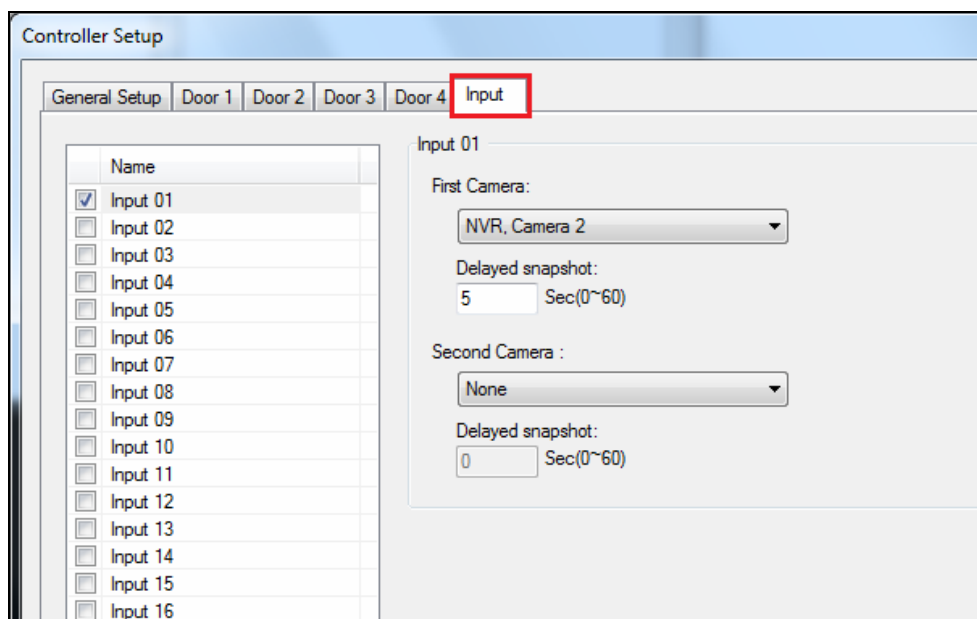


Figure 8-21

- On the left, select the inputs to monitor their status in the Device View.
- On the right, 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 the snapshot after input is triggered. For example, if the camera is installed 10 meters away from the emergency exit and it takes 5 seconds for the user to walk pass the camera after triggering the input, you can delay the snapshot for 5 seconds.
- Click **OK**.

The inputs will now be listed in the Device View window, 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.

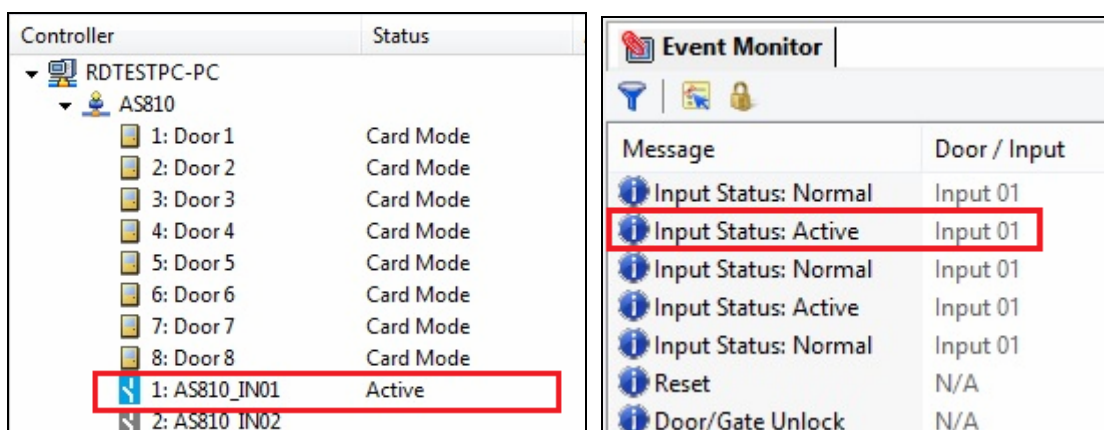


Figure 8-22

## 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** and select **Users**. The User List window appears.
2. Click the **Design Card Template** button on the toolbar. This dialog box appears.

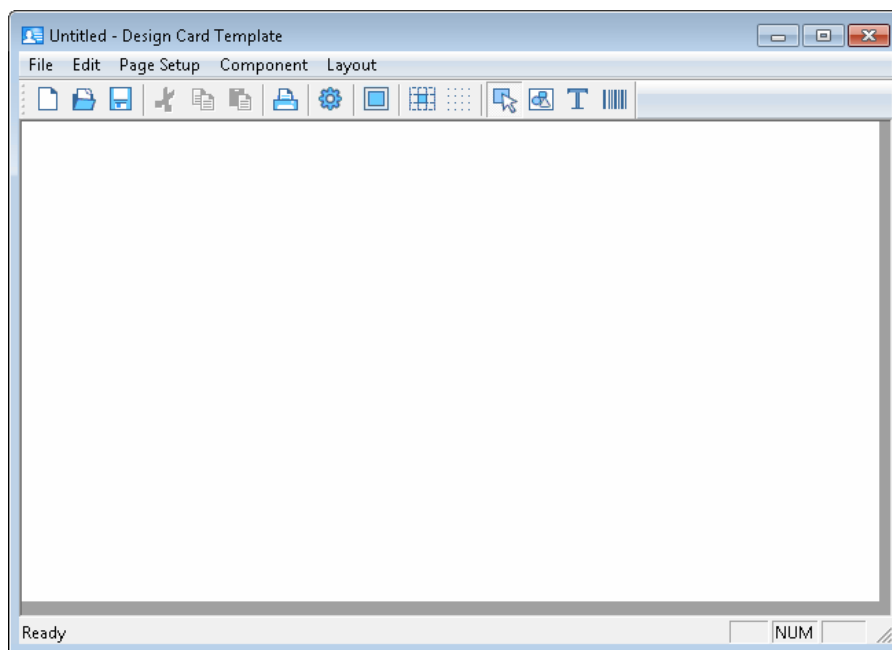


Figure 8-23

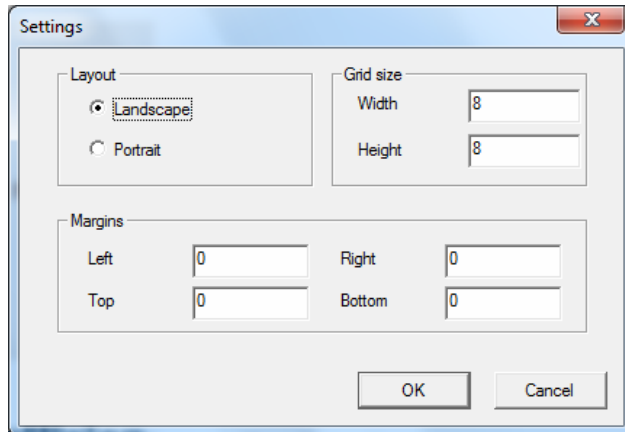
---

**Note:** If you do not want to design a template from scratch, you can click **File** and select **Template Sample** to use the template sample.


---

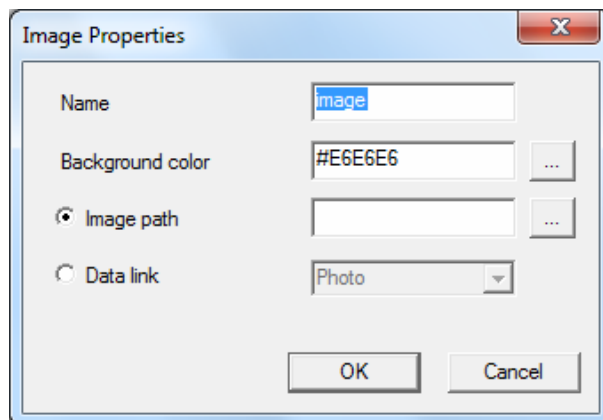
3. Click the **New** button  to create a new template.

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





*Figure 8-24*

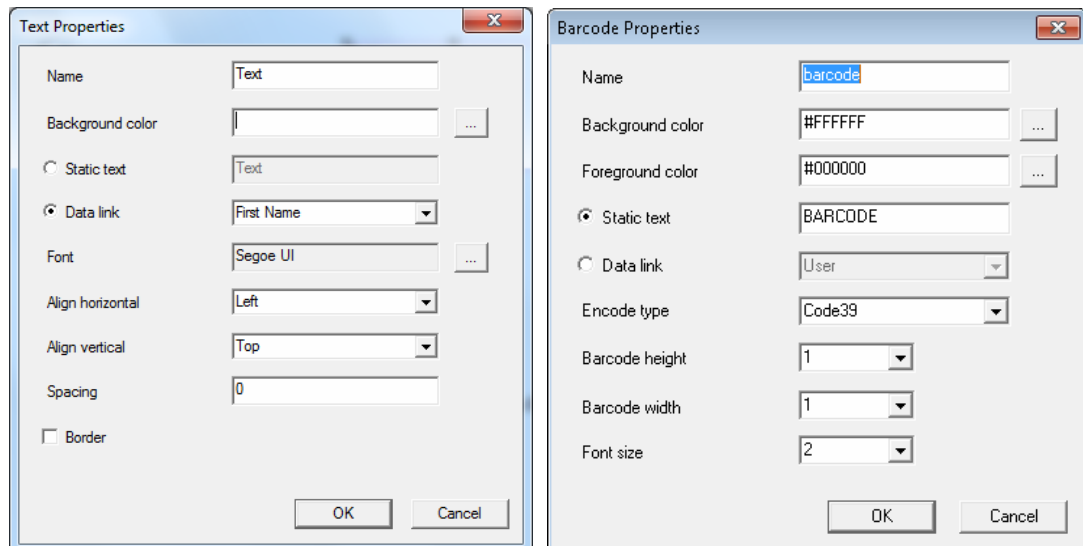
5. To add an image such as a background picture, user photo, or company logo, follow the steps below.
  - a. Click the **Image** button  and drag to define the size and location of the image.
  - b. Right-click the image and select **Properties**. This dialog box appears.





*Figure 8-25*

- 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 8-26*

- 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**.

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

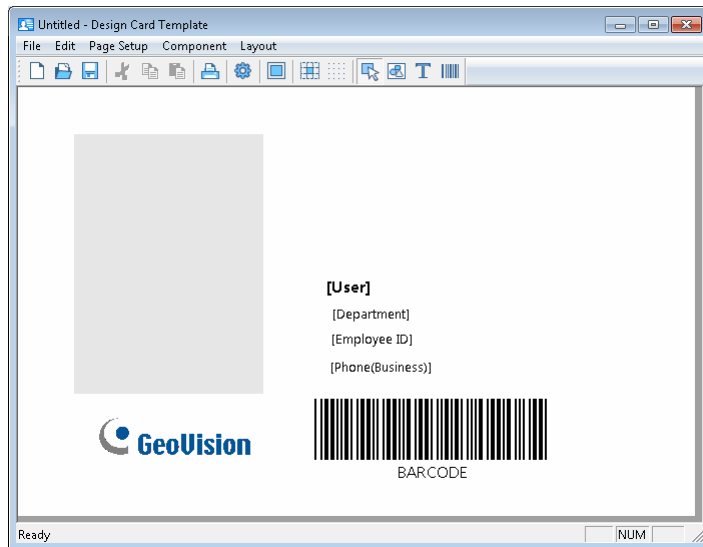


Figure 8-27

9. 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**.
10. To print the cards, select one or more users in the user list, right-click, select **Print** and select **Print Cards**.

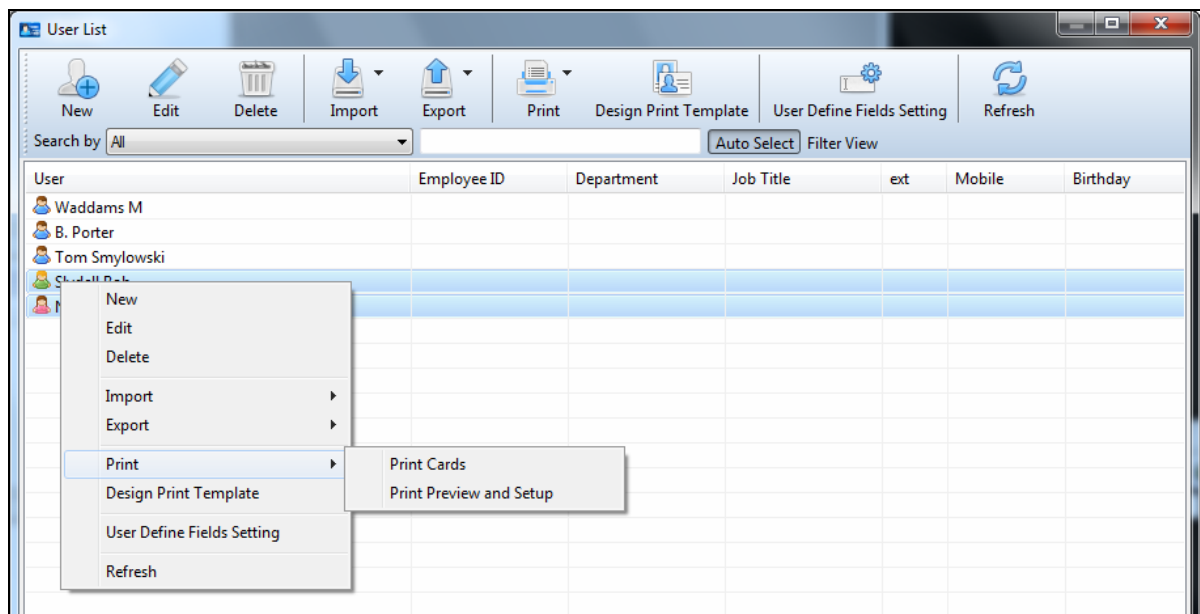
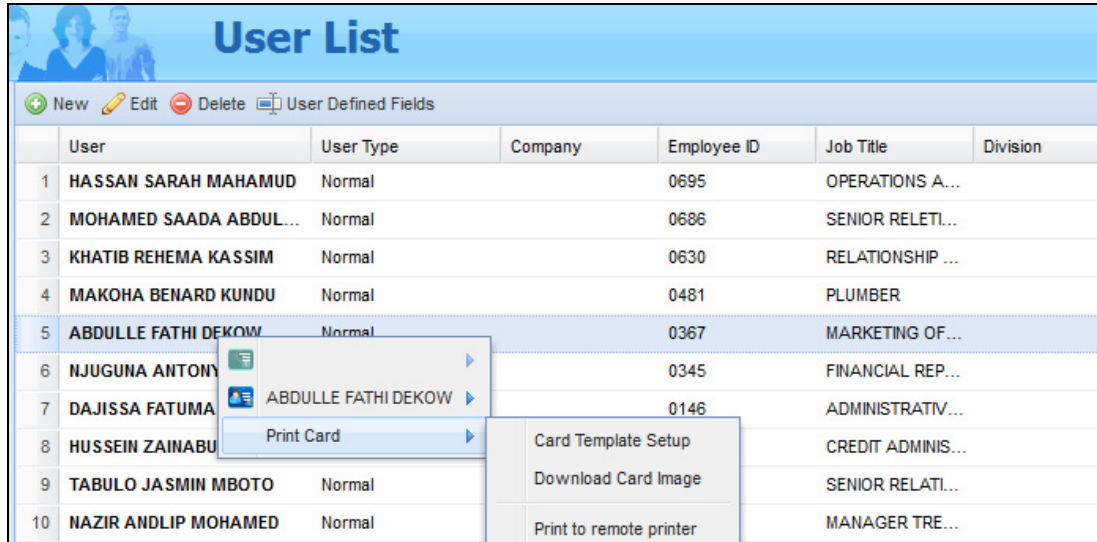


Figure 8-28

\*

**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** and select **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...	

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 job can specify the start and end of each type of job by entering different job codes on the GV-AS1010.

Follow the steps below to set up.

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

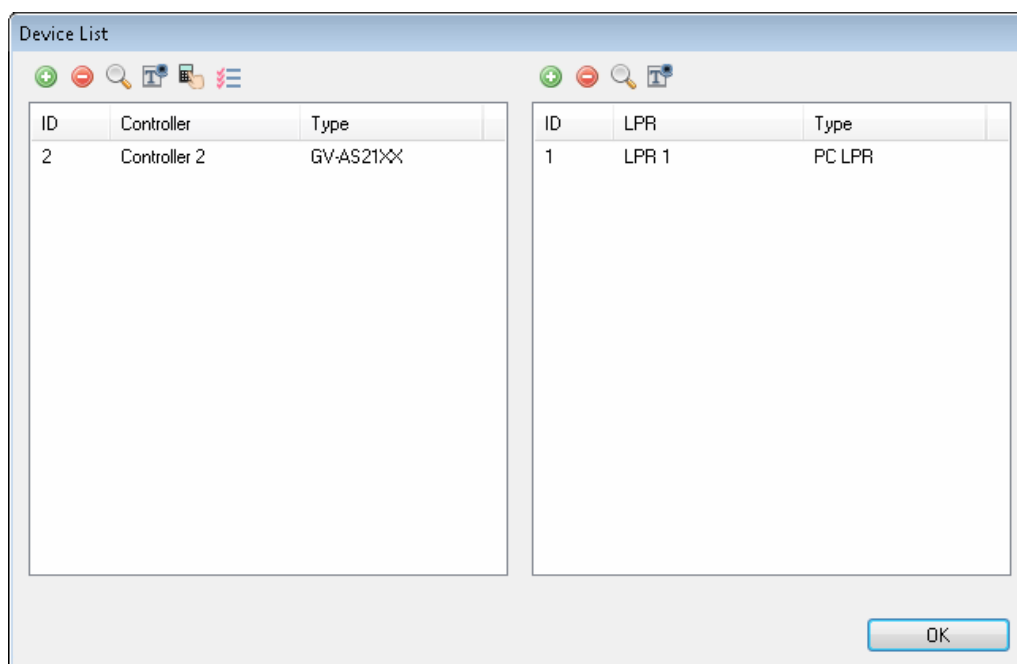



Figure 8-29

2. Click the **Job Code** button . A dialog box appears.
3. Select a checkbox, and type the **Job Code** and **Description**.

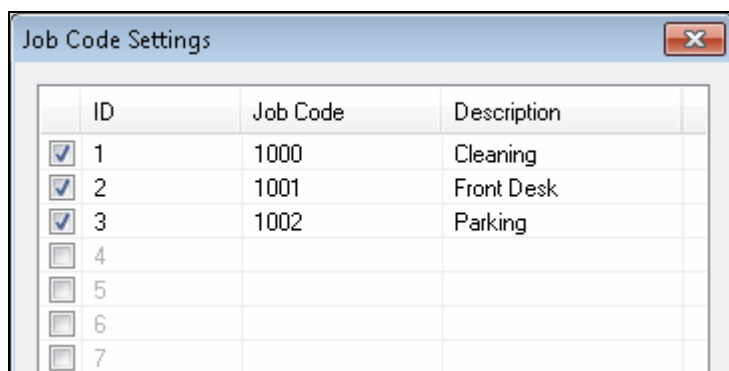


Figure 8-30

4. Click **OK**.

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

Advanced Setting		Function Key Configuration	
Function Configuration		Function Key	Function
Parameter Configuration			Authenticate
Card Configuration		F1	Work Time (Start) <input checked="" type="checkbox"/>
Card Information		F2	Work Time (End) <input checked="" type="checkbox"/>
Time Configuration		F3	Job code (Start) <input type="checkbox"/>
Input Configuration		F4	Job code (End) <input type="checkbox"/>
Function Key Configuration			
Extended Device		Submit	Cancel

Figure 8-31

### Example:

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

TA Shift Settings		Job Code Settings	
Name:	Weekday	ID	Job Code
Start Time:	9:00	1	1000
End Time:	17:00	2	1001
		3	

Figure 8-32

To differentiate the two jobs in the record, employee A would enter different job codes on GV-AS1010 at the start and end of each job.

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

You can look up the records in TA Report of GV-TAWeb using **Job Code** and **Job Code Summary**. Refer to *Chapter 11 GV-TAWeb* for detailed instructions.

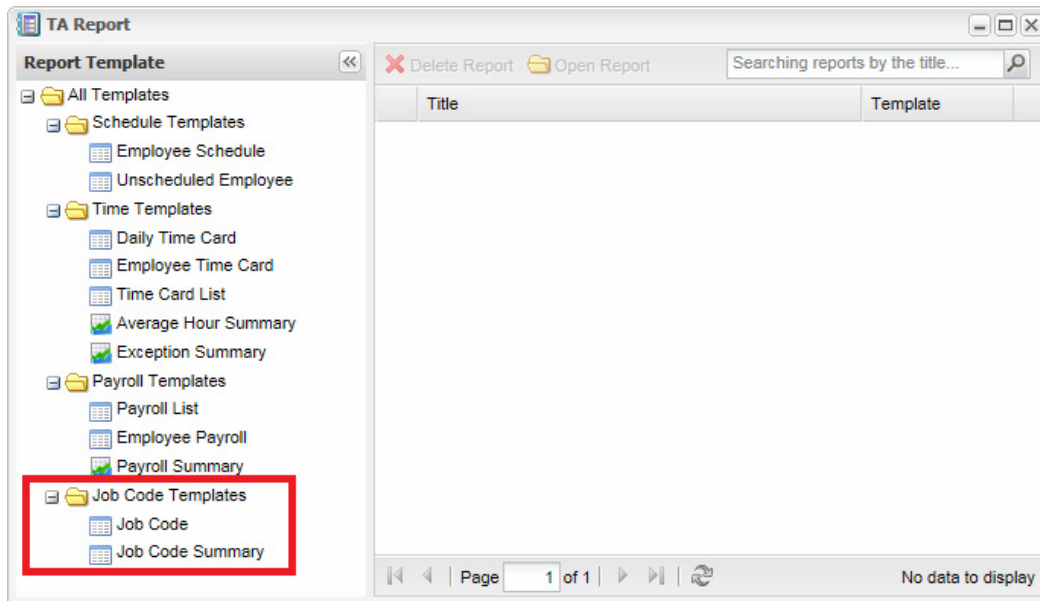
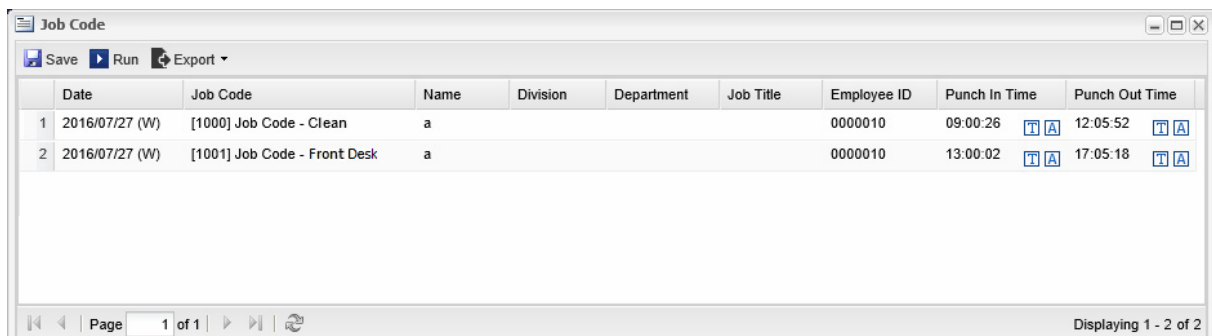


Figure 8-33

**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 8-34

**Job Code Summary** shows the total work hours of the 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 8-35


## Chapter 9 GV-ASRemote

The client software GV-ASRemote is designed to monitor multiple GV-ASManagers over the network. The 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 <http://www.geovision.com.tw/download/product/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

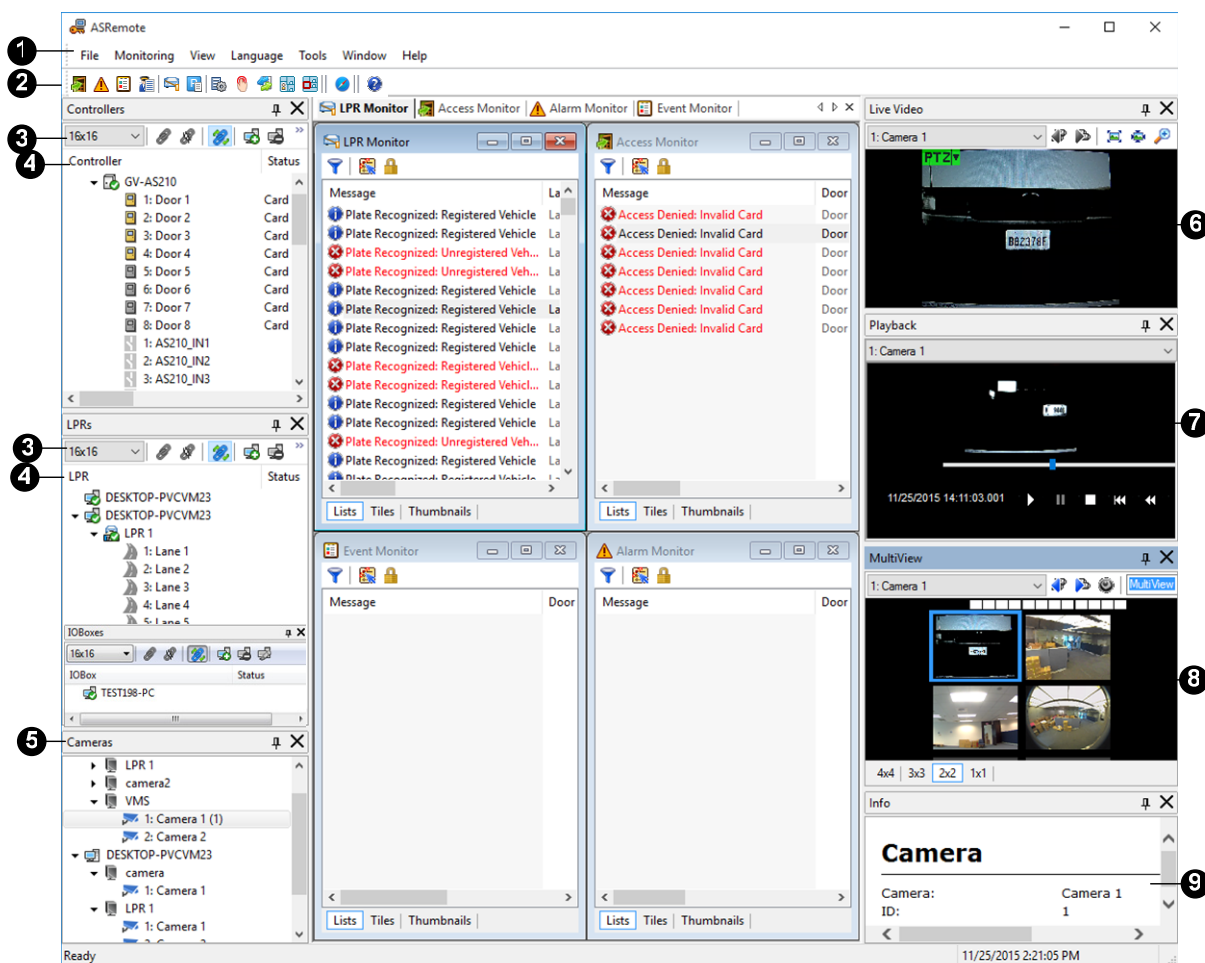


Figure 9-1

No.	Name	Function
1	Menu Bar	The Menu Bar includes the options of <b>File</b> (log in / out the GV-ASManager), <b>Monitoring</b> (display monitoring windows), <b>View</b> (display the function windows) and <b>Window</b> (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of various monitoring windows and <b>Web Browser</b> (open the GV-ASRemoteWeb).
3	Windows Toolbar	The Windows Toolbar includes the options of <b>Connect</b> , <b>Disconnect</b> , <b>Auto Connect</b> , <b>Add Host</b> , <b>Remove Host</b> , <b>Settings</b> and <b>Resolution</b> . 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 9.2.2 <i>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 9-3

The buttons on the Windows Toolbar of Controller / LPR / IOBox:

No.	Name	Function
1	Connect	Starts the connection with the GV-ASManager.
2	Disconnect	Ends the connection with the GV-ASManager.
3	Auto Connect	Retries to build the connection with the 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, the GV-ASManager must allow the remote access:

- Click **Tools** on the menu bar, select **Servers** and enable **Remote Monitor Server**.

When the server is started, the icon  appears at the bottom of the main screen.

To create a GV-ASManager host and enable connection to the GV-ASManager:

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

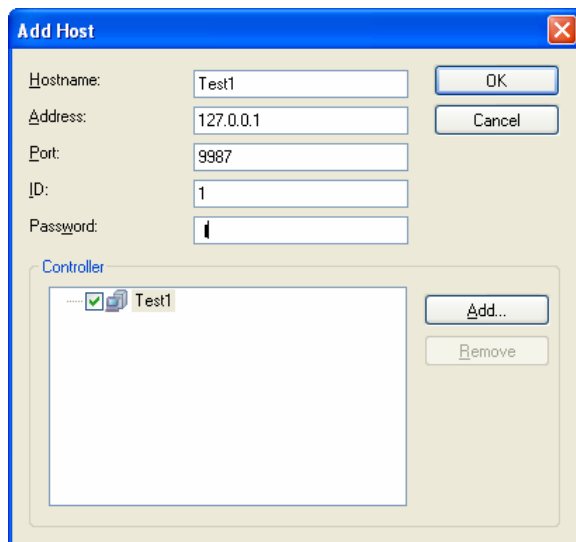


Figure 9-4

- Give a hostname, type the GV-ASManager's IP address, modify the port number if necessary, and type the GV-ASManager's login ID and password.
- Click **Add**. This dialog box appears.

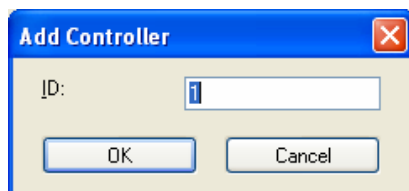
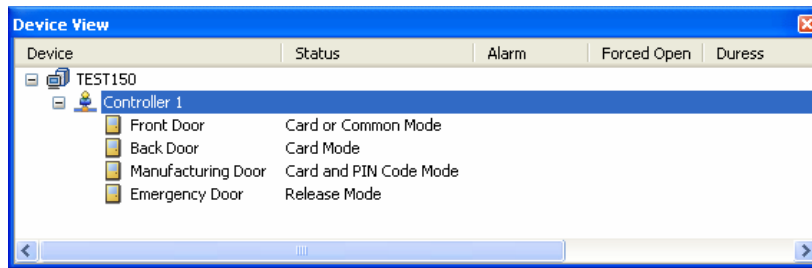


Figure 9-5


- Type the ID of the controller associated with the GV-ASManager and click **OK**.
- 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 Device View window as example below.



*Figure 9-6*

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 (Figure 4-9), see *D. Controller Status* in Appendix.

---

## 9.4 GV-ASRemoteWeb

The GV-ASRemoteWeb enables remote access to Access Log and LPR Log of multiple GV-ASManagers over the network.

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

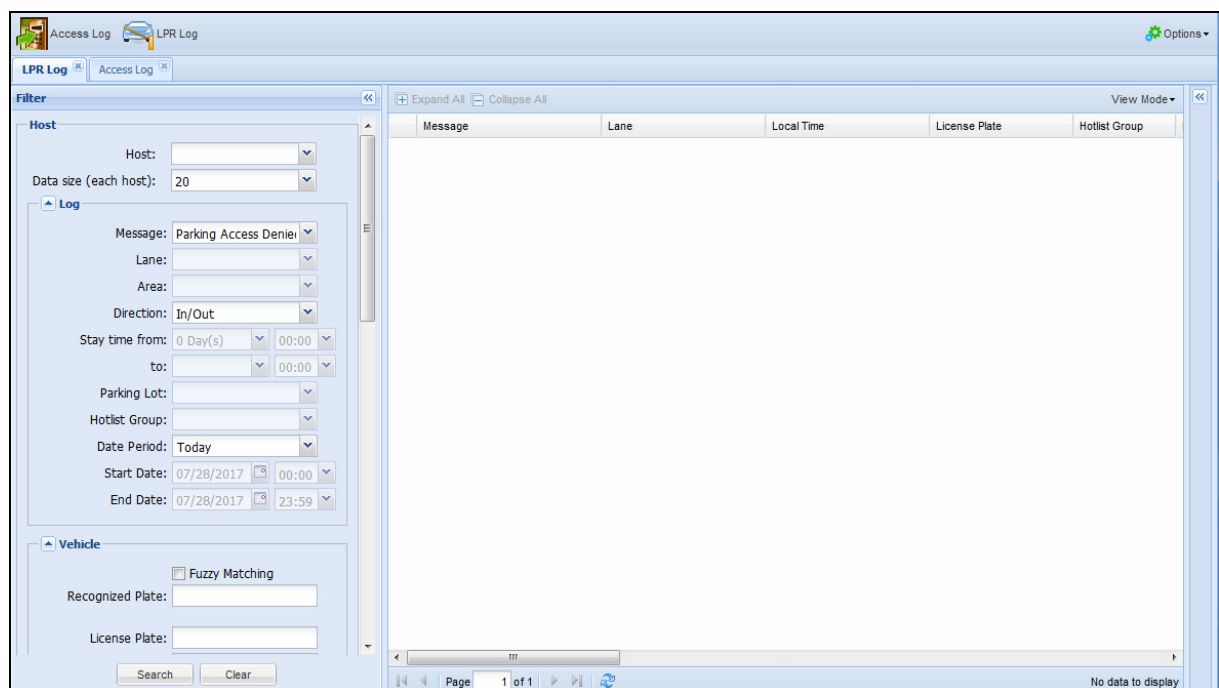


Figure 9-7

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

The GV-ASWeb allows you to access data and settings on the GV-ASManager over the network using a Web browser. Connecting to one GV-ASManager at a time, users can remotely watch live video, access logs, and set up camera / cards / users / vehicles / controllers / schedule / fingerprints / faces / patrol tours / parking lots / card formats / operator accounts using Web interface.

To use the GV-ASWeb, the version of browser in the client PC must be **Internet Explorer 9 or later**.

### 10.1 Connecting to GV-ASManager

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

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

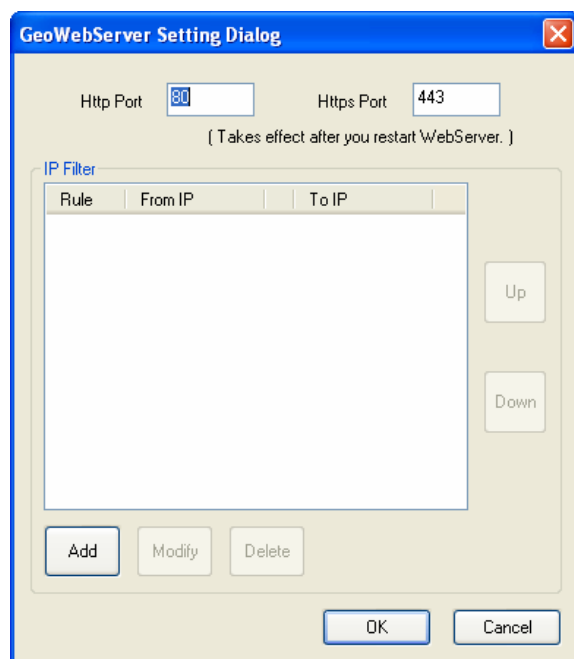



Figure 10-1

If you want to grant or deny the access from 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 of the main screen.

To start the GV-ASWeb:

1. There are two ways to link to GV-ASWeb:

- Under the device list, right-click the PC and click **ASWeb** or **ASWeb with SSL**.

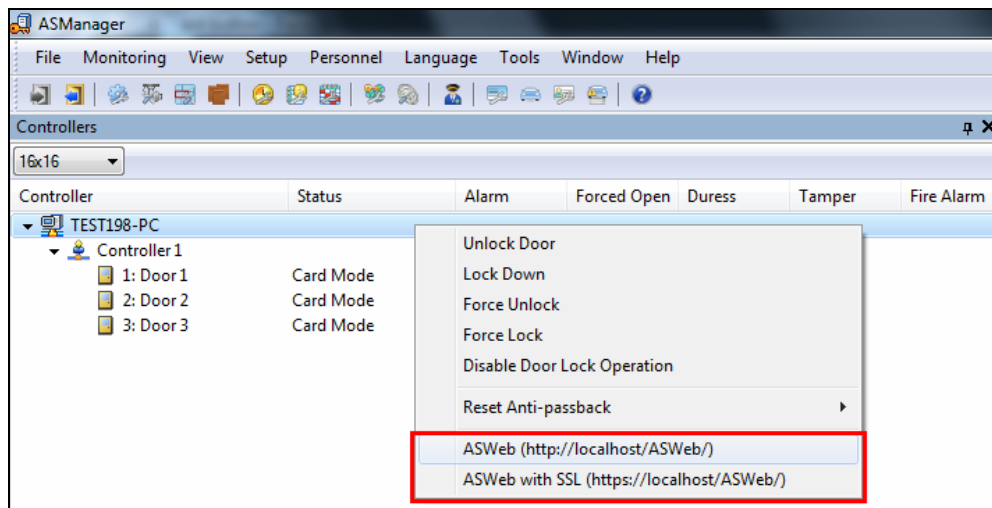


Figure 10-2

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

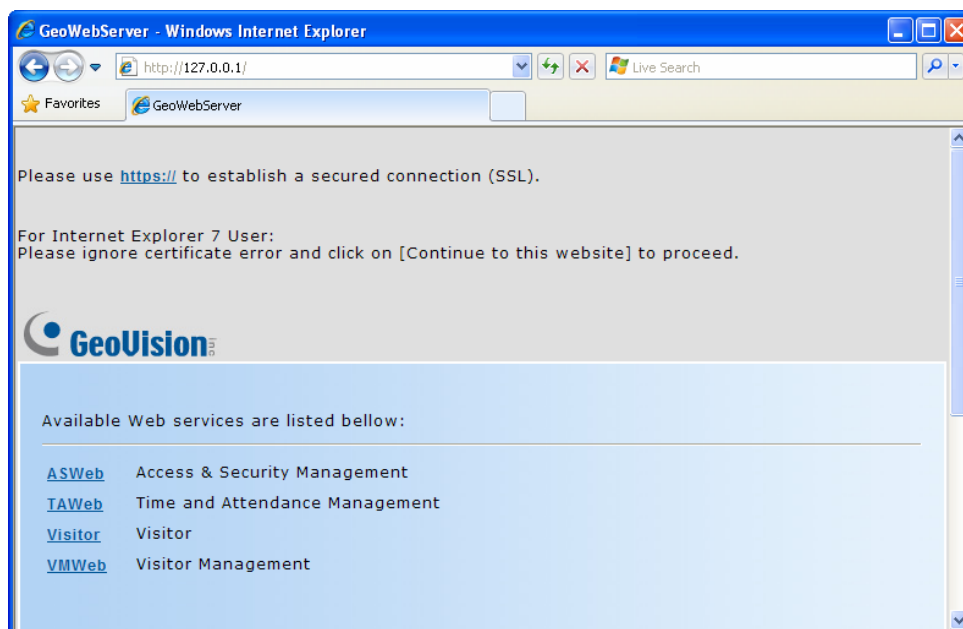
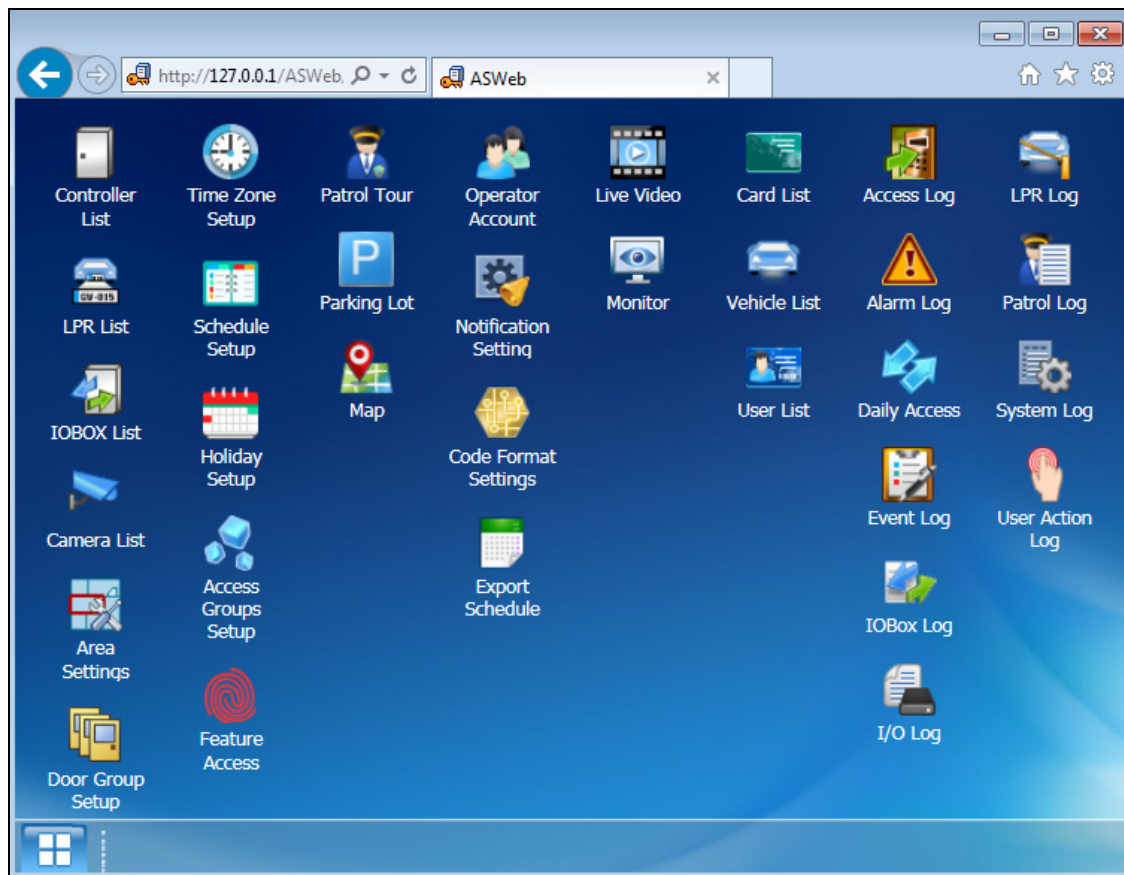


Figure 10-3

2. Click **https://** for SSL encrypted connection, or **ASWeb** for regular connection.

3. Enter a valid username and password for login. The GV-ASWeb page appears.

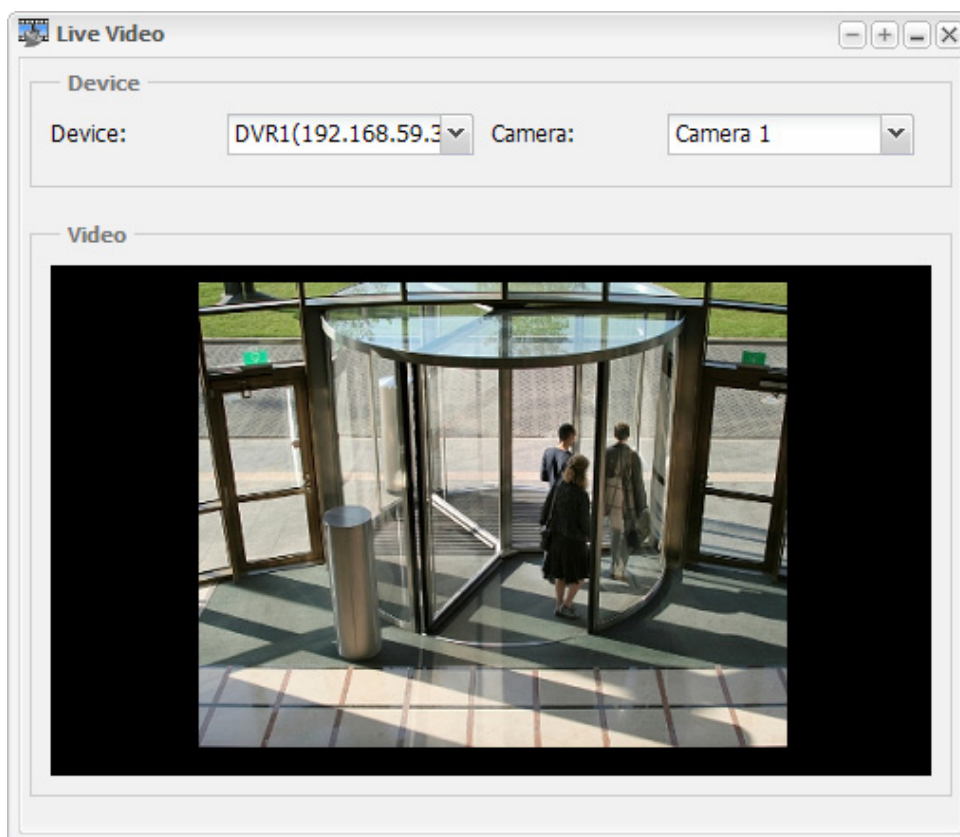


*Figure 10-4*

## 10.2 Accessing Live Video

You can use GV-ASWeb to remotely watch live video of devices connected to the GV-ASManager.

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



*Figure 10-5*

2. Click the **Device** drop-down list to select a connected GV-DVR / NVR or LPR.
3. Use the **Camera** drop-down list to select a camera. The live view will now be displayed.


---

**Note:** Live video will be displayed using MJPEG codec and a frame rate of 5 fps.

---

## 10.3 Monitoring GV-ASManager

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

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

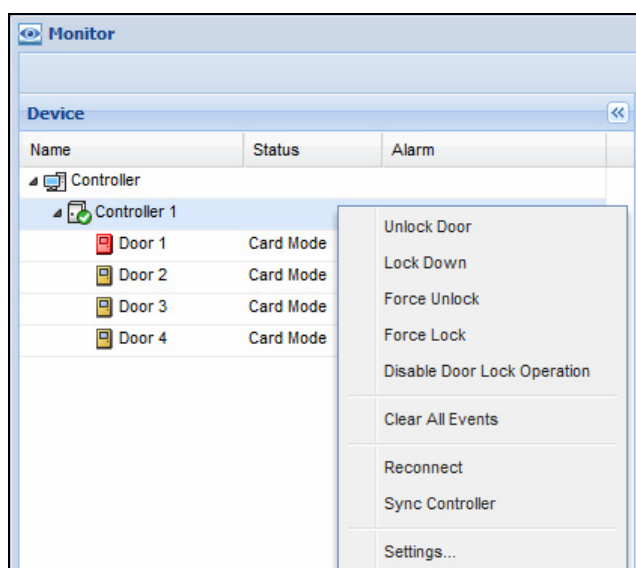


Figure 10-6

3. You can click **Monitor** in the upper-right corner to select the logs to display. Activities will appear in real time without refreshing the page.

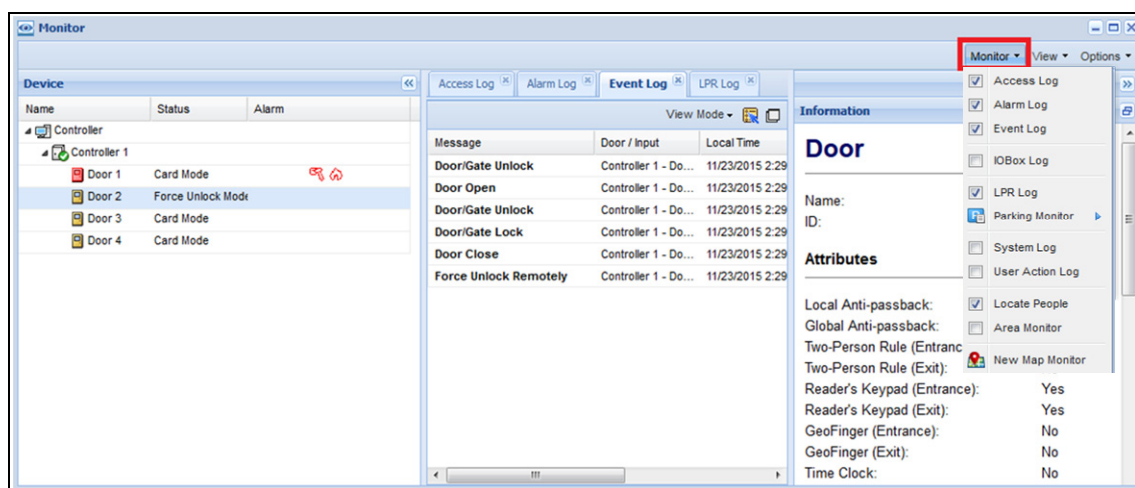


Figure 10-7

4. To see a pop-up map of the associated device upon an alarm event, click **Options** in the upper-right corner and select **Map (Alarm)**. Up to 6 pop-up events can be shown at a time. For details on how to set up the map, see *10.12 Creating Maps*.

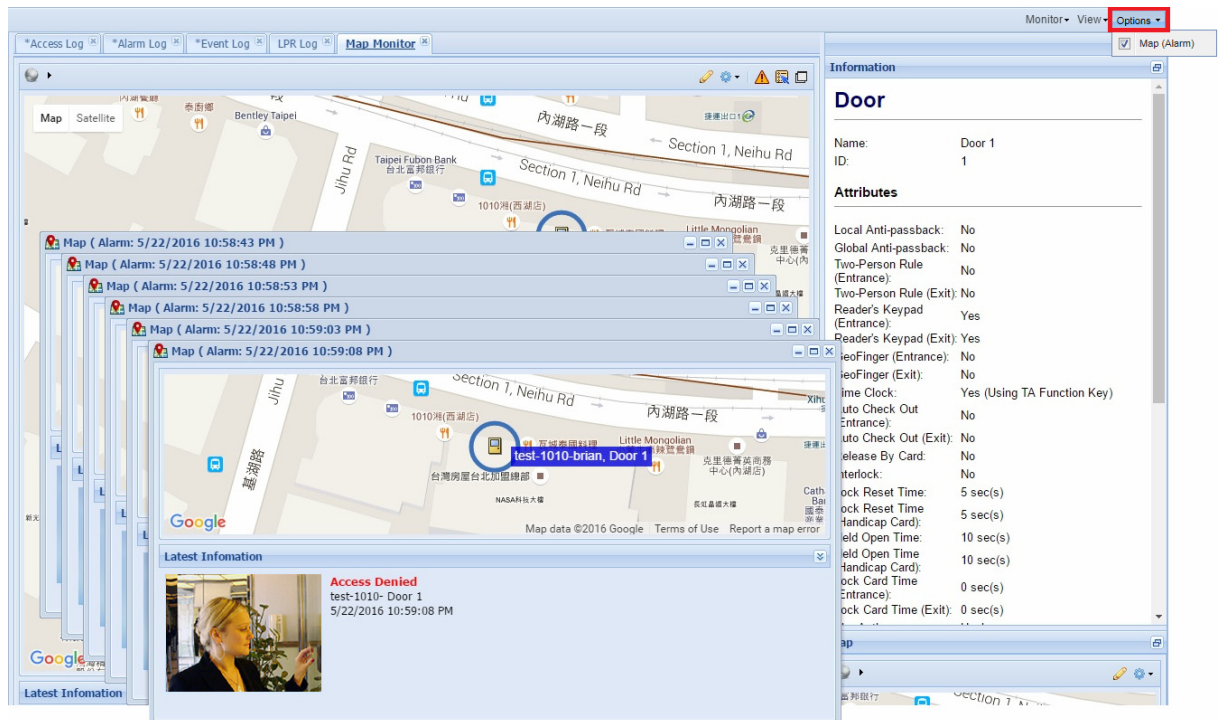


Figure 10-8



## 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 up search criteria to view the records more efficiently.

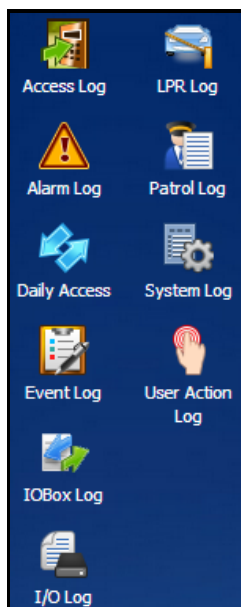


Figure 10-9

### 10.4.1 Setting Search Criteria

1. Select a log you want to view. Here we use Access Log as an example.
2. In the Filter section on the left, 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 1<sup>st</sup> to July 31<sup>st</sup>. The resulting filter window may look like this.

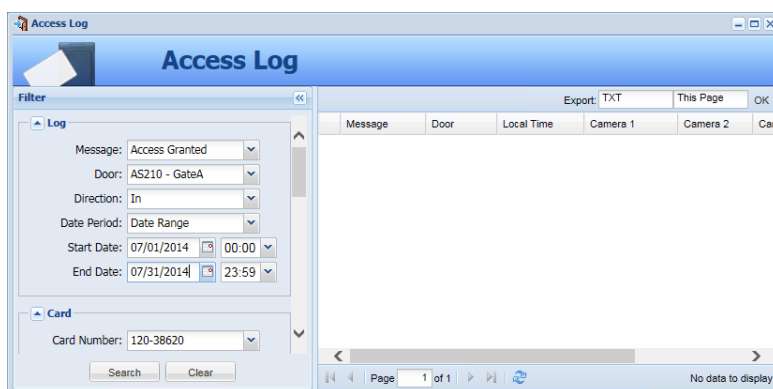


Figure 10-10

---

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

---

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

### 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 Controller List, Card List, User List, Access Log and Daily Access, you can right-click each search result to access more information such as card information  or user information



---

**Note:** You can play back video only when Remote ViewLog Service included in Control Center Server is enabled on the DVR. And the Remote ViewLog function is enabled on Video Server or Compact DVR.

---

### 10.4.3 Exporting Logs

You can download the logs of the connected GV-ASManager to the current computer in four formats: **txt**, **html**, **xls**, **html (zip)**, and **PDF**. When **html (zip)** is selected, 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 **TXT**, **HTML**, **Excel**, **HTML (ZIP)**, or **PDF**.
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 field must be first enabled on GV-ASManager before the content of the field can become searchable.

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

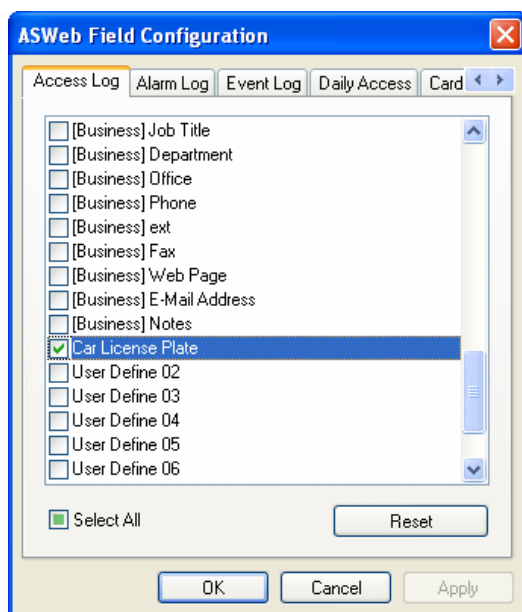


Figure 10-11

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

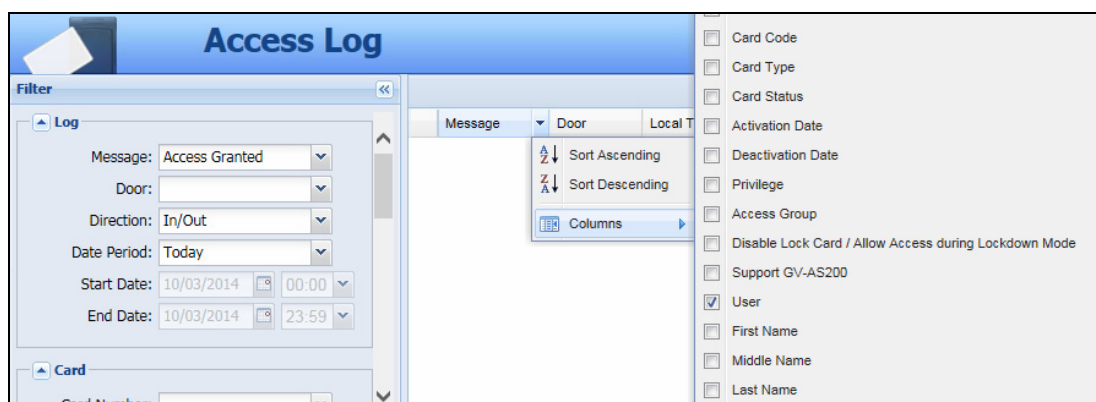


Figure 10-12

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

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

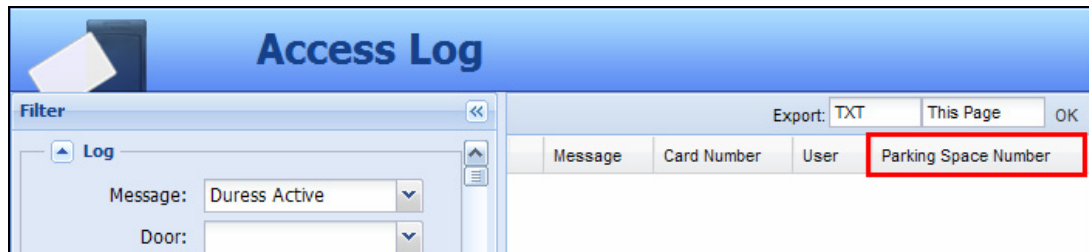


Figure 10-13

## 10.5 Adding and Deleting Controllers / LPR

You can use the Controller List and LPR List functions on GV-ASWeb to remotely add or delete controllers / LPR to the GV-ASManager. Here we use controllers as an example.

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

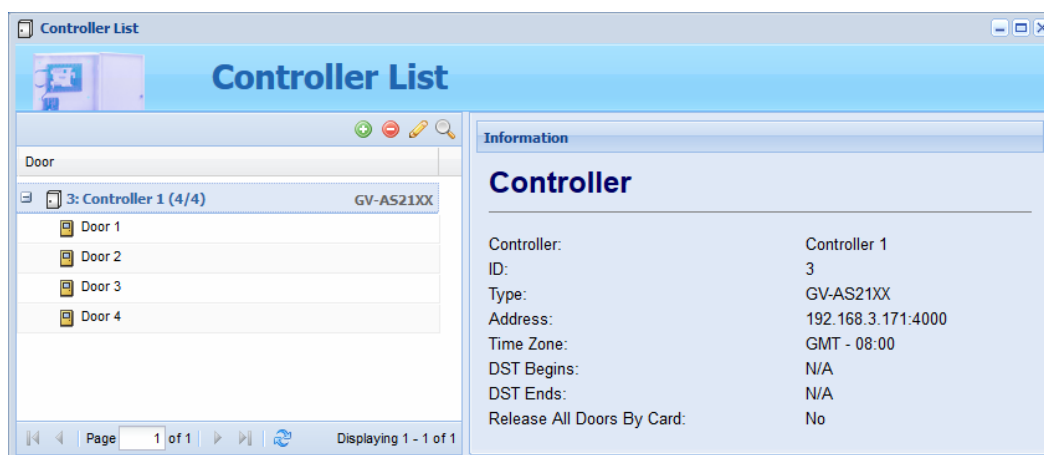




Figure 10-14

2. Click the **Add** button  to add a new controller. For details on the configurations, refer to *Step 1: Configuring a Controller* in Chapter 4.
3. To set the individual doors, click the **Edit** button  and select a door. For details, refer to *Step 2: Configuring the Doors or Elevator Floors* in Chapter 4.

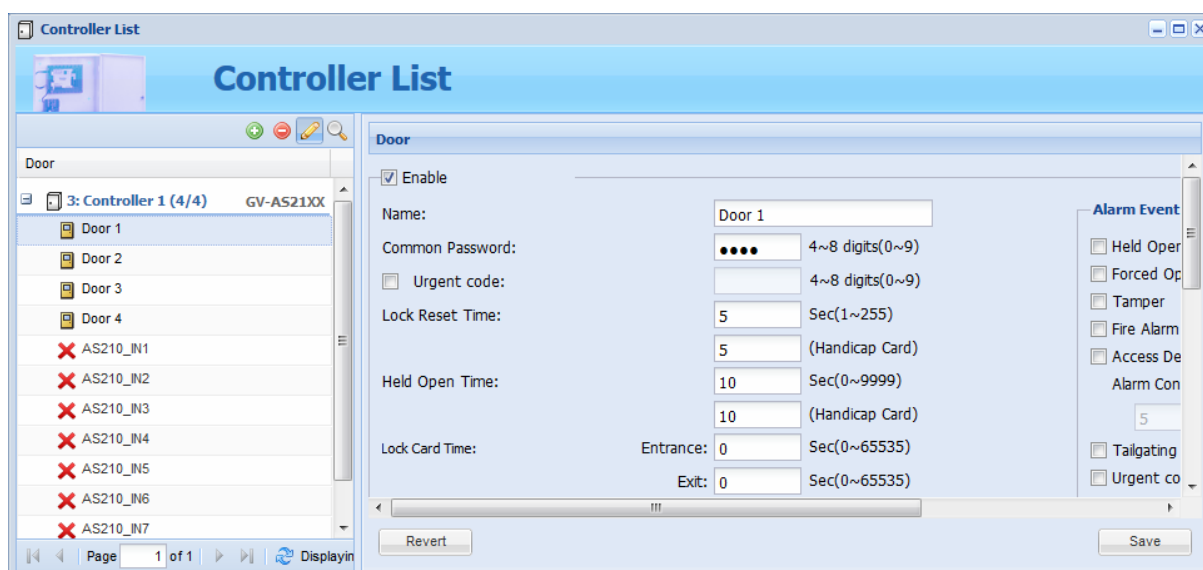


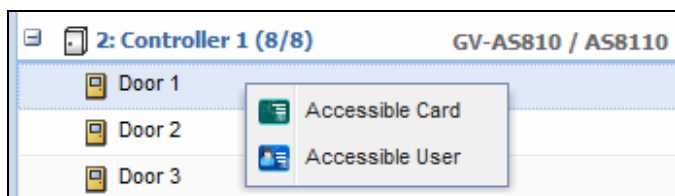
Figure 10-15

4. To delete a controller, select a controller and click the **Delete** button .

After adding or deleting a controller through GV-ASWeb, the change will be reflected in the Controller List in GV-ASManager.

---


**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.



## 10.6 Adding and Deleting Cards and Users

In addition to adding and deleting controllers, you can also use GV-ASWeb to remotely add or delete cards and users.

To add or delete cards:

1. On GV-ASWeb, click the **Card List** icon .
2. Click the **New** button. This dialog box appears.

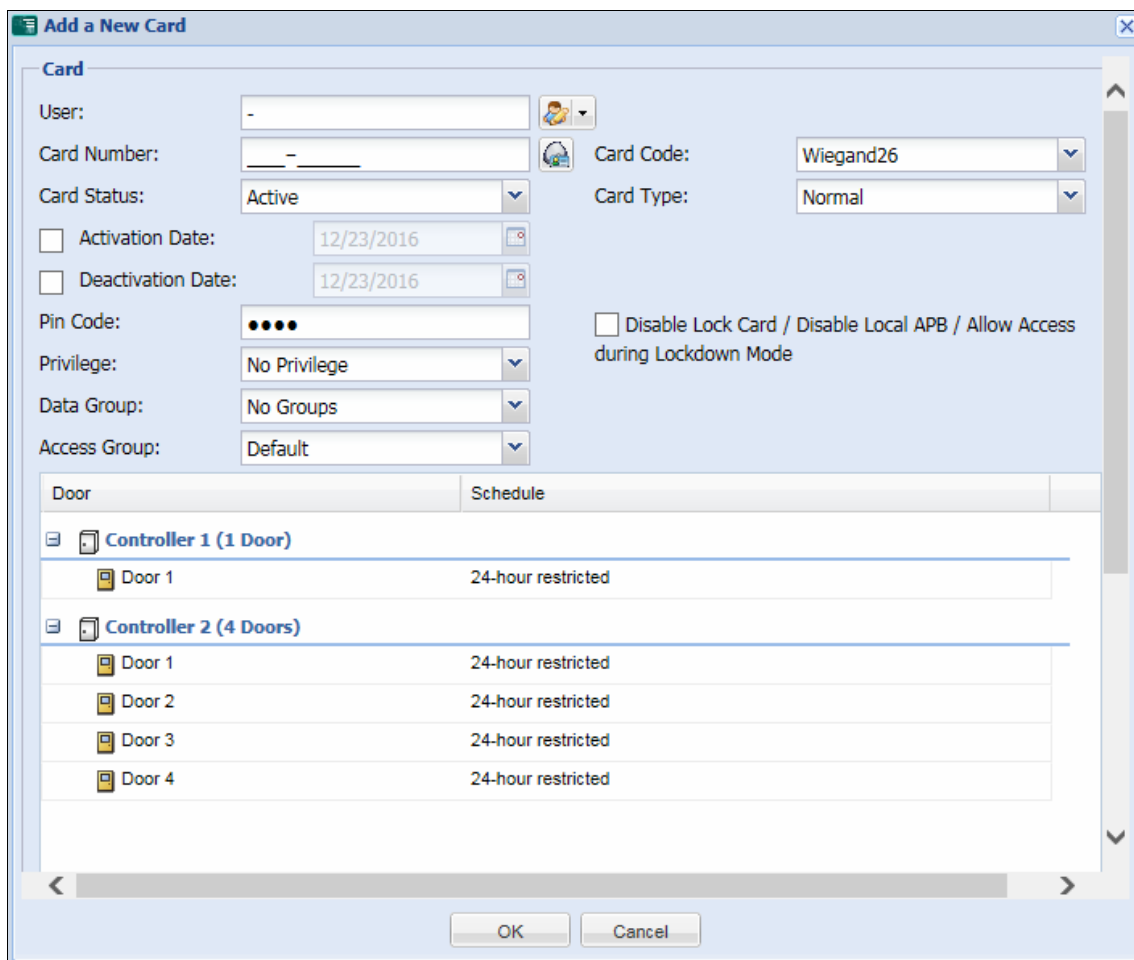



Figure 10-16

3. Fill out the required information. Refer to 4.3 *Setting Cards* for more details.
4. Click **OK** to save the settings.

5. If you have a GV-PCR310 Enrollment Reader installed, you can click **Card Reader**  to add a card using GV-PCR310.





 New  Edit  Delete  Card Reader         Export: <input type="text" value="TXT"/> <input type="text" value="This Page"/> <input type="button" value="OK"/>						
	Card Number	Card Type	Card Status	Activation Date	Deactivation Date	User
1	123-46578	Normal	Active	12/18/2013	-	-
2	123-4568	Normal	Active	12/24/2013	-	-

Figure 10-17

6. To delete cards, simply select the card and click the **Delete** button.


---

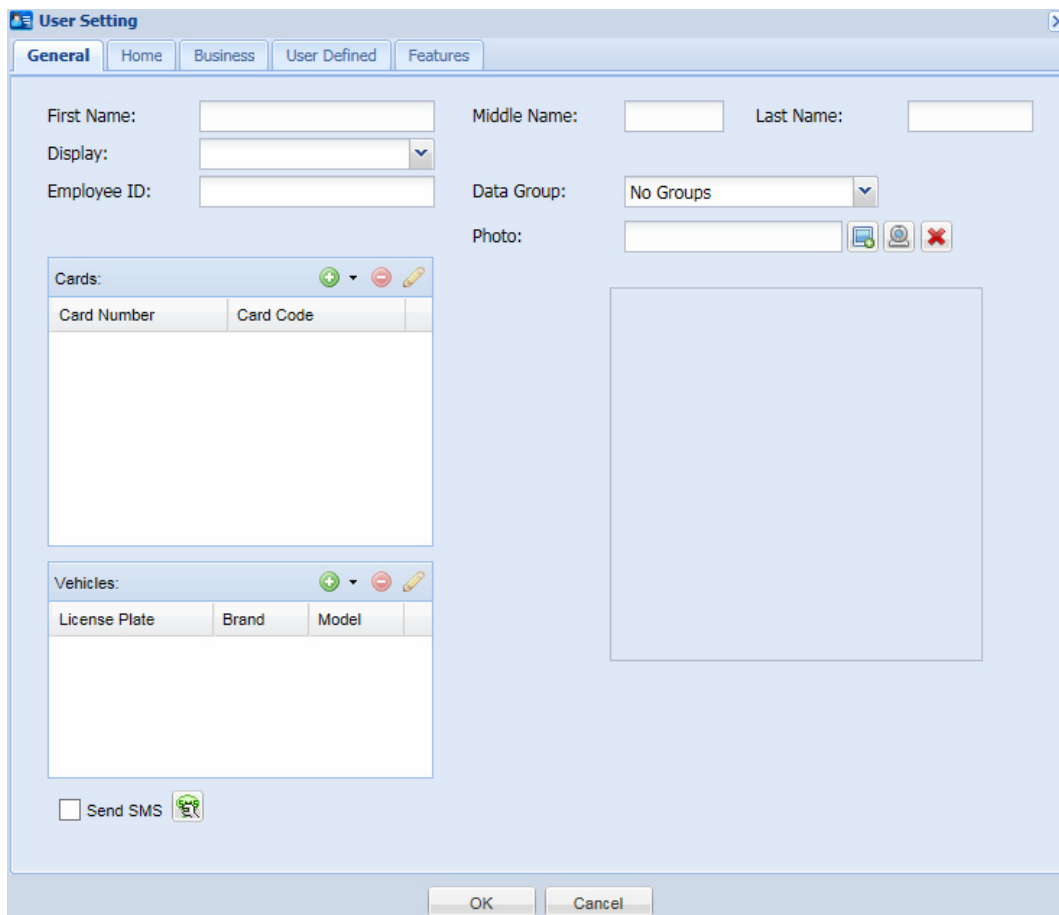
**Note:**

1. After adding or deleting a card through GV-ASWeb, the change will be reflected in the Card List in GV-ASManager.
  2. The Batch function and the card data import/export function are not supported on GV-ASWeb.
-






To add or delete users:

1. On GV-ASWeb, click the **User List** icon . The User List window appears.
2. Click the **New** button. This dialog box appears.









The **User Setting** dialog box has tabs for **General**, **Home**, **Business**, **User Defined**, and **Features**. The **General** tab is active.

Fields include:

- First Name:
- Middle Name:
- Last Name:
- Display:
- Employee ID:
- Data Group:
- Photo:    

There are two expandable sections:

- Cards:**   

Card Number	Card Code
- Vehicles:**   

License Plate	Brand	Model




At the bottom left, there is a checkbox for **Send SMS** . At the bottom right are **OK** and **Cancel** buttons.

Figure 10-18

3. Type the user's name. Other user information such as Employee ID, Home information and Business information are optional.
4. You can click the **Add** button  to assign a card or a vehicle to the user.
5. You can use the **Data Group** drop-down list to assign the user to a data group.
6. If you have a webcam installed, click the **Webcam** icon  to take a picture from the Webcam for the user profile.
7. Click **OK** to save the settings.
8. To delete a user, simply select the user and click the **Delete** button.

You can enroll fingerprints in the **Features** tab using GV-GF1921 / 1922. For details, refer to *Chapter 3 Fingerprint Only Mode* in the *GV-GF Fingerprint Reader User's Manual*.



---

**Note:**

1. After adding or deleting a user through GV-ASWeb, the change will be reflected in the User List in GV-ASManager.
  2. The user data import / export function is not supported on GV-ASWeb.
  3. The webcam function requires Flash Player 10 or later.
-

## 10.7 Searching, Adding and Deleting IP Cameras

You can use GV-ASWeb to remotely search and set up IP cameras by connecting to GV-DVR / NVR, GV-Video Servers, GV-Compact DVR or to IP cameras directly.

1. On GV-ASWeb, click the **Camera List** icon . The Camera List window appears.
2. To search for available IP devices under LAN, click the **Search** button  and select **Search DVR and NVR** or **Search IP Device**. This dialog box appears.

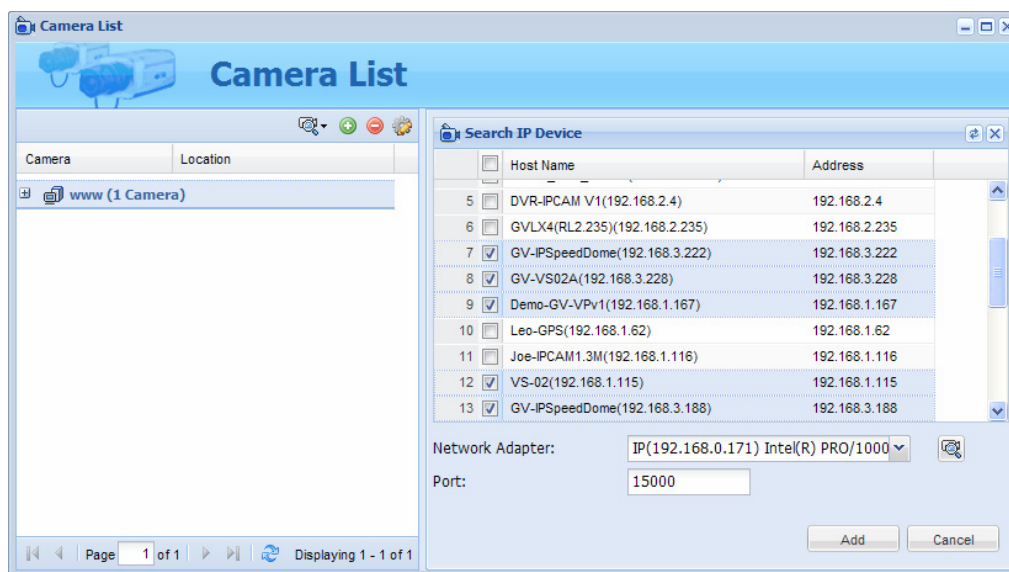



Figure 10-19

- a. Select the GV-DVR / NVR or IP devices to add from the search results.
- b. If necessary, you can select a different **Network Adaptor** and click the **Search** button again or modify the default port number 15000.
- c. Click **Add**. The GV-DVR / NVR or IP device is added to the camera list on the left.
- d. To login, select the GV-DVR / NVR or IP device, click the **Edit Mode** button , and type the User ID and password.

3. To manually add a device, click the **Add** button . This dialog box appears.

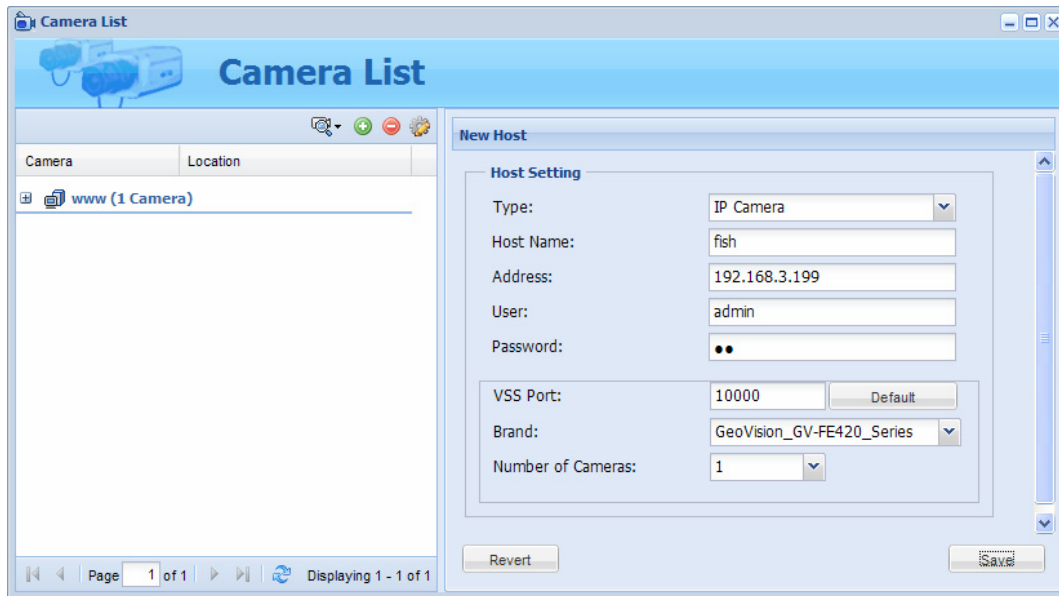




Figure 10-20

- a. Select the **Type** of device to add and type a **Host Name** to name the device.
  - b. Type the IP **Address**, **User** name and **Password** of the device.
  - c. Modify the default **Data Port** 5611, default **VSS Port** 10000, and default **Log Port** 5552 if necessary.
  - d. For IP cameras, use the **Brand** drop-down list to select the camera model. You can connect to third-party IP cameras through ONVIF, PSIA and RTSP protocols by selecting **Protocol** in the **Brand** drop-down list.
  - e. For GV-DVR / NVR, GV-Compact DVR and GV-Video Server, select a number from the **Number of Cameras** drop-down list to add channels between channel 1 and the selected channel. For example, if 3 is selected, channels 1-3 will be added.
  - f. Click **Save**.
4. To edit a device, click the **Edit** button  and select a device to begin editing.
5. To delete a device, select the device and click the **Delete** button .

---

**Note:** After adding or deleting a camera through GV-ASWeb, the change will be reflected in the Camera List in GV-ASManager.

---

## 10.8 Setting Schedule

You can use GV-ASWeb to remotely create daily schedules, set up weekly schedule and specify holidays. For more details on how to set up schedule, refer to Chapter 4.

### 10.8.1 Setting Daily Schedule

1. On GV-ASWeb, click the **Time Zone Setup** icon . This dialog box appears.

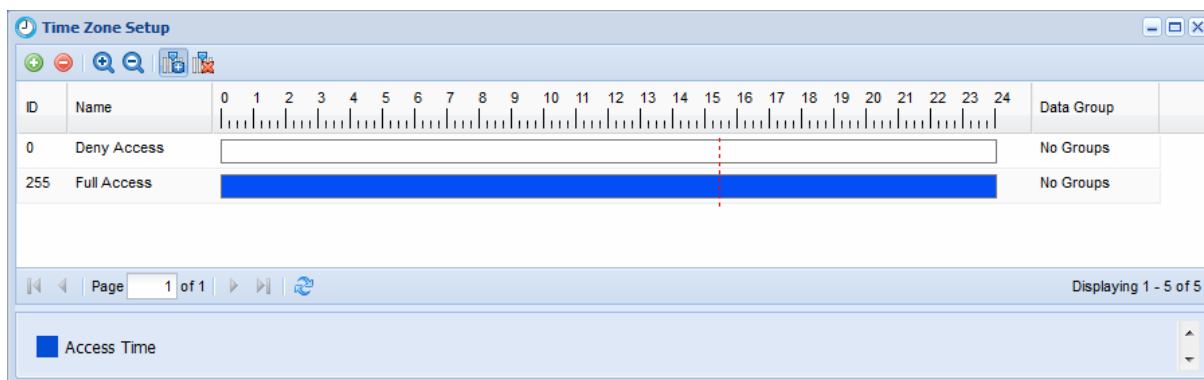


Figure 10-21

2. Click the **Add** button . A blank schedule appears.

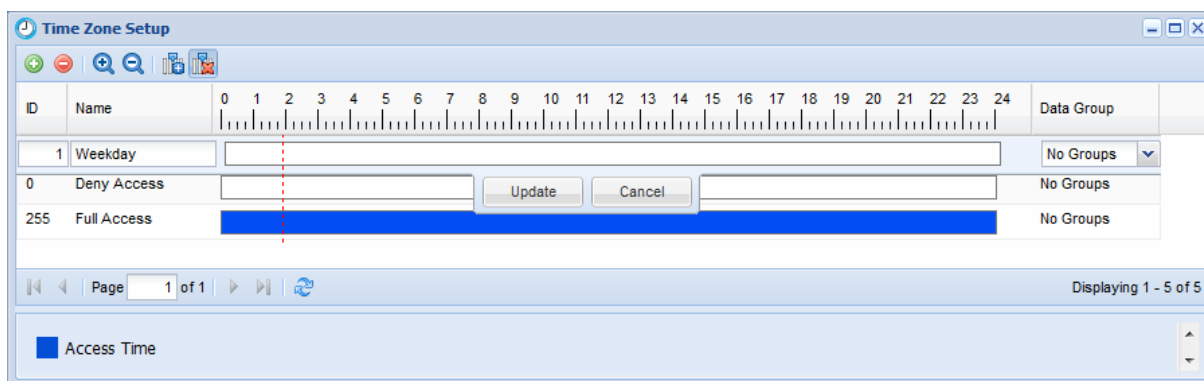

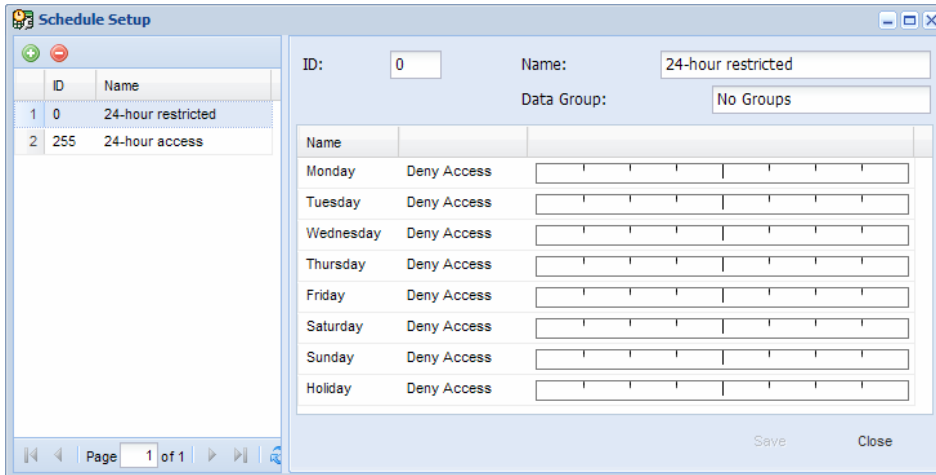


Figure 10-22

3. Type an ID and a name for the daily schedule.
4. Set the time by dragging the mouse on the timeline. To erase selected time, click the **Delete Access Time** button  and drag the mouse across the selected time.
5. You can use the **Data group** drop-down list to assign the time zone to a data group. You can then allow or forbid a user to read/write the functions listed under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.
6. Click **Update** to save.

## 10.8.2 Setting Weekly Schedule

1. On GV-ASWeb, click the **Schedule Setup** icon . This dialog box appears.




ID	Name
1 0	24-hour restricted
2 255	24-hour access

ID: 0 Name: 24-hour restricted Data Group: No Groups



Name	
Monday	Deny Access
Tuesday	Deny Access
Wednesday	Deny Access
Thursday	Deny Access
Friday	Deny Access
Saturday	Deny Access
Sunday	Deny Access
Holiday	Deny Access

Page 1 of 1 Save Close

Figure 10-23

2. Click the **Add** button . A blank schedule appears.
3. Type an ID and a name for the weekly schedule.
4. You can use the **Data Group** drop-down list to assign the weekly schedule to a data group. You can then allow or forbid a user to read/write the functions listed under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.
5. Click the timeline and assign the daily schedule created to the day of the week. The schedule selected for Holiday will be applied to the dates selected in the Holiday Setup page. Refer to the section below.
6. Click **Save**.

### 10.8.3 Specifying Holiday

On the main page of GV-ASWeb, click the **Holiday Setup** icon . To specify holidays or special days, click a color block and click the dates of the Holiday or special day. To remove holidays or special days, click **Remove Holiday**  and click the dates.

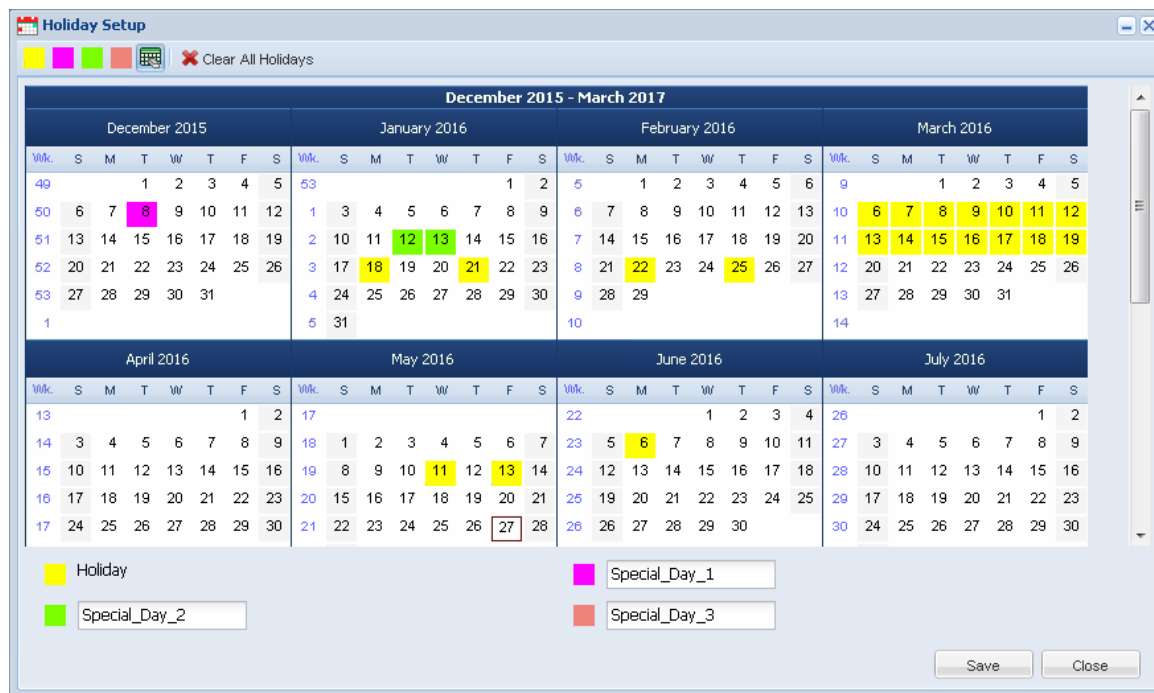



Figure 10-24

### 10.9 Setting Access Groups

Using GV-ASWeb, you can remotely set up access groups to restrict who can access which door at what time. On the main page of GV-ASWeb, click the **Access Groups** icon . For details on how to set up access groups, refer to *Setting Access Groups* in Chapter 4.

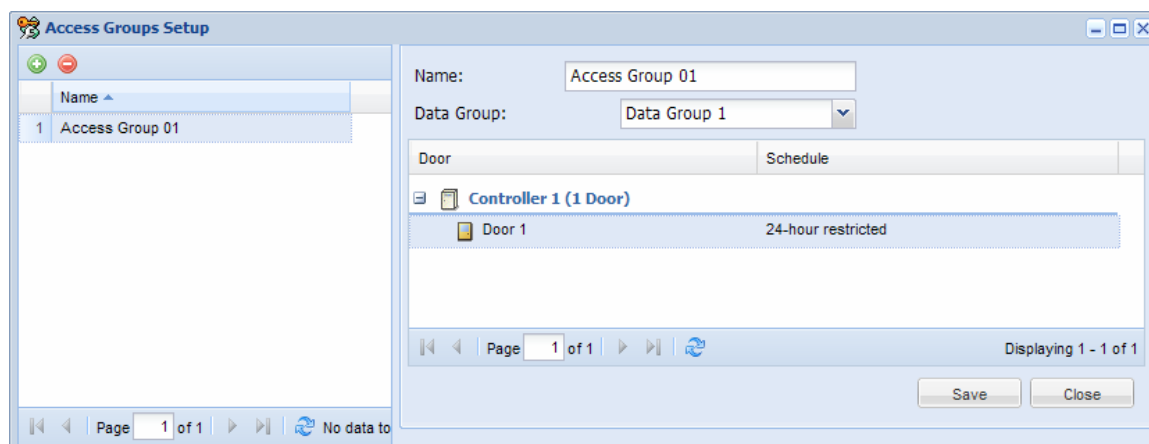


Figure 10-25

## 10.10 Setting Door Groups

Using GV-ASWeb, you can remotely organize controllers into different door groups, allowing you to quickly upload fingerprints and user data to the doors installed with fingerprint and face recognition readers respectively.

On the main page of GV-ASWeb, click the **Door Group Setup** icon . For details on how to set up door groups and upload fingerprints, refer to *Uploading Fingerprints to Controllers Using Door Groups* in Chapter 3 of *GV-GF Fingerprint Reader User's Manual*.

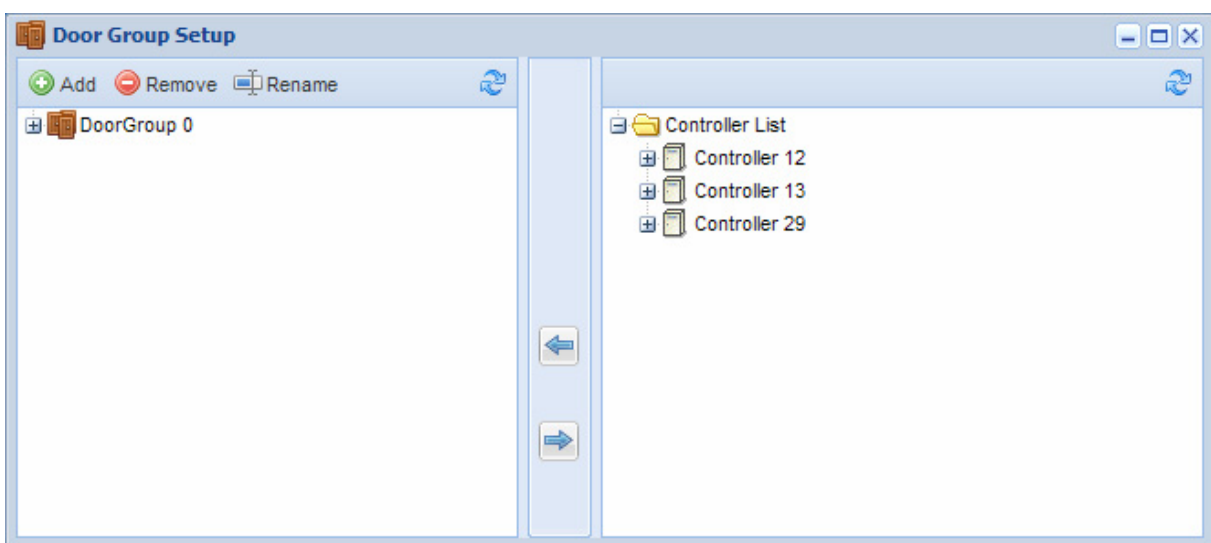


Figure 10-26



## 10.11 Configuring Areas for Anti-Passback

You can remotely define Entry and Exit areas for each door using GV-ASWeb.

1. On GV-ASWeb, click the **Area Settings** icon . This dialog box appears.

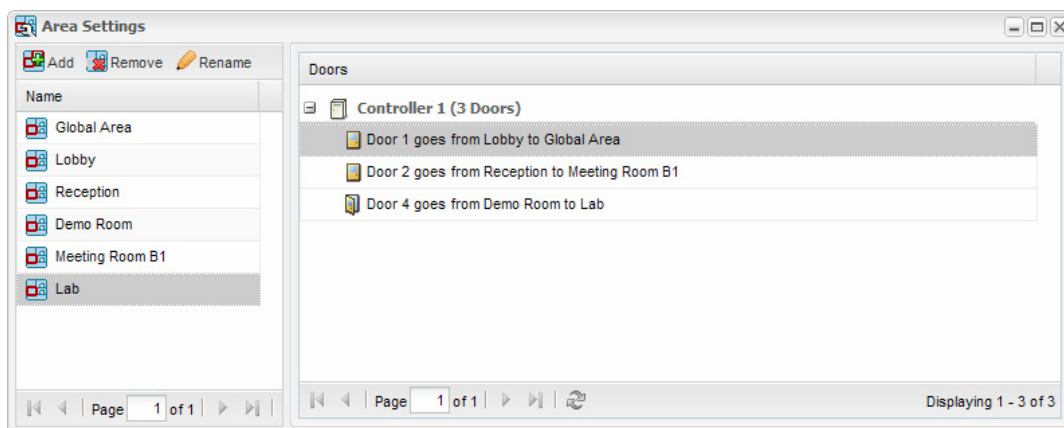


Figure 10-27

2. Click the **Add** button to add an area and double-click the name to rename the area.
3. Double-click a door and use the drop-down lists to assign the entry and exit area.

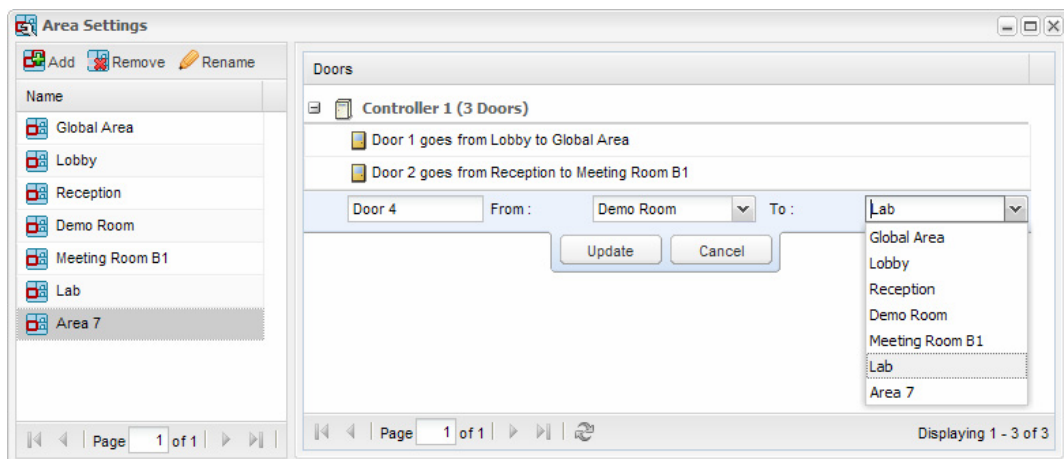


Figure 10-28

For more details on how to set up Anti-Passback, refer to Chapter 6.

---

**Note:** After defining areas for Anti-Passback through GV-ASWeb, the change will be reflected in the Area Settings page in GV-ASManager.

---

## 10.12 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 dialog box appears.

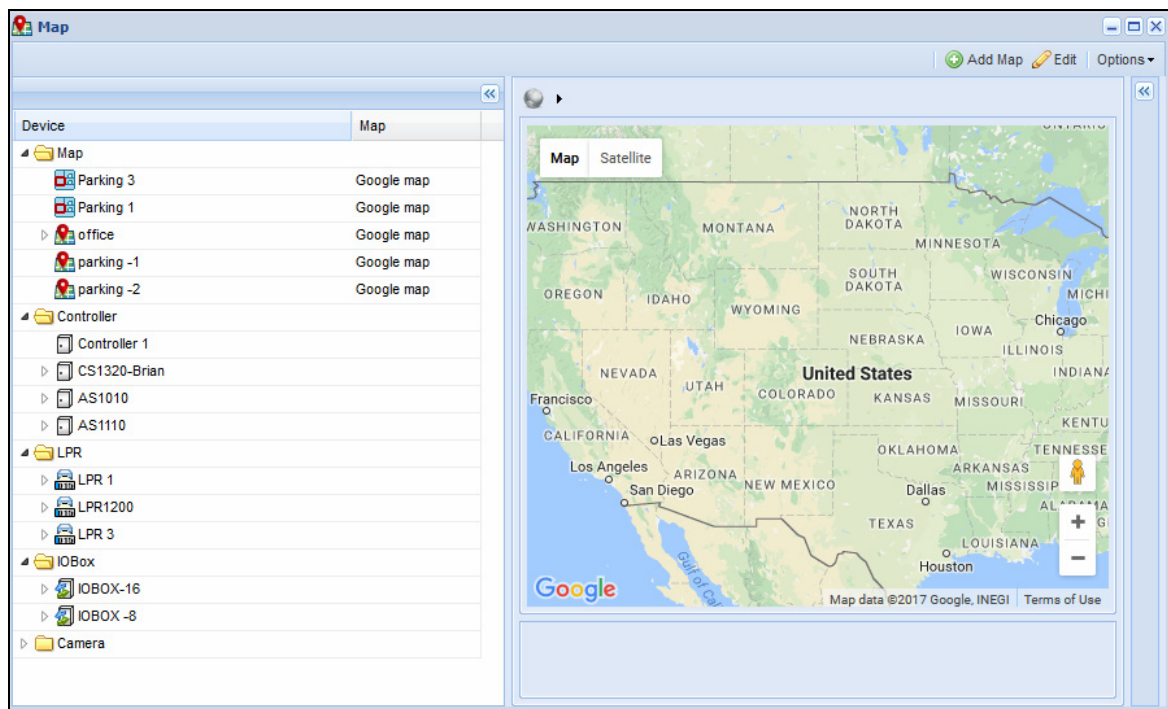


Figure 10-29

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.

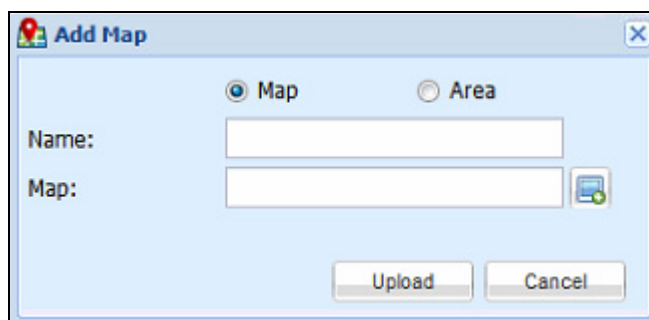



Figure 10-30

- 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.



- 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**.

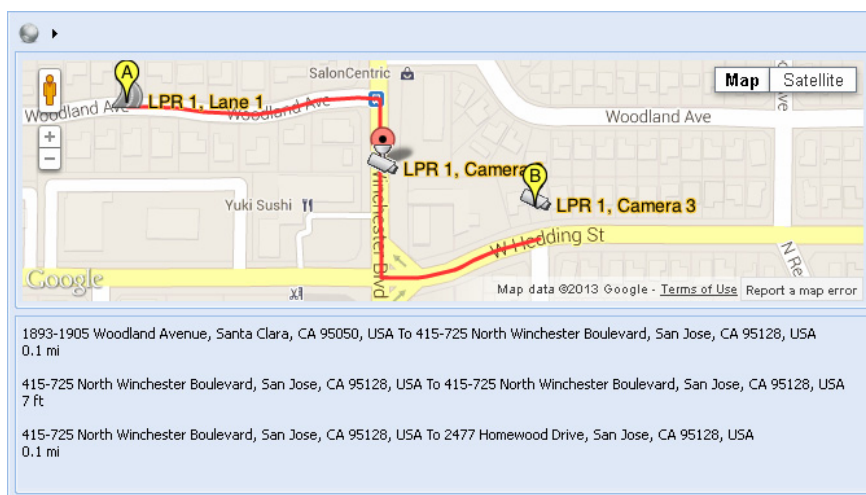
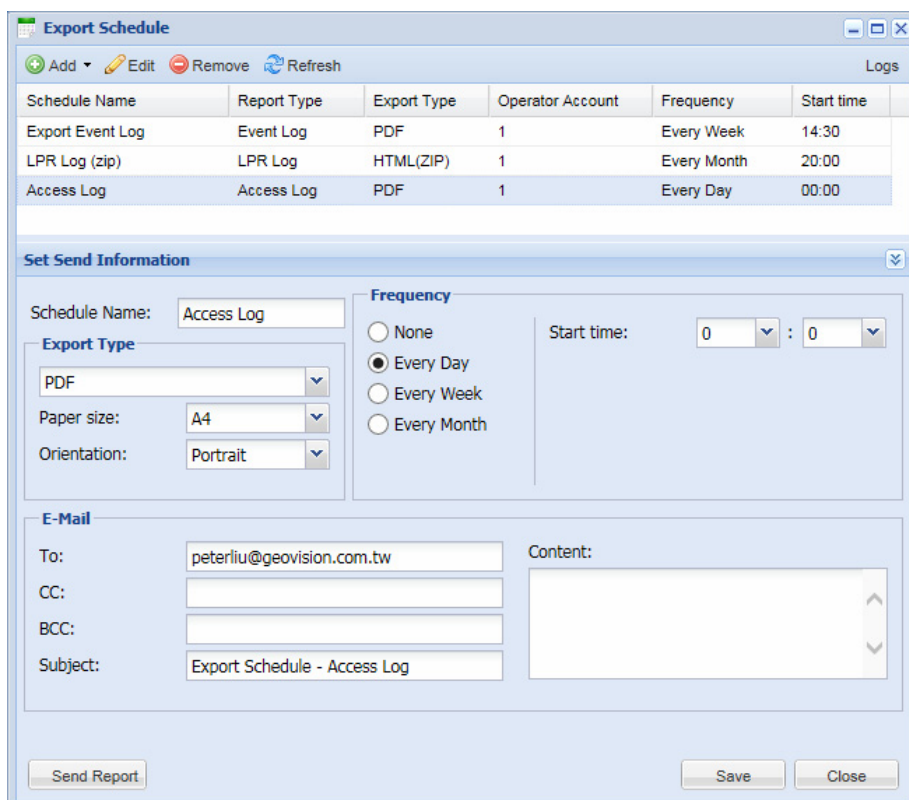


Figure 10-33

## 10.13 Setting Export Schedule for Lists and Logs

You can set up a schedule to regularly export lists and logs, and send them to the specified e-mail addresses.

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



The dialog box titled "Export Schedule" contains a table of existing schedules and configuration options for a new one.

Schedule Name	Report Type	Export Type	Operator Account	Frequency	Start time
Export Event Log	Event Log	PDF	1	Every Week	14:30
LPR Log (zip)	LPR Log	HTML(ZIP)	1	Every Month	20:00
Access Log	Access Log	PDF	1	Every Day	00:00

**Set Send Information**

Schedule Name:

**Export Type**

PDF (selected)

Paper size:

Orientation:

**Frequency**

☐ None  
☒ Every Day  
☐ Every Week  
☐ Every Month

Start time:  :

**E-Mail**

To:

CC:

BCC:

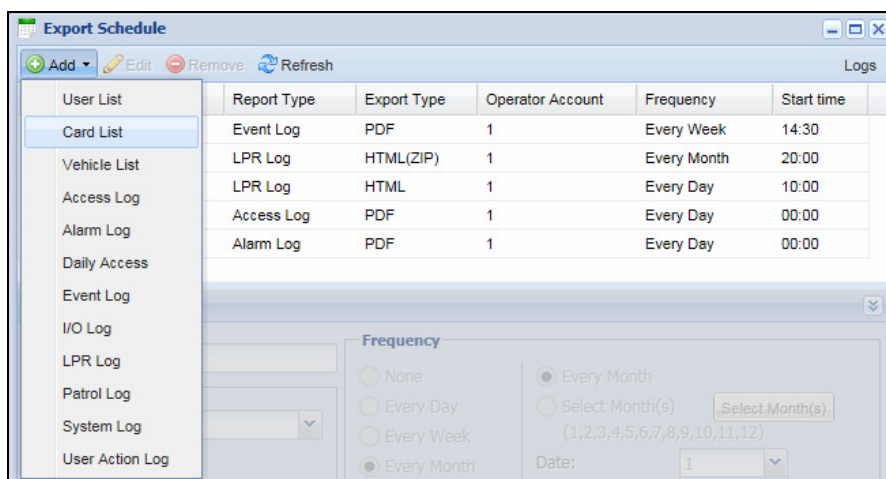
Subject:

Content:

Buttons: Send Report, Save, Close

Figure 10-34

2. Click the **Add** button and select the list or log you want to export.



The dialog box is shown with the "Add" button clicked, opening a menu of available reports and logs.

Report Type	Export Type	Operator Account	Frequency	Start time
Event Log	PDF	1	Every Week	14:30
LPR Log	HTML(ZIP)	1	Every Month	20:00
LPR Log	HTML	1	Every Day	10:00
Access Log	PDF	1	Every Day	00:00
Alarm Log	PDF	1	Every Day	00:00

**Add Menu:**

- User List
- Card List
- Vehicle List
- Access Log
- Alarm Log
- Daily Access
- Event Log
- I/O Log
- LPR Log
- Patrol Log
- System Log
- User Action Log

**Frequency**

☐ None  
☐ Every Day  
☐ Every Week  
☒ Every Month

Select Month(s):

Date:

Figure 10-35

- On the left side, set the filter criteria if you only want to export some of the data, and click **Save to Export Schedule**.

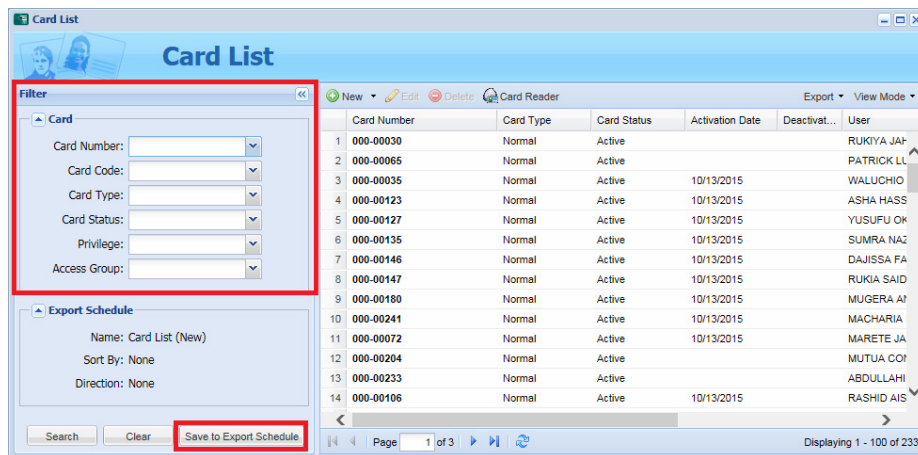


Figure 10-36

- Select a file format under **Export Type**, set the export **Frequency**, and type the **E-mail** of the recipient.

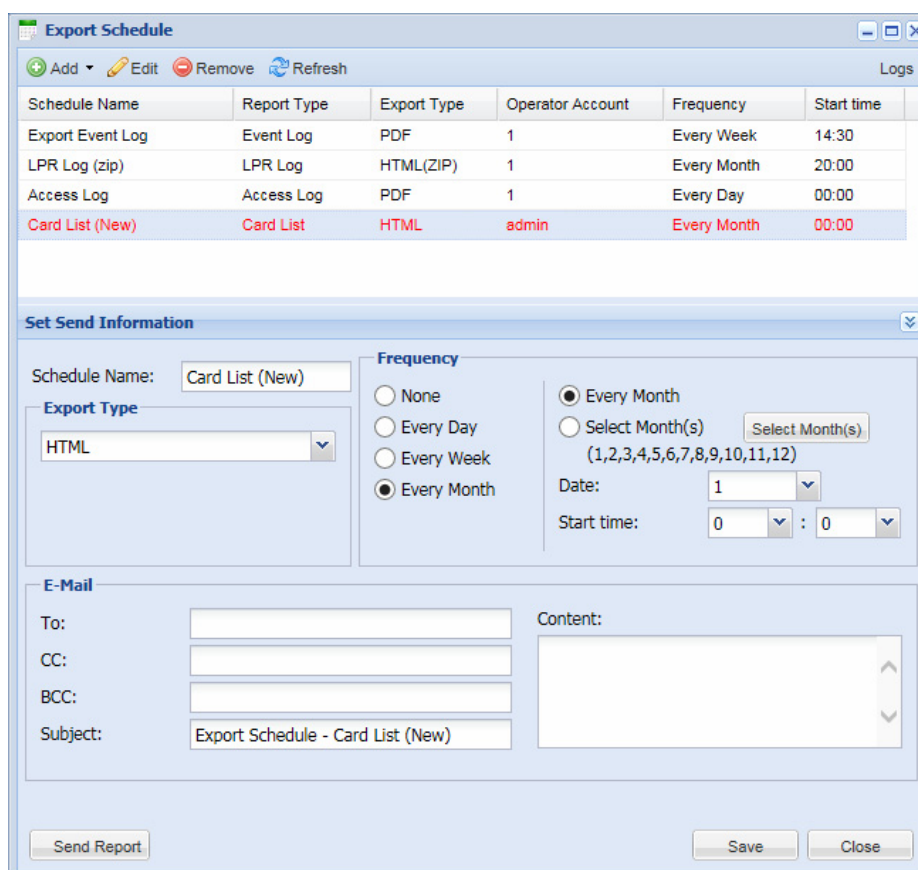


Figure 10-37

- Click **Save** to apply.

## 10.14 Setting Up Other Functions

Through GV-ASWeb, you can also set up the following functions: **Patrol Tour**, **Parking Lot**, **Operator Account**, **Notification Setting**, and **Code Format Setting**. The interfaces of these functions are similar to those of the GV-ASManager. Refer to the following sections to see how to set up these functions.

- **Patrol Tour:** See *Chapter 7 Patrol Tour*.
- **Parking Lot:** See *13.8 Managing Parking Lots*.
- **Operator Account:** See *8.1 Setting Up System User*.
- **Notification Setting:** See *8.2.3 Setting Notification*.
- **Code Format Setting:** See *8.9 Defining New Card Formats*.
- **Printing Card:** See *8.9 Designing and Printing Access Card Template*.



## 10.15 Creating Accounts to Manage GV-ASWeb

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

1. On the menu bar, click **Tools** and select **Operators**. A dialog box appears.

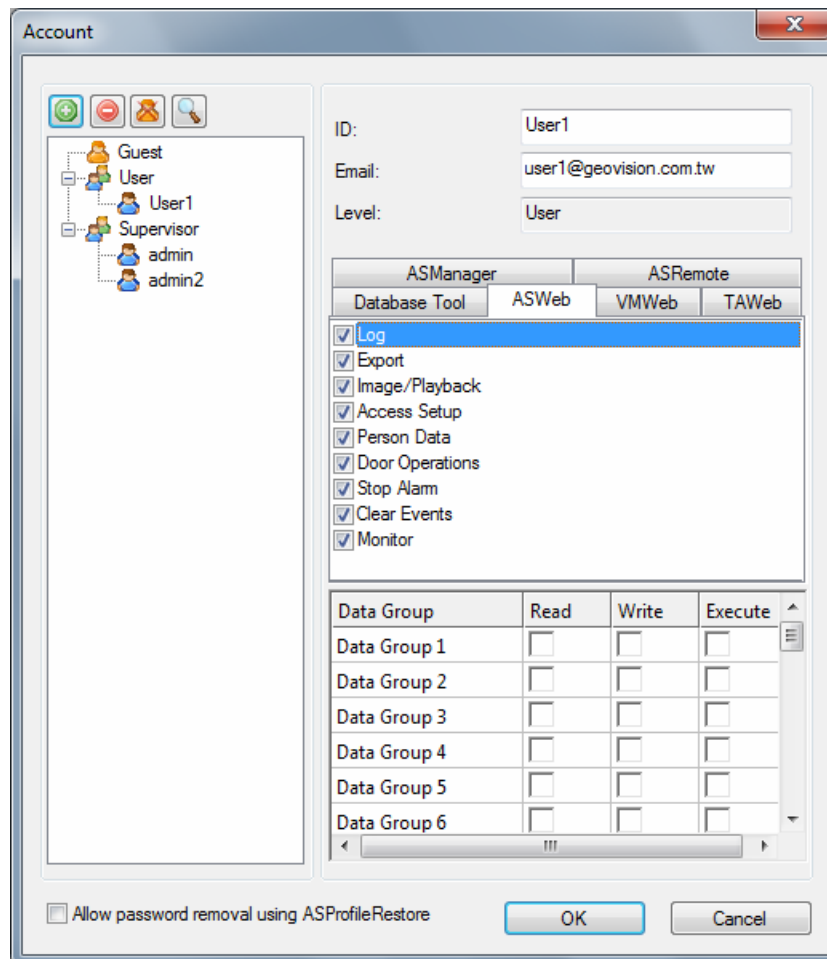



Figure 10-38

2. To create an account, click the **New** button  in the top left corner.
3. Type the account's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
4. In the **Level** drop-down list, select **Supervisor** to have access to all GV-ASWeb functions. To grant limited access, select **User**. Click **OK**.
5. Click the **ASWeb** tab in the middle.
6. Select the privileges you want to grant. The following options are available.
  - **Log:** View Alarm Log, Access Log, Daily Access, Event Log and I/O Log.
  - **Export:** Export Alarm Log, Access Log, Daily Access, Event Log and I/O Log.
  - **Image/Playback:** Play back recorded videos and snapshots from GV-ASWeb logs.



- **Access Setup:** Set up controller list, camera list, area settings, time zone, schedule, holidays and user-defined access group.
- **Person Data:** Add or edit cards and users.
- **Door Operations:** Control door operations in Monitor page.
- **Stop Alarm:** Stop alarm in Monitor page.
- **Clear Events:** Clear events in Monitor page.
- **Monitor:** Access Monitor page.

7. Click **OK**.

## 10.16 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 the GV-ASManager to be connected. This web page appears.



Figure 10-39

2. Click **ASWeb** and type the username and password of GV-ASManager to login. The controller / LPR list is shown.

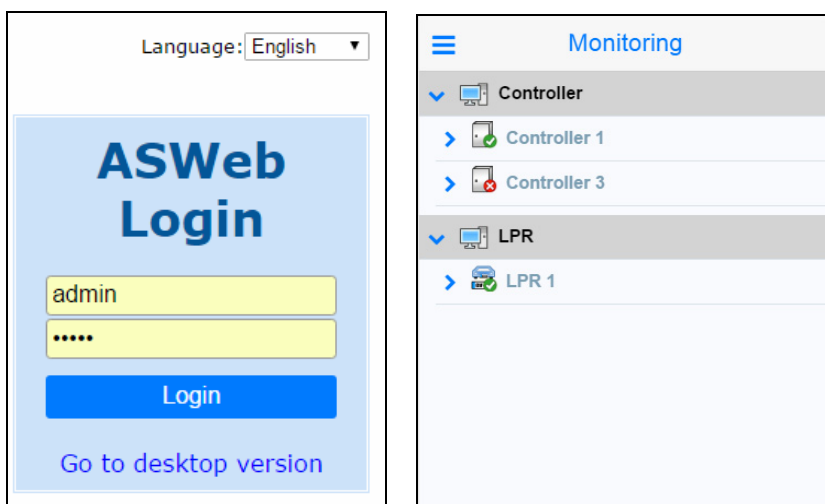


Figure 10-40

- You can tap on the arrow next to the controller or LPR to see the associated doors and lanes. When alert conditions occur, the alert icon will light up in red under the doors.

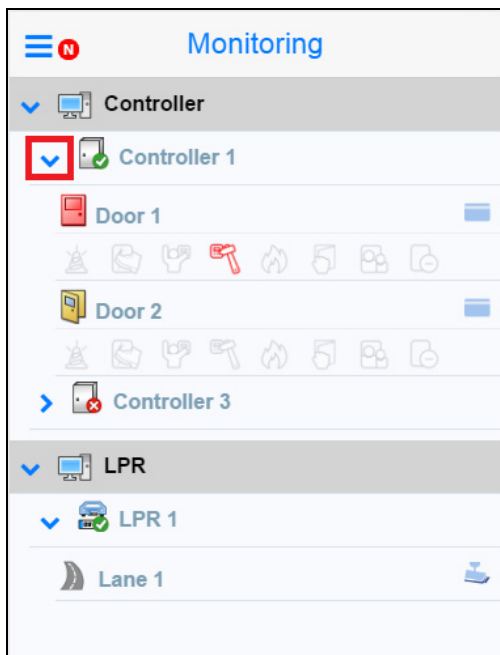


Figure 10-41

- To remotely control the device, tap on a controller, door, LPR or lane, and select an action.

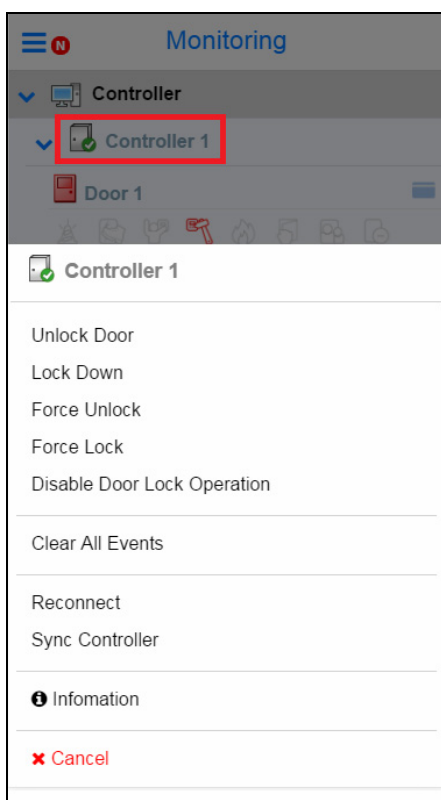



Figure 10-42

5. To watch live view of connected camera, tap the Menu button , tap **Live Video** and select the devices.

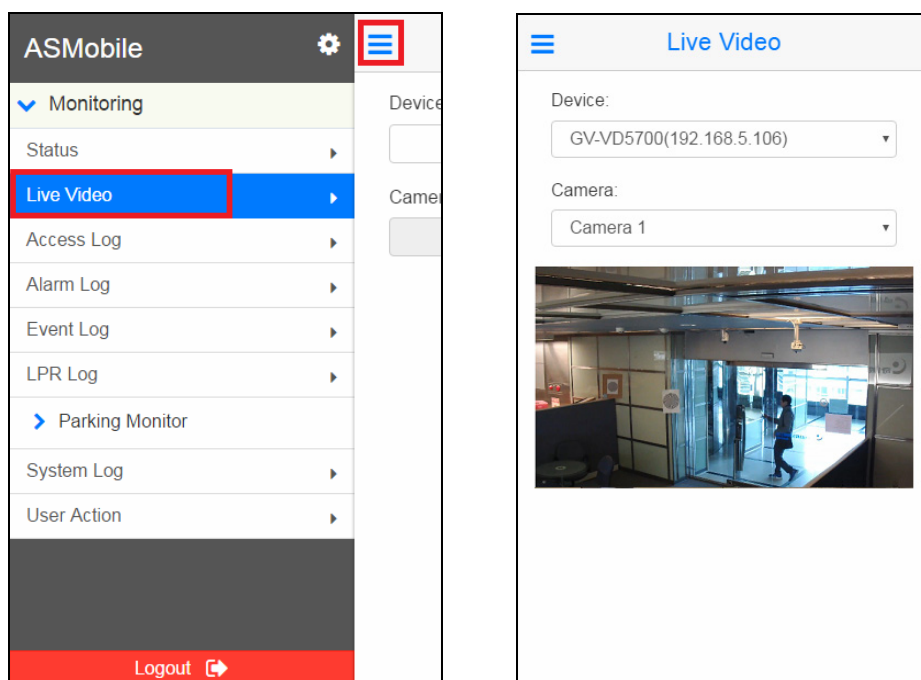



Figure 10-43

6. To look up the logs, tap the Menu button  and select one of the logs.

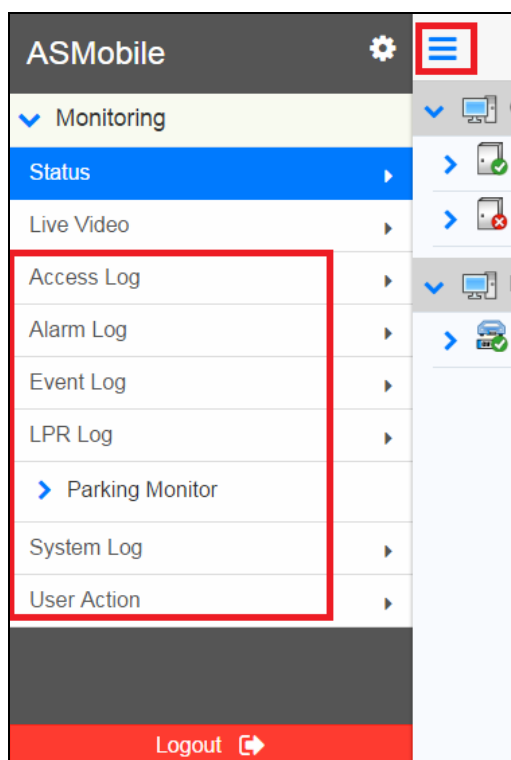


Figure 10-44

## 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 the specified e-mail addresses. Refer to *Setting Export Schedule for Lists and Logs* in Chapter 10.

To use the GV-TAWeb, the browser in the client PC must be **Internet Explorer 9 or later**.

## 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 enabled to allow remote access.

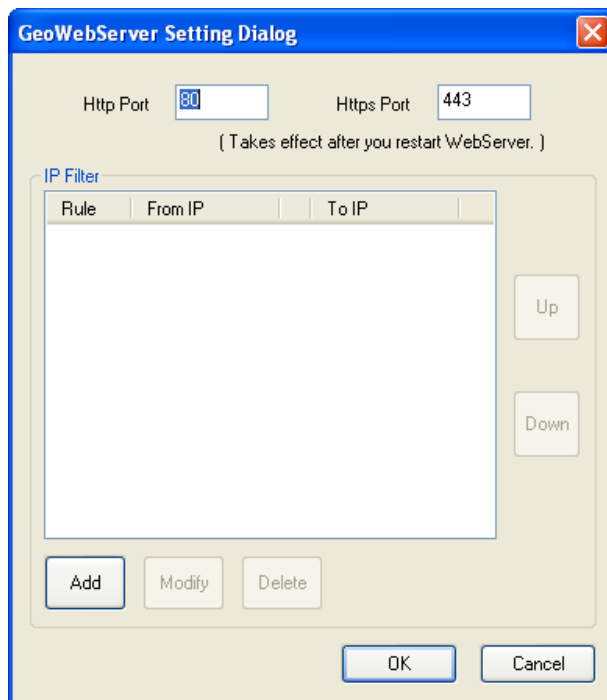
**Note:** The Time Clock option is not available for GV-AS1010. To use GV-AS1010 with GV-TAWeb, you must configure the built-in function keys on the Web interface of GV-AS1010. Refer to the *Function Key Configuration* section in Chapter 8 of *GV-ASEV Controller User Manual*.

1. On the menu bar, click **Setup**, select **Devices** and in the dialog box, double-click the GV-AS / GV-EV Controller you want to use to keep track of attendance. Select the **Door** tab and select **Time Clock**.


The screenshot shows the 'Controller Setup' window with the 'Door 1' tab selected. The 'Enable' checkbox is checked. The 'Name' field is 'Door 1'. The 'Common Password' field is masked with four dots. The 'Urgent Code' field is also masked. The 'Lock Reset Time' is set to 5 seconds. The 'Held Open Time' is set to 10 seconds. The 'Lock Card Time' is set to 0 seconds for both Entrance and Exit. The 'Fire Action' is set to 'Unchange'. The 'Reader's Keypad' section has 'Entrance' and 'Exit' checked. The 'Auto Check Out' section has 'Entrance' and 'Exit' unchecked. The 'GeoFinger' section has 'Entrance' checked and 'TCP/IP' selected. The 'IP Address...' field is '2167'. The 'Exit' section has 'TCP/IP' selected and 'IP Address...' field is '2167'. The 'Anti-Passback' section has 'Local Anti-Passback' and 'Global Anti-Passback' unchecked. The 'Two-Person Rule' section has 'Entrance' checked and 'Exit' unchecked. The 'Interlock' section has 'Door 3, Door 4' selected. The 'Time Clock' checkbox is checked and highlighted with a red box.

Figure 11-1

2. On the menu bar, click **Tools**, select **Servers** and enable **Web Server**. This dialog box appears.



*Figure 11-2*

If you want to grant or deny the access from 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 of the main screen.

To start the GV-TAWeb:

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

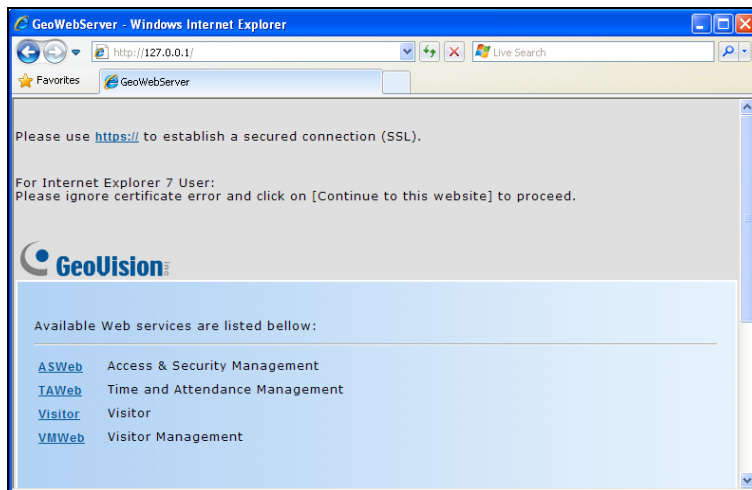


Figure 11-3

2. Click **https://** for SSL encrypted connection, or **TAWeb** for regular connection.
3. Enter a valid username and password for login. The GV-TAWeb page appears.

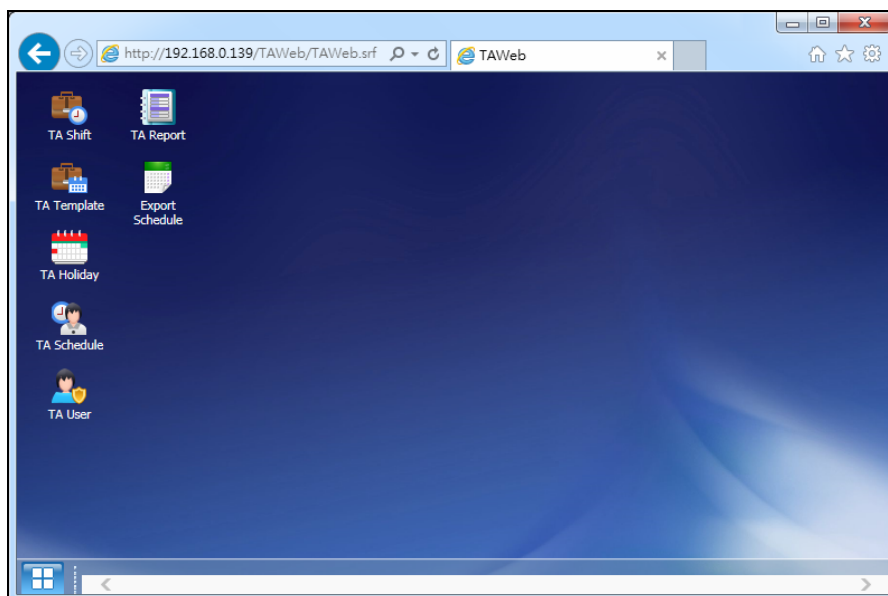


Figure 11-4



## 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 schedule to an employee or a group of employees using daily schedule in TA Shift or using long-term schedule from TA Template.

### 11.2.1 TA Shift: Setting Up a Daily Schedule

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

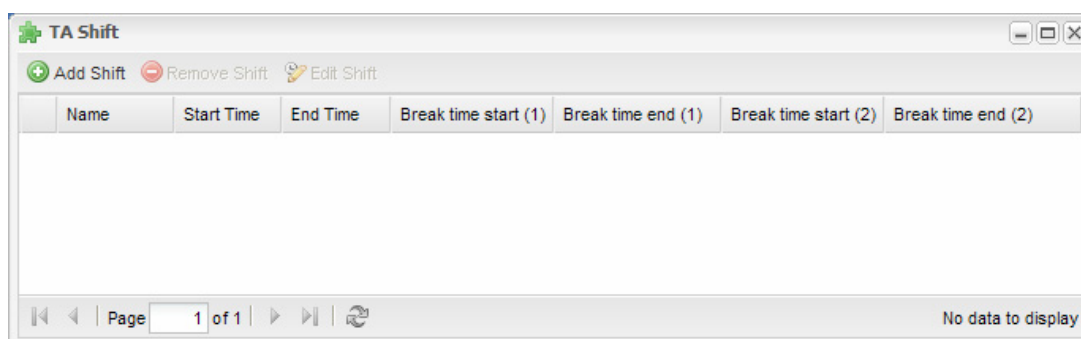


Figure 11-5

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

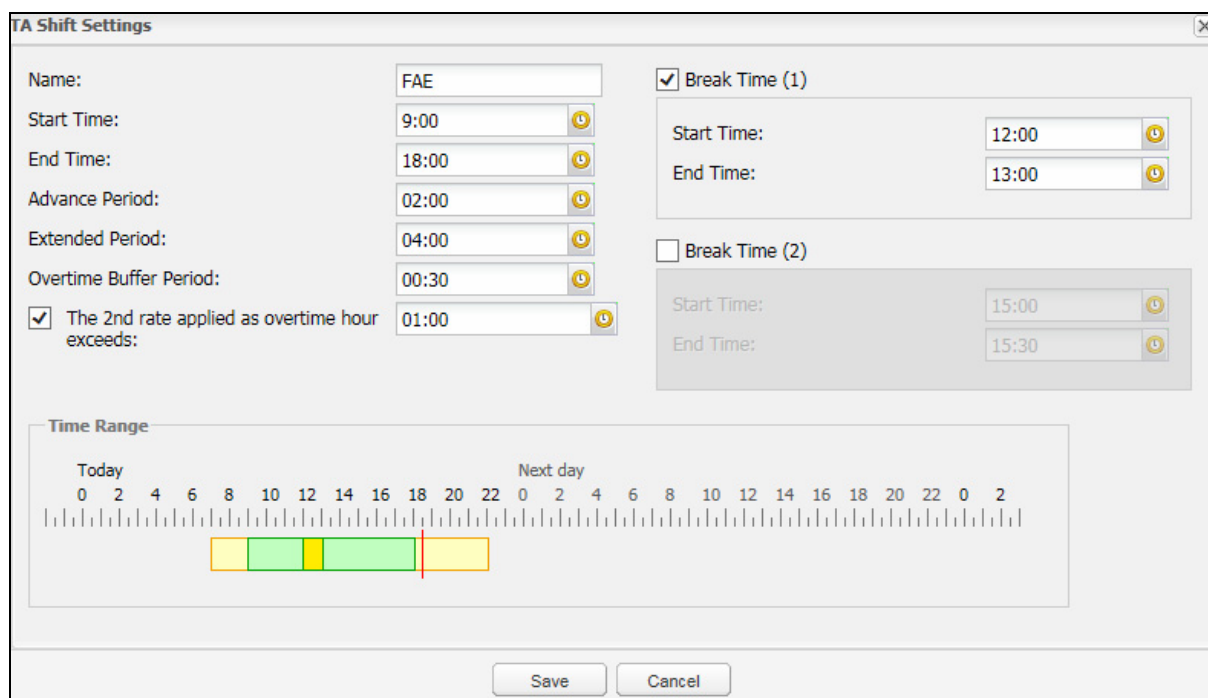


Figure 11-6

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 prior to the regular start time an employee can work. Employees arriving before the Advance Period will be recorded as working during Not Scheduled time in TA Record.
6. Specify an **Extended Period** to set the amount of time after the regular end time an employee can work and be counted toward overtime pay.
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 2<sup>nd</sup> 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 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 above figures as an example, an employee working 4 hours passed the 18:00 pm regular end time will receive overtime pay for 3.5 hours (18:30 ~ 22:00), while an employee working 20 minutes passed 18:00 will not receive overtime pay. The 2<sup>nd</sup> rate will be applied once the employee has worked passed 19:30, which is 1 hour after the Overtime Buffer Period.

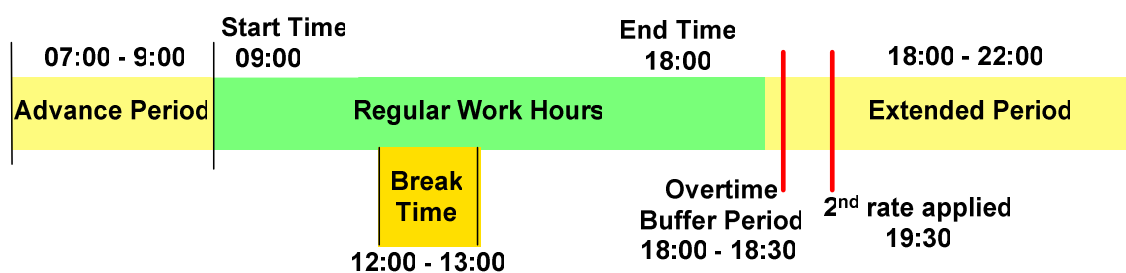


Figure 11-7

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.

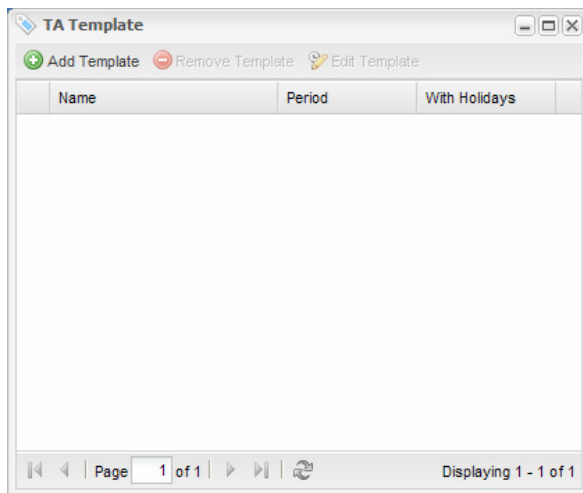


Figure 11-8

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

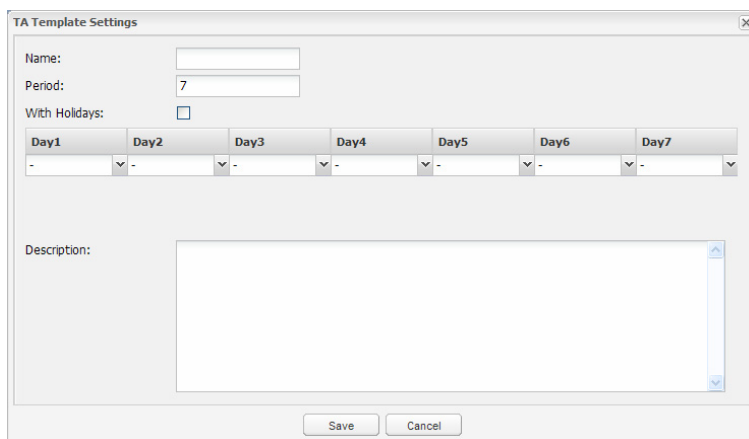
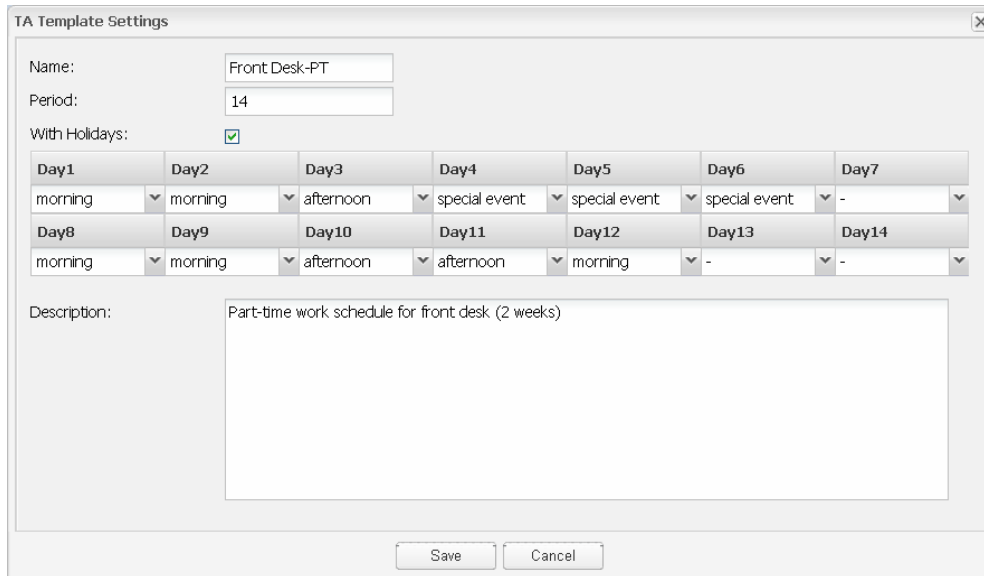


Figure 11-9

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.



TA Template Settings

Name: Front Desk-PT

Period: 14

With Holidays: ☒

Day1	Day2	Day3	Day4	Day5	Day6	Day7
morning	morning	afternoon	special event	special event	special event	-
Day8	Day9	Day10	Day11	Day12	Day13	Day14
morning	morning	afternoon	afternoon	morning	-	-

Description: Part-time work schedule for front desk (2 weeks)

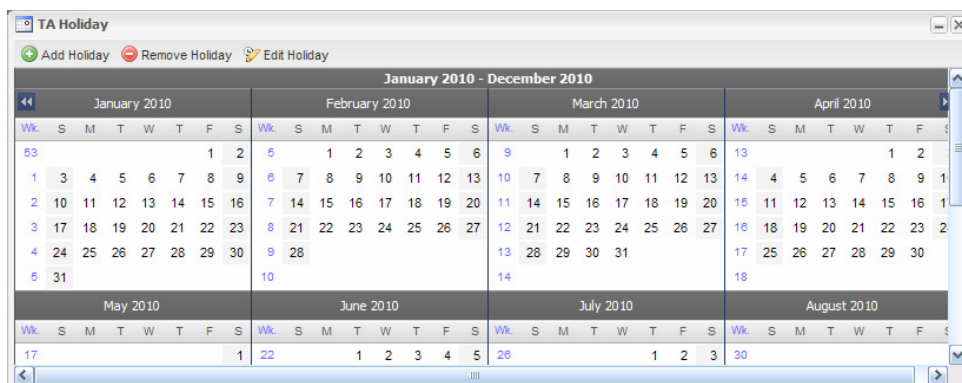
Save Cancel

Figure 11-10

- Click **Save**.

### 11.2.3 TA Holidays: Setting Certain Dates as Holidays

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



TA Holiday

+ Add Holiday - Remove Holiday Edit Holiday

January 2010 - December 2010

January 2010							February 2010							March 2010							April 2010											
Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S	Wk	S	M	T	W	T	F	S	
53							1	2	5	1	2	3	4	5	6	9	1	2	3	4	5	6	13	13	4	5	6	7	8	9	1	2
1	3	4	5	6	7	8	9	6	7	8	9	10	11	12	13	10	7	8	9	10	11	12	13	14	4	5	6	7	8	9	1	
2	10	11	12	13	14	15	16	7	14	15	16	17	18	19	20	11	14	15	16	17	18	19	20	15	11	12	13	14	15	16	1	
3	17	18	19	20	21	22	23	8	21	22	23	24	25	26	27	12	21	22	23	24	25	26	27	16	18	19	20	21	22	23	2	
4	24	25	26	27	28	29	30	9	28							13	28	29	30	31				17	25	26	27	28	29	30		
5	31							10								14								18								

May 2010 June 2010 July 2010 August 2010

17 1 22 1 2 3 4 5 26 1 2 3 30

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.

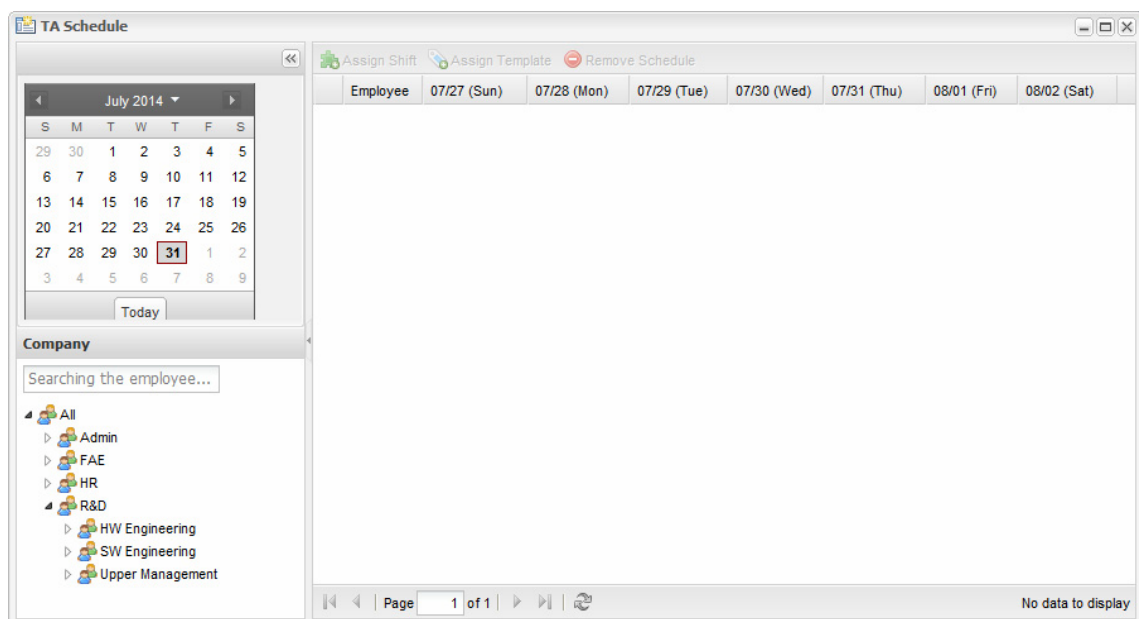
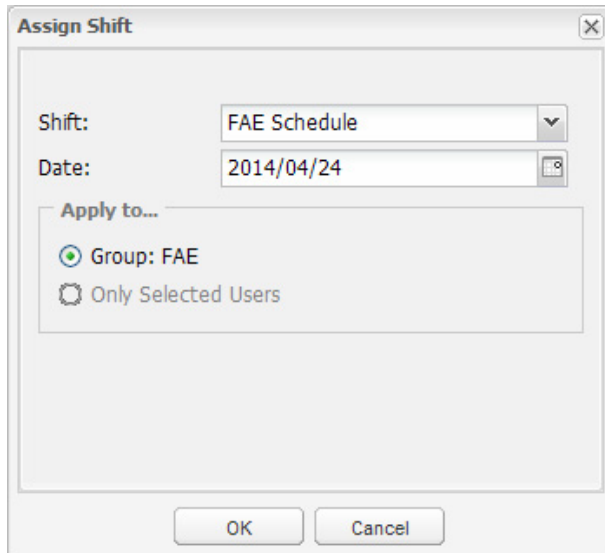


Figure 11-12

### To assign daily shift schedules day by day:

2. 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.

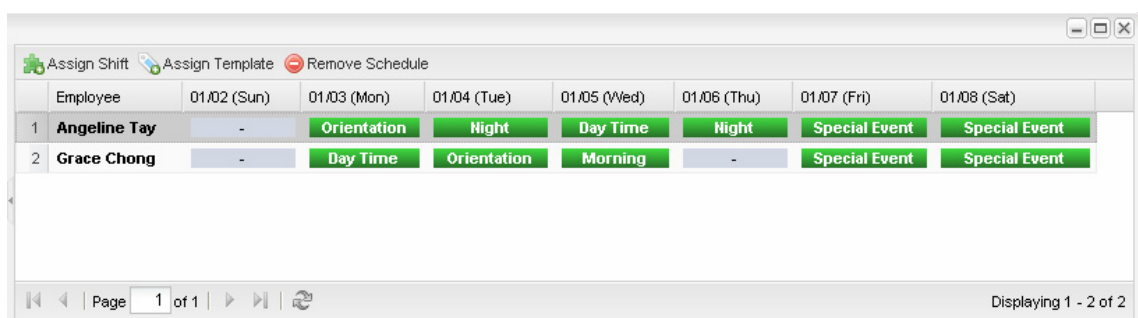


The 'Assign Shift' dialog box contains the following fields and options:

- Shift:** A dropdown menu showing 'FAE Schedule'.
- Date:** A text field showing '2014/04/24' with a calendar icon.
- Apply to...** section with two radio buttons:
  - ☒ Group: FAE
  - ☐ Only Selected Users
- Buttons:** 'OK' and 'Cancel' at the bottom.

Figure 11-13

3. Select a daily schedule and assign it to a date.
4. You can choose to apply the schedule to the entire group or only the selected users.
5. Repeat the steps for all the dates you want to schedule a shift.
6. 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.



The 'TA schedule window' displays a table of employee schedules. The table has columns for Employee, 01/02 (Sun), 01/03 (Mon), 01/04 (Tue), 01/05 (Wed), 01/06 (Thu), 01/07 (Fri), and 01/08 (Sat). The data is as follows:

	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

The window includes a toolbar with 'Assign Shift', 'Assign Template', and 'Remove Schedule' buttons. The status bar at the bottom shows 'Page 1 of 1' and 'Displaying 1 - 2 of 2'.

Figure 11-14

### To assign a schedule template:

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

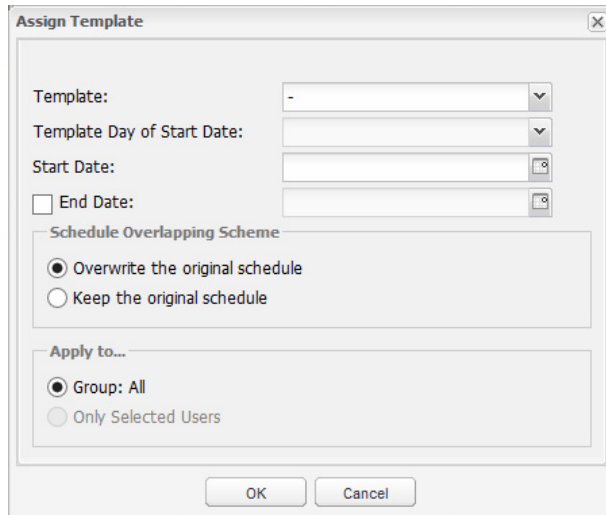


Figure 11-15

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

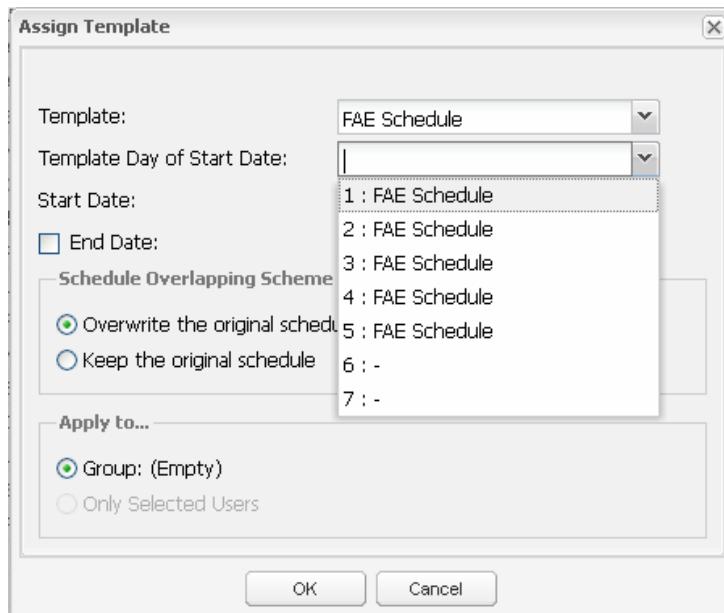


Figure 11-16

10. 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.

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.

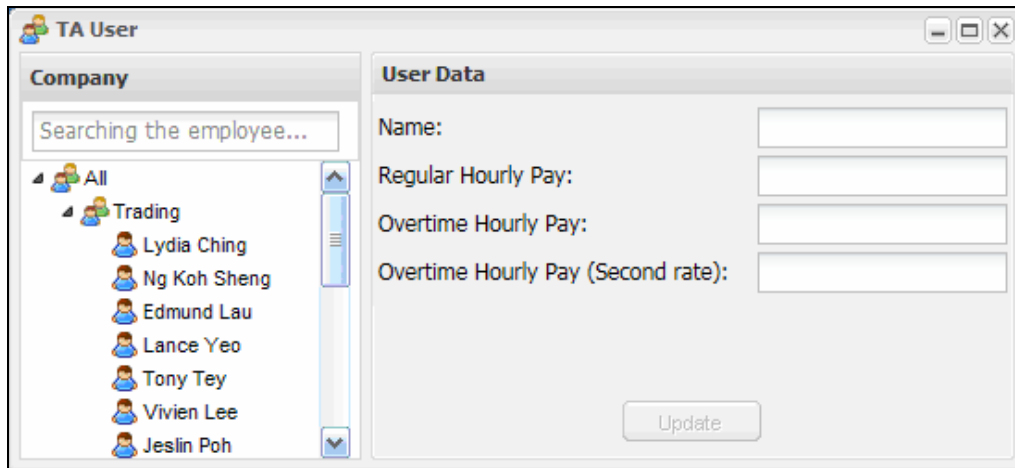


Figure 11-20

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. To see how to add, edit or delete users, refer to *4.6 Setting 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.

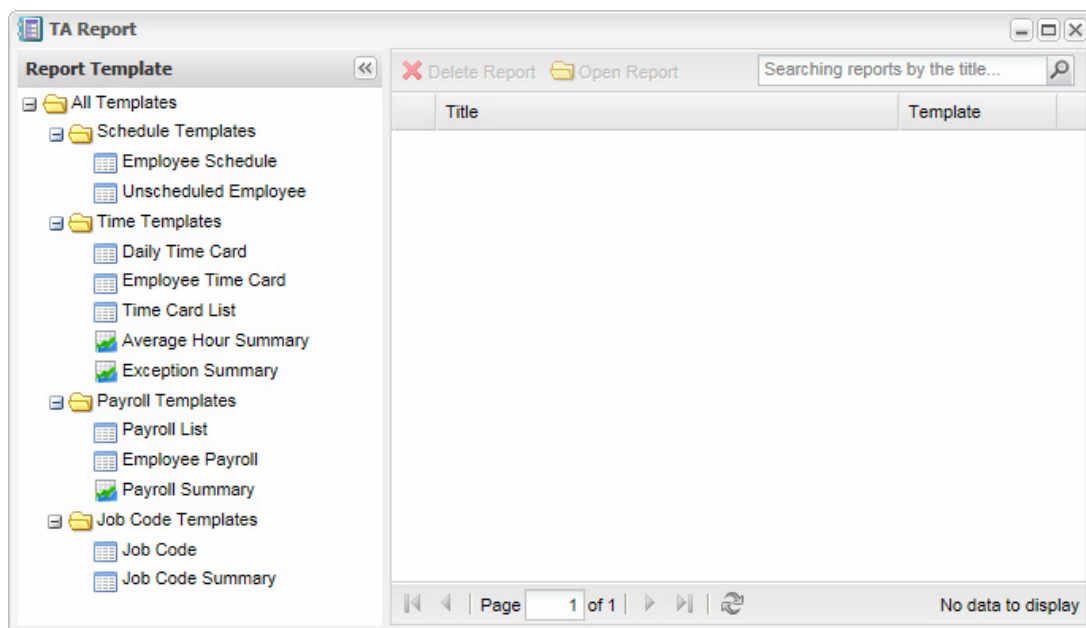


Figure 11-21

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

---

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

---

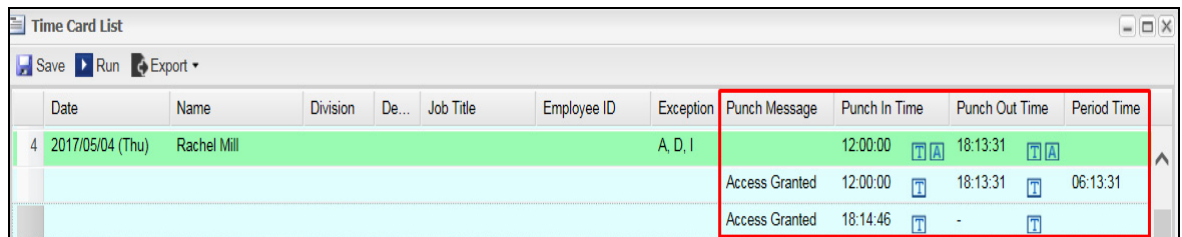
### [Schedule Templates]

- **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.
- **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.

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

The screenshot shows a 'Daily Time Card' dialog box. At the top, there are buttons for 'Save', 'Run', and 'Export'. Below these is a table with the following headers: Date, Name, Division, Department, Office, Job Title, Employee ID, Punch In Time, Punch Out Time, and Punch Out Time. The table body is empty. Below the table is a 'Report Settings' section. It contains the following fields: 'Title' (set to 'Daily Time Card'), 'Organization' (a dropdown menu showing '--- Select ---'), 'Date' (set to '2015/11/16'), and 'Calculation' (a dropdown menu showing 'Without direction'). Below these is an 'Exception' section with a grid of codes: A: In Late, B: In Early, C: Out Late, D: Out Early, E: Over Hours, F: Unscheduled Absence, G: Missed Punch, and H: Not Scheduled. At the bottom, there is a 'Description' field.

*Figure 11-23*

- Select the **Date** and **Organization** to look up the employees' scheduled shift and actual attendance record.
- 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 the 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	Curry	10:00	19:00	08:47	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.
8. 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		

Page 1 of 1

Displaying 1 - 14 of 14

Figure 11-25

9. 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.

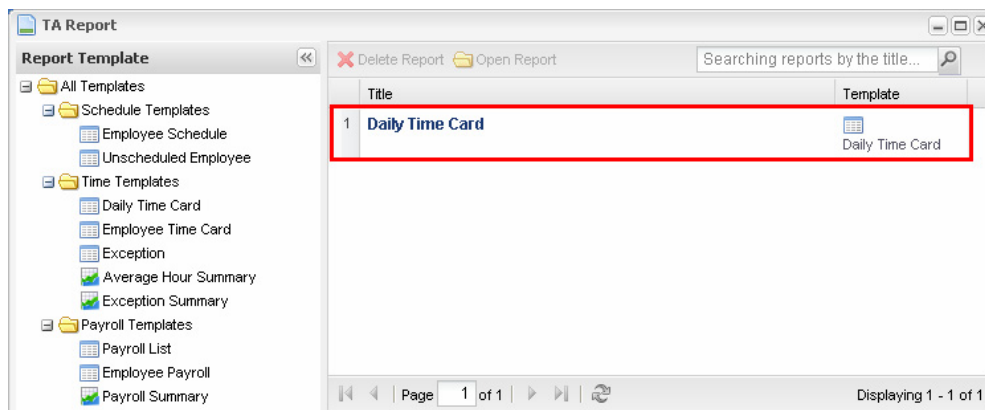


Figure 11-26

10. Click **Export** to export the data in excel (CSV), HTML or PDF format.
11. 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** and select **Operators**. A dialog box appears.

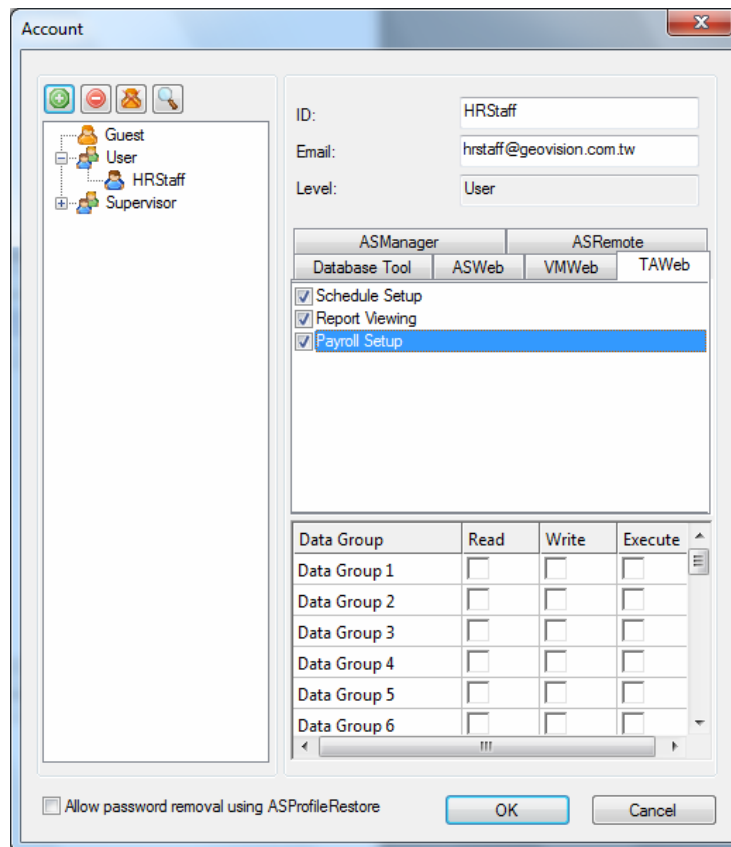


Figure 11-28

2. To create an account, click the **New** button in the bottom left corner.
3. Type the account's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
4. In the **Level** drop-down list, select **Supervisor** to have access to all GV-TAWeb functions. To grant limited access, select **User**. Click **OK**.
5. Click the **TAWeb** tab.
6. Select the privileges you want to grant. The following options are available.
  - **Schedule Setting:** Access TA Shift, TA Template and TA Schedule.
  - **Report viewing:** Access TA Report.
  - **Payroll settings:** Access TA User.
7. Click **OK**.



## Chapter 12 GV-VMWeb for Visitor Management

The GV-VMWeb is a visitor management system for internal business use where the administrator can create a visitor database and grant access to visitors on a LAN environment. GV-VMWeb can also be set up to allow visitors to register their own visitor account and create visit requests over the internet using the Visitor service.

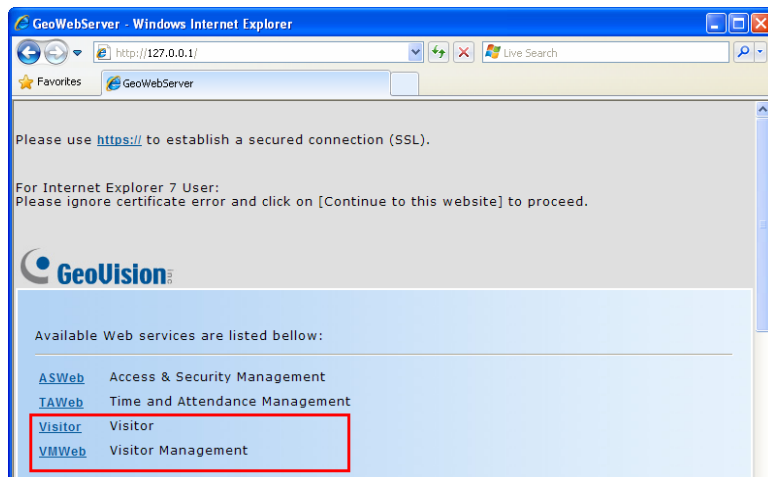


Figure 12-1

To use the GV-VMWeb, the browser in the client PC must be **Internet Explorer 9 or later**.

### 12.1 Connecting to GV-ASManager

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

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

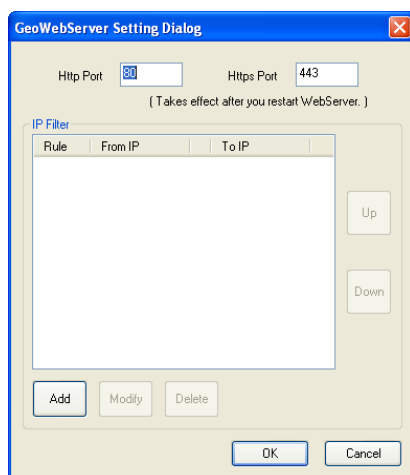



Figure 12-2

If you want to grant or deny the access from 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 of the main screen.

To start the GV-VMWeb:

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

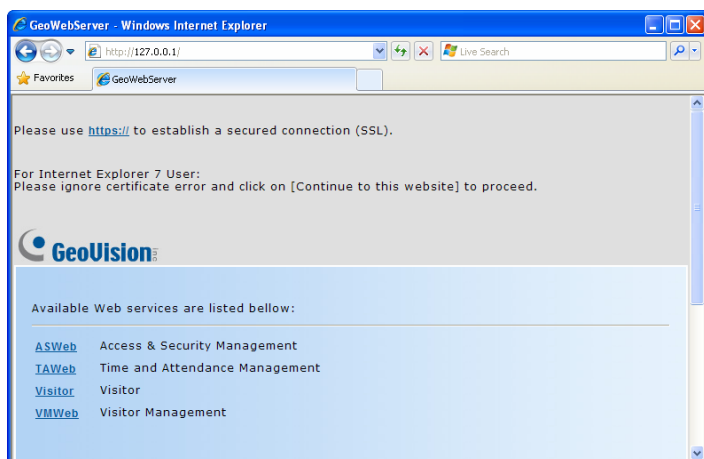


Figure 12-3

2. Click **https://** for SSL encrypted connection, or **VMWeb** for regular connection.
3. Enter a valid username and password for login. The GV-VMWeb page appears.

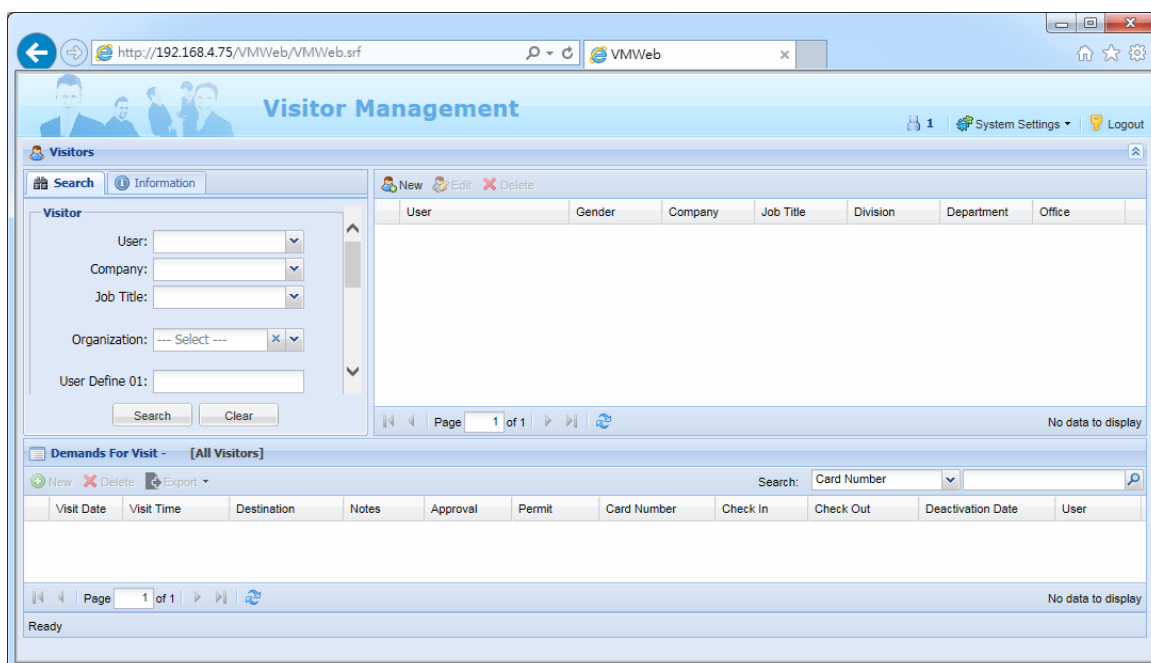
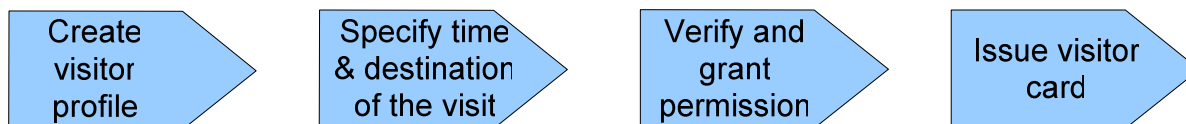


Figure 12-4

## 12.2 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 a visitor profile and a visit request for visitors, but the management staff needs to approve the visit and issue a card to the visitor before the visitor can be granted access.

---

**Note:** You need to create a visitor card before you can issue a card to a visitor. To see how to add a visitor card, refer to [4.3 Adding Cards](#).

---

To create accounts:

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

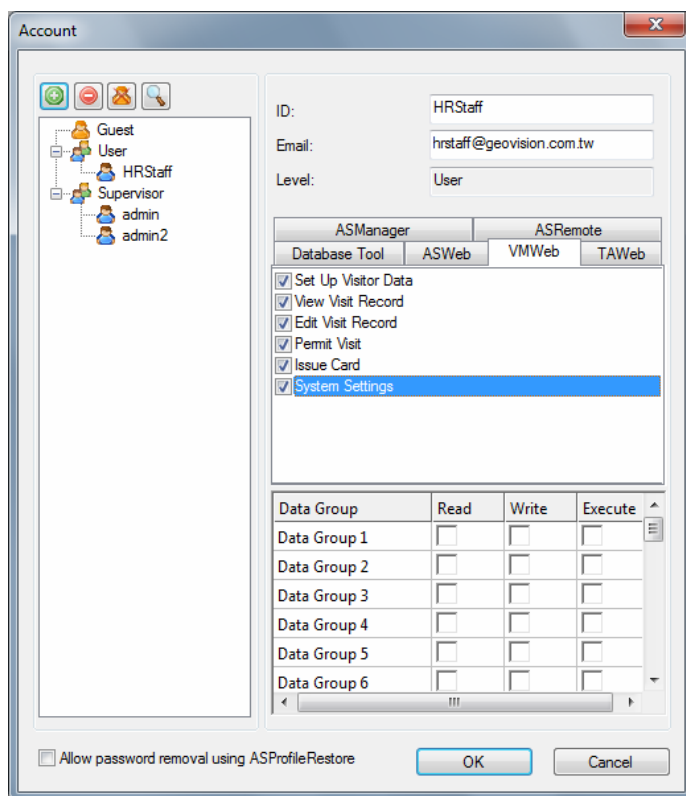
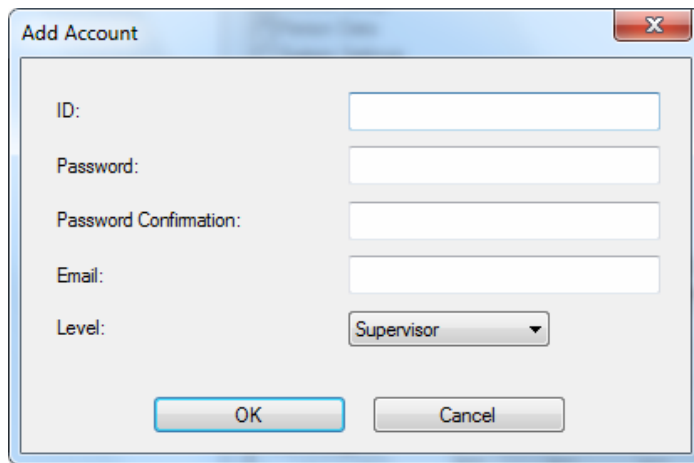



Figure 12-5

- To create an account, click the **New** button in the bottom left corner. This dialog box appears.



The image shows a Windows-style dialog box titled "Add Account". It has a standard title bar with a close button (X) in the top right corner. The dialog contains five input fields arranged vertically: "ID:", "Password:", "Password Confirmation:", "Email:", and "Level:". The "Level:" field is a drop-down menu currently showing "Supervisor". At the bottom of the dialog are two buttons: "OK" and "Cancel".

Figure 12-6

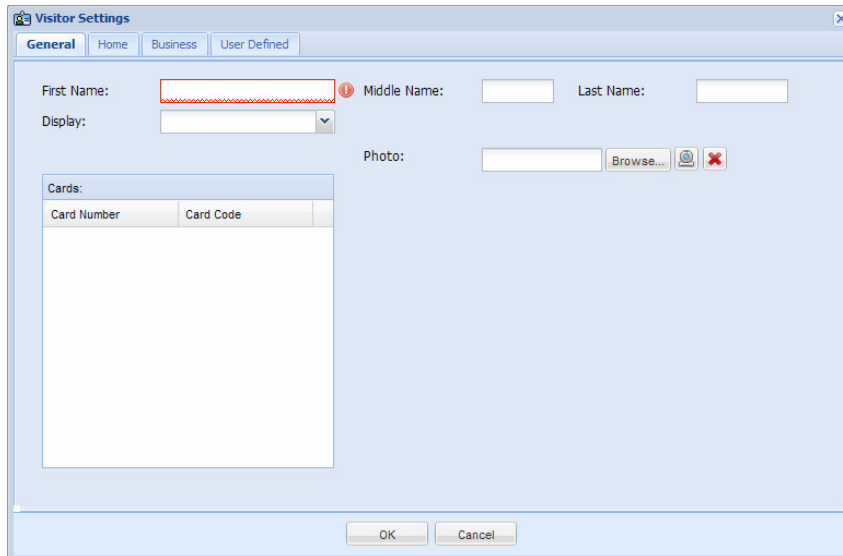
- Type the Supervisor's **ID** and **Password**. Re-type the password in the **Password Confirmation** field.
- In the **Level** drop-down list, select **Supervisor** to have access to all GV-VMWeb functions. Click **OK**. To grant limited access, select **User** and click **OK**.
- Click the **VMWeb** tab.
- Select the privileges you want to grant. The following options are available.
  - **Set Up Visitor Data:** Create or edit visitor profiles.
  - **View Visit Record:** Look up visit records in the past for each visitor.
  - **Edit Visit Record:** Create or edit visits in GV-VMWeb.
  - **Approve Visit:** Record the name of the account that approved the visit request.
  - **Permit Visit:** Grant permission to allow the visit in GV-VMWeb.
  - **Issue Card:** Assign a card to the visitor in GV-VMWeb. The Verify privilege must also be allowed for the account to have access to this option.
  - **System Settings:** Enable the Auto-Verify option under **Setting** drop-down list .
- Click **OK**.

## 12.3 Creating Visitor Profile

GV-VMWeb allows you to create visitors profile and grant different access to each visitor.

To create a visitor account:


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



The image shows a 'Visitor Settings' dialog box with four tabs: 'General', 'Home', 'Business', and 'User Defined'. The 'General' tab is active. It contains fields for 'First Name', 'Middle Name', and 'Last Name'. There is a red dashed border around the 'First Name' field and a red error icon to its right. Below these is a 'Display' dropdown menu. To the right is a 'Photo' field with a 'Browse...' button and icons for webcam and delete. At the bottom left is a 'Cards' section with a table header 'Card Number' and 'Card Code'. At the bottom are 'OK' and 'Cancel' buttons.

Card Number	Card Code
-------------	-----------

Figure 12-7

2. In the **General** tab, you can type the name of the visitor and click **Browse** to upload a photo of the visitor. If you have a webcam installed, click the **Webcam** icon  to take a picture from the webcam for the visitor profile. Any valid card number and card code for the visitor will be displayed under the **Cards** section.
3. In the **Home** and **Business** tab, you can fill out other personal information about the visitor, such as phone number, address, birthday and gender.
4. In the **User Defined** tab, customized field labels will be displayed. To see how to customize the fields, see *4.6.2 Customizing a Data Field*.
5. Click **OK** to save the visitor information.

---

### Note:

1. The visitor profile created will be updated to the User List in GV-ASManager.
  2. The webcam function requires Flash Player 10 or later.
-

## 12.4 Granting Visitor Access

After the visitor's account is created, access permission can be granted to visitors using the **Demand for Visits** section. In this section, you can specify the date and time of the visit, assign an access card to the visitor and view visit record.

1. Select the visitor account in the Visitors section and click the **New** button in the Demands for Visit section.

Figure 12-8

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. Under **Approval**, the account that permitted the access will automatically be recorded after permission is granted.
5. Select the **Permit** checkbox to grant access permission.
6. Click the **Card Number** drop-down list. This dialog box appears.

	Card Number	Card Type	Card Status	Activation Date
1	123-45678	Visitor	Active	11/11/2015
2	234-56789	Visitor	Active	11/11/2015
3	123-45687	Visitor	Active	11/11/2015

Setting


Deactivation: All Day

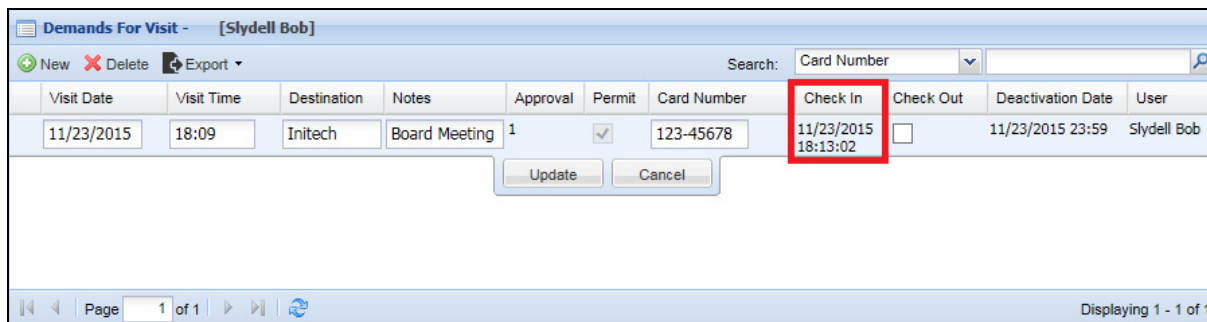
Date: 11/18/2015

Time: 23:59

Figure 12-9

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

7. Select a visitor card to assign to the visitor and use the **Deactivation** drop-down list to specify when the card will be deactivated. You can click the **Add** button  to create a new visitor card if needed.
8. Click the **Update** button to continue editing the Demand for Visit entry.
9. The **Check-In** time is the time when the Demand for Visit entry is created. After the visitor has returned the visitor card, you can return to this visit record and select the **Check-Out** checkbox to check out the card. You can also choose to automatically check out the visitor card when the visitor presents the card at an exit door. Refer to *Step 2: Configuring the Doors or Elevator Floors* in Chapter 4 to see how to set up automatic check out.



The screenshot shows a web application window titled "Demands For Visit - [Slydell Bob]". It features a search bar with "Card Number" selected. Below the search bar is a table with the following columns: Visit Date, Visit Time, Destination, Notes, Approval, Permit, Card Number, Check In, Check Out, Deactivation Date, and User. A single row of data is displayed, with the "Check In" field highlighted by a red rectangular box. Below the table are "Update" and "Cancel" buttons. At the bottom of the window, there is a pagination bar showing "Page 1 of 1" and a status bar indicating "Displaying 1 - 1 of 1".

Visit Date	Visit Time	Destination	Notes	Approval	Permit	Card Number	Check In	Check Out	Deactivation Date	User
11/23/2015	18:09	Initech	Board Meeting	1	<input checked="" type="checkbox"/>	123-45678	11/23/2015 18:13:02	<input type="checkbox"/>	11/23/2015 23:59	Slydell Bob

Figure 12-10

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

## 12.5 Searching GV-VMWeb Database

To search for visitors with certain criteria, type the visitor's information in the **Filter** section on the left and click the **Search** button. The search results will be listed in the **Visitors** section. You can also search visit records from the past by using the **Search** function under Demands For Visit section. Use the drop-down list to search by Card Number, Destination, Notes, User or the person who approved the visit.

The screenshot displays the GV-VMWeb interface. On the left, the 'Visitors' section contains a search filter with the following fields: User (dropdown), Company (dropdown), Job Title (dropdown), Organization (dropdown with '--- Select ---'), User Define 01 (text input), and User Define 02 (text input). A 'Search' button and a 'Clear' button are at the bottom of this section. On the right, the 'Demands For Visit' section for user 'G Peter' shows a search dropdown menu with options: Card Number, Card Number, Destination, Notes, User, and Approval. Below this, a table lists visitors:

	User	Gender	Company	Job Title	Division	Departm...	Office
1	Slydell Bob	Female	-	-	-	-	-
2	G Peter	Female	-	-	-	-	-

At the bottom of the 'Demands For Visit' section, a table with columns: Visit Date, Visit Time, Destination, Notes, Approval, Permit, Card Number, Deactivation Date, and User is shown. The status 'No data to display' is at the bottom right.

Figure 12-11

## 12.6 Visitor Self Registration

Visitors can create a visitor account over the Internet and request permission to access the premise.

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 will show up in GV-VMWeb for the administrator to grant or deny access.





## 12.6.1 Setting Up Mail Server in GV-VMWeb

The administrator must first set up the mail server in GV-VMWeb. The mail server will be used to send a confirmation e-mail to the visitor when they register an account.

1. Open an Internet browser, and type the IP address of the GV-ASManager to be connected.
2. Click **https://** and then **VMWeb** for SSL encrypted connection, or **VMWeb** for regular connection.
3. Enter a valid username and password for login. The GV-VMWeb page appears.
4. In the top-right corner, click **System Settings** and select **Visitor Web**.

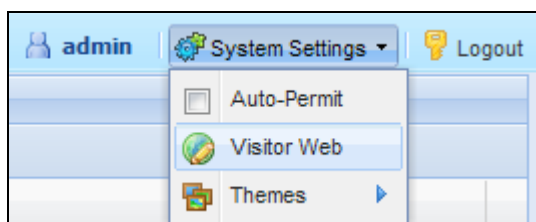
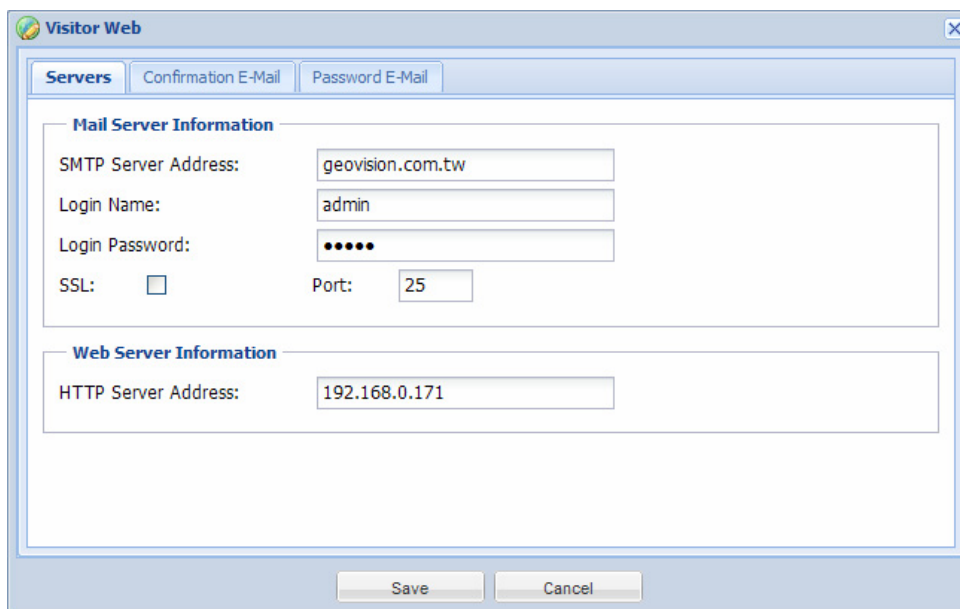


Figure 12-12

5. Under the Servers tab, set up the mail server.

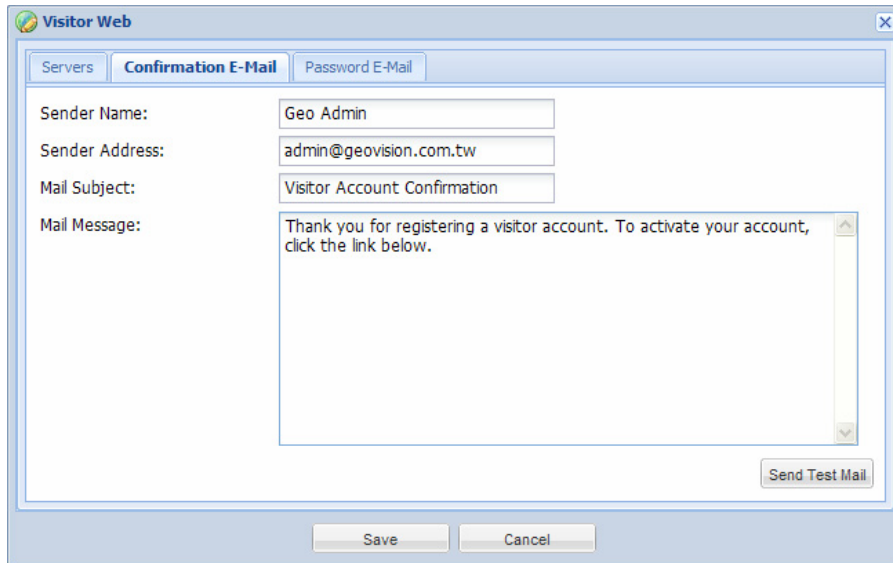


The screenshot shows the 'Visitor Web' configuration window with the 'Servers' tab selected. It contains two sections: 'Mail Server Information' and 'Web Server Information'. The 'Mail Server Information' section has fields for 'SMTP Server Address' (geovision.com.tw), 'Login Name' (admin), 'Login Password' (masked with dots), 'SSL' (unchecked), and 'Port' (25). The 'Web Server Information' section has a field for 'HTTP Server Address' (192.168.0.171). At the bottom are 'Save' and 'Cancel' buttons.

Figure 12-13

- **SMTP Server Address:** Type your mail server's URL address or IP address.
- **Login Name / Password:** Type the login name and password of the mail server.
- **SSL:** Select SSL if your e-mail server requires the SSL authentication for connection.

- **Port:** Keep the default port 25 or type a new port number for webmail providers that may use different SMTP port such as Yahoo and Hotmail.
  - **HTTP Server Address:** Type the IP address or the domain name of the GV-ASManager.
6. Click the **Confirmation E-Mail** tab and type the **Sender Name**, **Sender Address**, **Mail Subject** and **Mail Message**. 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.



The screenshot shows a window titled "Visitor Web" with three tabs: "Servers", "Confirmation E-Mail", and "Password E-Mail". The "Confirmation E-Mail" tab is selected. It contains the following fields:

- Sender Name:** Geo Admin
- Sender Address:** admin@geovision.com.tw
- Mail Subject:** Visitor Account Confirmation
- Mail Message:** Thank you for registering a visitor account. To activate your account, click the link below.

At the bottom right of the form is a "Send Test Mail" button. At the bottom of the window are "Save" and "Cancel" buttons.

Figure 12-14

7. Click the **Password E-Mail** tab and fill out the information. The visitor will be able to retrieve a forgotten password by clicking the "Forgot your password?" link at the login page. An e-mail with the password will be sent to the visitor.

## 12.6.2 Creating a Visitor Account

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

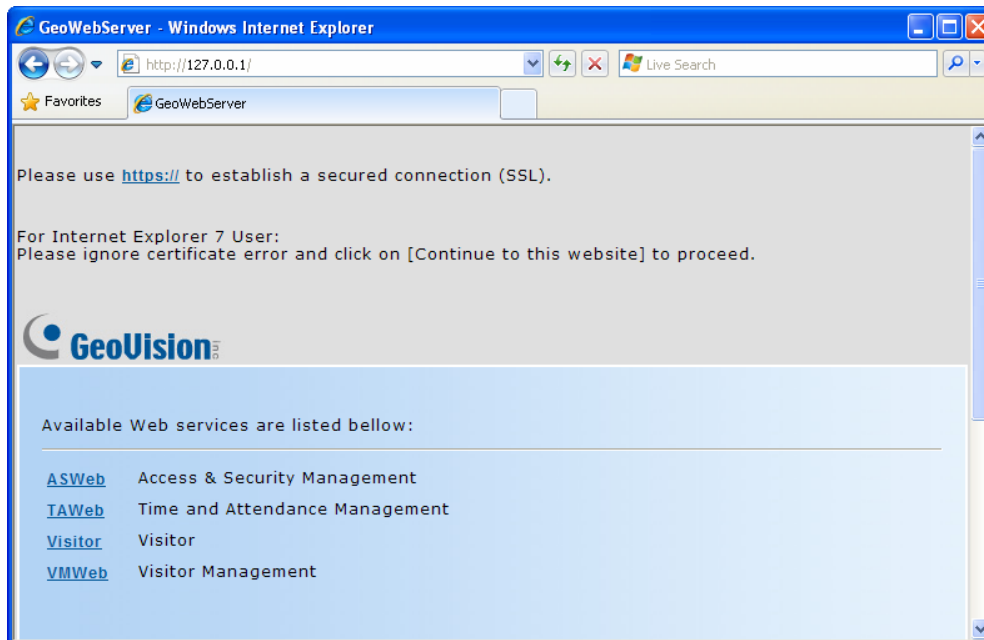


Figure 12-15

2. Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** directly for regular connection. The Visitor Login page appears.

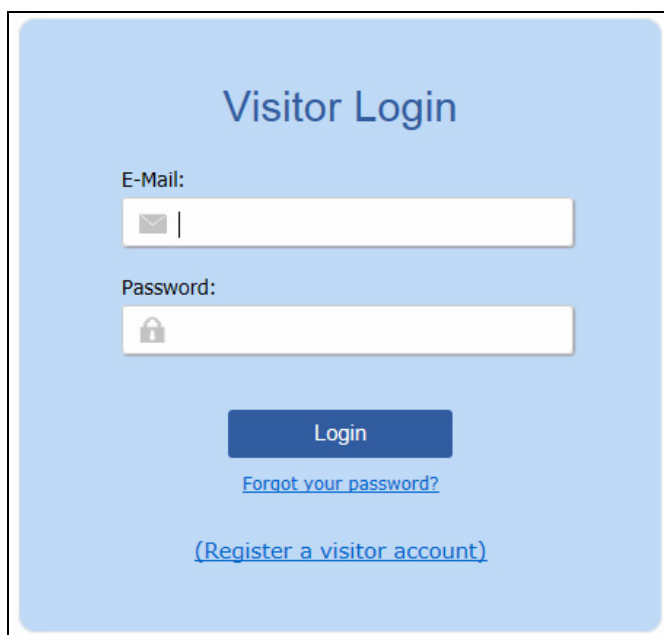


Figure 12-16

- Click **Register a Visitor Account**. This window appears.

Figure 12-17

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

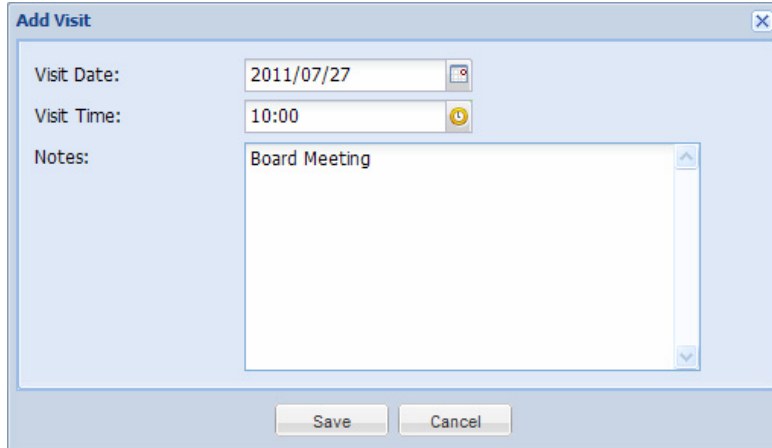
### 12.6.3 Creating a Visit Request

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

- Open an Internet browser, and type the IP address of the GV-ASManager to be connected. A web page appears.
- Click **https://** and then **Visitor** for SSL encrypted connection, or **Visitor** directly for regular connection. The Visitor Login page appears.
- Type the visitor account and password, and click **Login**. This window appears.

Figure 12-18

4. Click the **Visitor Setting** button to complete the visitor profile. Refer to *Creating Visitor Profile* earlier this chapter for more details.
5. Click the **Add Visit** button. This dialog box appears.



The 'Add Visit' dialog box contains the following fields:

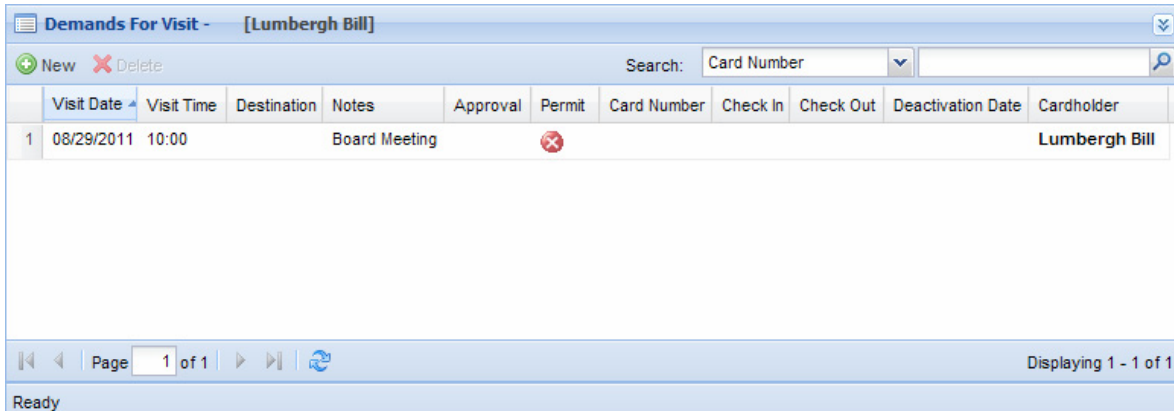
- Visit Date:** 2011/07/27
- Visit Time:** 10:00
- Notes:** Board Meeting

At the bottom are 'Save' and 'Cancel' buttons.

*Figure 12-19*

6. Specify the planned visit date and time.
7. Click **Save**.

When the administrator logs into GV-VMWeb, he or she can click the visitor's name to see the visit request submitted.



The window title is 'Demands For Visit - [Lumbergh Bill]'. It includes a search bar with 'Card Number' and a search icon. Below the search bar is a table with the following data:

	Visit Date	Visit Time	Destination	Notes	Approval	Permit	Card Number	Check In	Check Out	Deactivation Date	Cardholder
1	08/29/2011	10:00		Board Meeting							Lumbergh Bill

At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying 1 - 1 of 1'.

*Figure 12-20*

The administrator can double-click the visit request to grant access and assign visitor card to the visitor.

## Chapter 13 License Plate Recognition

The License Plate Recognition functions allow GV-LPR1200, GV-DSP LPR, GV-DVR LPR and GV-VMS LPR to grant access when the detected license plate numbers match the vehicle registered in GV-ASManager's database. GV-ASManager can connect with up to 255 GV-LPR1200, GV-DSP LPR, GV-DVR LPR and / or GV-VMS LPR, which can recognize license plates detected in the connected cameras.

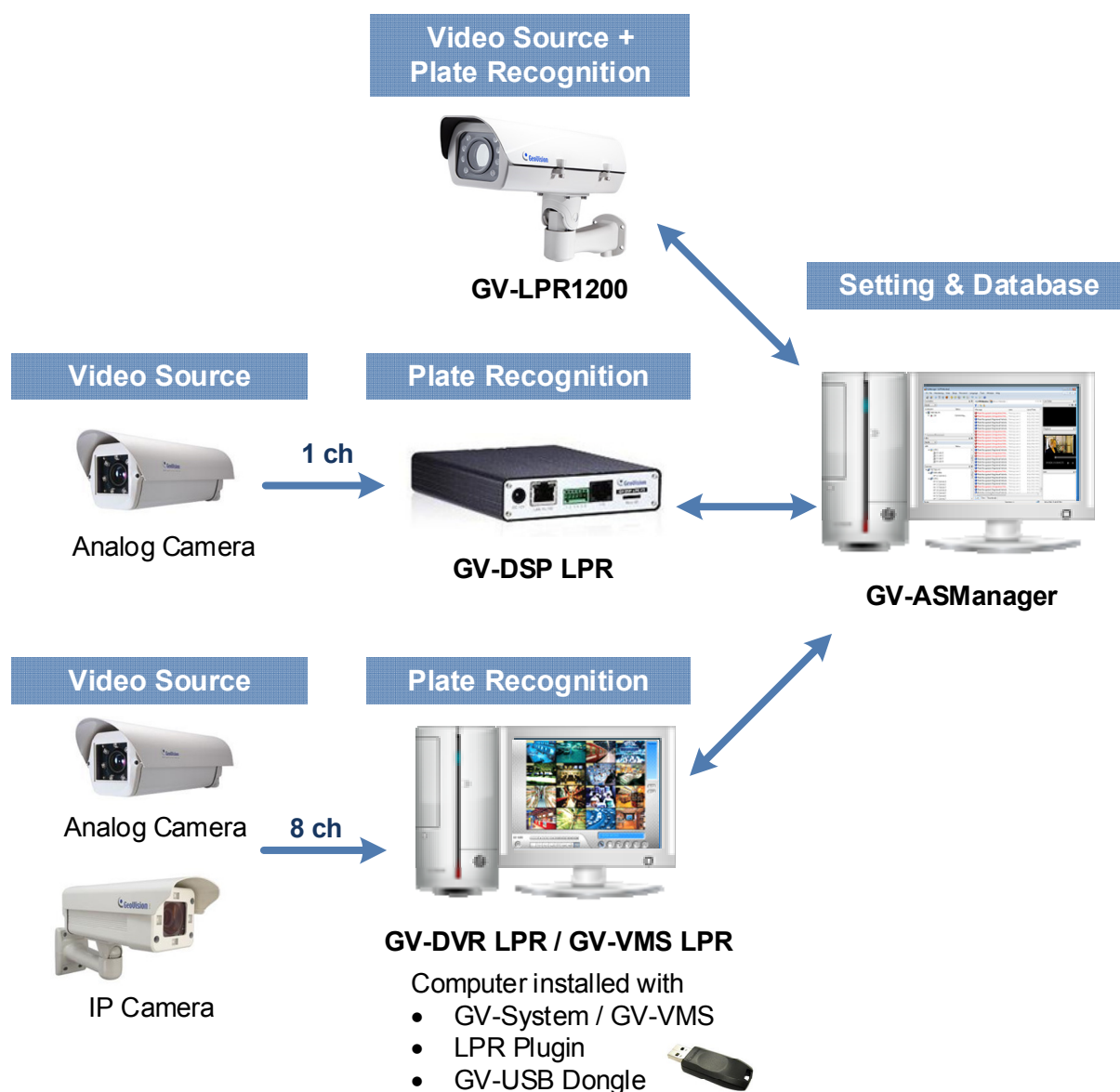


Figure 13-1

## Main Screen

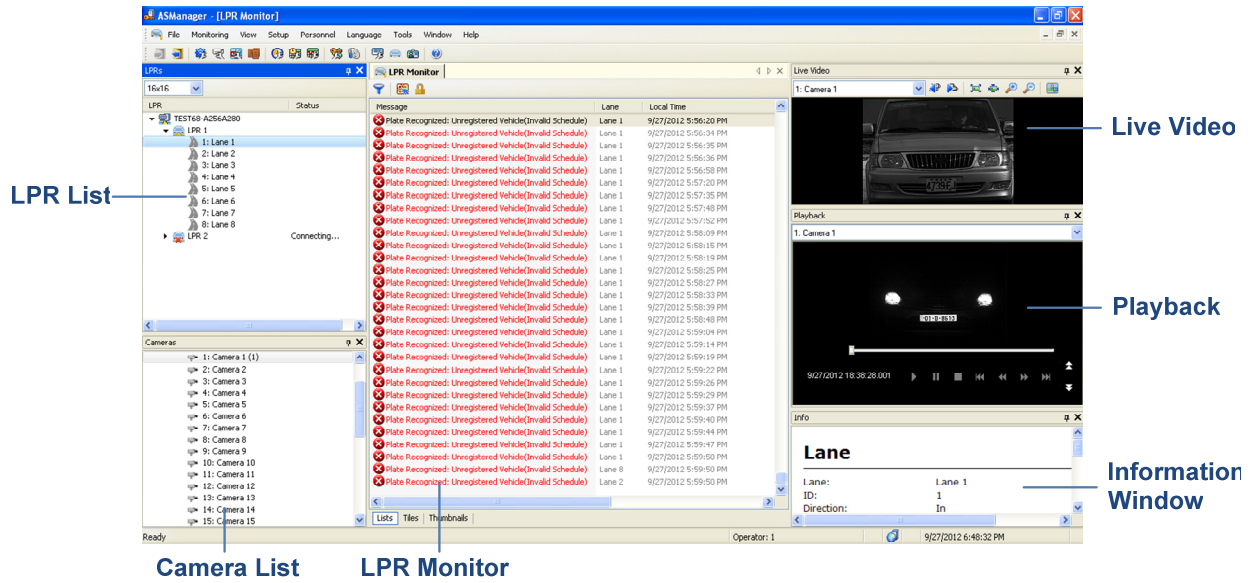


Figure 13-2

## 13.1 Installing PC LPR

A GV-DVR / NVR or GV-VMS can be turned into a GV-DVR LPR / GV-VMS LPR simply by installing the LPR Plugin from the GeoVision Website and by inserting an LPR Dongle.

---

**Note:** Refer to *Appendix E. Supported Recognition Engines of PC LPR* to see the recognition engines supported.

---

### 13.1.1 System Requirements

Depending on the resolution settings and the number of channels, you will need different CPU capacity. Before setting up GV-DVR LPR / GV-VMS LPR, make sure the PC meets the minimum system requirements.

#### GV-DVR LPR

Number of Channels		1-4 Channels	5-8 Channels
OS		64-bit Windows 7 / 8 / 8.1 / 10 / Server 2008 R2 / Server 2012 R2	
CPU	1.3 MP	Core i5 2400, 3.1 GHz	Core i7 2600, 3.4 GHz
	2 MP	Core i7 4770, 3.4 GHz	Core i7 6700, 3.4 GHz
Memory		2 x 2 GB Dual Channels	
Hard Disk		500 GB	
VGA		PCI-Express, 1280 x 1024 , 32-bit color and support DirectX 10c	
DirectX		End-User Runtimes (November 2008)	
GV-DVR / NVR		<b>GV-ASManager V4.2.1 - V4.2.3:</b> V8.5.9.0 <b>GV-ASManager V4.3:</b> V8.6.0.0 <b>GV-ASManager V4.3.5 - V4.4:</b> V8.6.2.0 <b>GV-ASManager V4.4.1:</b> V8.6.2.0 or V8.7.0.0 <b>GV-ASManager V4.4.2:</b> V8.7.0.0 or V8.7.1.0 <b>GV-ASManager V4.4.3:</b> V8.7.1.0 <b>GV-ASManager V5.0:</b> V8.7.1.0 <b>GV-ASManager V5.0.1.0 – V5.0.2.0:</b> V8.7.3.0	

**Note:** The above system requirements were determined with a bit rate of 2 Mbits for 1.3 MP resolution and 2 MP resolution.



### GV-VMS LPR (for 32 CH)

Number of Channels		1-4 Channels	5-8 Channels
OS		64-bit Windows 7 / 8 / 8.1 / 10 / Server 2008 R2 / Server 2012 R2	
CPU	1.3 MP	Core i7 3770, 3.4 GHz	Core i7 4770, 3.4 GHz
	2 MP		
Memory		2 x 2 GB Dual Channels	
Hard Disk		500 GB	
VGA		PCI-Express, 1280 x 1024 , 32-bit color and support DirectX 10c	
DirectX		End-User Runtimes (November 2008)	
GV-VMS		<b>GV-ASManager V4.3.5 – V4.4.1:</b> V15.10.1.0 <b>GV-ASManager V4.4.2:</b> V15.10 or V15.11 <b>GV-ASManager V4.4.3:</b> V15.11.3 <b>GV-ASManager V5.0.0.0:</b> V16.10.3.0 <b>GV-ASManager V5.0.1.0 – V5.0.2.0:</b> V16.11.0.0	
<b>Note:</b> The above system requirements were determined with a bit rate of 2 Mbits for 1.3 MP resolution and 2 MP resolution.			

### GV-VMS LPR (for 64 CH)


Number of Channels		1-4 Channels	5-8 Channels
OS		64-bit Windows 7 / 8 / 8.1 / 10 / Server 2008 R2 / Server 2012 R2	
CPU	1.3 MP	Core i7 6770, 3.4 GHz (Only 2 Lanes)	N/A
	2 MP	Core i7 6700, 3.4 Ghz (Only 1 Lane)	
Memory		2 x 2 GB Dual Channels	
Hard Disk		500 GB	
VGA		PCI-Express, 1280 x 1024 , 32-bit color and support DirectX 10c	
DirectX		End-User Runtimes (November 2008)	
GV-VMS		<b>GV-ASManager V4.3.5 – V4.4.1:</b> V15.10.1.0 <b>GV-ASManager V4.4.2:</b> V15.10 or V15.11 <b>GV-ASManager V4.4.3:</b> V15.11.3 <b>GV-ASManager V5.0:</b> V16.10.3.0 <b>GV-ASManager V5.0.1.0 – V5.0.2.0:</b> V16.11.0.0	
<b>Note:</b> The above system requirements were determined with a bit rate of 2 Mbits for 1.3 MP resolution and 2 MP resolution.			

**Note:**

1. It is recommended to use separate PCs for GV-ASManager and GV-DVR LPR / GV-VMS LPR.
2. 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.
3. The total number of recognition cameras and overview cameras connected per GV-DVR / NVR / VMS cannot exceed 16 cameras.

### 13.1.2 Installing LPR Plugin

#### Downloading from GeoVision Website

1. Go to the Software Download and Upgrading page of GeoVision Website:  
<http://www.geovision.com.tw/download/product/GV-LPR>
2. Select **Primary Applications** from the drop-down list, and
3. Click the **Download** icon  of **GV-LPR Plugin**.





Show	50	entries	Primary Applications	
Type	Title	Ver.	Size	Download
	GV-ASManager	V4.4.3.0	390MB	
	GV-LPR Plugin (for GV-DVR/NVR V8.7.0.0 & GV-VMS V15.10.0.0)	V4.4.2.0	25.9MB	

Figure 13-3

### 13.1.3 Inserting LPR Dongle

To see recognition results, an LPR Dongle needs to be inserted to the computer of the GV-DVR / NVR / VMS. 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 Dongle are supported:

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

---

#### Note:

1. 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.
  2. If no LPR dongle is inserted, license plates will be captured but the plate numbers will not be recognized.
-

### 13.1.4 Accessing Recognition Results on 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 the GV-DVR / NVR / VMS 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.

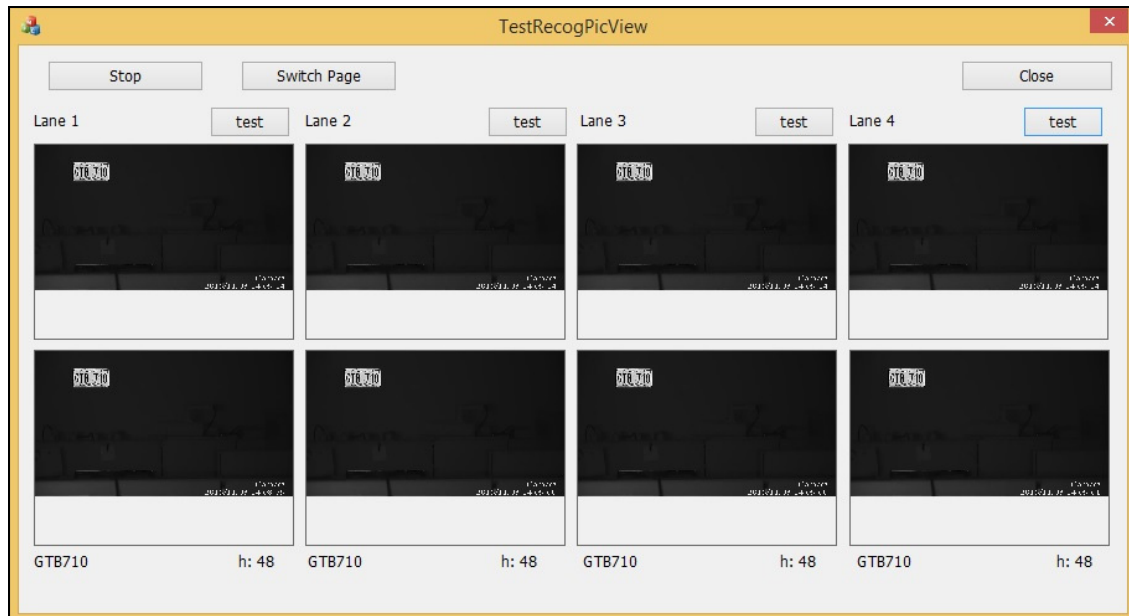


Figure 13-4

2. To see the results from channels 5 to 8, click **Switch Page** to switch to page 2.
3. To manually force the GV-DVR LPR / GV-VMS LPR to detect license plates, click the **Test** buttons.

## 13.2 Setting Up PC LPR

To set up GV-DVR LPR / GV-VMS LPR, follow the requirements listed in *13.1 Installing GV-DVR LPR / GV-VMS LPR* and then follow the steps below:

- **Step 1 Enabling LPR Functions on GV-DVR LPR / GV-VMS LPR**

Enable the recognition cameras and/or the overview cameras on GV-DVR LPR / GV-VMS LPR.

- **Step 2 Adding GV-DVR LPR to GV-ASManager**

Establish the communication between GV-ASManager and GV-DVR LPR / GV-VMS LPR.

- **Step 3 Configuring a Channel**

Set up the related cameras and the recognition conditions of the channel.

---

**Note:** For optimal results, the recognition cameras should be cameras specialized for license plate recognition, such as GeoVision's LPR Camera Series. For more information, visit GeoVision's website at: <http://www.geovision.com.tw/products.php?c2=124>

---

### 13.2.1 Step 1: Enabling LPR Functions on PC LPR

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

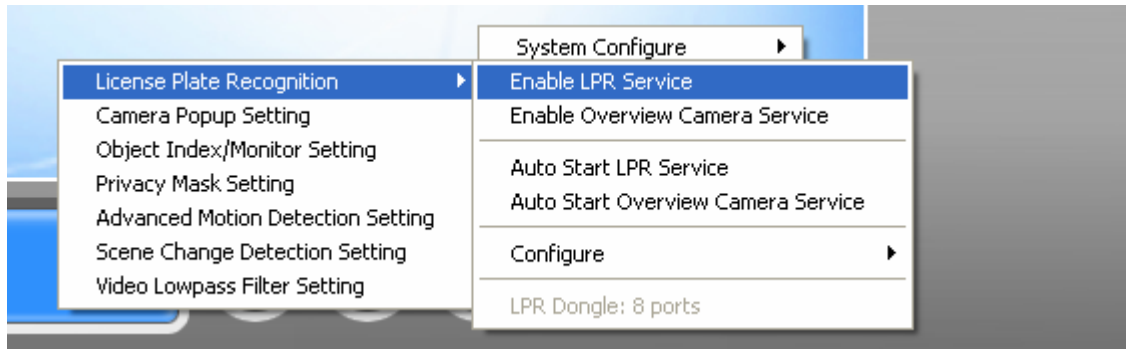





Figure 13-5

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

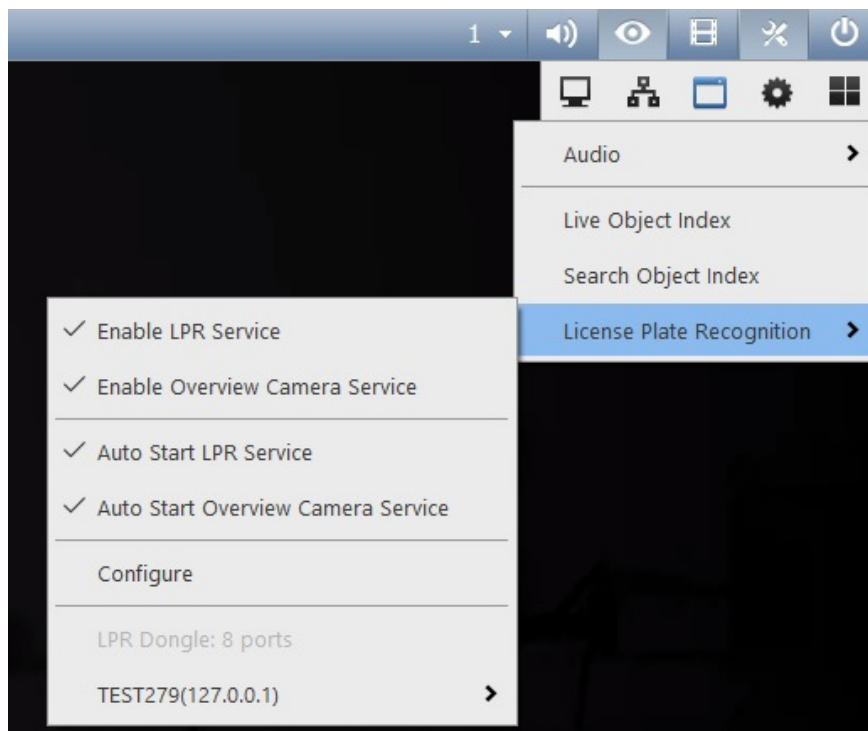


Figure 13-6

- **Enable LPR Service:** Enable recognition of license plates detected in the Recognition Camera.
- **Enable Overview Camera Service:** Allow GV-ASManager to use cameras connected to the GV-DVR/ NVR / VMS as overview camera.

- **Auto Start LPR Service:** Automatically start LPR Service at GV-DVR / NVR / VMS startup.
- **Auto Start Overview Camera Service:** Automatically start Overview Camera Service at GV-DVR / NVR / VMS startup.
- **Configure:** Allows you to export LPR data. See *Exporting LPR Data* section below.

---

**Note:** Make sure the LPR dongle is inserted to the computer of the GV-DVR / NVR / VMS.

---

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

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

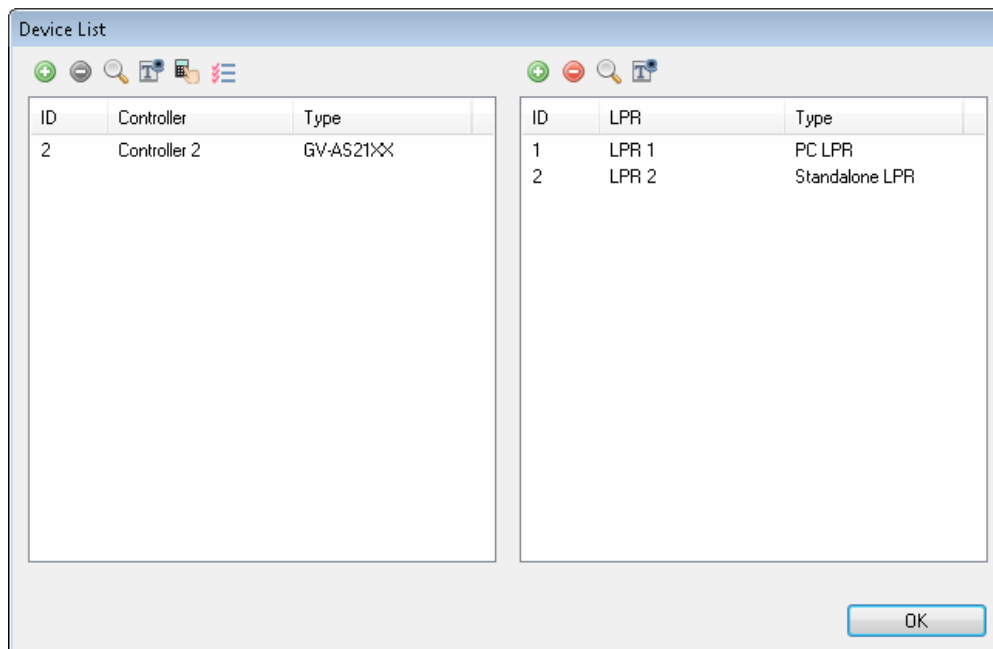


Figure 13-7

---

**Note:** You can also click the **Search** button  to search for GV-DVR LPR / GV-VMS LPR detected in the same LAN.

---

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

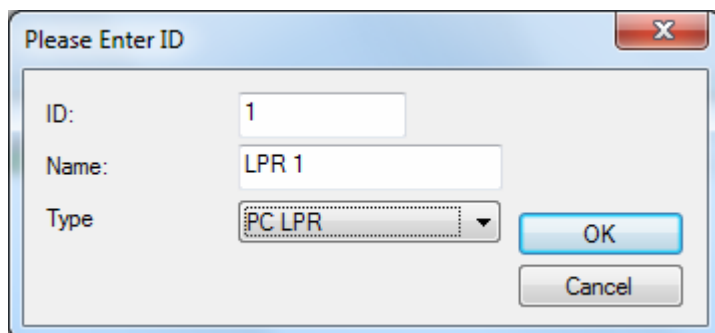


Figure 13-8

3. Type an **ID** number and **Name** for the LPR.
4. Use the drop-down list to select **PC-LPR**.



5. Click **OK**. This dialog box appears.

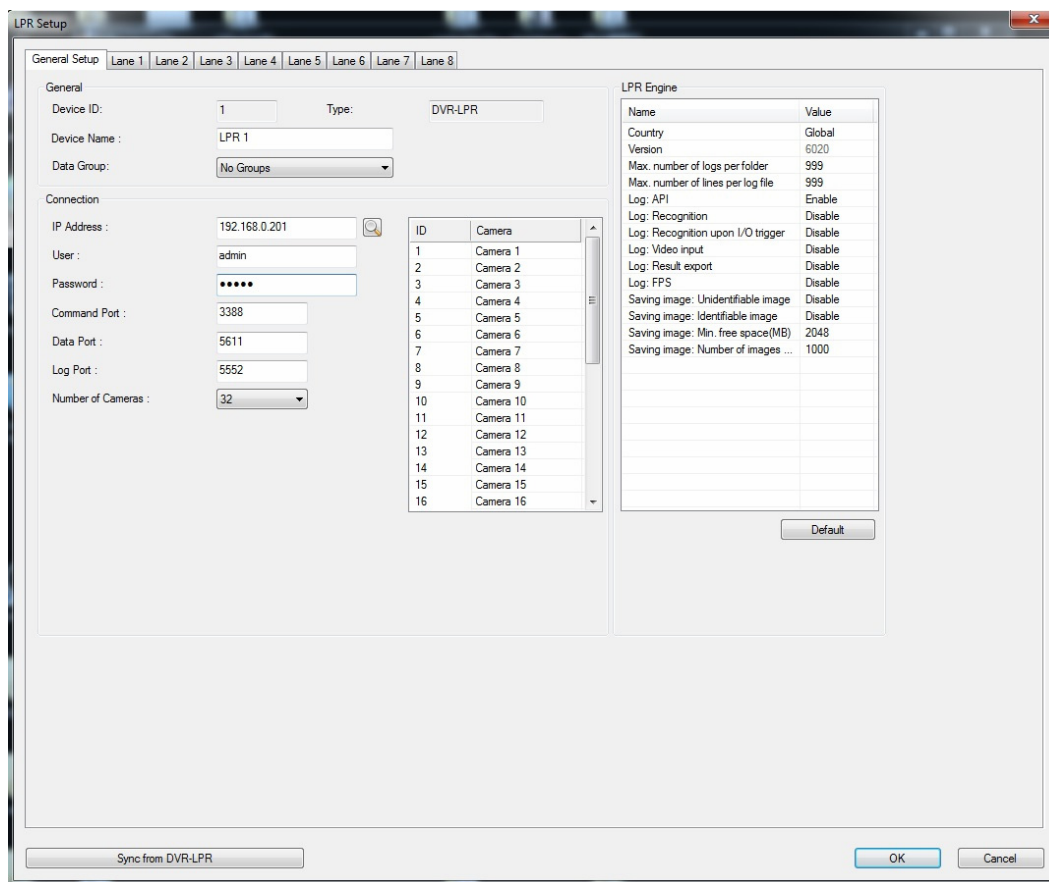



Figure 13-9

6. Assign the PC LPR to a **Data Group** if needed or select **No Groups** to disable the data group function. You can then allow or forbid a user to read / write / execute the functions assigned under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.
7. Under 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.
8. You can modify the following settings if necessary.
  - **Command Port:** The default command port is 3388.
  - **Data Port:** The default data port is 5611.
  - **Log Port:** The default log port is 5552.
  - **Number of Cameras:** Select the number of cameras supported by the GV-DVR / NVR / VMS.
  - **Camera Name:** On the right side of the dialog box, select a camera to modify the camera name.

9. Under **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 the channel, select a **Lane** tab. This dialog box appears.

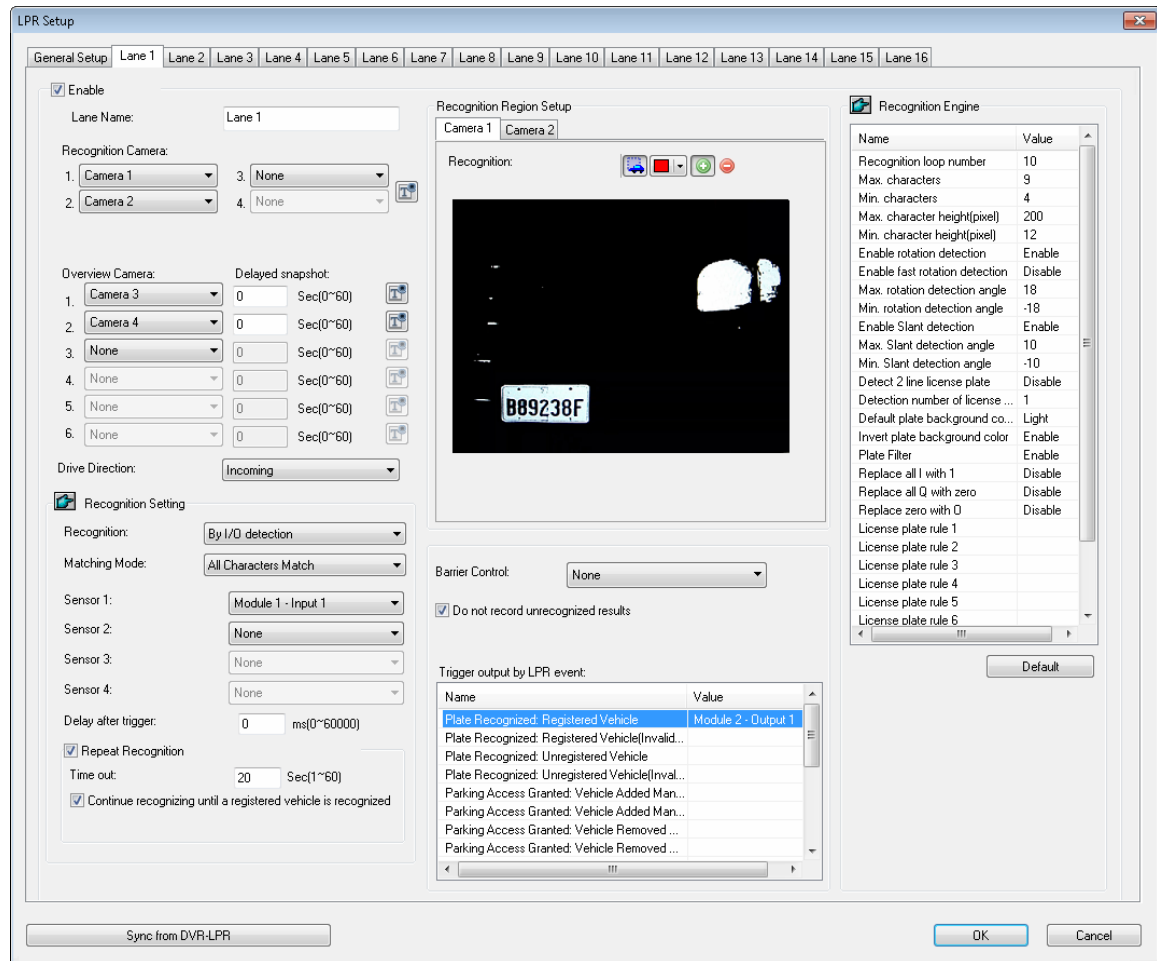


Figure 13-10

2. Select **Enable**.

**Note:** To apply the current settings of the connected GV-DVR LPR / GV-VMS LPR, click **Sync from DVR LPR** and skip to step 9.

3. Select up to four cameras connected to the GV-DVR / NVR / VMS to be the **Recognition Camera**. 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.

---

4. Select up to six **Overview Cameras** to capture the overall appearance of the vehicle. The overview camera must be connected to the GV-DVR / NVR / VMS. Under **Delayed snapshot**, you can type the number of seconds to delay the capturing of snapshot after the license plate is recognized.
5. Next to **Drive Direction**, select **Incoming** to designate an LPR lane as the entrance of the parking lot or select **Outgoing** to set the lane as the exit of the parking lot.
6. Configure the Recognition Settings:
  - **Recognition:** Select to start license plate detection upon **motion detection** or **I/O detection**. For I/O detection, PC LPR will only capture up to 1 license plate per I/O trigger.
  - **Matching Mode:** To trigger the output device specified in Barrier Control only when the detected license plate matches a registered license plate completely, select **All Characters Match**. When **Allow 1 mismatched character** or **Allow 2 mismatched characters** is selected, 1 or 2 mismatched characters will be tolerated, and the first and last characters must be unchanged. 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 start detecting license plate upon motion detection. If you select an **Input**, the PC LPR will only conduct plate detection during the time period when the selected input is being triggered. Multiple license plates can be captured during an input trigger.
  - **Sensitivity:** Adjust the sensitivity level for 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**.
7. Adjust the **Recognition Region Setup** for each camera if needed: Only license plates inside the area drawn will be recognized.
  8. Use the **Barrier Control** drop-down list to select an output device. The output device will be triggered when the detected license plate matches a registered license plate according to the Matching Mode set in step 5.
  9. Select **Do not record unrecognized results** to omit unrecognized results from LPR log.
  10. Under **Trigger output by LPR event**, you can click the field under Value to select an output device to trigger when the LPR event occurs.
  11. Under **Recognition Engine**, adjust the settings below to improve recognition accuracy.
    - **Recognition loop number:** Repeat recognition for the number of times specified.
    - **Max. / Min. characters:** Set the maximum or minimum 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.
    - **Max. / Min. height of characters:** You can set the maximum and minimum height of characters on the license plate in pixels to activate the recognition process.
    - **Enable rotation detection:** License plates tilted horizontally can be detected.
    - **Enable fast rotation detection:** This option can increase the recognition speed by 10 % but decrease the accuracy by 3%.
    - **Max. / Min. rotation detection angle:** Set the maximum and minimum tilt angle to be allowed to activate the recognition process.
    - **Enable Slant Detection:** License plates tilted vertically can be detected.
    - **Max. / Min. slant detection angle:** Set the maximum and minimum tilt angle to activate the recognition process.
    - **Detect 2 line license plate:** Recognize two rows of characters on license plates. Note this option is only available on the engine version of V5000 or later.
    - **Detection number of license plates:** Set the maximum number of plates to be recognized simultaneously.
    - **Default plate background color:** Select **Light** 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:** Select **Enable** 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:** Always identify the character “I” as “1” (one).
- **Replace zero with O:** Always identify the character “0” as “O” (letter O).
- **Replace Q with zero:** Always identify the character “Q” as “0” (zero). Note this option is only available on the engine version of V5000 or later.
- **License Plate Rule:** You can customize up to six license plate rules and the recognized plates will be converted to similar character to follow the rule. The rule must be between 4 and 9 characters and consists of “A” (Alphabets), “D” (Numeric digits) and “X” (Any). For example, if the rule is AA-DDDD, a license plate detected as XY-123A will be converted to XY-1234 to follow the rule. The rule will be ignored if none of the detected plate numbers follow the rule.


---

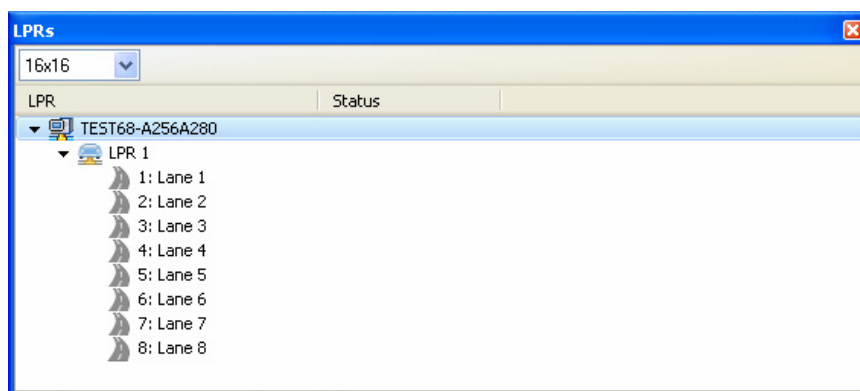
**Note:** Refer to *Appendix E. Supported Recognition Engines of PC LPR* to see the recognition engines supported by GV-DVR LPR / GV-VMS LPR.

---

12. Click **OK** to apply the settings and return to the main screen. An LPR folder tree will be displayed on the Device View window as shown below.

If the icon  appears, it indicates the connection between the GV-DVR LPR / GV-VMS LPR and GV-ASManager has been established.

If the icon  appears, it indicates the connection failed. Make sure the above connection setup is correctly configured.



*Figure 13-11*

---

**Note:**

1. The Overview Cameras need to be set to round-the-clock recording on GV-DVR / NVR / VMS.
  2. 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
  3. To open a gate when the detected license plate is recognized as a registered vehicle:
    - a. Set up I/O devices on the GV-DVR LPR / GV-VMS LPR (**Configure** button > **Accessories > I/O Device > I/O Device Setup**). Refer to *6.1 I/O Device Setup* in the *DVR 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 page also allows you to customize a storage path to store captured license plates.

On GV-DVR LPR, click the **Configure** button, select **Video Analysis**, select **License Plate Recognition**, select **Configure** and click **Export Setting**.

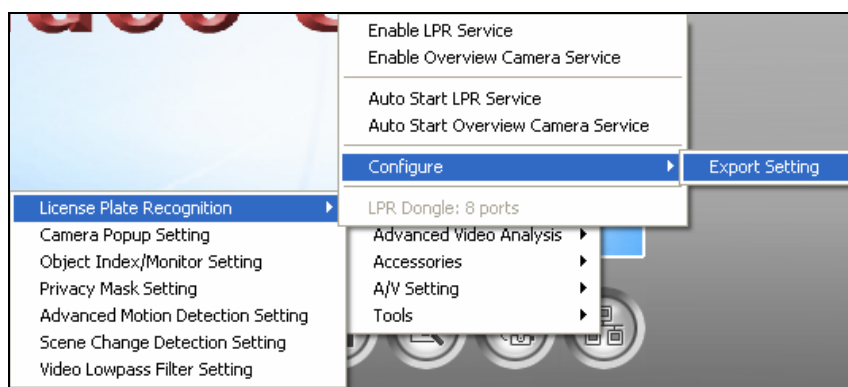





Figure 13-12

On GV-VMS LPR, click the **Home** button , select **Toolbar** , select **Tools** , select **License Plate Recognition**, select **Configure**, and select **Export Setting**.

## Export through RS-232

1. If you are connecting the computer to a machine using RS-232 connection, click the **Export Through RS232** tab and select **Enable Export through RS232**.

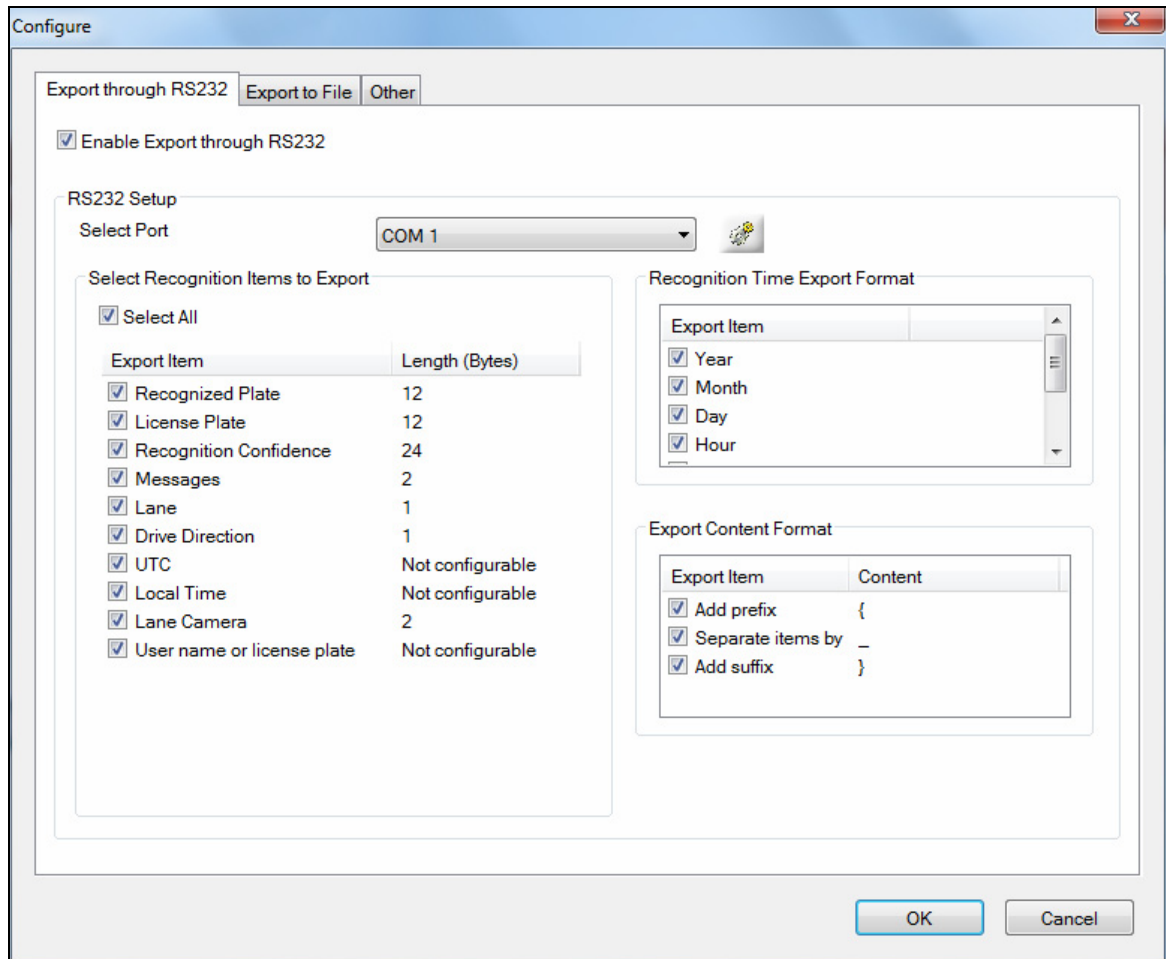


Figure 13-13

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**.

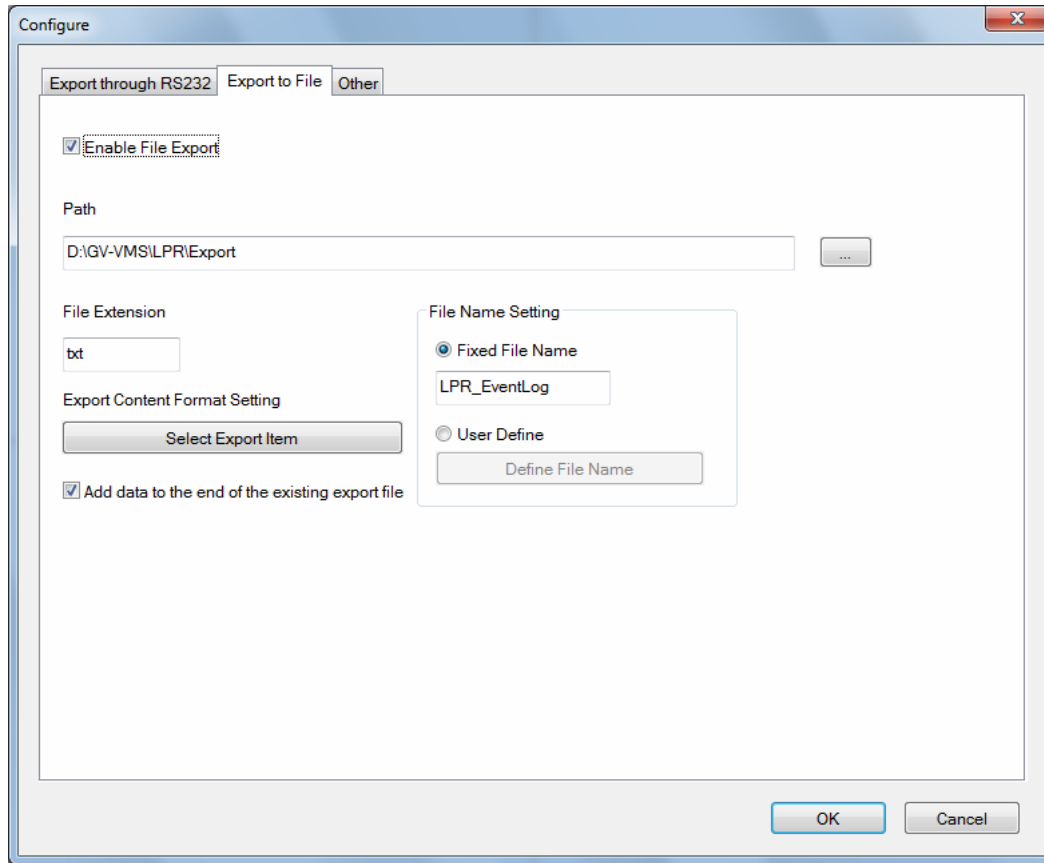


Figure 13-14

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.

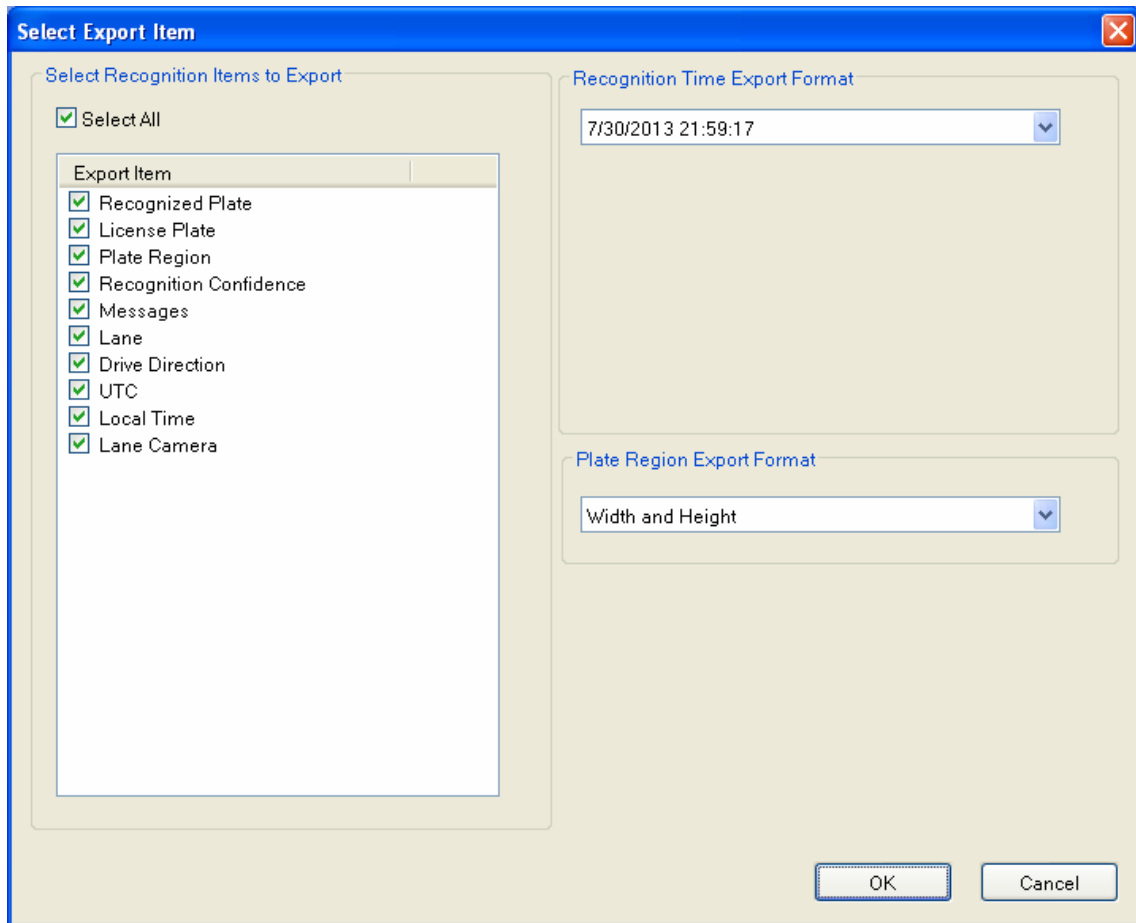
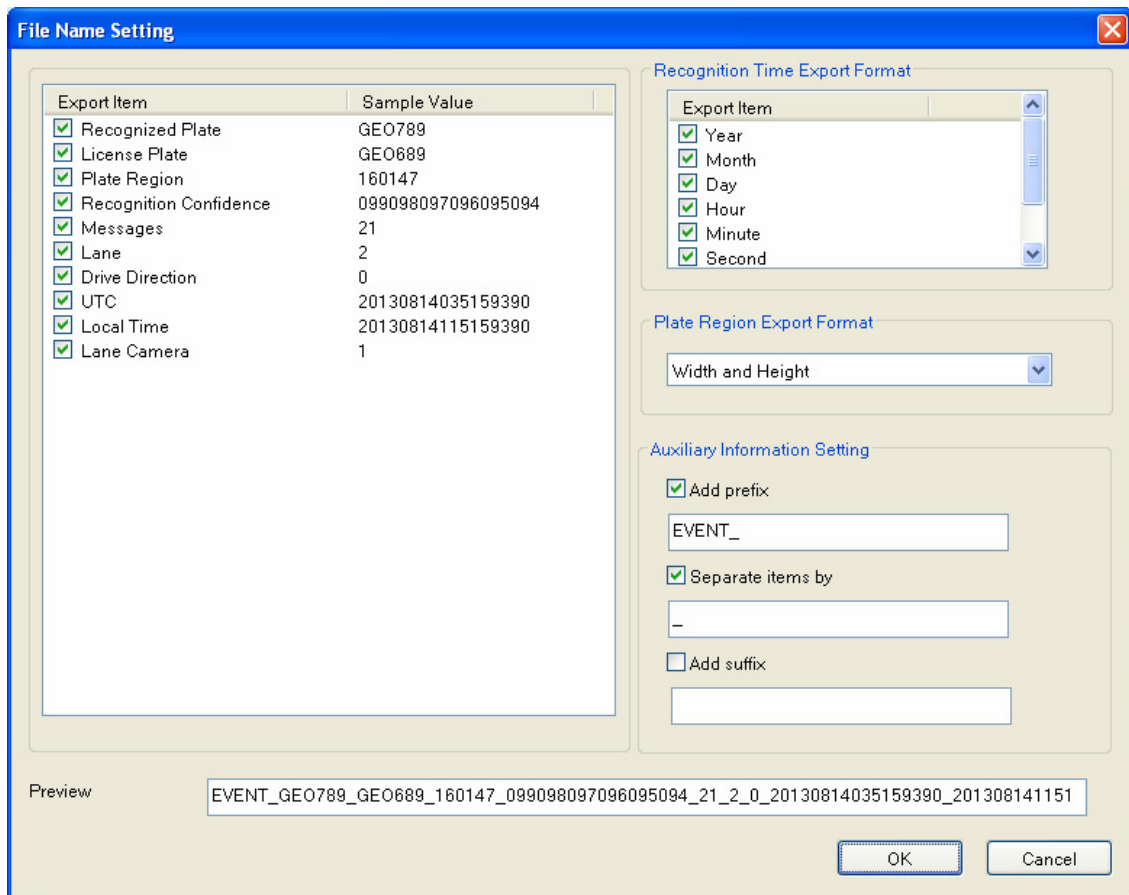


Figure 13-15

- Select the items you want to export.
- Use the **Recognition Time Export Format** to select how you want to display the recognition time.
- Use the **Plate Region Export Format** drop-down list to specify how you want to display the position of the license plate detected.
- 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.



The **File Name Setting** dialog box is shown with the following sections:

- Export Item Table:**

Export Item	Sample Value
<input checked="" type="checkbox"/> Recognized Plate	GEO789
<input checked="" type="checkbox"/> License Plate	GEO689
<input checked="" type="checkbox"/> Plate Region	160147
<input checked="" type="checkbox"/> Recognition Confidence	099098097096095094
<input checked="" type="checkbox"/> Messages	21
<input checked="" type="checkbox"/> Lane	2
<input checked="" type="checkbox"/> Drive Direction	0
<input checked="" type="checkbox"/> UTC	20130814035159390
<input checked="" type="checkbox"/> Local Time	20130814115159390
<input checked="" type="checkbox"/> Lane Camera	1
- Recognition Time Export Format:**
  - ☒ Year
  - ☒ Month
  - ☒ Day
  - ☒ Hour
  - ☒ Minute
  - ☒ Second
- Plate Region Export Format:**
  - Width and Height
- Auxiliary Information Setting:**
  - ☒ Add prefix:
  - ☒ Separate items by:
  - ☐ Add suffix:
- Preview:**
- Buttons:** OK, Cancel

Figure 13-16

- 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.
- Click **OK**.

### Customize Storage Path for Storing Captured License Plates

1. Click the **Other** tab.

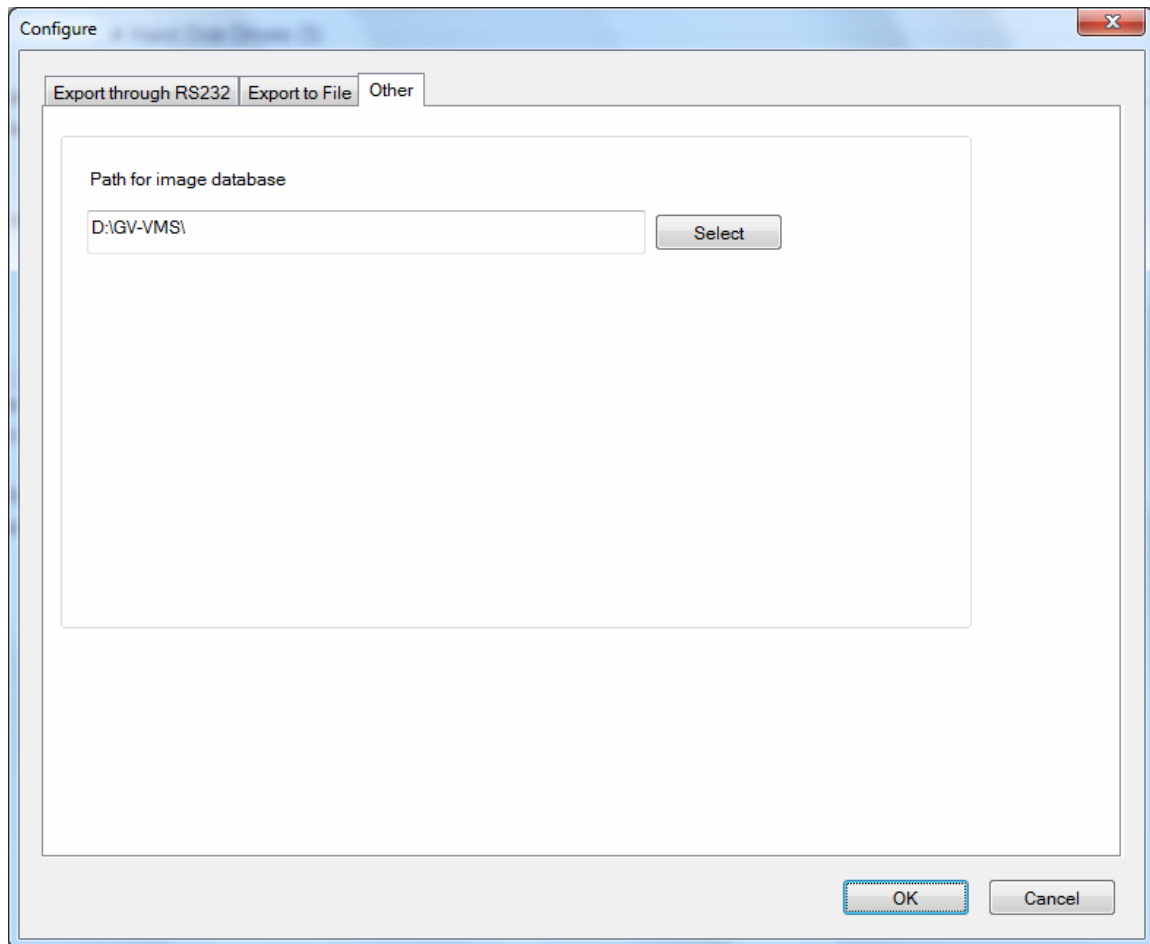


Figure 13-17

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

### 13.3 Setting Up Standalone LPR

To set up GV-DSP LPR / GV-LPR1200 functions on the GV-ASManager, follow the steps below.

Model	Firmware Version	GV-ASManager
GV-DSP LPR	V2.0.3	V4.2.1
	V2.0.4	V4.2.3
	V2.1	V4.3 – V4.3.5
	V2.2	V4.4 – V4.4.3
	V2.3	V5.0
GV-LPR1200	V1.01	V4.3 – V4.3.5
	V1.1	V4.4 – V4.4.3
	V1.2	V5.0

- **Step 1 Enabling Connection with GV-ASManager**

Enable connection with GV-ASManager on GV-DSP LPR / GV-LPR1200.

- **Step 2 Adding Standalone LPR to GV-ASManager**

Establish the communication between GV-ASManager and GV-DSP LPR / GV-LPR1200.

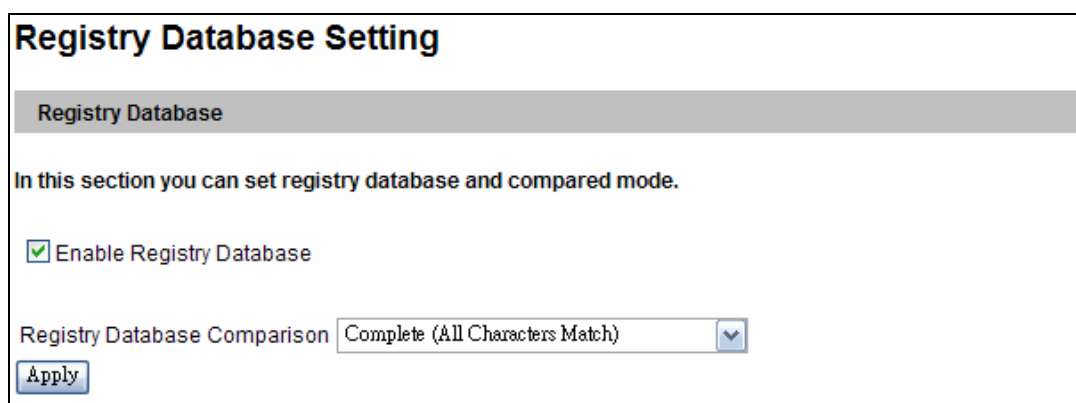
- **Step 3 Configuring a Channel**

Set up the related cameras and the recognition conditions of the 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 mini or micro SD card is inserted to the standalone LPR and formatted. Next, log in 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.



The image shows a web interface window titled "Registry Database Setting". At the top, there is a grey header bar with the text "Registry Database". Below the header, a message states: "In this section you can set registry database and compared mode." There is a checkbox labeled "Enable Registry Database" which is checked. Below this is a label "Registry Database Comparison" followed by a dropdown menu currently showing "Complete (All Characters Match)". At the bottom left of the window is an "Apply" button.

Figure 13-18

2. Select **Enable Registry Database**.
3. Use the **Registry Database Comparison** drop-down list to select one of these options:
  - **Complete (All Characters Match):** Detected license plate must match a registered license plate completely.
  - **Like (One Character Mismatch):** 1 mismatched character will be tolerated and the order of the characters will be ignored. For example, license plate ABC-123 will be considered matching with ZBC-321.
  - **Somewhat Like (Two Characters Mismatch):** 2 mismatched characters will be tolerated and the order of the characters will be ignored.
4. Click the **Apply** button.

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** and select **Devices**. This dialog box appears.

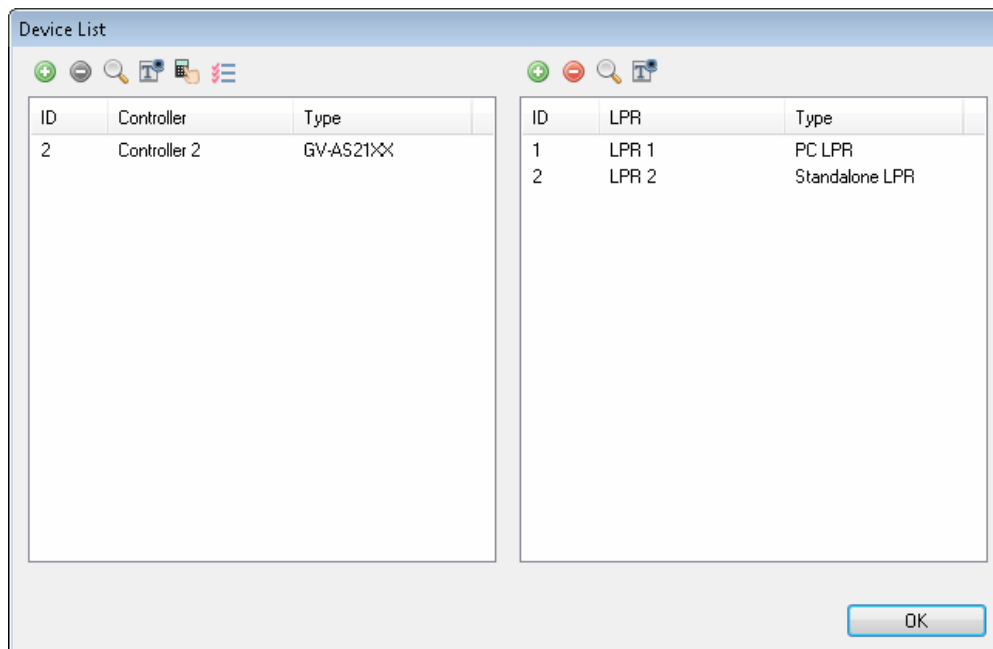


Figure 13-19

---

**Note:** You can also click the **Search** button  to search for GV-DSP LPR / GV-LPR1200 detected in the same LAN.

---

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

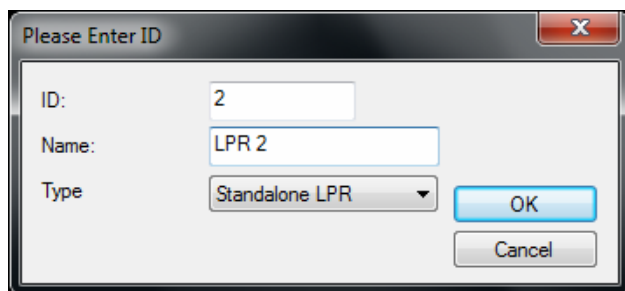


Figure 13-20

3. Type an **ID** number and **Name** for the LPR.
4. Use the drop-down list to select **Standalone LPR**.

- Click **OK**. The LPR Setup page appears.

The screenshot shows the 'LPR Setup' window with two tabs: 'General Setup' and 'Lane 1'. The 'General Setup' tab is active. It contains two sections: 'General' and 'Connection'.


**General Section:**

- Device ID:** 2
- Type:** DSP-LPR
- Device Name:** LPR 2
- Data Group:** No Groups (dropdown menu)

**Connection Section:**

- IP Address:** 192.168.0.63 (with a search icon)
- User:** admin
- Password:** (masked with dots)
- Https Port:** 443
- VSS Port:** 10000
- Number of Cameras:** 1 (dropdown menu)

Figure 13-21

- Assign the standalone LPR to a **Data Group** if needed or select **No Groups** to disable the data group function. You can then allow or forbid a user to read / write / execute the functions assigned under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.
- Under 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 detected in the same LAN.
- You can modify the following settings if necessary.
  - **Https Port:** The default Https port is 443.
  - **VSS Port:** The default VSS port is 10000.



### 13.3.3 Step 3: Configuring a Channel

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

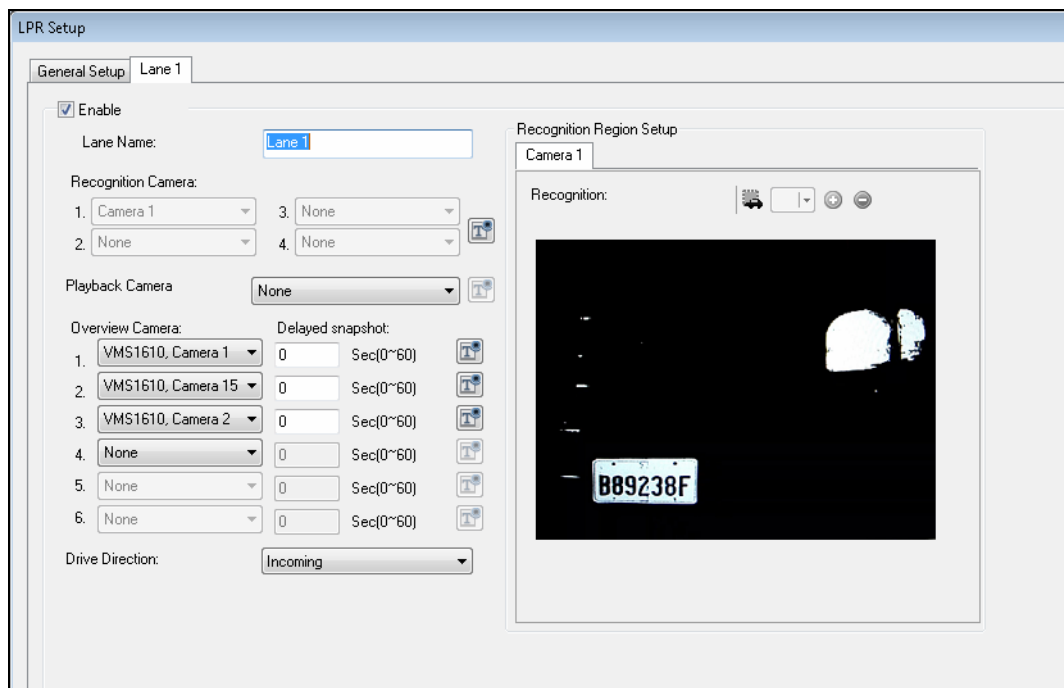


Figure 13-22

- Select **Enable**.
- Select a **Playback Camera**. The playback camera needs to be connected to a GV-DVR / NVR and the GV-DVR / NVR needs to be added to the camera list. You can select an event in the monitoring window, and GV-ASManager will play back the camera view recorded at the time of the event. Refer to *Retrieving Recording Video* in Chapter 5 for details.
- Select up to six **Overview Cameras** to capture the overall appearance of the vehicle. The overview camera must be connected to a GV-DVR / NVR and the GV-DVR / NVR needs to be added to the camera list:
  - Right-click the GV-DVR / NVR in the Camera List and select **Settings**.
  - Click the **Add** button and select **Add DVR Mapping**.
  - Type the connection information of the overview camera and click **OK**.
- Next to **Drive Direction**, select **Incoming** to designate an LPR lane as the entrance of the parking lot or select **Outgoing** to set the lane as the exit of the parking lot
- Click **OK** to apply the settings.

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 on GV-DVR / NVR in either round-the-clock mode or upon motion detection.
  2. The Overview Cameras need to be set to round-the-clock recording on GV-DVR / NVR.
  3. To ensure optimal performance, the total number of Overview Cameras supported in a GV-DVR / NVR 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
-

## 13.4 Adding Vehicles

Once you have set up the PC LPR or standalone LPR, you will need to create a vehicle database. The detected license plate number must match the license plate number of a registered vehicle before access can be granted.

1. There are two ways to add a vehicle:

- When an unregistered vehicle is detected, the message *Plate Recognized: Unregistered Vehicle* is displayed. Right-click the message and select **New / Edit Vehicle**. The Adding a New Vehicle dialog box appears with the detected license plate number (Figure 13-24).
- On the menu bar, click **Personnel** and select **Vehicles**. This dialog box appears.

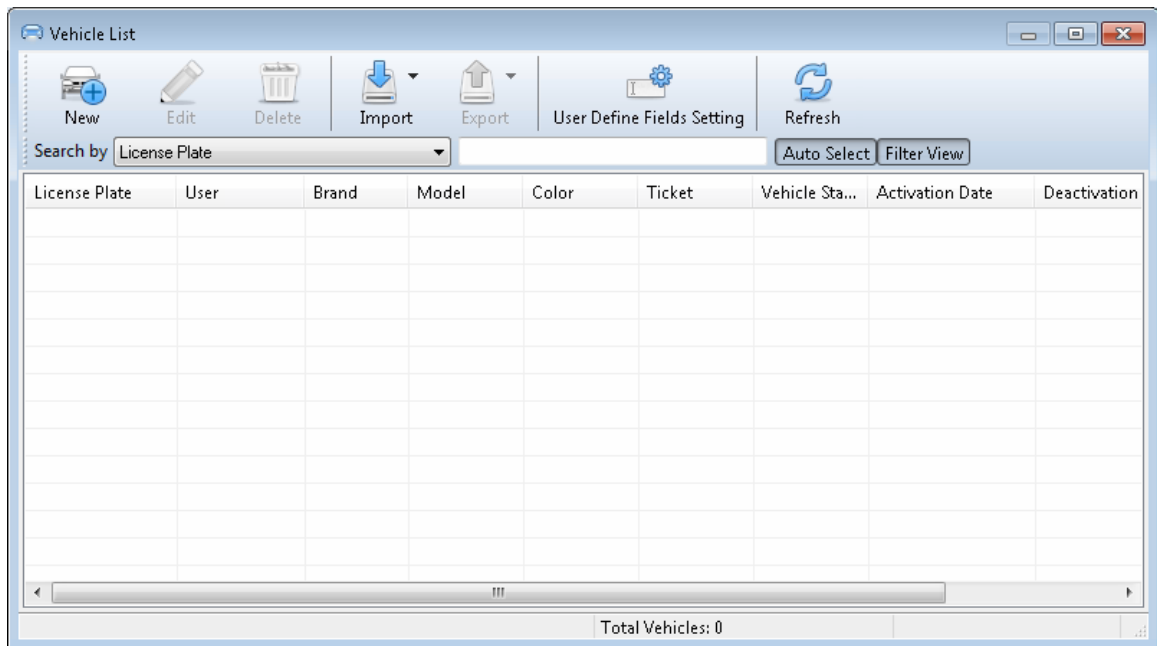


Figure 13-23

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

The dialog box is titled "Add a new vehicle". It contains the following fields and controls:

- User:** A text input field with a user icon button.
- License Plate:** A text input field containing "AB-1234".
- Brand:** A dropdown menu.
- Model:** A dropdown menu.
- Color:** A dropdown menu containing "Black".
- Ticket:** A text input field.
- Vehicle Status:** A dropdown menu containing "Active".
- Activation Date:** A date and time picker showing "5/19/2016" and "18:37".
- Deactivation Date:** A date and time picker showing "5/19/2016" and "19:37".
- User Define 01-06:** Six dropdown menus for user-defined fields.
- Access Group:** A dropdown menu set to "Default", with a list box showing "LPR 1" and "Lane 1" (24-hour restricted).
- Data Group:** A dropdown menu set to "No Groups".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figure 13-24

3. The settings are available for the card:
- **User:** 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:** You can 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.
  - **Activation/Deactivation Date:** Specify a time to activate and deactivate the vehicle access.

- **User Define:** Type the data for any customized data fields. Up to six user-defined data fields can be created. For details, see *4.6.2 Customizing a Data Field*.
- **Access Group:** Access Groups control which vehicle can access which channel and at what time. For details, see *4.5 Setting Access Groups*.

For first-time users of the GV-ASManager, the access group is not yet established. Select **User Define** for test run.

- **LPR:** The LPR column displays the associated channels. The selection for each channel will be automatically brought up if an access group was selected.

When setting up LPR functions for the first time, select **24-hour access** for each channel for test run.

- **Data Group:** Assign the vehicle to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions listed under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.

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

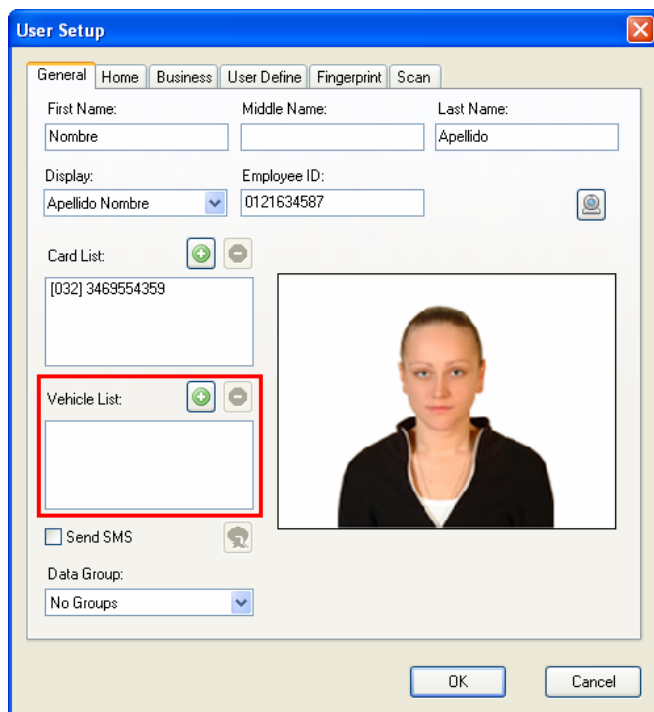


Figure 13-25

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

## 13.5 Monitoring LPR Activities

### 13.5.1 LPR Device View

The LPR Device View displays the connection status of the connected LPRs. To open the LPR Device View, click **View** on the menu bar and select **LPRs**.

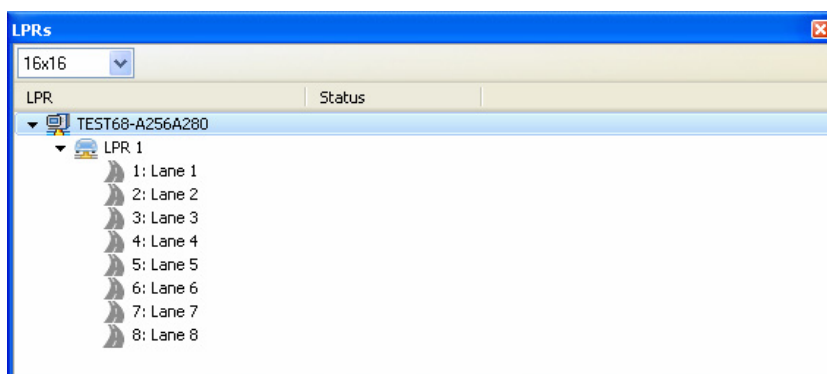


Figure 13-26

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

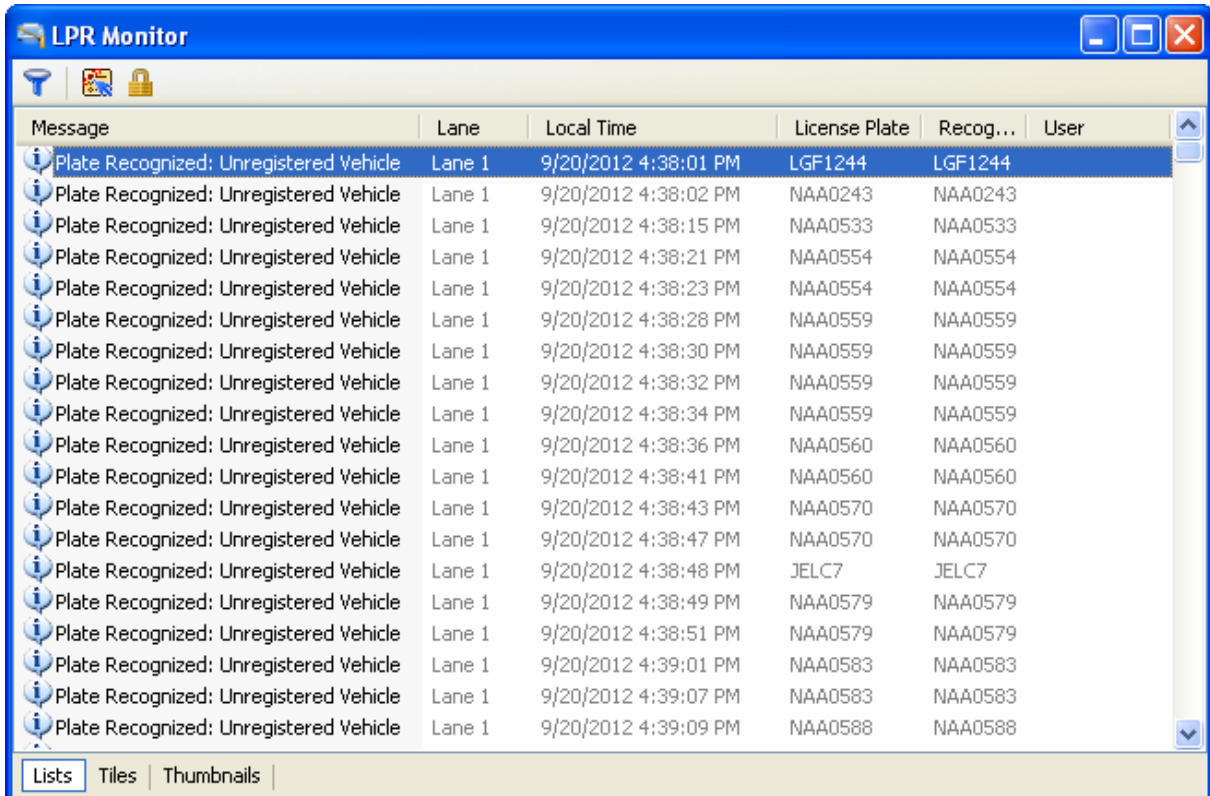
Name	Function
Reconnect	Reconnects with the LPR.
Sync LPR	After modifying the LPR settings, clicking <b>Sync LPR</b> will renew the settings immediately.
Settings	Accesses the LPR setup dialog box.

Right-click an **LPR channel** to access the following options:

Name	Function
Unlock Door	Opens the gate barrier for the time period specified for the output device. Make sure the gate barrier has been set up as the designated output device. For PC LPR, refer to the Barrier Control option in <i>13.2.3 Step 3: 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	Forces license plate recognition.
Settings	Modifies the controller settings in the Controller Setup dialog box.

## 13.5.2 Monitoring Windows

To monitor LPR activities, click **Monitoring** and select **New LPR Monitor**. This dialog box appears.



The screenshot shows the 'LPR Monitor' window with a table of recognized vehicles. The table has columns for Message, Lane, Local Time, License Plate, and User. The messages are all 'Plate Recognized: Unregistered Vehicle'. The lanes are all 'Lane 1'. The local times range from 9/20/2012 4:38:01 PM to 9/20/2012 4:39:09 PM. The license plates range from LGF1244 to NAA0588. The user column is empty.

Message	Lane	Local Time	License Plate	Recog...	User
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:01 PM	LGF1244	LGF1244	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:02 PM	NAA0243	NAA0243	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:15 PM	NAA0533	NAA0533	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:21 PM	NAA0554	NAA0554	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:23 PM	NAA0554	NAA0554	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:28 PM	NAA0559	NAA0559	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:30 PM	NAA0559	NAA0559	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:32 PM	NAA0559	NAA0559	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:34 PM	NAA0559	NAA0559	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:36 PM	NAA0560	NAA0560	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:41 PM	NAA0560	NAA0560	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:43 PM	NAA0570	NAA0570	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:47 PM	NAA0570	NAA0570	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:48 PM	JELC7	JELC7	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:49 PM	NAA0579	NAA0579	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:38:51 PM	NAA0579	NAA0579	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:39:01 PM	NAA0583	NAA0583	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:39:07 PM	NAA0583	NAA0583	
Plate Recognized: Unregistered Vehicle	Lane 1	9/20/2012 4:39:09 PM	NAA0588	NAA0588	

Figure 13-27

For details on the Monitoring Windows, refer to [3.3 Monitoring Windows](#).

## 13.6 Receiving Notifications for LPR Activities

When alarm conditions occur, the system can automatically send e-mail and SMS alerts to one or multiple recipients.

To set up LPR or vehicle hotlist notifications, click **Tools**, select **Notifications**, and click the **LPR** or **Hotlist** tab. This dialog box appears. Select an event to start setting up alert methods.

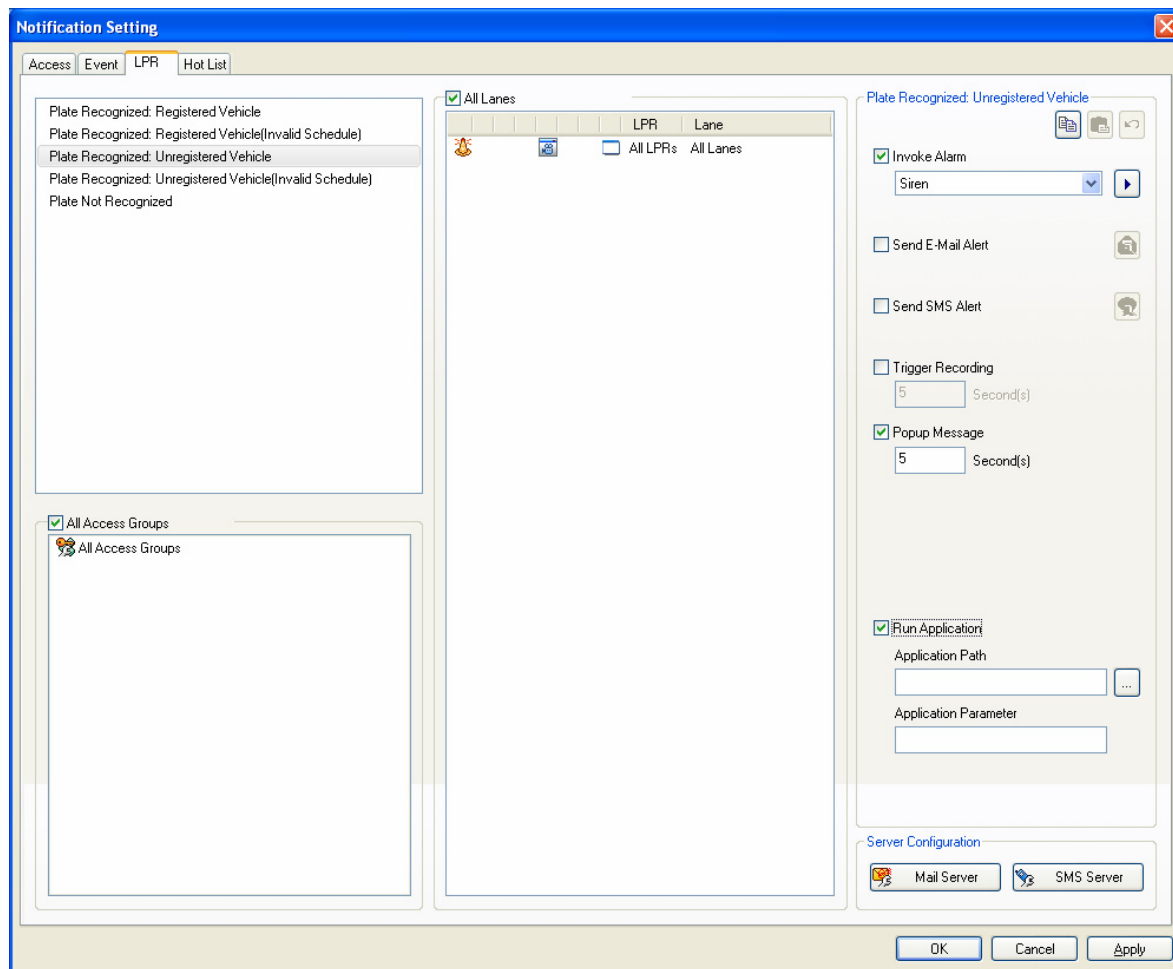


Figure 13-28

For detailed settings, refer to *8.2 Setting Up Alert Notification*.



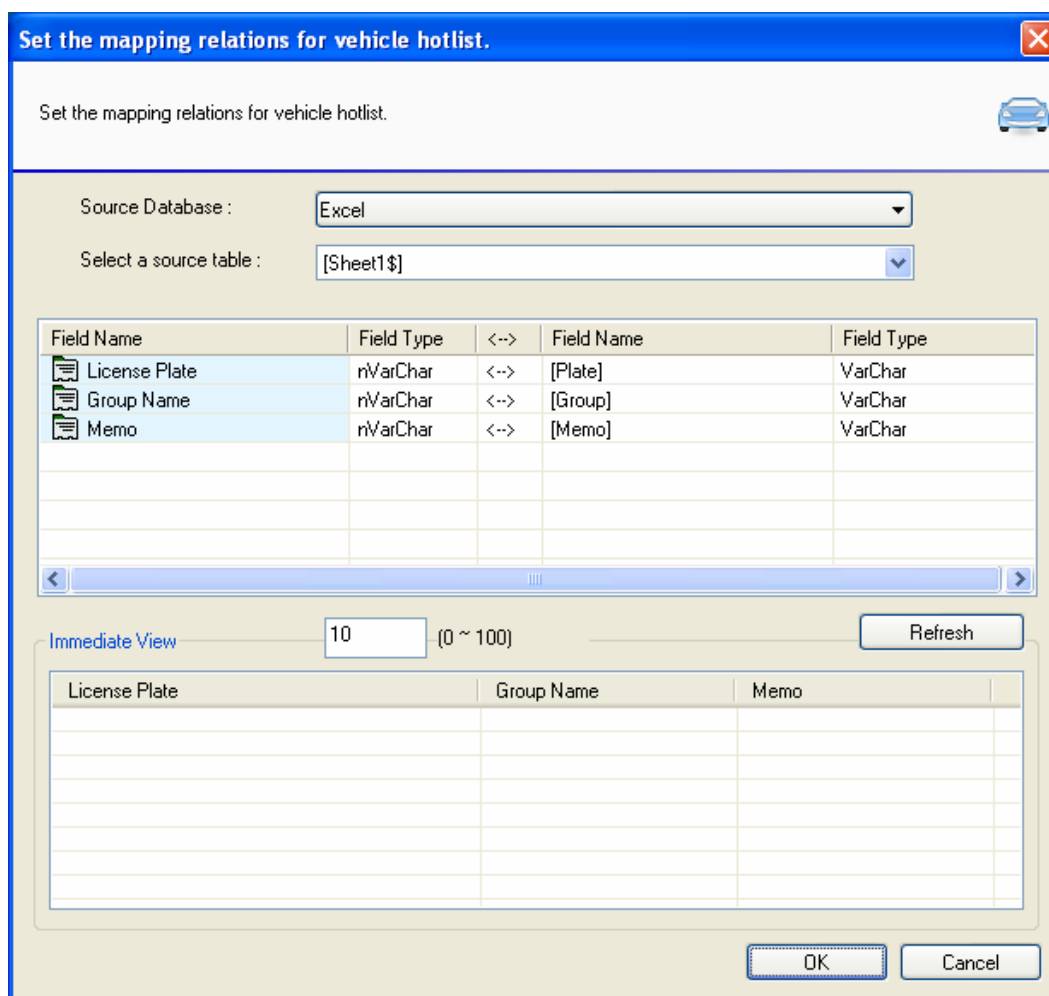
## 13.7 Setting Up Vehicle Hotlist

The vehicle hotlist is a list of stolen vehicles or other vehicles of interest. There are three ways to add vehicles to the hotlist: manually add vehicles, import from vehicle list 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 a 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** and select **Set the mapping relations for vehicle hotlist**. This dialog box appears.



**Set the mapping relations for vehicle hotlist.**

Set the mapping relations for vehicle hotlist.

Source Database :

Select a source table :

Field Name	Field Type	<-->	Field Name	Field Type
License Plate	nVarChar	<-->	[Plate]	VarChar
Group Name	nVarChar	<-->	[Group]	VarChar
Memo	nVarChar	<-->	[Memo]	VarChar

Immediate View  (0 ~ 100)

License Plate	Group Name	Memo

Figure 13-29

3. Use the **Source Database** drop-down list to select if you want to use the same database as other data, an excel database or other types of database.
4. Select the path of the database and click **Open**.
5. Next to **Select a source table**, select the appropriate tab in the database.
6. Match the License Plate, Group Name and Memo to the appropriate fields.
7. Click **OK** to import.

### 13.7.2 Adding License Plates to the Hotlist

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

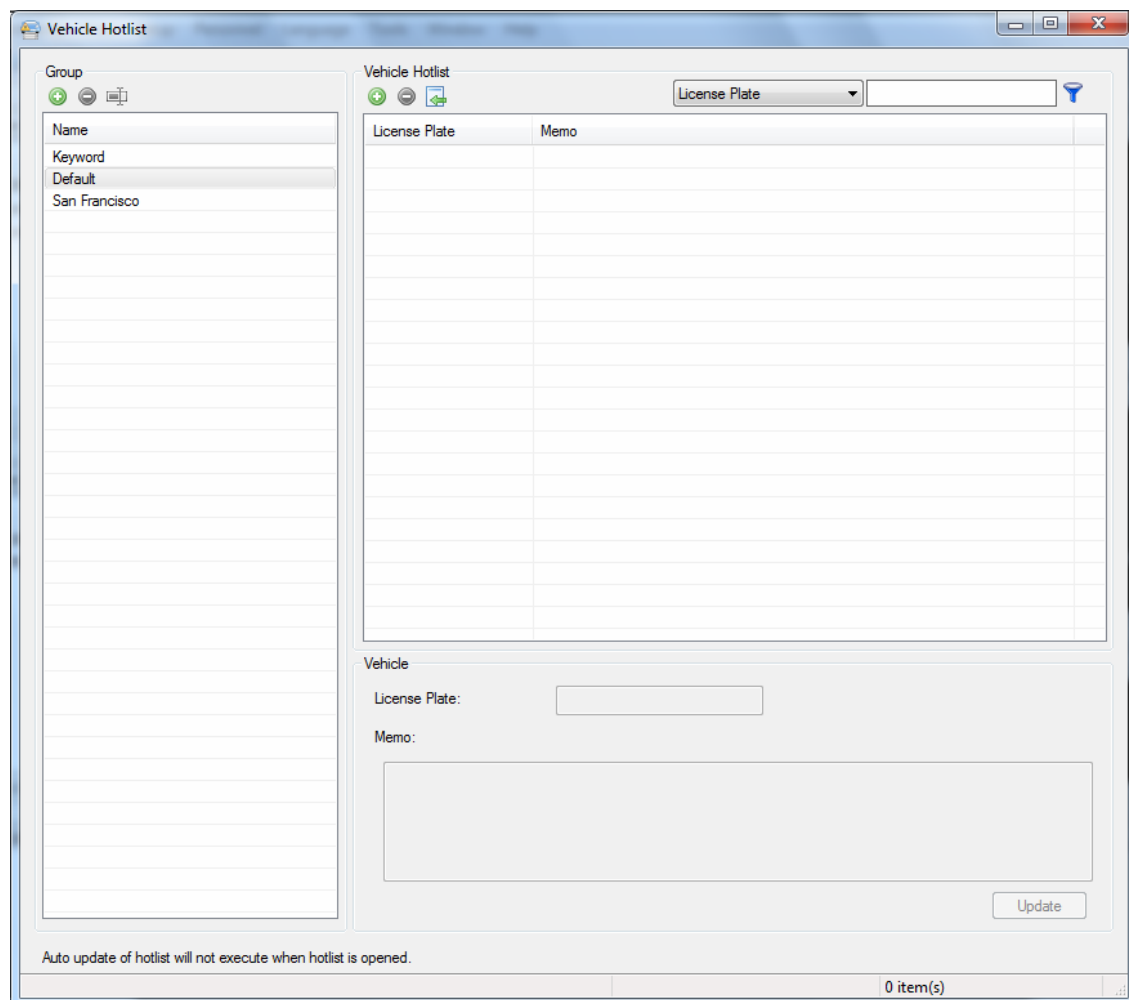


Figure 13-30



### Setting Keywords for Partial Match

You can create keywords, which are partial license plates.

- a. Select **Keyword** under Group, and click the **Add** button  under Vehicle Hotlist.

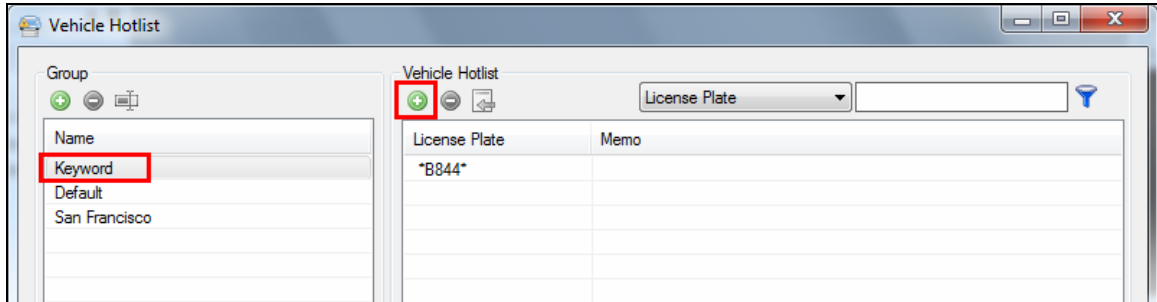


Figure 13-33

- b. Under Add a New Keyword, type a partial license plate for **Keyword**.

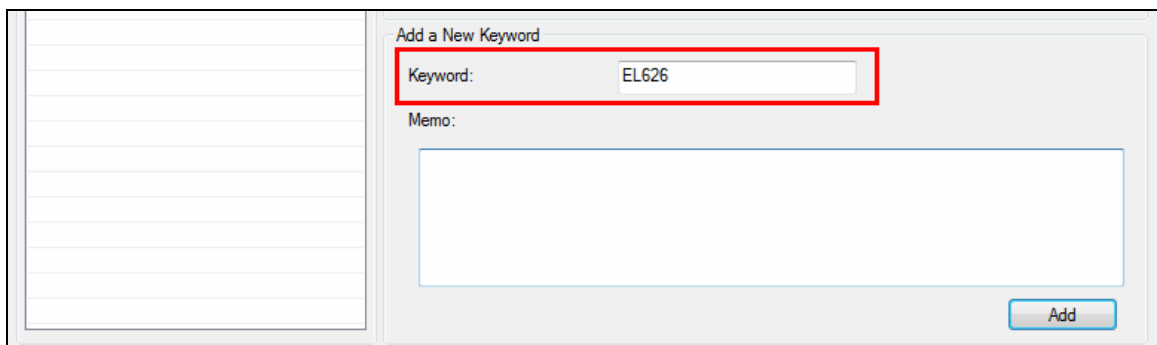


Figure 13-34

- c. Click **Add**. License plates that contain the keyword will be highlighted.

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.

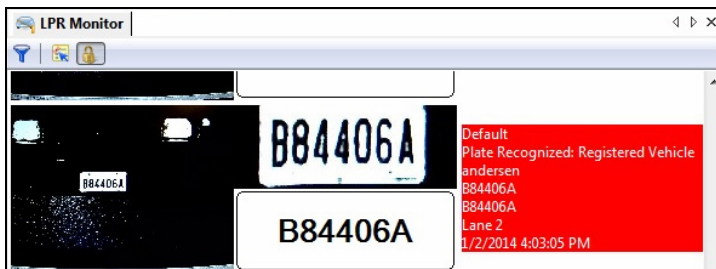


Figure 13-35

## 13.8 Managing Parking Lots

You can manage parking lots by setting LPR lanes as the entry or exit of a parking lot. Only registered vehicles with access to these LPR lanes will be allowed to enter and exit the parking lot. You can set a maximum parking capacity and a maximum stay time allowed for the parking lot.

---

**Note:** For the parking lot function to work properly:

1. GV-DSP LPR / GV-DVR LPR / GV-VMS LPR must remain connected to GV-ASManager.
  2. The time of GV-ASManager and GV-DSP LPR / GV-DVR LPR / GV-VMS LPR must be synchronized to the same NTP server.
  3. GV-LPR1200 cannot be used for parking lot functions.
  4. The following versions should be used.
    - GV-ASManager V4.3 or later
    - GV-DVR LPR using GV-LPR Plugin for GV-DVR / NVR V8.6.0.0 or later
    - GV-VMS LPR using GV-LPR Plugin for GV-VMS V15.10.0.0 or later
    - GV-DSP LPR firmware V2.1 or later
- 

### 13.8.1 Setting Up a Parking Lot

1. On the menu bar, click **Setup** and select **Parking Lots**.
2. Click the **Add** button .

3. Type a new **Parking Lot ID** and **Parking Lot Name** if needed, and click **OK**. This dialog box appears.

Figure 13-36

4. Under General Setup, the following settings are available.
- **Parking Lot Name:** Rename the parking lot if needed.
  - **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.
  - **Parking Space Count:** Set 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:** The default setting is **Enable**. When **No Incoming** is selected, outgoing vehicles will be allowed, but no vehicles can enter the parking lot. When **Disable** is selected, vehicles cannot enter or exit the parking lot.

- **Data Group:** You can use the **Data Group** drop-down list to assign the parking lot to a data group or select **No Groups** to disable the data group function. You can then allow or forbid a user to read/write/execute the functions assigned under the data group. Refer to *Setting Up System User* in Chapter 8 for more details.
- **Anti-Back Time:** Specify the time interval in seconds the same license number is prohibited from entering or exiting the parking lot.
- **Share Space:** You can set up Share Space if multiple vehicles are sharing the same set of parking spaces.
  - a. Under Share Group, click the **Add** button to create a group.

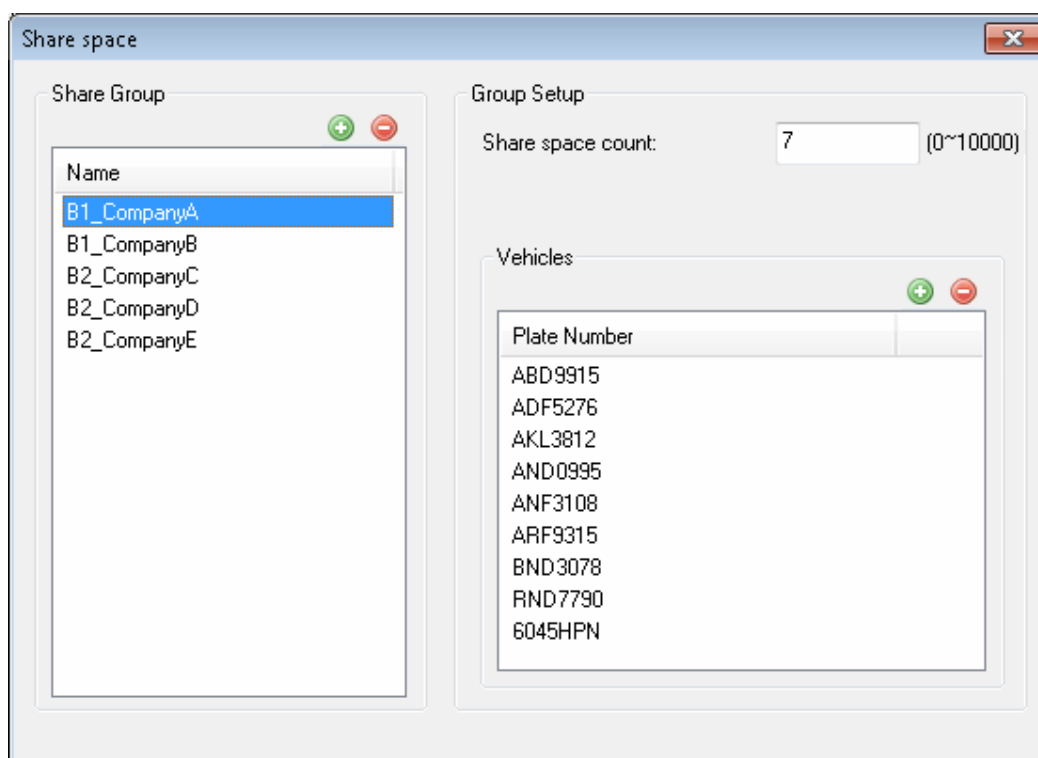


Figure 13-37

- b. Next to Share space count, type the number of parking spaces shared by that group.
- c. Under Vehicles, click the **Add** button to select the license plates of vehicles that will be sharing 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.

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



Figure 13-38

6. For exit, select **Outgoing**, select another LPR lane, and click the **Add** button. You can set multiple incoming and outgoing lanes.
7. Click **OK**.

You can set GV-ASManager to send e-mail / SMS notifications, trigger recording, or pop up messages upon the specified parking lot activities. On the menu bar, click **Tools**, select **Notifications**, and click **LPR**.



## 13.8.2 Monitoring Parking Lots

Using the Parking Lot Monitor, you can see the 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.

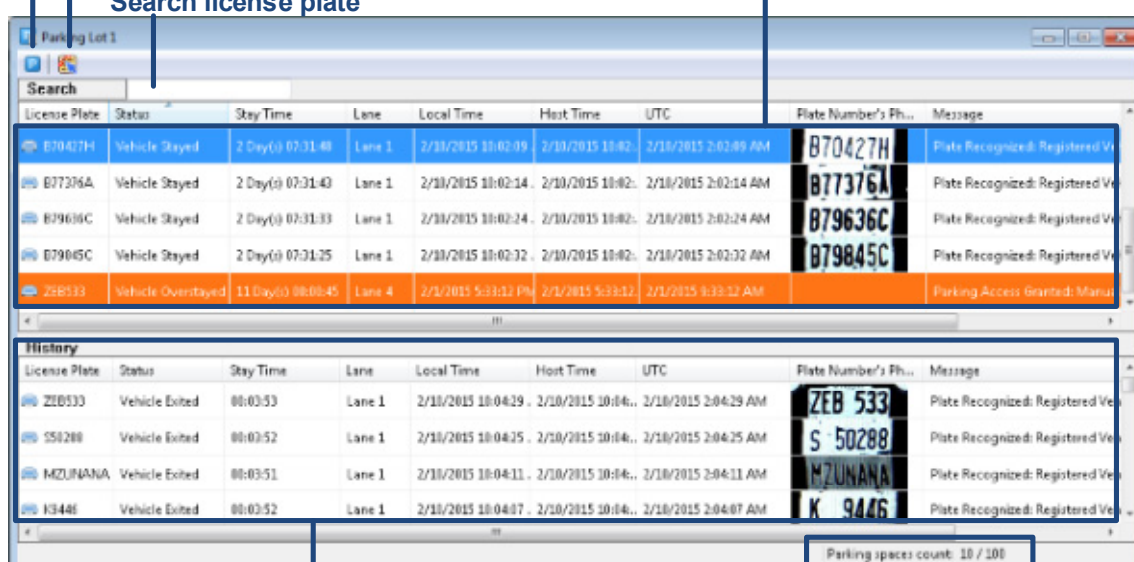
1. On the menu bar, click **Monitoring** and select **New Parking Lot Monitor**.
2. Select a parking lot and click **OK**. This window appears.

Select a parking lot

Auto select

Search license plate

Vehicles inside or entering the parking lot



License Plate	Status	Stay Time	Lane	Local Time	Host Time	UTC	Plate Number's Ph...	Message
B70427H	Vehicle Stayed	2 Day(s) 07:31:40	Lane 1	2/10/2015 10:02:09	2/10/2015 10:02	2/10/2015 2:02:09 AM	B70427H	Plate Recognized: Registered Ve
B77376A	Vehicle Stayed	2 Day(s) 07:31:43	Lane 1	2/10/2015 10:02:14	2/10/2015 10:02	2/10/2015 2:02:14 AM	B77376A	Plate Recognized: Registered Ve
B79636C	Vehicle Stayed	2 Day(s) 07:31:33	Lane 1	2/10/2015 10:02:24	2/10/2015 10:02	2/10/2015 2:02:24 AM	B79636C	Plate Recognized: Registered Ve
B79845C	Vehicle Stayed	2 Day(s) 07:31:25	Lane 1	2/10/2015 10:02:32	2/10/2015 10:02	2/10/2015 2:02:32 AM	B79845C	Plate Recognized: Registered Ve
ZEB533	Vehicle OverStayed	11 Day(s) 08:00:45	Lane 4	2/10/2015 5:33:12 PM	2/10/2015 5:33:12	2/10/2015 8:33:12 AM	ZEB 533	Parking Access Granted: Manual

License Plate	Status	Stay Time	Lane	Local Time	Host Time	UTC	Plate Number's Ph...	Message
ZEB533	Vehicle Exited	00:03:53	Lane 1	2/10/2015 10:04:29	2/10/2015 10:04	2/10/2015 2:04:29 AM	ZEB 533	Plate Recognized: Registered Ve
S50288	Vehicle Exited	00:03:52	Lane 1	2/10/2015 10:04:25	2/10/2015 10:04	2/10/2015 2:04:25 AM	S 50288	Plate Recognized: Registered Ve
MZUNANA	Vehicle Exited	00:03:51	Lane 1	2/10/2015 10:04:11	2/10/2015 10:04	2/10/2015 2:04:11 AM	MZUNANA	Plate Recognized: Registered Ve
K9446	Vehicle Exited	00:03:52	Lane 1	2/10/2015 10:04:07	2/10/2015 10:04	2/10/2015 2:04:07 AM	K 9446	Plate Recognized: Registered Ve

History: Vehicles that have exited the parking lot and vehicles that have been denied access

Parking spaces count: 10 / 100

Current vehicle count

Figure 13-39

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.

3. To manually 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 manually add to 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		2/10/2015
B79636C	Vehicle Stayed	2 Day(s) 07:31:33	Lane 1	2/10/2015		2/10/2015
B79845C	Vehicle Stayed	2 Day(s) 07:31:25	Lane 1	2/10/2015		2/10/2015
ZEB533	Vehicle Overstayed	11 Day(s) 00:00:45	Lane 4	2/1/2015		2/1/2015

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

Figure 13-40

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

Add Parking Vehicle

Plate Number

Date:

Time:

Figure 13-41

---

**Note:**

1. If the vehicle had to be manually added because its license plate is not in the GV-ASManager database, remember 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 was incorrectly recognized, you can click **Modify Plate Number** to manually edit the plate number.
-

4. To manually 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, you can select **Remove and Open Gate**.
  - c. Select the exit lane, and select the exit time.

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

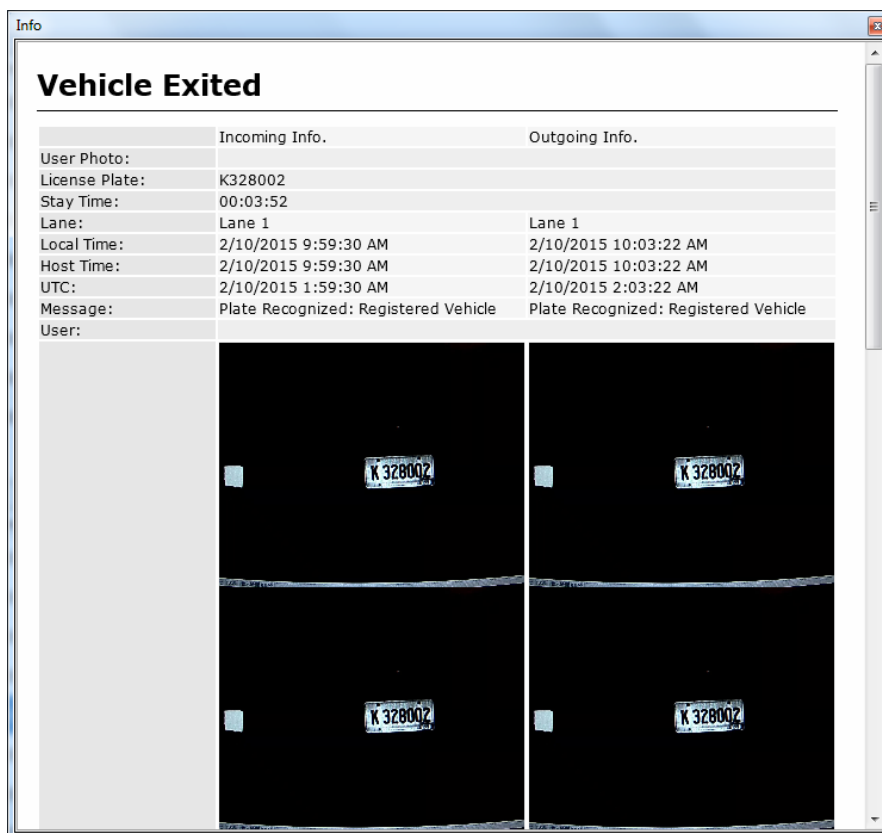


Figure 13-42

### 13.9 LPR Functions in GV-ASWeb

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

- **LPR List:** Adds and deletes PC and standalone LPR to / from GV-ASManager.
- **Vehicle List:** Adds, deletes, edits and searches vehicles.
- **LPR Log:** Searches records of license plate detected and plays back recordings.
- **Parking Lot:** Sets up parking lots. See *13.8 Managing Parking Lots* for instructions.
- **Access Group Setup:** Sets up access groups to restrict who can access which channels at what time.

Refer to *10.1 Connecting to GV-ASManager* to see how to log into GV-ASWeb.

### 13.9.1 LPR List

You can use LPR List to remotely add and delete a standalone / PC LPR to GV-ASManager, set up channels and delete an LPR.



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

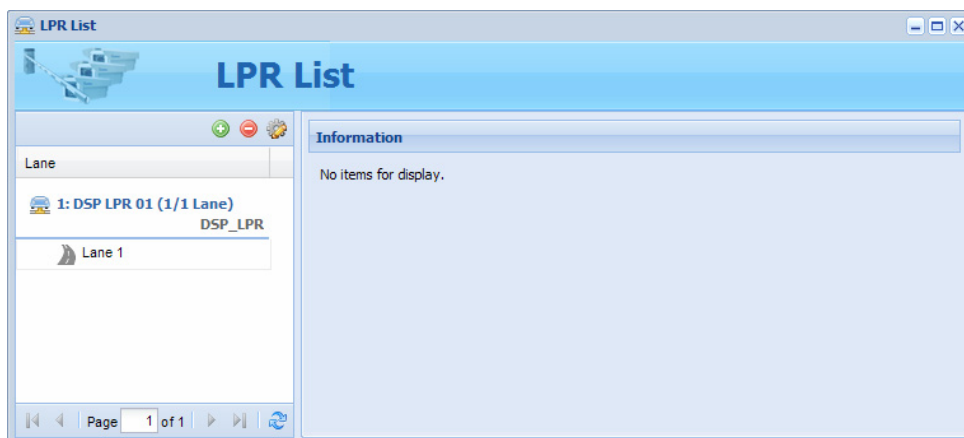





Figure 13-43

2. Click the **Add** button  to add an LPR. For details on the settings, see *13.2.2 Adding PC LPR to GV-ASManager* and *13.3.2 Adding Standalone LPR to GV-ASManager*.
3. To set the individual channels, click the **Edit** button  and select a channel. For details on the configurations, refer to *13.2.3* and *13.3.3 Configuring a Channel*.
4. To delete an LPR, select an LPR and click the **Delete** button .



---

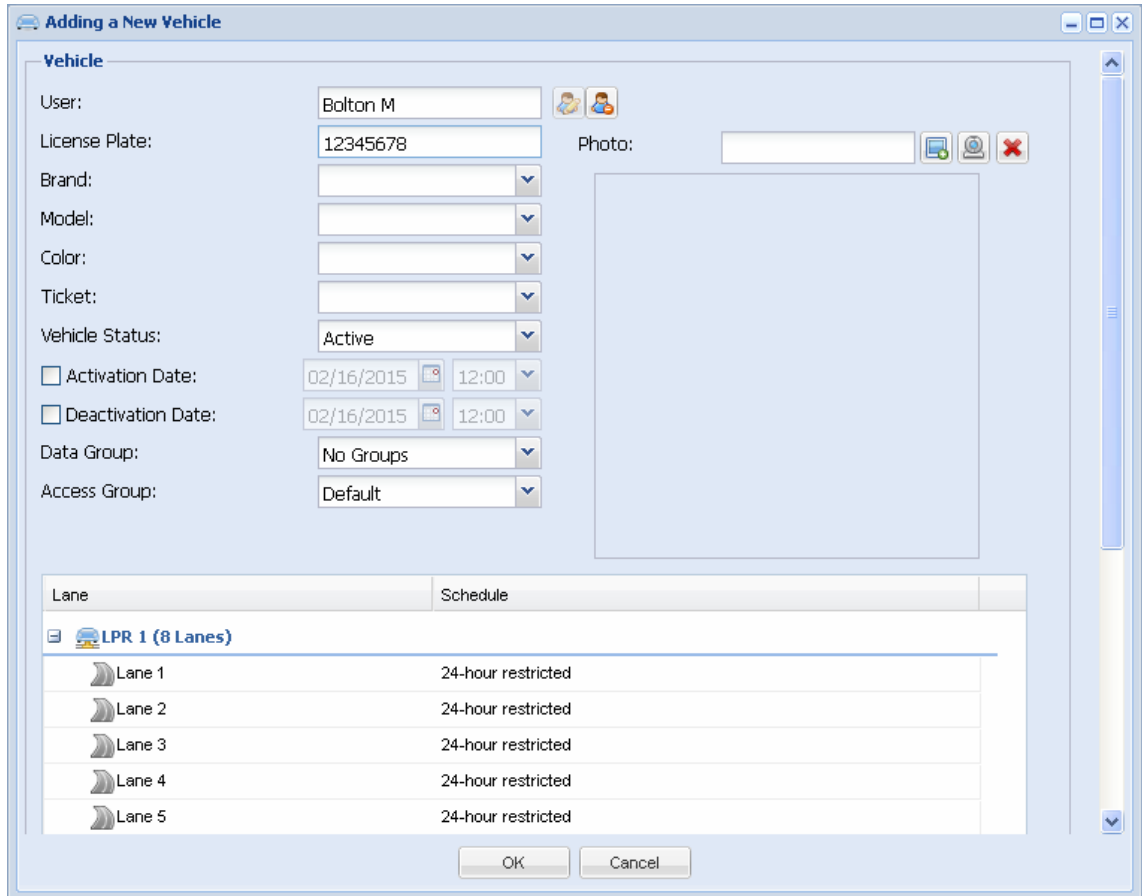
**Note:** After adding or deleting an LPR through GV-ASWeb, the change will be reflected in the LPR List in GV-ASManager.

---

### 13.9.2 Vehicle List

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

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



**Adding a New Vehicle**

**Vehicle**

User: Bolton M

License Plate: 12345678

Brand: [Dropdown]

Model: [Dropdown]

Color: [Dropdown]

Ticket: [Dropdown]

Vehicle Status: Active

☐ Activation Date: 02/16/2015 12:00

☐ Deactivation Date: 02/16/2015 12:00

Data Group: No Groups

Access Group: Default

Photo: [Image Icon] [Camera Icon] [Red X Icon]

Lane	Schedule
<b>LPR 1 (8 Lanes)</b>	
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

OK Cancel

Figure 13-44

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

---

**Note:** After adding, editing or deleting a vehicle through GV-ASWeb, the change will be reflected in the Vehicle List in GV-ASManager.

---

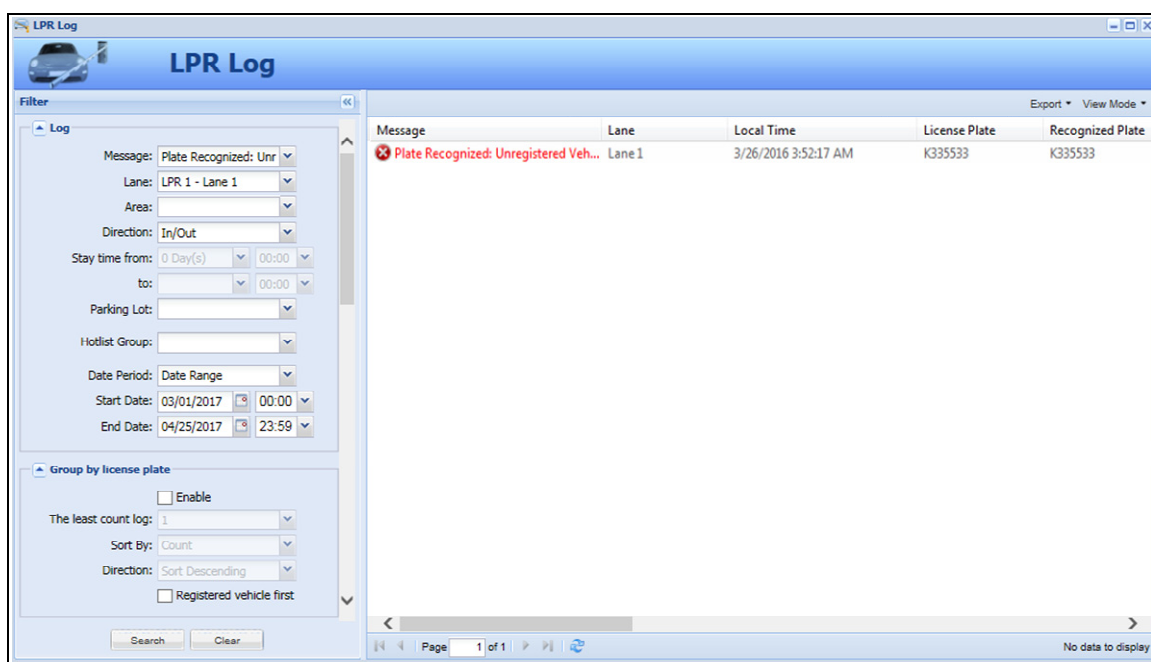
### 13.9.3 LPR Log

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

#### Setting Search Criteria

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

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



The screenshot shows the LPR Log application window. On the left is a 'Filter' panel with various search criteria. The 'Log' section is expanded, showing filters for Message, Lane, Area, Direction, Stay time, Parking Lot, Hotlist Group, Date Period, Start Date, and End Date. The 'Group by license plate' section is also visible. The 'Search' button is at the bottom of the filter panel. On the right is a table with the following columns: Message, Lane, Local Time, License Plate, and Recognized Plate. The table contains one row with the message 'Plate Recognized: Unregistered Veh...', Lane 1, Local Time 3/26/2016 3:52:17 AM, License Plate K335533, and Recognized Plate K335533. The status bar at the bottom indicates 'Page 1 of 1' and 'No data to display'.

Message	Lane	Local Time	License Plate	Recognized Plate
Plate Recognized: Unregistered Veh...	Lane 1	3/26/2016 3:52:17 AM	K335533	K335533

Figure 13-45

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 the 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.

### Search Results Window

Below is an example of a search results window.

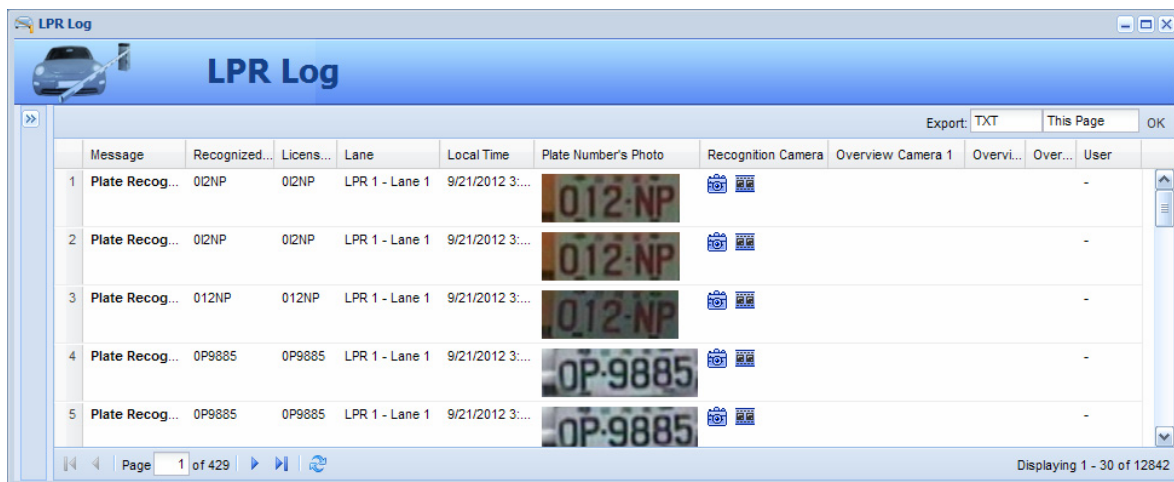





Figure 13-46

A snapshot of the detected license plate will be displayed.

: Indicates the availability of the recorded video.

: Indicates 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).

To see how to export logs, refer to *10.4.3 Exporting Logs* for details. To see how to customize the search results columns, refer to *10.4.4 Defining Columns* for details.



**Note:** You can play back video only when Remote ViewLog Service included in Control Center Server is enabled on the DVR. And the Remote ViewLog function is enabled on Video Server or Compact DVR.

## Obtaining the positions

If the license plates of vehicles that have entered and exited the monitored areas are recognized in the connected LPR cameras, their driving routes will be displayed on the map. To track the positions 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*.

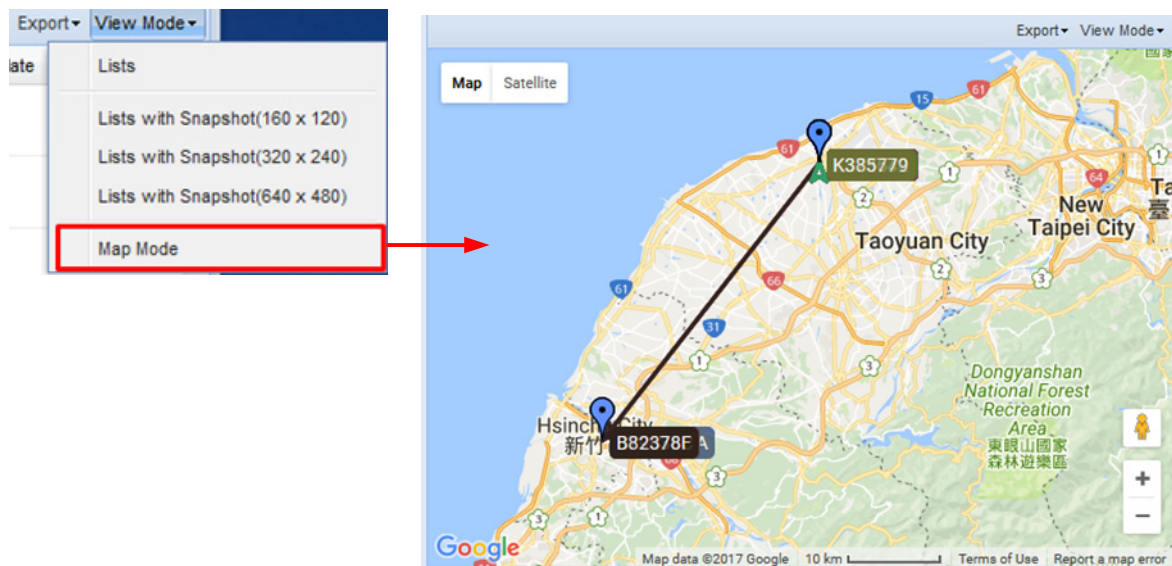


Figure 13-47

### 13.9.4 Access Group Setup

Using GV-ASWeb, you can remotely set up access groups to restrict who can access which channel at what time. On the main page of GV-ASWeb, click the **Access Groups** icon



For details on how to set up access groups, refer to *Setting Access Groups* in Chapter 4.

 The screenshot shows the 'Access Groups Setup' window. On the left is a list of access groups: 'Default' (selected) and 'FAE'. The main area displays the configuration for the 'Default' group. At the top, 'Name' is 'Default' and 'Data Group' is 'No Groups'. Below are two sections: 'Controller A\_Reception (2 Doors)' and 'LPR 1 (8 Lanes)'. The 'Controller A\_Reception' section has a table with 2 rows: 'Gate A' and 'Gate B', both with a '24-hour restricted' schedule. The 'LPR 1' section has a table with 8 rows: 'Lane 1' through 'Lane 8', all with a '24-hour restricted' schedule. The 'Lane 1' row is highlighted. At the bottom are 'Save' and 'Close' buttons.
 

Door	Schedule
<b>Controller A_Reception (2 Doors)</b>	
Gate A	24-hour restricted
Gate B	24-hour restricted

Lane	Schedule
<b>LPR 1 (8 Lanes)</b>	
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
Lane 6	24-hour restricted
Lane 7	24-hour restricted
Lane 8	24-hour restricted

Figure 13-48

## **Chapter 14 GV-Access Mobile Applications**

GV-Access Mobile Applications allow you to access up to 5 GV-ASManagers through an iOS or Android mobile device. You can watch camera live view, check door status, unlock doors and open an LPR lane.

For details on system requirements, installation and setup, visit our website:

<http://www.geovision.com.tw/products.php?c2=147>

## Chapter 15 GV-ASNotify

GV-ASNotify is an application that allows you to watch live view and communicate with the surveillance site through the cameras and GV-CS1320 connected with GV-ASManager. You can connect to multiple GV-ASManagers at a time, and remotely unlock the doors when needed.

If a GV-CS1320 is connected, a notification message and snapshot appear when the bell button (touch pad) on the GV-CS1320 is activated. You can then use the microphone and speaker functions of GV-ASNotify to communicate with the visitor requesting access to the building, while monitoring the live view of the GV-CS1320 at the same time.

GV-ASNotify also supports two-way audio for GV-IP Cameras with audio functions, but the bell button notification function is only available for GV-CS1320.

### 15.1 Installing GV-ASNotify

The GV-ASNotify App can be downloaded from the GeoVision website.

- **Downloading from GeoVision Website**

Go to <http://www.geovision.com.tw/download/product/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: <http://www.microsoft.com/en-us/download/details.aspx?id=15805>.

---

## 15.2 Connecting to GV-ASManager

Before GV-ASNotify can connect to a GV-ASManager, you must enable Remote Monitor Server on the GV-ASManager to allow the remote access:

- Click **Tools** on the menu bar of the GV-ASManager, select **Servers** and enable **Remote Monitor Server**. When the server is started, the icon  appears at the bottom of the main screen.

- Run **GV-ASNotify.exe**.
- To connect to a GV-ASManager, click the **Add Host** button. This dialog box appears.

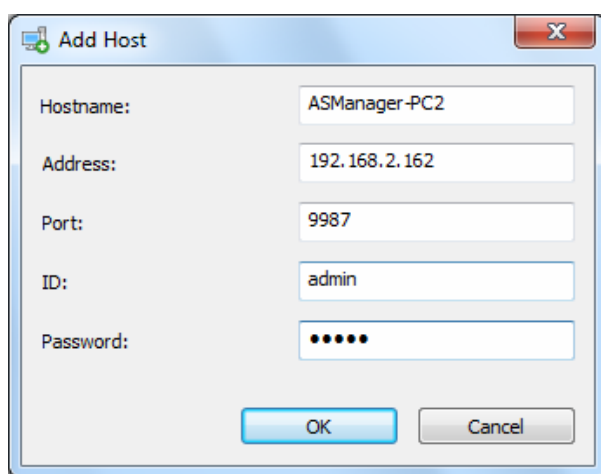


Figure 15-1

- Type the IP address, login ID, and password of the GV-ASManager. Modify the default port 9987 if needed.
- Click **OK**. The GV-ASManager is added to the host list.

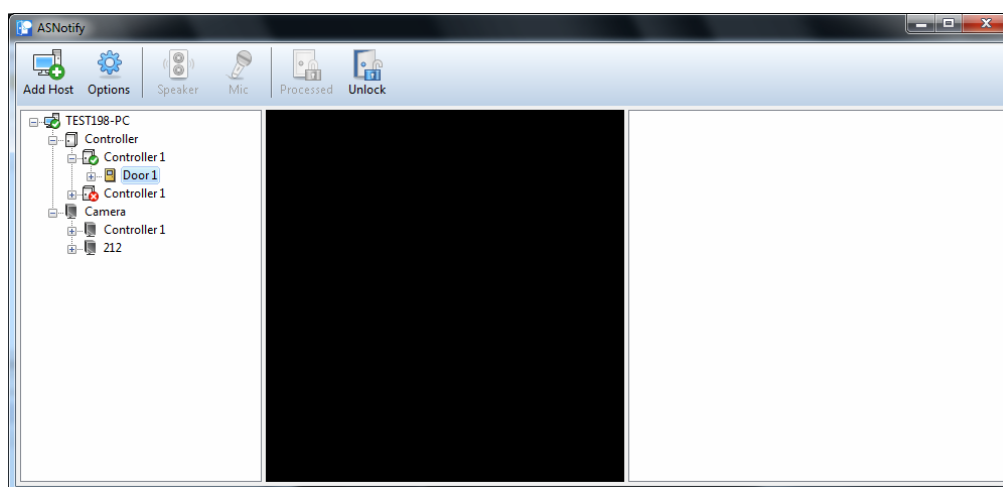


Figure 15-2

### 15.3 Utilizing GV-ASNotify

1. In the host list, select a camera or GV-CS1320 connected to the GV-ASManager to access its live view

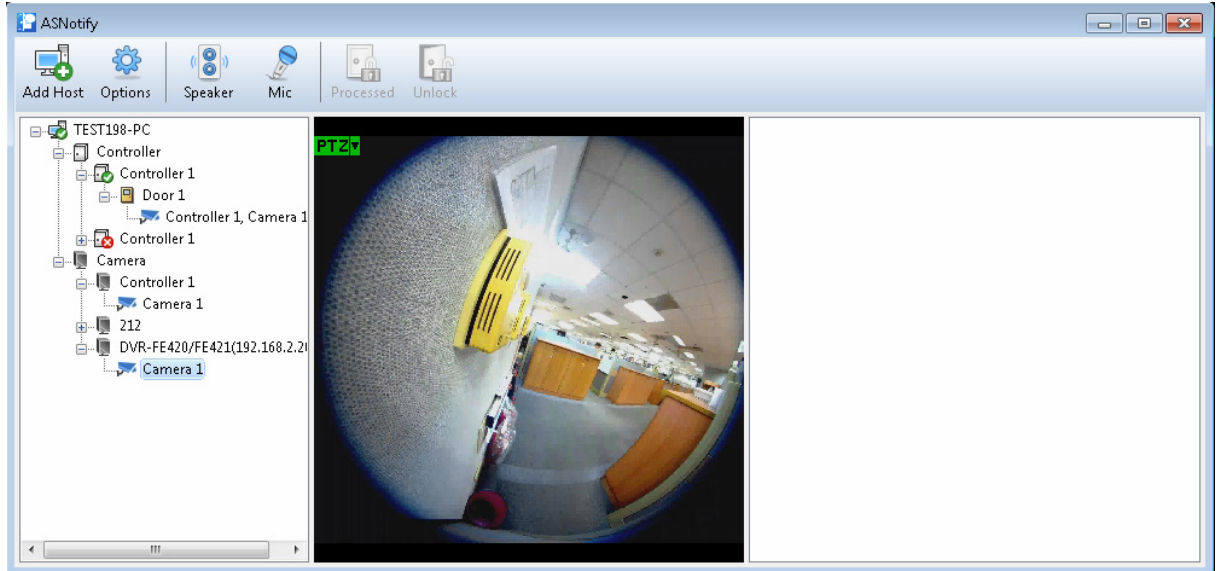


Figure 15-3

2. To speak to the surveillance site, click the **Mic** button.
3. To listen to audio from the surveillance site, click the **Speaker** button.

---

**Note:** To use the two-way audio function:

- The device must be a GV-IP Camera with audio functions or a GV-CS1320.
  - GV-ASManager must be connected to the GV-IP Camera / GV-CS1320 directly. Audio is not supported when the GV-ASManager is connected to the camera through a GV-DVR / GV-NVR / GV-VMS / GV-Video Server / GV-Compact DVR.
-

## GV-CS1320 Functions

If the GV-ASManager is connected to a GV-CS1320, a snapshot and notification will appear on the right when the bell button on the GV-CS1320 is activated.

1. You can use the **Speaker** and **Mic** buttons to communicate with the surveillance site or use the **Unlock** button to grant access.
2. After handling the event, you can mark the notification as “Processed” by selecting the notification and then clicking the **Processed** button. Events marked as Processed will be grayed out.

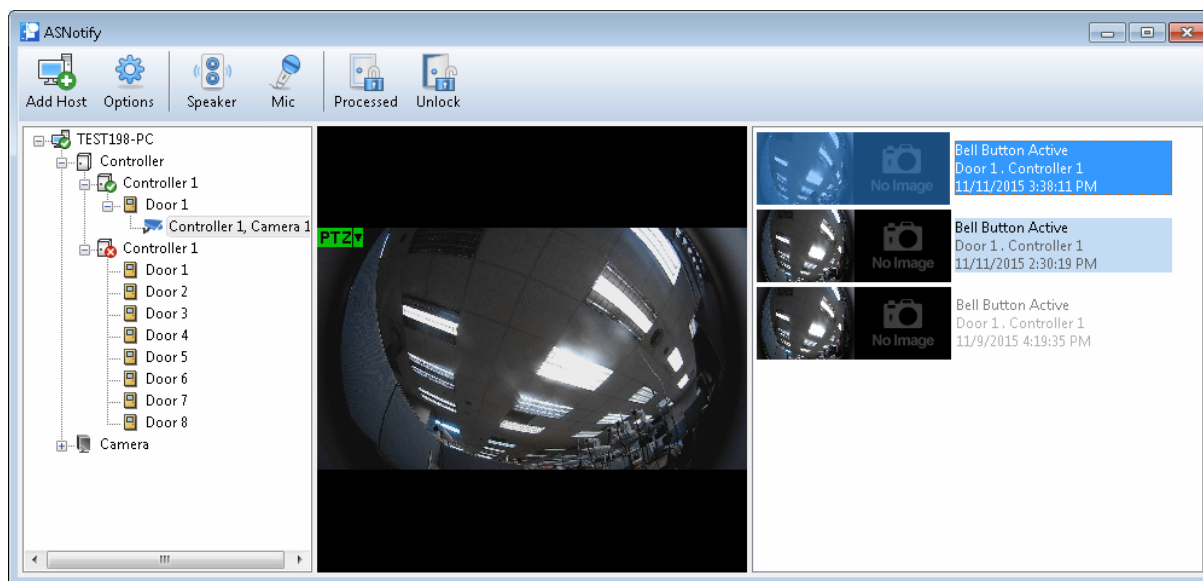


Figure 15-4

3. To trigger a computer audio alarm when the bell button is activated, click the **Options** button, select **Invoke Alarm**, and use the drop-down list to select an alarm sound.

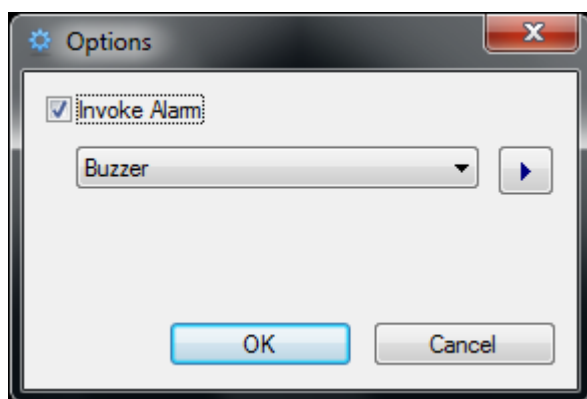


Figure 15-5

## Chapter 16 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 Access or SQL Server formats.

---

**Note:** GV-ASManager has a 2 GB database size limit. To get additional data allowance, you can install and create a Microsoft SQL Server.

---

### 16.1 Starting the Database Tools

To start the Database Tools, you may use one of the methods:

- When you log in the GV-ASManager for the first time, this message will pop up: “*Cannot open database. Would you like to set up database?*”. Click **Yes**. The following Database Tools dialog box will appear.
- You can also run **ASDBManager.exe** from the program folder to access the Database Tools.

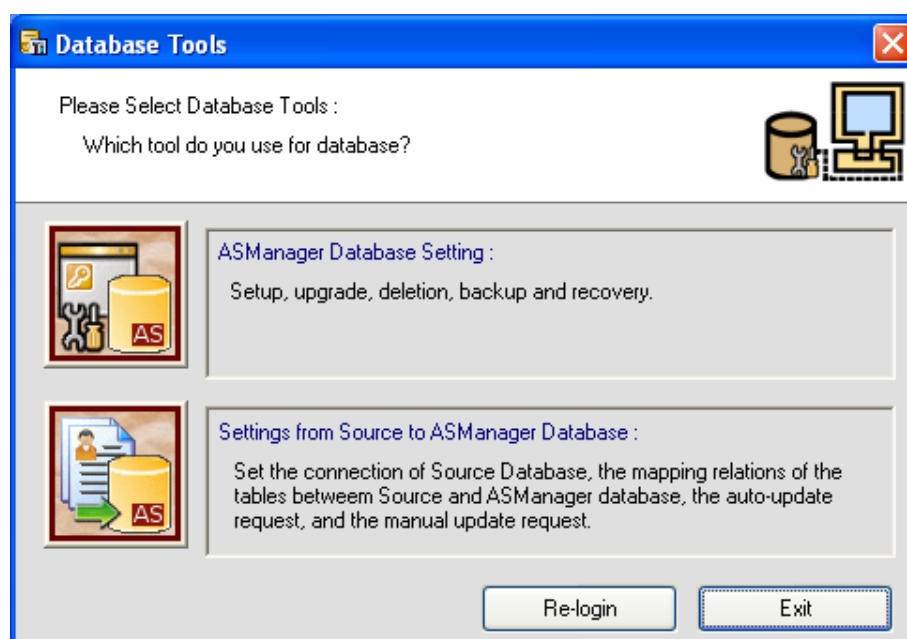


Figure 16-1



## 16.2 Creating a Database

You can select either Microsoft Office Access or Microsoft SQL Server as the database of GV-ASManager.

1. Click the **ASManager Database Setting** button on the Database Tools dialog box (Figure 16-1).
2. Click the **Setup MDB/MSSQL Database for ASManager** button. This dialog box appears.

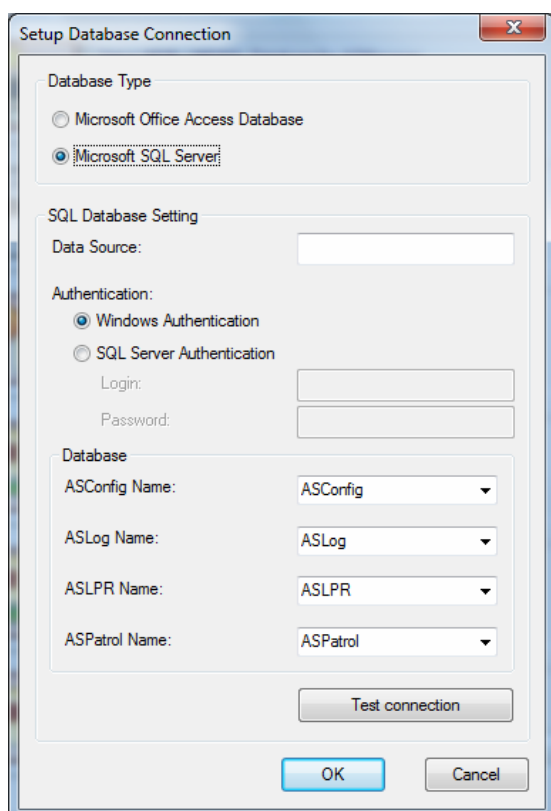


Figure 16-2

3. To use Access as the database, select **Microsoft Office Access Database** and click **OK**. The database is created in the local computer.
4. To use 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. Under Database, name the databases for Configuration files and Log files that will be created on the SQL server separately.
  - c. Click **Test Connection** to test the connection to the SQL server.
  - d. Click **OK**. The databases are created in the SQL server.

### 16.3 Other Database Settings

You can upgrade, delete, back up, restore, and compact the database of GV-ASManager. Click **ASManager Database Setting** button on the Database Tools dialog box (Figure 16-1). This dialog box appears.



Figure 16-3

**[Upgrade to latest database version]** You can manually upgrade the database to the latest version.

**[Delete ASManager Database]** Removes the database from the local computer or the SQL Server.

**[Backup Database]** Set the backup storage path and select the type of files you want to back up: Config, Logs, Account Profiles. You can also set up a **Schedule** to automatically back up the database.

**[Recovery Database]** You can restore the Config, Logs, Account Profiles you backed up previously to the current computer or import them to another computer.

**[Compact Database]** Compacts the database to reduce the size of the database. You can also set up a **Schedule** to automatically compact the database.

---

**Note:** To automatically back up Log and Image files, use the **Auto Backup** function. See [8.3 Startup, Backup and Export Setup](#).

---

## 16.4 Mapping Source Database

The Source Database function can convert **OLE DB**, **Active Directory** database and **excel** files into GV-ASManager (Access or SQL Server) database. Click the **Setting from Source to ASManager Database** button on the Database Tools dialog box (Figure 16-1). This dialog box appears.

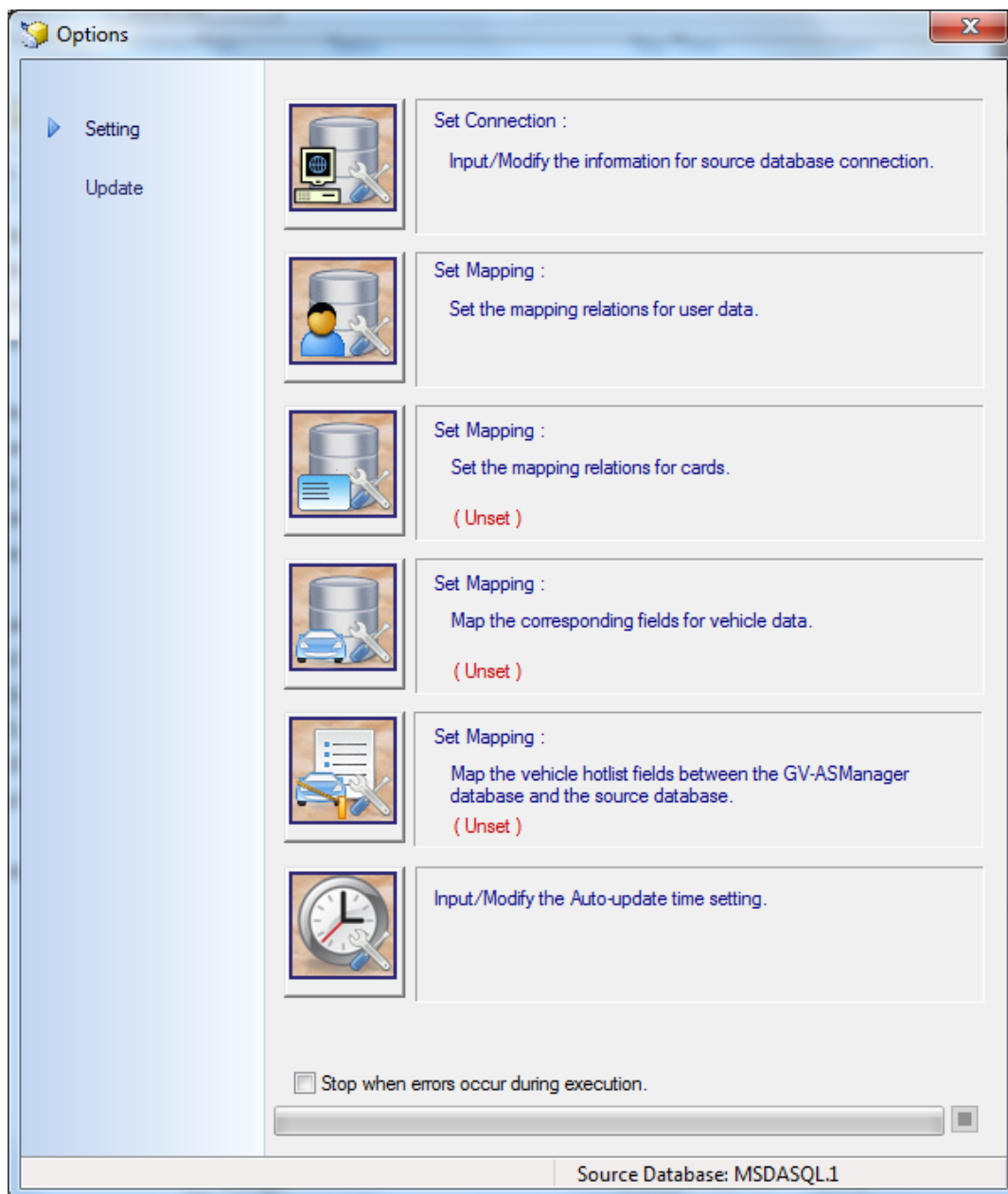


Figure 16-4

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.

### 16.4.1 Converting Data from the Active Directory Database

1. Click the **Set Connection** button on the Options dialog box (Figure 16-4). The Source Database dialog box appears.
2. Select **Active Directory**. This dialog box appears.

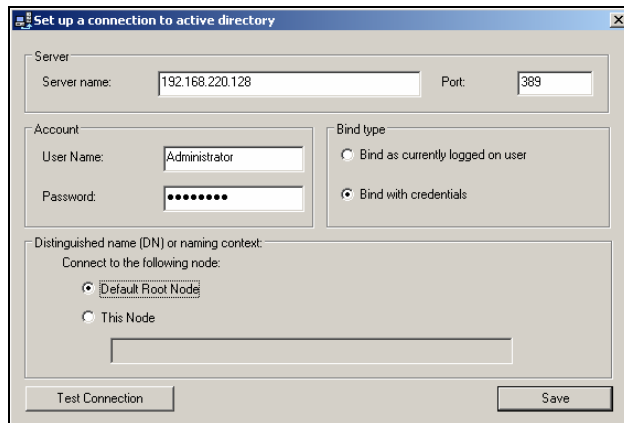


Figure 16-5

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 16-4) 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 15-4) 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 16-4) and specify the time in minutes.

## 16.4.2 Converting Data from the OLE Database

To convert data from the OLE database, you need to go through these instructions:

- A. Connect an OLE database
- B. Map the user data
- C. Map the card / vehicle data
- D. Convert the data from the source database

### A. To connect an OLE database:

1. Click the **Set Connection** button on the Options dialog box (Figure 16-4). The Source Database dialog box appears.
2. Select **Other Database**. This dialog box appears.

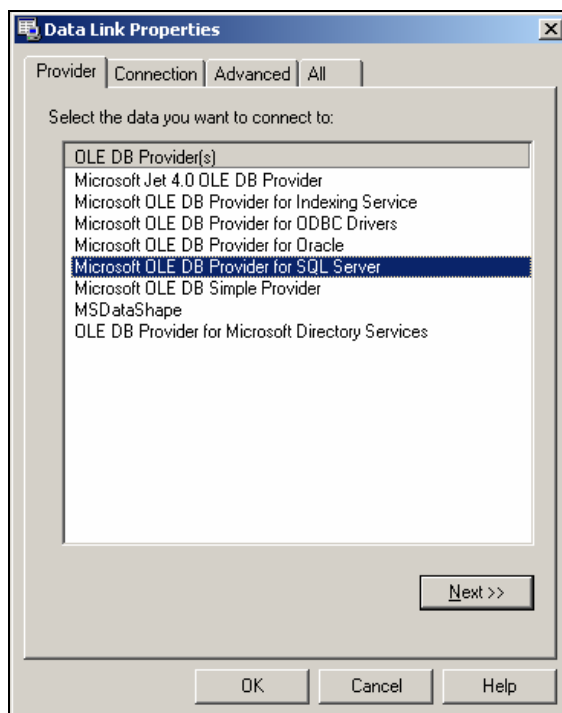


Figure 16-6

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.

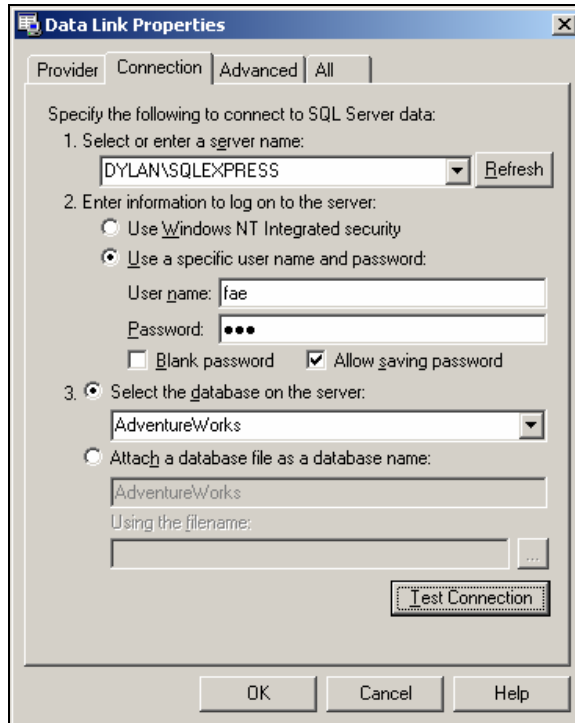


Figure 16-7

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.



## B. To map the user data:

1. Click the **Set the mapping relations for user** button in the Options dialog box (Figure 15-4). This window appears.

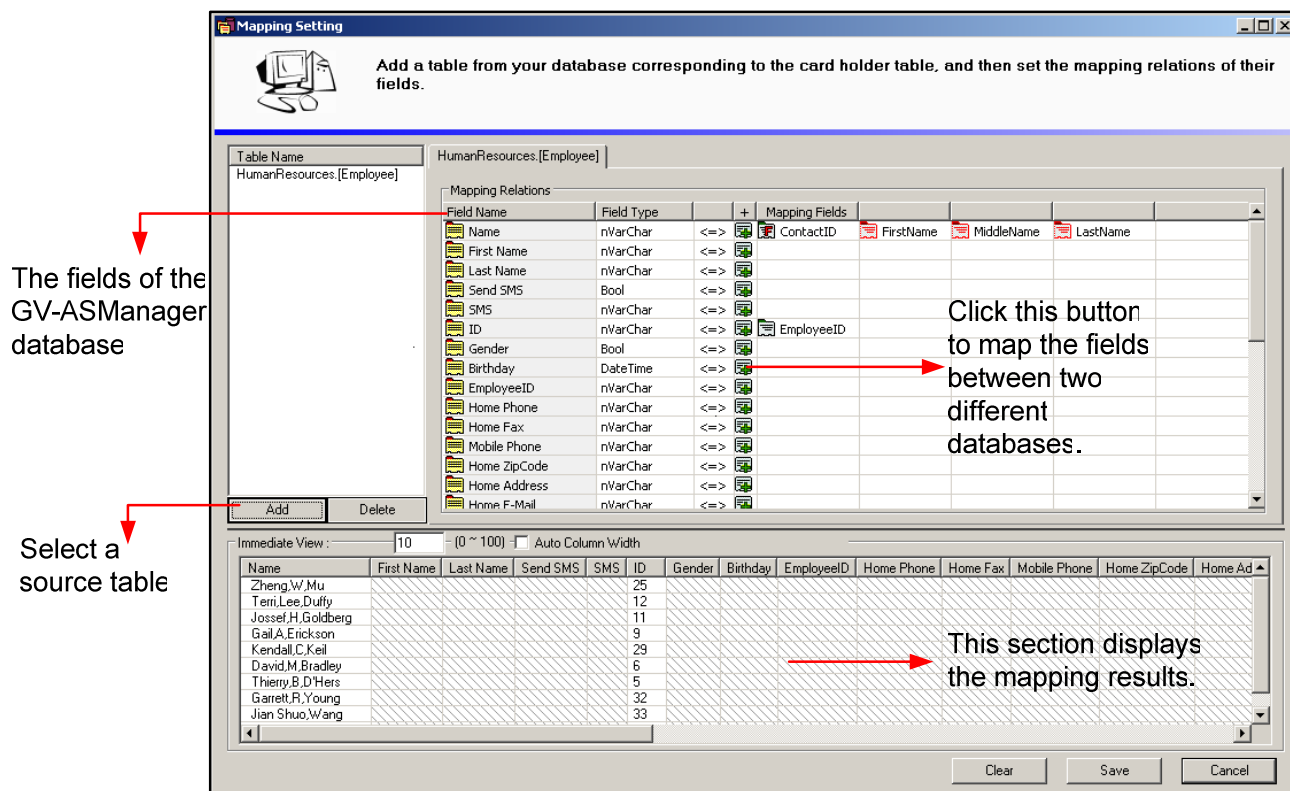




Figure 16-8

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.

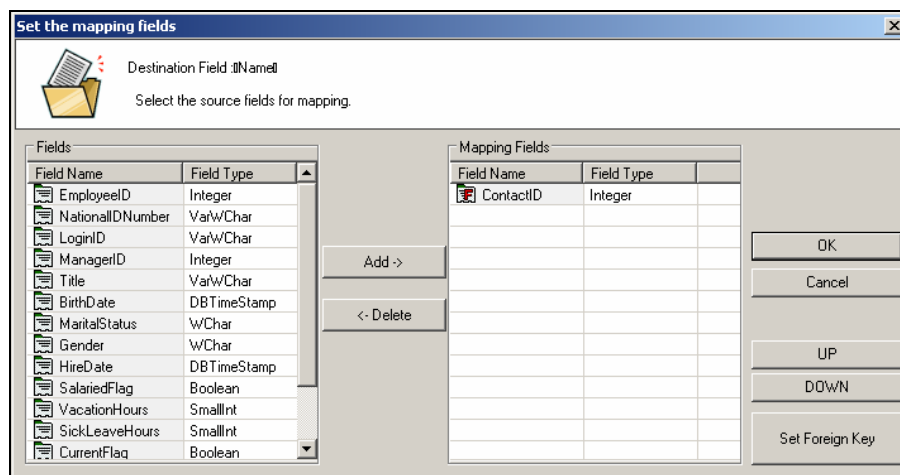


Figure 16-9

5. In the left side 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 16-9), 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.

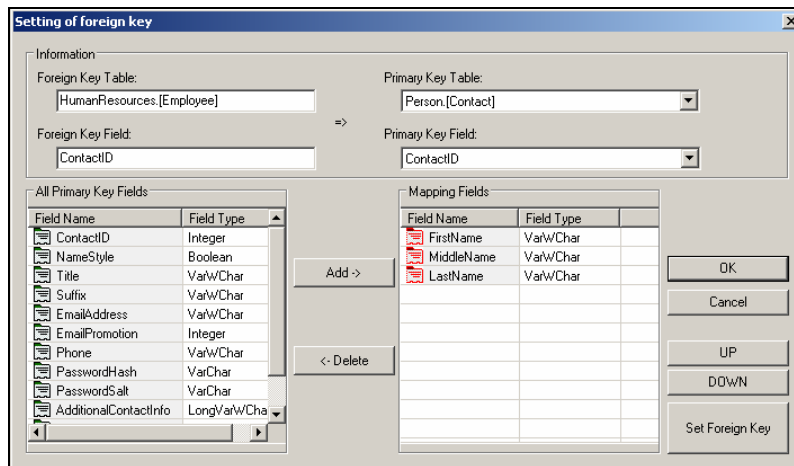
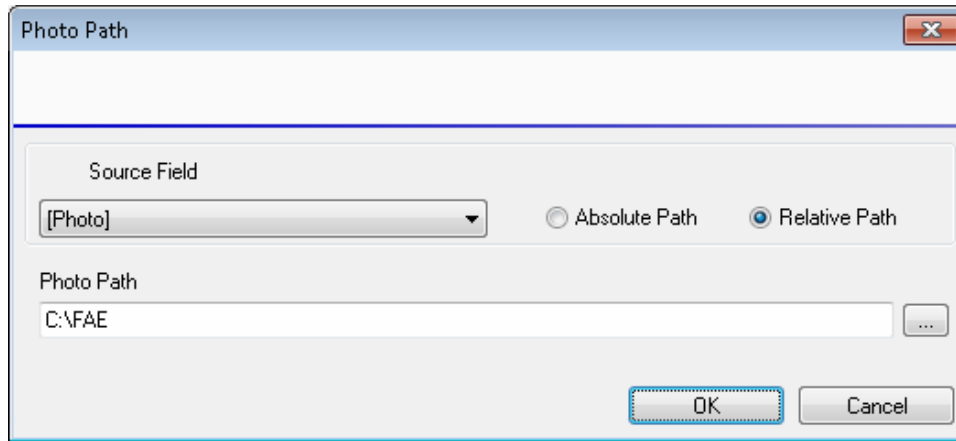


Figure 16-10

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 side 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 16-10), 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 16-8), 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**.



The dialog box titled "Photo Path" has a "Source Field" dropdown menu with "[Photo]" selected. Below it, there are two radio buttons: "Absolute Path" (unselected) and "Relative Path" (selected). A "Photo Path" text field contains "C:\FAE". At the bottom are "OK" and "Cancel" buttons.

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

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

### C. To map the card / vehicle data:

1. Click the **Set the mapping relations for cards / vehicles** button in the Options dialog box (Figure 16-4). This window appears.

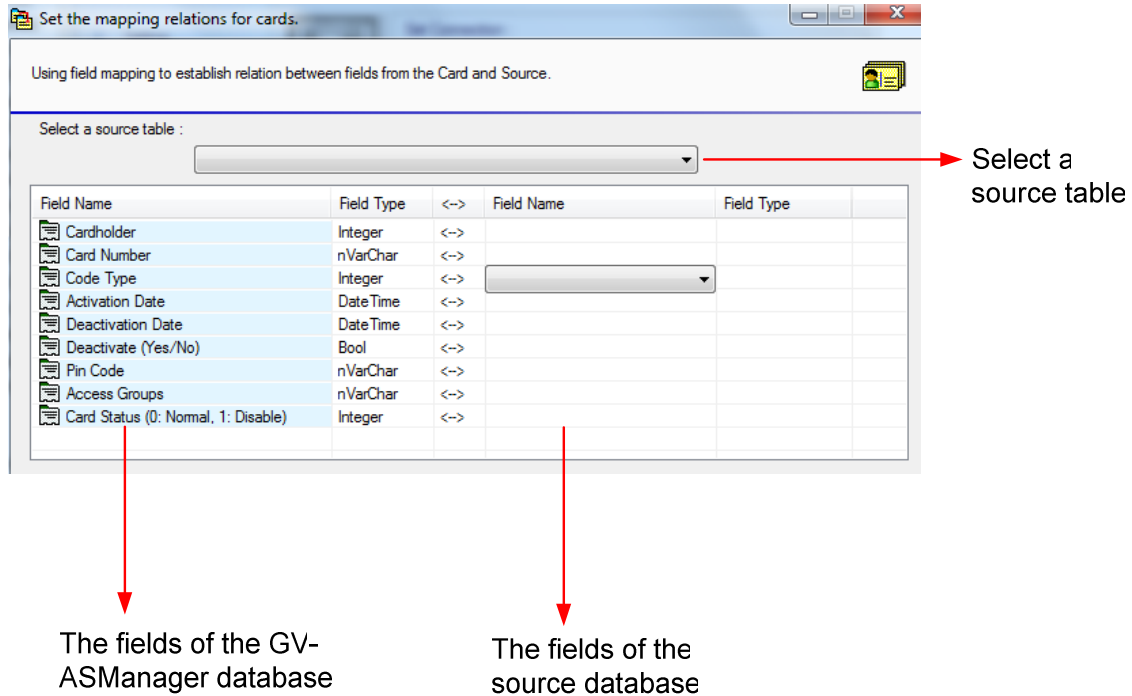


Figure 16-11

2. Select a related table on the source database.
3. Click the **Field Name** column on the right side to map each field of the GV-ASManager database and the source database.

### D. To convert the data from the source database:

1. Click the **Update Cardholder Data manually** button in the Options dialog box (Figure 16-4) 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 16-4) 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 16-4) and specify the update time.

### 16.4.3 Converting Data from an Excel File

To convert data from an excel file:

1. Click the **Set Connection** button on the Options dialog box (Figure 16-4). The Source Database dialog box appears.
2. Select **Other Database**, select **Excel File**, and click **OK**.

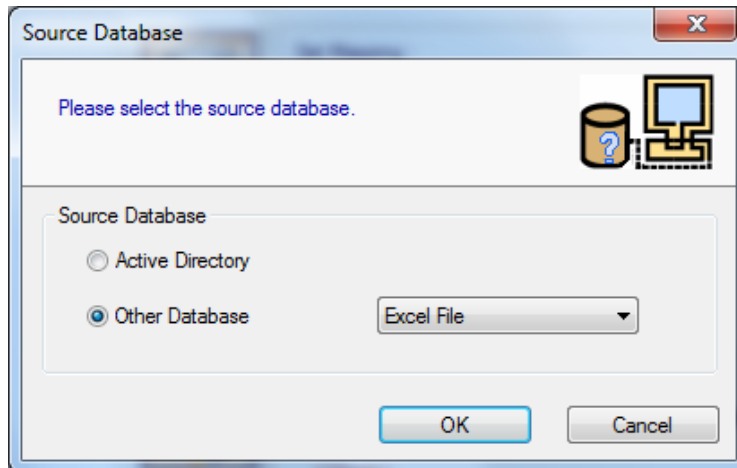



Figure 16-12

3. Locate the storage path of the excel file.
4. Follow the steps in *To map the card / vehicle data* and *To map the user data* in the previous section to match the columns of the excel files with the fields in GV-ASManager.

## Chapter 17 Net Module Utility

With the **Net Module Utility** installed, you can change settings and update the firmware of the GV-AS / GV-EV Controller.

1. Visit <http://www.geovision.com.tw/download/product/GV-ASManager>, select

**Supplemental Utilities**, click the **Download** icon  of **Net Module Utility** and follow the onscreen instructions to install the program.

2. Run **Net Module Utility**. This window appears.

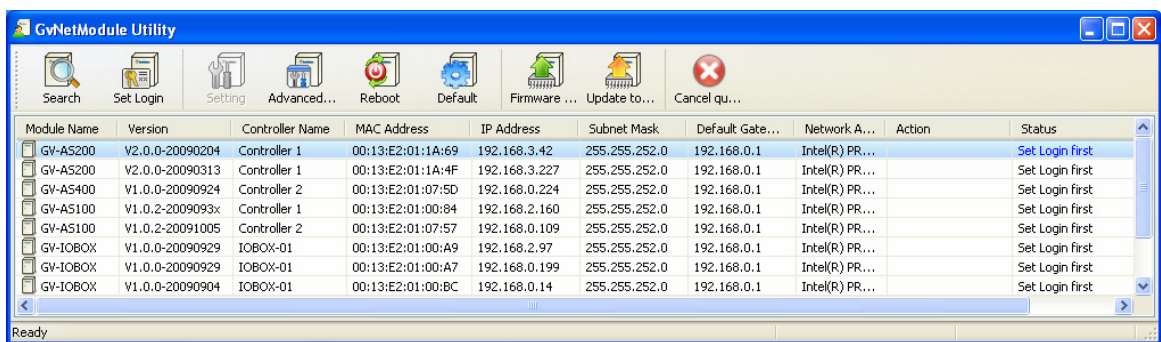


Figure 17-1

The buttons on the window:

- **Search:** Click this button to locate any GV-AS / GV-EV Controller or GV-I/O device on the same LAN.
- **Set Login:** You can select the desired modules from the list, and click this button to log on to these modules with the same ID and password together.
- **Setting:** Click this button to change the Machine Name, IP address, 3DES Code, Device Port, login ID and password.
- **Advanced Setting:** Click this button to directly link to the Web interface of the selected module.
- **Reboot:** Click this button to perform a warm boot of the selected module. This operation will keep the current configuration.
- **Default:** Click this button to reset all configuration parameters to their factory settings. This may take 5 seconds to complete.
- **Firmware Update:** Click this button and assign the firmware file for update.
- **Update to the latest firmware version:** The GV-ASManager software comes with the latest GV-AS / GV-EV Controller firmware. Clicking this button can upgrade your controller firmware.

## Chapter 18 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 the fixed IP to the GV-ASManager and GV-AS / GV-EV Controller respectively. This way can determine if the problem is caused by the faulty devices and incorrect network settings.

1. Disconnect the hub or switch, which connects the GV-ASManager and GV-AS / GV-EV Controller, from the network.
2. Give the GV-ASManager a fixed IP address that is NOT used by another device, e.g. 192.168.0.154.

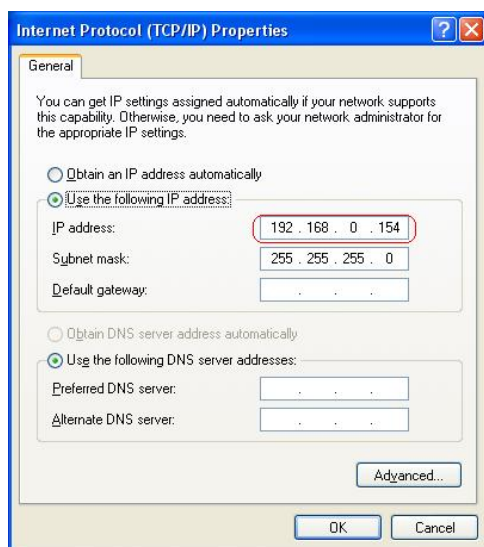


Figure 18-1

3. Reset the GV-AS / GV-EV Controller module and Ethernet module to factory defaults.
  - a. Plug the GV-ASKeypad to the 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.

4. Open the browser and enter the GV-AS / GV-EV Controller default address:

<http://192.168.0.100>

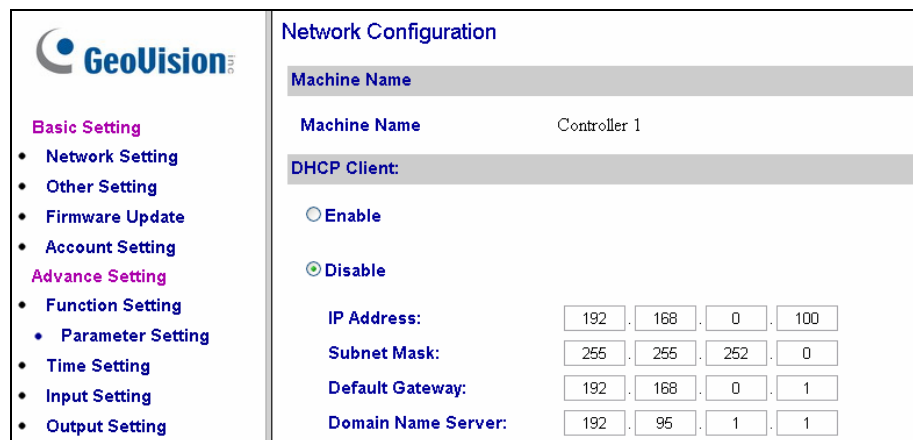


Figure 18-2

5. In the IP address field, give the controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
6. On the GV-ASManager, enter the following settings:

**Controller ID:** 1

**Network:** TCP/IP

**IP:** 192.168.0.XXX

**Port:** 4000

**User:** admin

**Password:** admin

**Crypto key:** 12345678

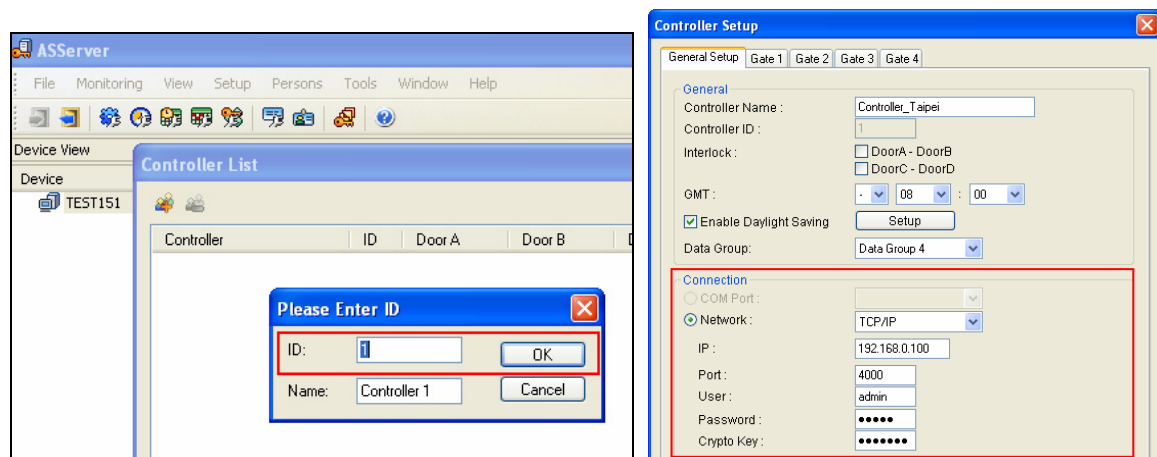



Figure 18-3

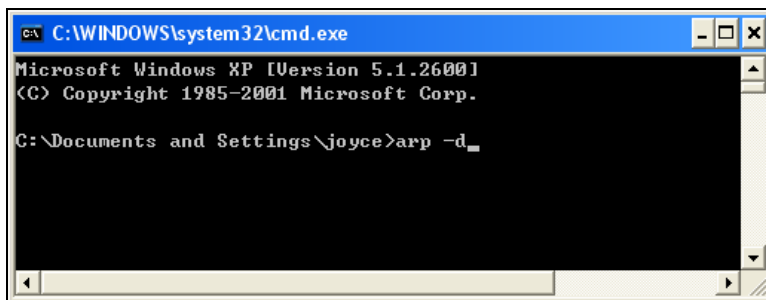


7. The connection between the GV-ASManager and the controller should be established, and the connection icon  should appear. If disconnection happens after you connect the hub or switch to the network, then it should be other network problems. Please contact your network administrator.

## **Q2: The connection established between the 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:

1. Disconnect the hub or switch, which connects to the GV-ASManager and GV-AS / GV-EV Controller, from the network.
2. Run Windows **Command Prompt**. Take Classic Windows Start Menu for example, click **Start**, select **Accessories** and click **Command Prompt**.
3. Type **arp -d** and press **Enter**.



*Figure 18-4*

4. Give the GV-ASManager a fixed IP address that is NOT used by another device. See Figure 17-1.
5. Open the browser and enter the assigned IP address of the controller. The Network Configuration page appears. See Figure 18-2.
6. In the IP address field, give the controller an IP address that is NOT used by another device, e.g. 192.168.0.XXX.
7. On the GV-ASManager, enter the following settings. See Figure 18-3.

**Controller ID:** 1

**Network:** TCP/IP


**IP:** 192.168.0.XXX

**Port:** 4000

**User:** admin

**Password:** admin

**Crypto key:** 12345678

8. The connection between the 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 the card when the connection between the 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 settings. Refer to Step 3 in Question 1.

**Q4: The GV-ASManager cannot retrieve the video from the DVR for playback.**

1. Make sure the **Remote ViewLog Service** on **Control Center Server** is enabled on the DVR.
2. Make sure the time on the GV-ASManager and the DVR is consistent.
3. Make sure the event file you want to play back has been created completely on the DVR. For example, the assigned time length of every recorded event on the 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: The GV-ASManager cannot receive card messages from the GV-Reader connected to the GV-AS / GV-EV Controller through RS-485 interface.**

1. Make sure the GV-Reader is correctly wiring to the controller and Switch 4 on the 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 the 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, refer to the Download Guide or visit <https://www.microsoft.com/en-us/download/details.aspx?id=15805>

**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 the push notification of the 'door bell activated' event, 2 additional ports are required: 2195 (for iOS) and 443 (for 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](mailto:support@geovision.com.tw)

## Appendix

### A. Compatible IP Devices

This list provides the supported IP device brands. For detailed information on the supported IP devices, refer to Supported IP Camera List on GeoVision's Website:

[http://www.geovision.com.tw/\\_upload/files/support\\_list.pdf](http://www.geovision.com.tw/_upload/files/support_list.pdf)

GeoVision
ACTi
Arecont Vision
AVTech
AXIS
Bosch
Canon
CNB
D-Link
Etrovision
Hikvision
Hunt
IQeye
JVC
LG
MESSOA
MOBOTIX
Panasonic
Pelco
RIVA
Samsung
Sanyo
SONY
UDP
Verint
VIVOTEK

## B. 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 <i>GV-AS / GV-EV Controller User’s Manual</i> . For software settings, see Step 4 in <i>4.2.2 Step 2: Configuring the Doors or Elevator Floors</i> .
Fire Alarm	Fire Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in <i>GV-AS / EV Controller User’s Manual</i> . For software settings, see Step 5 in <i>4.2.2 Step 2: Configuring the Doors</i> .
Held Open	Door <name> is held open over the specified time. See Step 2 and 5 in <i>4.2.2 Step 2: Configuring the Doors</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 <Number> is suspended.
Access Denied: Wrong PIN	The access is rejected because the PIN number entered is wrong.
Access Denied: Card Expired	The access is rejected because Card <Number> 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. 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 <i>GV-AS / GV-EV Controller User’s Manual</i> . For software settings, see Step 4 in <i>4.2.2 Step 2: Configuring the Doors or Elevator Floors</i> .
Fire Alarm	Fire Inputs are triggered. For hardware settings, see <i>Connecting Input Devices</i> in <i>GV-AS / GV-EV Controller User’s Manual</i> . For software settings, see Step 4 in <i>4.2.2 Step 2: Configuring the Doors or Elevator Floors</i> .
Held Open	Door <name> is held open over the specified time. See <i>4.2.2 Step 2: Configuring the 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. <i>See 4.2.2 Step 2: Configuring the Doors or Elevator Floors.</i>
Card or Common Mode	Door <name> is on the Card or Common Mode. <i>See 4.2.2 Step 2: Configuring the Doors or Elevator Floors.</i>
Card and PIN Code Mode	Door <name> is on the Card and PIN Code mode. <i>See 4.2.2 Step 2: Configuring the Doors or Elevator Floors.</i>
Card Mode	Door <name> is on the Card mode. <i>See 4.2.2 Step 2: Configuring the Doors or Elevator Floors.</i>
Fire Unlock Mode	Door <name> is unlocked after Fire Inputs are triggered. <i>See "Fire Action" in 4.2.2 Step 2: Configuring the Doors or Elevator Floors.</i>
Fire Lock Mode	Door <name> is locked after Fire Inputs are triggered. <i>See "Fire Action" in 4.2.2 Step 2: 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.

## C. E-Mail and SMS Alert Symbols

Icon	Description
	%M (Message): include related alert message.
	%T (Controller): include door controller's name.
	%D (Door): include triggered door's name.
	%L (Local Time): include local time.
	%U (UTC): include UTC time.
	%S (Snapshot): include snapshot.
	%Q (Direction): include directions for LPR lanes.
	%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 photo.

## D. 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.

## E. Supported Recognition Engines of PC LPR

GV-DVR LPR / GV-VMS LPR V5.0.2.0 only supports the following versions of 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			