



User's Manual V4.2.1





© 2014 GeoVision, Inc. All rights reserved.

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

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

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

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

May 2014

Contents

Note for Us	sers l	Jpgrading GV-ASManager	vi
Software C	omp	atibility	viii
Chapter 1	r 1 Introduction		1
	1.1	Main Features	2
	1.2	Concepts	
	1.3	Optional Devices	
Chapter 2	Inst	allation	7
	2.1	System Requirements	7
	2.2	Installing the GV-ASManager	
	2.3	Logging in	
Chapter 3	The	Main Screen of GV-ASManager	
	3.1	Main Screen	11
		3.1.1 Toolbar	12
	3.2	Device View	14
		3.2.1 Controls on the Window	14
	3.3	Monitoring Windows	16
		3.3.1 Controls on the Window	16
		3.3.2 Customizing a Monitoring Window	17
		3.3.3 Arranging Monitoring Windows	18
Chapter 4	Sett	ings	
	4.1	Setup Flowchart	19
	4.2	Adding Controllers	20
		4.2.1 Step 1: Configuring a Controller	20
		4.2.2 Step 2: Configuring the Doors or Elevator F	Floors23
	4.3	Setting Cards	31
		4.3.1 Adding a Single Card	31
		4.3.2 Adding a Group of Cards	
		4.3.3 Importing/Exporting Card Data	35
	4.4	Setting Weekly Schedules	
		4.4.1 Step 1: Setting Time Zones	
		4.4.2 Step 2: Setting Weekly Schedules	
		4.4.3 Step 3: Setting Holidays	41
	4.5	Setting Access Groups	42
	4.6	Setting Users	44
		4.6.1 Adding a User	44
		4.6.2 Assigning a Card to a User	45
		4.6.3 Sending SMS Alerts	45

		4.6.4 Customizing a Data	Field	45
		4.6.5 Importing/Exporting	User Data	47
Chapter 5	Vid	o Integration		48
	5.1	Mapping Cameras		48
	5.2	Accessing a Live View		50
		5.2.1 Live Video Window		51
	5.3	Accessing a Video Image		52
	5.4	The MultiView Window		52
		5.4.1 Adding a Matrix View	v	54
	5.5	Retrieving Recorded Video		55
Chapter 6	Ant	Passback		57
	6.1	Anti-Passback		58
	6.2	Local Anti-Passback		59
	6.3	Global Anti-Passback		61
		6.3.1 Step 1: Enabling Glo	bal Anti-Passback	61
		6.3.2 Step 2: Configuring A	Areas	62
		6.3.3 Step 3: Configuring I	Readers	62
		6.3.4 Step 4: Configuring I	Door Contacts	63
		6.3.5 Step 5: Locating Use	Prs	64
Chapter 7	Pat	ol Tour		65
	7.1	Creating Patrol Tour		65
	7.2	Activating the Patrol Tour		68
	7.3	Monitoring Patrol Activities		70
	7.4	Accessing Patrol Log		71
Chapter 8	Oth	r Functions		72
	8.1	Setting Up System User		72
		8.1.1 Adding a New User.		72
		8.1.2 Editing an Exiting Us	er	74
	8.2	Setting Up Alert Notification		75
		8.2.1 Setting SMS Server.		75
		8.2.2 Setting E-Mail Serve	r	76
		8.2.3 Setting Notification		77
	8.3	Startup, Backup and Export S	Setup	79
	8.4	Setting Up GV-GF Fingerprin	It Readers	81
	8.5	Scanning Driver's Licenses a	Ind Business Card	82
	8.6	Setting Hot Keys to Quickly (Control Doors	84
	8.7	Defining New Card Formats.		85
Chapter 9	GV-	ASRemote		87
	9.1	Installing GV-ASRemote		87

	9.2	The GV-ASRemote Window	87
		9.2.1 Toolbar	89
	9.3	Connecting to GV-ASManager	90
Chapter 10	GV	-ASWeb	92
	10.1	Connecting to GV-ASManager	92
	10.2	Accessing Live Video	95
	10.3	Accessing Logs	96
		10.3.1 Setting Search Criteria	96
		10.3.2 Log Window Icons	97
		10.3.3 Exporting Logs	97
		10.3.4 Defining Columns	97
	10.4	Adding and Deleting Controllers	99
	10.5	Adding and Deleting Cards and Users	100
	10.6	Searching, Adding and Deleting IP Cameras	104
	10.7	Setting Schedule	106
		10.7.1 Setting Daily Schedule	106
		10.7.2 Setting Weekly Schedule	107
		10.7.3 Specifying Holiday	108
	10.8	Setting Access Groups	108
	10.9	Setting Door Groups	109
	10.10	Configuring Areas for Anti-Passback	110
	10.11	1 Creating Maps	111
	10.12	2 Creating Accounts to Manage GV-ASWeb	114
Chapter 11	GV	-TAWeb for Workforce Schedule and Payroll	116
	11.1	Connecting to GV-ASManager	117
	11.2	Setting Up Workforce Schedule	119
		11.2.1 TA Shift: Setting Up a Daily Schedule	119
		11.2.2 TA Template: Setting Up a Schedule Template	122
		11.2.3 TA Holidays: Setting Certain Dates as Holidays	123
		11.2.4 TA Schedule: Assigning Schedules to Employees	124
	11.3	TA User: Specifying Hourly Pay	128
	11.4	TA Report: Looking Up Records	129
	11.5	Creating Accounts to Manage GV-TAWeb	133
Chapter 12	GV	-VMWeb for Visitor Management	134
	12.1	Connecting to GV-ASManager	134
	12.2	Creating Accounts to Manage GV-VMWeb	136
	12.3	Creating Visitor Profile	138
	12.4	Granting Visitor Access	139
	12.5	Searching GV-VMWeb Database	141

	12.6	Visitor \$	Self Registration	141
		12.6.1	Setting Up Mail Server in GV-VMWeb	142
		12.6.2	Creating a Visitor Account	144
		12.6.3	Creating a Visit Request	145
Chapter 13	Lice	ense Pla	ate Recognition	147
	13.1	Installir	g GV-DVR LPR	149
		13.1.1	System Requirements	149
		13.1.2	Installing LPR Plugin	150
		13.1.3	Inserting LPR Dongle	150
		13.1.4	Accessing Recognition Results on GV-DVR LPR	151
	13.2	Setting	Up GV-DVR LPR	152
		13.2.1	Step 1: Enabling LPR Functions on GV-DVR LPR	153
		13.2.2	Step 2: Adding GV-DVR LPR to GV-ASManager	154
		13.2.3	Step 3: Configuring a Channel	156
		13.2.4	Exporting LPR Data	
		13.2.5	Recognition Engine Version	164
	13.3	Setting	Up GV-DSP LPR	165
		13.3.1	Step 1: Enabling Connection with GV-ASManager on	GV-DSP
		LPR	165	
		13.3.2	Step 2: Adding GV-DSP LPR to GV-ASManager	167
		13.3.3	Step 3: Configuring a Channel	169
	13.4	Adding	Vehicles	171
	13.5	Monitor	ing LPR Activities	174
		13.5.1	LPR Device View	174
		13.5.2	Monitoring Windows	175
	13.6	Receivi	ng Notifications for LPR Activities	176
	13.7	Setting	Up Vehicle Hotlist	177
	13.8	LPR Fu	nctions in GV-ASWeb	
		13.8.1	LPR List	181
		13.8.2	Vehicle List	
		13.8.3	LPR Log	
		13.8.4	Access Group Setup	
Chapter 14	GV-	Access	Mobile Applications	186
	14.1	Installir	g GV-Access	
	14.2	Connec	ting to GV-ASManager	187
	14.3	Managi	ng Controllers	
	14.4	Managi	ng LPR	191
Chapter 15	Data	abase S	Settings	193
	15.1	Starting	the Database Tools	

	15.2	Creating a Database	194
	15.3	Other Database Settings	195
	15.4	Mapping Source Database	196
		15.5.1 Converting Data from the Active Directory Database.	198
		15.5.2 Converting Data from the OLE Database	199
Chapter 16	Ne	t Module Utility	204
Chapter 17	Tro	oubleshooting	205
Appendix 2	10		
	A.	Compatible IP Devices	210
	В.	Event Notifications	211
	C.	E-Mail and SMS Alert Symbols	215
	D.	Controller Status	216

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.

Organize	in library 🔻 Share with 🔻	Burn New folder	Contraction	- 4 9 Si
☆ Favorites	Name	Date modified	Туре	Size
📃 Desktop	ASConfig	12/14/2011 3:15 PM	Microsoft Office A	1 KB
📜 Downloads	ASConfig	12/14/2011 3:15 PM	Microsoft Office A	628 KB
🔛 Recent Places	ASLog	12/14/2011 3:15 PM	Microsoft Office A	1 KB
	ASLog	12/14/2011 3:15 PM	Microsoft Office A	168 KB
词 Libraries				
Documents				
J Music				

- 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.

🖉 🗢 📕 🕨 Compu	ter → Local Disk (C:) → Access Control11	1111 + ASManager + ASRes		•	4 9
Organize 👻 Include	in library 🔻 Share with 🔻 Burn	New folder			
🔆 Favorites	Name	Date modified	Туре	Size	
📃 Desktop	ASConfig	12/14/2011 3:15 PM	Microsoft Office A		1 K
\rm Downloads 🗐 Recent Places	ASLog	12/14/2011 3:15 PM	Microsoft Office A		1 K

- 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.

🕞 ASManage	r Database Setting	
	Setup MDB / MSSQL Database for ASManager	
	Upgrade to latest database version ASManager Database version incompatible. Please upgrade it first.	
	Delete ASManager Database	
	Backup Database	
	Recovery Database	
Database versio	on: 2.1.0.0	

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 16*.



Software Compatibility

The GV-System versions compatible with GV-ASManager V4.0 - V4.2.1 are listed below.

GV-ASManager Version	Compatible GV-System Version
GV-ASManager V4.2.1	GV-System V8.5.9.0
GV-ASManager V4.2	GV-System V8.5.8.0
GV-ASManager V4.1	GV-System V8.5.7.0
GV-ASManager V4.0	GV-System V8.5.5.0 / V8.5.6.0



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 40,000 cards
- 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-System, GV-NVR, 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
- Vehicle hotlist to help locate stolen vehicles or other vehicles of interest
- User interface in English, French, Portuguese, Russian, Spanish, Traditional Chinese

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 add or delete cards, users, controllers, access groups, cameras
- Web interface for historical log search with corresponding video and snapshot
- Log export in Excel, Text, HTML or Zip 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 and / or GV-DSP LPR
- Up to 40,000 vehicles
- Multiple vehicles per user
- Import / export of vehicle data in Access or Excel file format
- GV-ASWeb: Remotely enroll vehicles and set up GV-DVR LPR or GV-DSP LPR
- GV-ASWeb: Remotely search detected vehicles, see license plate snapshots, watch recordings from connected GV-DVR LPR or GV-DSP LPR

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.

Weekly Schedule	A weekly schedule is certain days of the week when a user is granted access to a secure site.
	For details, see 4.4 Setting Weekly Schedule.
Access Group	An access group is a group of users with identical location restrictions during the same time restraints.
	For details, see 4.5 Setting Access Group.
Alarm Condition	An alarm condition is a monitored condition through sensing devices, and an alarm condition may activate alarms. For example, the AS100 Controller has the ability to monitor 3 sensors, such as door status sensor, smoke detector and tamper detector. The AS100 Controller also provides 3 output relays for activating and deactivating electric lock, siren and emergency door release when the alarm condition occurs.
	For settings of alarm conditions see <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>
Anti-Duress	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.
Anti-Passback	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 4.2.2 Step 2: Configuring the Doors.
Interlock	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.
	For settings, see 4.2. I Step 1. Configuring a Controller.



Two-person A/B rule	The door unlock only when two assigned cards are presented together. Two Person Card A must be presented before Two Person Card B. For settings, see <i>4.3.1 Adding a Single Card</i> .
IP device	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-System, GV-NVR, 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. For details, see <i>Chapter 5 Video Integration</i> .
Data Group	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. For details, see <i>8.1.1 Adding a New User</i> .
Door Group	When a large number of GV-AS / GV-EV Controllers are connected to the GV-ASManager, the controllers can be organized into different door groups, allowing you to quickly upload fingerprints to all the controllers in a door group instead of uploading to each controller one by one. For details, see <i>Uploading Fingerprints to Controllers Using Door</i> <i>Groups</i> section in Chapter 3 of <i>GV-GF Fingerprint Reader User's</i> <i>Manual.</i>



1.3 Optional Devices

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

GV-GF1911 Fingerprint Reader	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.
	Fingerprints can be enrolled locally or remotely using a GV-GF1921 / 1922 Fingerprint Reader through TCP/IP connection with GV-ASManager.
GV-GF1921 / 1922 Fingerprint Reader	For local fingerprint enrollment , the user needs to register his or her fingerprints onsite using a reader connected with GV-ASManager. For remote fingerprint enrollment , 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.
GV-PCR310 Enrollment Reader	The GV-PCR310 is a USB card reader designed to assist with card enrollment to GV-ASManager. It reads and transfers the identification data of a detected card to GV-ASManager. The user can conveniently establish user accounts on GV-ASManager by inserting the cards in the GV-PCR310 Enrollment Reader.

Chapter 2 Installation

2.1 System Requirements

For GV-ASManager version 4.1 or later, the minimum hardware and software requirements are:

OS	32-bit	Windows XP / Vista / 7 / 8 / Server 2008		
	64-bit	Windows Vista / 7 / 8 / Server 2008 / Server 2012		
CPU		Core 2 Duo E8400, 3.0 GHz		
Memo	ry	2 x 1 GB Dual Channels		
Hard [Disk	500 GB		
VGA		AGP or PCI-Express, 1280 x 1024 , 32-bit color and support DirectX 10		
DirectX		End-User Runtimes (November 2008)		
Softwa	are	.NET Framework 3.5		
		SQL Server 2005 Express (optional)		
Browser Internet Explorer 7.0 or later		Internet Explorer 7.0 or later		
Note: The software programs End-User Runtimes (November 2008) and .NET Fran				
3.5 are required to run the GV-ASManager. The		t to run the GV-ASManager. The software programs can be found in the		
supplied software DVD.				

2.2 Installing the GV-ASManager

Starting from version 4.0, 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 3.0, no USB dongle is needed to connect to IP cameras.

To install the USB Dongle drivers:

- 1. Insert the USB Dongle to your computer.
- Insert Software DVD to your computer and a window will pop up automatically. Select Install or Remove GeoVision GV-Series Driver and click Install Geovision USB Devices Driver.

To install the GV-ASManager:

GV-ASManager V2.0 or later must run with DirectX End-User Runtimes (November 2008) and .NET Framework. Follow these steps to install the programs.

- 1. Insert Software DVD to your computer and a window will pop up automatically.
- 2. If you don't have DirectX 9.0c installed in your computer, select Install DirectX 9.0c.
- 3. Select Install DirectX End-User Runtimes (November 2008).
- 4. Select Install Microsoft .NET Framework Version 3.5.
- 5. Select Install GeoVision Access Control System, click GeoVision Access Control System and follow on-screen instructions to complete the installation.



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 you start the system for the first time, the system will prompt you for a Supervisor ID and Password as below.

ASManager	
The system execut Please enter super	tes at first time visor ID and password.
ID:	admin
Password:	••••
Password Confirmation:	••••
	OK Cancel

Figure 2-1

2. Type a name you wish to be the Supervisor in the ID field and type the password. This dialog box appears.



Figure 2-2

3. Re-type the **ID** and **Password**. If you want to skip the login process in the future, select **Auto Login**.



- 4. Click **OK**. The message "*Can't open database. Would you like to set up database?*" appears.
- 5. 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.

🚮 Database Too	ols	×
Please Select D Which tool de	Patabase Tools : o you use for database?	
	ASManager Database Setting : Setup, upgrade, deletion, backup and recovery.	
	Settings from Source to ASManager Database : Set the connection of Source Database, the mapping relations of the tables betweem Source and ASManager database, the auto-update request, and the manual update request.	-
	Re-login Exit	· · · · · ·

Figure 2-3

- 6. Select **ASManager Database Setting**. The ASManager Database Setting dialog box appears.
- 7. 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.
- 8. 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 File (log in / out the GV-ASManager), Monitoring (display monitor windows of alarm, access and event), View (display the function windows), Setup (set up connected devices and schedules), Personnel (set up the users' accounts), Language (select language of user interface), Tools (set up for notification and log) and Window (arrange the display of different windows).
2	Toolbar	The Toolbar includes the options of Login, Logout, Devices, Areas, Door Groups, Time Zones, Weekly Schedules, Holidays, Access Groups, Cards, Vehicles, Users and About.



3	Device View	Displays a list of connected doors 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	Event Monitor	Displays monitored events of doors.
5	Alarm Monitor	Displays alarm events of doors.
6	Access Monitor	Displays access activities of doors.
7	MultiView	Displays live views of connected cameras from multiple IP devices. For details, see <i>5.4 The MultiView Window</i> .
8	Information Window	Displays the information of doors, card readers and monitored events.
9	Playback	Plays back recorded events from a compatible GeoVision IP device. For details, see <i>5.5 Retrieving Recorded Video</i> .
10	Live Video	Displays the live view of one connected camera. For details, see <i>5.2 Accessing a Live View</i> .
11	Camera List	Displays a list of connected cameras.

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-ASManage	er:
--------------------	------------------------	-----

No.	Name	Function
1	Login	Logs in the GV-ASManager.
2	Logout	Logs out the GV-ASManager.

3	Devices	Defines controllers and doors.
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 6.3 Global Anti-Passback.
6	Door Groups	Assigns controllers into door groups to be able to quickly upload fingerprints to multiple controllers. For details, see <i>Uploading Fingerprints to Controllers Using Door Groups</i> section in Chapter 3 of <i>GV-GF Fingerprint Reader User's</i> <i>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</i> <i>Groups</i> .
11	Fingerprint Access	Uploads the enrolled fingerprints to the controllers. For details, see <i>Chapter 3 Fingerprint Only Mode</i> in the <i>GV-GF Fingerprint Reader User's Manual</i> .
12	Cards	Creates and edits a database of card information. For details, see <i>4.3 Setting Cards</i> .
13	Vehicles	Creates and edits a database of vehicle information. For details, see <i>Chapter 13 License Plate Recognition</i> .
14	Users	Creates and edits a database of user information. For details, see <i>4.6 Setting Users</i> .
15	About	Displays the version of GV-ASManager.

3.2 Device View

The Device View displays the activity and status of the connected doors.

• To open the Device View window, click **View** on the menu bar and select **Controllers**.

Device Vie	ew								д X
16x16	*								
Device			Status	Alarm	Forced Open	Duress	Tamper	Fire Alarm	Held Open
	TEST85	troller 1 Front Door Back Door Emergency Door Facotry Door	Card Mode Release Mode Card and PIN Code M Card or Common Mode				12. 12.		

Figure 3-3

3.2.1 Controls on the Window

You can control a connected controller or door by right-clicking it in the Controller window.

Name	Function
Unlock Door, Lock Down, Force Unlock, Force Lock,	Controls the selected door or all doors associated with the selected controller.
Disable Door Lock Operation	The options of Force Unlock and Force Lock will let the door stay open or locked until you select Disable Door Lock Operation .
	The Unlock Door option will let the door open temporarily until the specified time is expired. See "Lock Reset Time" at Step 2 in <i>4.2.2 Step 2: Configuring the Doors</i> .
	The Lock Down function 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.
Reset Anti-Passback	Clicking this option enables a user to re-access the entry or exit reader.
	See Chapter 6 Anti-Passback.
Settings	Accesses the setting page of the selected controller or door.

The following control options are available for both doors and controllers:

Name	Function
Reset Anti-Passback	Clicking this option enables a user to re-access the entry or exit reader.
	See Chapter 6 Anti-Passback.
Reconnect	Reconnects with the controller.
Sync Controller	After the controller settings are modified, clicking Sync Controller can immediately renew the settings.

The following control options are only available when right-clicking a **Controller**:

The following control options are only available when right-clicking a **Door**:

Name	Function
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 <i>4.2.2 Step 2: Configuring the Doors</i> .
Sync GeoFinger	If fingerprint data failed to upload to the controllers, click Sync GeoFinger to re-upload the selected fingerprint data.



3.3 Monitoring Windows

Three monitoring windows are provided for users to oversee different types of door activities: Access Monitor, Alarm Monitor and Event Monitor.

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

3.3.1 Controls on the Window

The three monitoring windows of Access Monitor, Alarm Monitor and Event Monitor have the same controls on the window.

We use the Access Monitor window as example to explain the controls.

🌱 🔛 🔒					
Message	Door	Local Time	Card Number	User	^
🔀 Access Denied: Invalid Schedule	Door 1	9/4/2012 6:27:01 PM	009-33091	Eric Hu	
🔀 Access Denied: Invalid Card	Door 1	9/4/2012 6:27:31 PM	108-45859		
Access Granted	Door 1	9/4/2012 6:28:33 PM	009-33091	Eric Hu	
Access Granted	Door 1	9/4/2012 6:28:47 PM	067-63348	Steven Yap	
🔀 Access Denied: Invalid Schedule	Door 1	9/4/2012 6:28:52 PM	108-45859		
Access Granted	Door 1	9/4/2012 6:29:01 PM	108-45859		
Access Granted	Door 1	9/4/2012 6:29:03 PM	067-63348	Steven Yap	
Access Granted	Door 1	9/4/2012 6:29:06 PM	009-33091	Eric Hu	
Access Granted	Door 1	9/4/2012 6:29:10 PM	067-63348	Steven Yap	
🗘 Access Granted	Door 1	9/4/2012 6:29:34 PM	108-45859	Allan Ngai	
Access Granted	Door 1	9/4/2012 6:29:58 PM	067-63348	Paul Bradsh	~

Figure 3-4

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.	

The following options are only accessible on the **Access Monitor** window. Right-clicking one message allows you to access its detailed information.

Name	Function
New/Edit Card	Enrolls a new card or edits the card information.
Browse Card Information	Views the card information.
Browse User Information	Views the user information.
Show Image	If the camera monitors when the activity happened, the related image is available.

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.

- To add one monitoring window, click Monitoring on the menu bar. Then select New Alarm Monitor, New Access Monitor or New Event Monitor.
- 2. Click the **Filter** button on the monitoring window. This dialog box appears.

Filter	×
Message:	
Alarm Messages	
Tamper	
↓ Hold Open	
Door:	
🖃 🖂 🗊 TEST111	
Controller 1	
Controller 2	
	_
OK Cancel	

Figure 3-5

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.





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 monitor windows and click **Window** to arrange them.



Figure 3-7



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 **Device**. This dialog box appears.





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

Please Ent		
ID:	2	
Name:	Controller 2	ОК
Туре	GV-AS400 💌	Cancel

Figure 4-2



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

Controller Setup			
General Setup Gate 1 Gate 2 Gate 3 Gate 4 Gate 5 Gate 6 Gate 7 Gate 8			
General Controller Name : Controller ID :	Controller 1		
GMT:	+ • 08 • :	00 🗸	
	No Groups	<u> </u>	
Release All Doors By Lard			
Enable Daylight Saving	Setup		
Connection			
O COM Port :		<u>v</u>	
Network :	TCP/IP	×	
IP:	192.168.5.57		
Port :	4001		
User:	admin		
Password :	•••••		
Crypto Key :	•••••		

Figure 4-3

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

- 4. 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.



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 $\stackrel{\texttt{s}}{=}$ appearing on the Device View window indicates the connection is established.

Note: For the disconnection messages displayed on the Status column (Figure 4-6), 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 **Interlock** and **Release All Doors by Card** functions are 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 / Gate** tab. This dialog box appears.

V Enable		Alam Event
Name: Common Password : Ugent Code : Lock Reset Time : Held Open Time : Lock Card Time : Ent Fire Action : Reader's Keypad Entrance Exit Auto Check Out Entrance	Door 1 4 ~8 digits(0~9) 4 ~8 digits(0~9) 5 Sec(1~255) 5 (Handicap Card) 10 Sec(5~9999) 10 (Handicap Card) 10 Sec(0~65535) Exit: 0 Sec(0~65535) Unlock Door Anti-Passback Clocal Anti-Passback Globe Anti-Passback Two-Person Rule	Aam Event Held Open Forced Open Tamper Fire Alam Access Denied Tailgating Urgent Code Alam Continuous Time : 5 Sec(1~10) Camera Mapping First Camera: GV-BX120D/BX120D-E(192.168.!
GeoFinger Fatance P Address 2167 Kat IP Address 2167	Exit Interlock Time Clock	Authentication Schedule Exit Button Schedule

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, the door with the urgent code will unlock. However, the door will not unlock if it is in Release by Card Mode. The Urgent Code function is only supported by GV-AS210 / 410 / 810.

- 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 a fire alarm condition 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 4 below.
 - Anti-Passback: To perform the Anti-Passback application, 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.



- Interlock: Enable Interlock function with the selected doors. Doors that are interlocked cannot be open at the same time. The door only unlocks when the other door is close. Using the settings in *Figure 4-4* as an example, Gate 1 will not unlock if either of Gate 4 and 5 is opened, and when Gate 1 is opened, Gate 4 and 5 cannot be opened.
- **Time Clock:** This option must be selected to enable GV-TAWeb. See *Chapter 11 GV-TAWeb for Workforce Schedule* for more details.
- 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; otherwise the default access mode is **Card Mode** that requires users to present the card only to be granted access.

Working Time Setup			
•			
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24		
Mon			
Tue	09:55		
Wed			
Thu			
Fri			
Sat			
Sun			
Hol.			
 Release Mode Release By 0 Card and PIN Co 	Card or Common Mode		
	OK Cancel		



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.



- **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 then enter the card's PIN code on the keypad. For the following controllers, the user can gain access by entering the card number and pin code:

Model	Supported Firmware	Command (Example: Card 12345678, Pin 0000)
GV-AS100	V1.04 or later	Card Number + Pin Code Example: 123456780000
GV-AS110	V1.04 or later	*Card Number + Pin Code # Example: *123456780000#
GV-AS400	V1.04 or later	Pin Code + Card Number Example: 000012345678
GV-AS210 / 410 / 810	V1.0 or later	Pin Code + Card Number Example: 000012345678

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.


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. This function is only supported by GV-AS210 / 410 / 810.

Exit Button Schedule	and the second sec	
0000		
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 25 23 24]
Monday		
Tuesday		
Wednesday		
Thursday		1
Friday		
Saturday		
Sunday		
Hol.		
Access Time (Exit	Button)	
	OK Cancel	

Figure 4-6

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 $\stackrel{2}{=}$ appears, it indicates the connection between the controller and GV-ASManager has been established. If the icon $\stackrel{2}{=}$ appears, it indicates the connection failed. Make sure the above connection setup is correctly configured.

Device Viev	V					ą 🗙
16x16	~					
Device		Status	Alarm	Forced Open Duress	Tamper	
🖃 🗐 TES	5T85					~
= 🚊	Controller 1					
	📃 Front Door	Card Mode				=
	📃 Back Door	Release Mode				
	📃 Emergency Doc	or Card and PIN Code M				
	🧾 Facotry Door	Card Mode				~

Figure 4-7



B. GV-EV Controller: Floors

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

Elevator	X
General Setup Floors	
Floors	General
ID Name	Name: Elevator Common Password : •••• 4~8 digits(0~9)
2 Floor 2 3 Floor 3	Relay Reset Time 5 Sec(1~255) 5 (Handicap Card)
4 Floor 4 5 Floor 5 6 Floor 6 7 Floor 7 8 Floor 8 9 Floor 9	Two-Person Rule
10 Floor 10 ≡ 11 Floor 11 12 Floor 12 13 Floor 13	Authentication Schedule
14 Floor 14 15 Floor 15 16 Floor 16	IP Address : 2167
17 Floor 17 18 Floor 18 19 Floor 19	IP Address : 2167
20 Hoor 20 21 Floor 21 22 Floor 22 23 Floor 22	First Camera:
23 Floor 23 24 Floor 24 25 Floor 25 20 Floor 25	
26 Hoor 26 27 Hoor 27 28 Hoor 28	
30 Floor 30 31 Floor 31	
32 Floor 32 *	
	OK Cancel

Figure 4-8

- 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.

Working Time Se	etup
I I I I I I I I I I I I I I I I I I I	
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
Mon	
Tue	09:55
Wed	
Thu	
Fri	
Sat	
Sun	
Hol.	
 Release Mode Release By Condiand BIN C 	Card or Common Mode
Lard and PIN L	ode Mode Card Mode OK Cancel

Figure 4-9



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.
- **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. The user can also be granted access by entering Pin Code + Card Number. For example, if the card number is 12345678 and the Pin is 0000, the command will be 000012345678.
- 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.
- 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 4 appears, it indicates the connection between the controller and GV-ASManager has been established.

If the icon ⁴ appears, it indicates the connection failed. 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. Up to 40,000 cards can be stored using a GV-AS / GV-EV Controller. 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 4-11). Then follow Step 3 to complete other settings.
 - On the menu bar, click **Personnel** and select **Cards**. This window appears.

🛋 Card List											X
New Bat	ch New	Edit D	elete	Card Reader	Import Exp	ort Refresh					
Search by Card N	umber		•	/		Auto Se	elect 🛛 Filter Viev	,			
Card Number	Card Type	Card Bits	User	Card Status	Activation Date	Deactivation D	Privilege	Access Group	GV	Disa	^
20353-72987	Normal	32		Active	10/20/2010		No Privilege	Default	\bigcirc		
3463064247	Normal	32		Active	9/14/2010		No Privilege	Default	\bigcirc		
2082427835	Normal	32		Inactive	10/20/2010		No Privilege	Default	\bigcirc		
💼 3379309239	Normal	32		Inactive	9/15/2010		No Privilege	Default	\bigcirc		
💼 3469554359	Normal	32		Inactive	9/15/2010		No Privilege	Default	\bigcirc		
34020-50231	Normal	32		Active	10/27/2010		No Privilege	Default	\bigcirc		
= 3298664375	Normal	32		Inactive	10/27/2010		No Privilege	Default	\bigcirc		
💼 0545008279	Normal	32		Inactive	10/27/2010		No Privilege	Default	\bigcirc		
60550174871	Normal	32		Inactive	10/12/2010		No Privilege	Default	\bigcirc		~
L-0-		.1	1.			1		10.02.02			
						Total Cards: 370					

Figure 4-10

Note: You can also enroll card 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 more details.



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

User: Card Card Activ I D Pin C	r: d Number: d Status: vation Date: Deactivation Date: Code:	123-45678 Active 12/17/2013 5/17/2014		Code Type: Card Type: Privilege:	[Wiegand26 Normal	v
Card Card Activ V D Pin C	d Number: d Status: vation Date: Deactivation Date: Code:	123-45678 Active 12/17/2013 5/17/2014		Code Type: Card Type: Privilege:) [[Wiegand26 Normal	v
Card Card Activ I D Pin C	d Number: d Status: vation Date: Deactivation Date: Code:	123-45678 Active 12/17/2013 5/17/2014		Code Type: Card Type:	, [[Wiegand26 Normal	× ×
Card Activ I D Pin C	d Status: vation Date: Deactivation Date: Code:	Active 12/17/2013 5/17/2014		Card Type: Card Type: Privilege: Disable Lo	[Normal	~
Activ D Pin C	vation Date: Deactivation Date: Code:	12/17/2013 5/17/2014			1		
☑ D Pin C	Deactivation Date: Code:	5/17/2014		Privilege: Disable L c	1		
Pin C	Code:	••••		Privilege:	[
				Disable Lo		No Privilege	~
	-				ck Card	_	
Acce	ess Group:	Default		~			
Ξ (Controller 1						
C	Door 1		24-hour restricted				
C	Door 2		24-hour restricted				
	Door 3		24-hour restricted				
	Door 4		24-hour restricted				
± (Controller 2						
± (Controller 3						
Data	a Group:	No Groups		~		ОК	Cancel

Figure 4-11

- 3. The settings are available for the card:
 - **Card Number:** Enter the card number.
 - **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 when the card is active or inactive.
- **PIN Code:** Enter a four-digit personal code for the card. The default setting is 1234.
- 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: When the option is selected, the card will be exempt from the Lock Card Time setting. For details on Lock Card Time, refer to Step 2: Configuring the Doors or Elevator Floors in Chapter 4.
- 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: GV-AS200 only supports the first 10,000 cards. All other controllers can support up to 40,000 cards.



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.

Batch new cards			
Card Number:	100-00000 ~ 100-00500	Code Type:	Wiegand26
Card Status:	Active	Card Type:	Normal
Activation Date:	12/17/2013		
Deactivation Date:	04/17/2014		
Pin Code:	••••	Privilege:	No Privilege 💌
Access Group:	Default 💌	Disable Lock Card	
Data Group:	No Groups 💌		OK Cancel

Figure 4-12

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 Importing/Exporting Card Data

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

To export card data:

- 1. On the Card List window (Figure 4-8), 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 4-10), click the **Import** button and select one of these options: **Import from Access** or **Import form Excel**.
- 2. Assign the file path and type the **Password** if necessary. Click **OK**. This dialog box appears.

Import Cards You can define the field ma field in the Source.	appings. Set Mappings to s	pecify the	correspondence	between fields in the Ca	rd and
Select Source Table:	Sheet1\$		*	Auto mapping	Clear mapping
Card Fields	Туре	<>	Source Fields	Туре	
CardNo	adVarWChar	<>			
CodeType	adUnsignedTinyInt	<>			
CardType	adUnsignedTinyInt	<>			
CardStatus	adUnsignedTinyInt	<>			
ActivationDate	adDBTimeStamp	<>			
Deactivation	adBoolean	<>			
DeactivationDate	adDBTimeStamp	<>			
PinCode	adVarWChar	<>			
Privilege	adUnsignedTinyInt	<>			
DisableLockCard	adBoolean	<>			
				Import	Cancel

Figure 4-13

- 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.



4.4 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.

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.

Time Zone Setup	
🎽 🛎 🖉 🥰	
	0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 🦂
0 : Deny Access	
255 : Full Access	
1 : Day Shift	
2 : Night shift	
3 : Supervisor	
	19:00
Access Time	
Data Group:	Data Group 4 V Cancel

Figure 4-14

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

Please E	nter ID	
ID:	1	ОК
Name:	day shift	Cancel



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 **(O)**. 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.

- 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.
- 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.

Schedule Setup			
Full Access	Monday	Deny Acce	~
	Tuesday	Deny Acce	~
	Wednesday	Deny Acce	~
	Thursday	Deny Acce	~
	Friday	Deny Acce	~
	Saturday	Deny Acce	~
	Sunday	Deny Acce	~
	Hol.	Deny Acce	~
	Data Group:	No Groups OK Can	cel

Figure 4-16

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

Please F	inter ID	
ID:	1	ОК
Name:	Schedule-empl	Cancel

Figure 4-17

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.

Schedule Setup		Σ
a a		
Deny Access Full Access	Monday	Day Shift
Schedule-Day shift	Tuesday	Day Shift
	Wednesday	Day Shift
	Thursday	Day Shift
	Friday	Day Shift
	Saturday	Deny Acce
	Sunday	Deny Acce
	Hol.	Deny Acce
	Data Group:	No Groups V OK Cancel

Figure 4-18

- 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.
- 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.

ichedule Setup		
<i>🏟 🛎</i>		
Deny Access Full Access	Monday	Supervisor
Schedule-Day shift	Tuesday	Supervisor
Schedule-Night shift	Wednesday	Supervisor
Schedule-Supervisor	Thursday	Supervisor
	Friday	Supervisor
	Saturday	Supervisor
	Sunday	Supervisor
	Hol.	Supervisor
	Data Group:	No Groups 💌 OK Cancel

Figure 4-19

- 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 on the system:

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

Holiday Setting				
Dec 2006	Jan 2007	Feb 2007	Mar 2007	Apr 2007
SMTWTFS	SMTWTFS	SMTWTFS	SMTWTFS	SMTWTFS
1 2	1 2 3 4 5 6	1 2 3	1 2 3	1 2 3 4 5 6 7
3 4 5 6 7 8 9	7 8 910111213 14151617181920	4 5 6 / 8 910 11 12 13 14 15 16 17	4 5 6 / 8 910 11 12 13 14 15 16 17	8 9 10 11 12 13 14
17 18 19 20 21 22 23	21 22 23 24 25 26 27	18 19 20 21 22 23 24	18 19 20 21 22 23 24	22 23 24 25 26 27 28
24 25 26 27 28 29 30	28 29 30 31	25 26 27 28	25 26 27 28 29 30 31	29 30
31				
May 2007	Jun 2007	Jul 2007	Aug 2007	Sep 2007
SMTWTFS	SMTWTFS	SMTWTFS	SMTWTFS	SMTWTFS
1 2 3 4 5	1 2	1 2 3 4 5 6 7	1 2 3 4	1
6 / 8 9101112	3456789	8 9 10 11 12 13 14	5 6 / 8 91011	2 3 4 5 6 / 8
20 21 22 23 24 25 26	17 18 19 20 21 22 23	22 23 24 25 26 27 28	19 20 21 22 23 24 25	16 17 18 19 20 21 22
27 28 29 30 31	24 25 26 27 28 29 30	29 30 31	26 27 28 29 30 31	23 24 25 26 27 28 29
				30
Oct 2007	Nov 2007	Dec 2007	Jan 2008	
SMTWTFS	SMTWTFS	SMTWTFS	SMTWTFS	
1 2 3 4 5 6	1 2 3	1	12345	
7 8 9 10 11 12 13	4 5 6 7 8 9 10	2 3 4 5 6 7 8	6 7 8 9 10 11 12	
14 15 16 17 18 19 20	11 12 13 14 15 16 17	9 10 11 12 13 14 15	13 14 15 16 17 18 19	
28 29 30 31	25 26 27 28 29 30	23 24 25 26 27 28 29	20 21 22 23 24 23 20	
		30 31		
<u> </u>				
	(OK Cancel]	

Figure 4-20

- 2. Click the Holiday icon and click the dates you want to set as holidays. For example,
 - Dec 24, 2007 Christmas Eve
 - Dec 25, 2007 Christmas Day
 - Dec 31, 2007 New Year's Eve
 - Jan 01, 2008 New Year's Day
- 3. To delete the holiday, click the **Non Holiday** icon and click the date you want to delete.

Note: Holiday dates 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.

Access Groups					×
	⊂ Off	ice Staff			
	Ac	cess Group Name	Office Staff]
Default		Controller 1			
Office Staff		Door 1	Schedule-Day shift		-
		Door 2	Schedule-Day shift		-
		Door 3	Schedule-Day shift		
		Door 4	Schedule-Day shift		
		Controller 2			
		Door 1	24-hour restricted		
		Door 2	24-hour restricted		
		IPR 1			-
		LPR 1			-
		Lane 1	24-hour access		-
		Data Gr	oup:	No Groups	✓

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

- Figure 4-21
- 2. Click the **New** button (2), and give a **Name** to the new access group. For example, name the access group **Office Staff**.



- 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.

	ie cui u					
Use	я г .			2		
Caro	d Number:	123-46578		Code Type:	Wiegand26	1
Caro	d Status:	Active	~	Card Type:	Normal	1
Acti	vation Date:	12/18/2013	~			
	Deactivation Date:	12/18/2013	~			
Pin I	Code:	••••		Privilege:	No Privilege	1
				Disable Lock Card Support GV-AS200		
Acc	ess Group:	Office Staff	~			
	Controller 1					
	Door 1		Schedule-Day shift			
	Door 2		Schedule-Day shift			
	Door 3		Schedule-Day shift			
	Door 4		Schedule-Day shift			
Ξ	Controller 2					
-	Door 1		24-hour restricted			
	Door 2		24-hour restricted			

7. Double-click one listed card. This dialog box appears.

Figure 4-22

 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.



4.6 Setting Users

This section describes how to create a database of user information 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.



Figure 4-23

- 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. 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.

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 Assigning a Card to a User

There are two methods to assign a card to a user.

Note: At this step we assume that you have followed the instructions in *4.3 Setting Cards* to complete your card enrollment.

- 1. On the User Setup dialog box (Figure 4-23), click **Add** and double-click one listed card to assign the card to the user.
- 2. On the Edit Card dialog box (Figure 4-22), click the **Assign User** icon and double-click one listed user to assign the user to that card.

4.6.3 Sending SMS Alerts

If you want to send SMS alerts whenever the card(s) assigned to the user is presented to the reader, select **Send SMS** in the User Setup dialog box.

Before sending the SMS, 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*.

4.6.4 Customizing a 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.

User Define Fields Setting	×
User Define 01:	User Define 06:
Parking Space Number	
User Define 02:	User Define 07:
User Define 03:	User Define 08:
User Define 04:	User Define 09:
User Define 05:	User Define 10:
	OK Cancel

Figure 4-24

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.
- 4. 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:

User Setup	
General Home Business User Define F	fingerprint Scan
User: Adeline Tan	Employee ID:
Parking Space Number:	User Define 06:
Lot C #32 💌	¥
User Define 02:	User Define 07:
Y	¥
User Define 03:	User Define 08:
×	×

Figure 4-25



4.6.5 Importing/Exporting User Data

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

GeoVision

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 for monitoring and surveillance purposes.

The GV-ASManager provides the following video features:

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

Note:

- 1. GeoVision IP devices include GV-System, GV-NVR, 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-System of version 8.120 or later.
- 4. GV-Fisheye IP Camera is currently not supported on GV-ASManager.

Hint: In the following sections the term "DVR" refers to GV-System and GV-NVR, the term "Video Server" refers to GV-Video Server, and the term "Compact DVR" refers to GV-Compact DVR.

5.1 Mapping Cameras

If you want to map a camera from the DVR to a door, the DVR must be enabled for video access ahead:

• Enable Control Center Server (CCS)

To map cameras to a door:

- 1. On the menu bar, click Setup and select Device. The Controller List dialog box appears.
- 2. Double-click one listed controller. The Controller Setup dialog box appears.



- 3. Click a Gate tab.
- 4. In the Camera Mapping section, click the first Arrow button.



Figure 5-1

5. To connect one IP device to the GV-ASManager, use one of these ways:

DVR List
Search Add Modify Remove
OK Cancel



- 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-Systems on the same LAN. After the found device is added, click the **Modify** button to enter its login ID and password.
- Expand the Host folder listed in the DVR List dialog box (Figure 5-2), select one camera and click OK. The mapped Host Name and Camera are displayed on the Controller Setup dialog box.
- To map the second camera to the door, click the second Arrow button, and follow Steps 5 and 6 to add another camera.
- 8. Click **OK** and return to the main screen.
- 9. 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 5-2) by clicking the listed name directly.
- 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 Device View 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	Best Fit	Rescales the image to fit any resized window.
3	Actual Size	Displays the image in its original size.
4	Zoom	Zooms in or out the image.
5	Thumbnail	Displays a thumbnail view (No. 6). 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.
6	Thumbnail View	See the description in No. 5.

GeoVision

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:

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

The video generated by the camera appears in this frame. If a different camera view already exists in this frame, the new video takes its place.



Figure 5-4



The controls on the MultiView window:

No.	Name	Function
1	Frame	The frame displays live video from the assigned camera. The camera number and name, controller ID and name will be displayed in the upper left corner.
2	3D	 Click this option to have a dynamic 3D live view. In the 3D live view: Double-click one camera view to switch between 3D mode and thumbnails. Then right-click the 3D image to have different 3D effects. Double-click one camera view in thumbnails to change different divisions (4, 9 and 16 divisions).
3	Camera List	Select the desired camera. The selected camera will be displayed with mouse focus.
4	Previous / Next Page	Go to the previous or next page of camera views.
5	Matrix View	Select an existing Matrix View (a group of views) 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.
8	Resolution	Select the image resolution. Double-click one camera view to rescale the image to fit the MultiView window or restore to its set resolution.

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.

GeoVision

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

• DVR: Enable **Remote ViewLog Service** on Control Center Server

To play back video:

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











Play Mode	Includes these options:
	• Frame by Frame: Plays back video frame by frame.
	• Real Time: Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback.
	Auto Play Next 5 Minutes: Plays back video up to 5 minutes.
	Audio: Turns on or off the video sound.
Render	Includes these options:
	• Deinterlace: Converts the interlaced video into non-interlaced video.
	 Scaling: Smoothens mosaic squares when enlarging a playback video.
	 Deblocking: Removes the block-like artifacts from low-quality and highly compressed video.
	Defog: Enhances image visibility.
	Stabilizer: Reduces camera shake.
	• Text overlay's camera name and time: Overlays camera name and time onto the video.
	 Text overlay's POS/GV-Wiegand: Overlays POS or GV-Wiegand Capture data onto the video.
	• Full Screen: Switches to the full screen view.
Tools	Snapshot: Saves a video image.
	• Save as AVI: Saves a video as avi format.
	• Download: Downloads the video clip from a GeoVision IP device to the local computer.



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	Yes	Yes (GV-ASBox or	Yes (GV-ASBox or
		GV-ASNet required)	GV-ASNet required)
GV-AS110	Yes	Yes (GV-ASBox or	Yes (GV-ASBox or
		GV-ASNet required)	GV-ASNet required)
GV-AS120	Yes	Yes (GV-ASBox or	Yes (GV-ASBox or
		GV-ASNet required)	GV-ASNet required)
GV-AS210	Yes	Yes	Yes
GV-AS410	Yes	Yes	Yes
GV-AS810	Yes	Yes	Yes



6.1 Anti-Passback

Anti-Passback is used on **one controller only**. For this application, select **Local Anti-Passback** at the **Gate** tab of the Controller Setup dialog box (Figure 4-3).

General Setup Gate 1 Gate 2 Gate 3 Gate 4					
General					
Name:	Gate A				
Password :	•••• 4~8 digits(0~9)				
Lock Reset Time :	5 Sec(1~255)				
	5 (Handicap Card)				
Held Open Time :	10 Sec(5~9999)				
	10 (Handicap Card)				
Fire Action	Unchange 🔽				
Reader's Keypad	Anti-Passback				
Entrance	🗹 Local Anti-Passback				
Exit	Globe Anti-Passback				

Figure 6-1

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



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 use three **GV-AS400 Controllers** as example to 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.

Controller No. 1 IP:192.168.0.11 APB IP:192.168.0.12 Controller No. 2 IP:192.168.0.12 APB IP:192.168.0.13 Controller No. 3 IP:192.168.0.13 APB IP:192.168.0.11



To configure Anti-Passback for the three GV-AS400 Controllers:

 Access the AS400 Setting page of the Controller No. 1 Web interface. In the Anti-Passback section, select Enable and enter Info IP that is the IP address of Controller No. 2, e.g. 192.168.0.12.

Advance Setting Function Setting Parameter Setting Time Setting	Function Authentication Mode Door/Gate D	Door Control Authentication Schedule Mode
Input Setting Output Setting Wiegand Setting	Function Authentication Mode	Door Control
Extend Device Extend Reader Extend IO 	Anti-Passback Enable/Disable Info IP	Enable 192 . 168 . 0 . 12
	Submit Cancel	

Figure 6-2

- Access the AS400 Setting page of the Controller No. 2 Web interface. In the Anti-Passback 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 **AS400 Setting** page of the Controller No. 3 Web interface. In the Anti-Passback 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.

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

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 **Global Anti-Passback** at each **Gate** tab of the Controller Setup dialog box (Figure 4-3).



6.3.2 Step 2: Configuring Areas

This step is to define the Entry and Exit areas for each door/gate 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:

- Gate A: Enter to Reception; Exit to Outside
- Gate B: Enter to Sales; Exit to Reception
- Gate C: Enter to Meeting Room; Exit to Sales
- Gate 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/gate. 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, you can use GV-ASKeypad or the Web interface of the GV-AS / GV-EV Controller. Here we use the GV-AS400 Web interface as example to define Wiegand readers. For this case, Wiegand reader A (Entry) goes from Outside to Reception, Wiegand reader B (Exit) goes from Reception to Outside and etc.

	AS400 Wiegand	Configuration
	Wiegand Function	
Basic Setting	Wiegand A	Door/Gate A Entry 🔽
Network SettingOther Setting	Wiegand B	Door/Gate A Exit 💌
Firmware UpdateAccount Setting	Wiegand C	Door/Gate B Entry 💌
Advance Setting	Wiegand D	Door/Gate B Exit 💌
Function SettingParameter Setting	Wiegand E	Door/Gate C Entry 👻
Time SettingInput Setting	Wiegand F	Door/Gate C Exit 💌
Output Setting	Wiegand G	Door/Gate D Entry 🚩
Wiegand Setting Extend Device	Wiegand H	Door/Gate D Exit 💌
Extend ReaderExtend IO	Submit Canc	el

Figure 6-5

6.3.4 Step 4: Configuring Door Contacts

This step is to define the door contact sensor for each door/gate. 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, you need to use the Web interface of GV-AS / GV-EV Controller. In this example of GV-AS400 Web interface, Input 01 is used as Door Contact of Door A, Input 02 is used as Door Contact of Door B and etc.

• Coollicion	AS400 Input Configuration									
	Input Function									
Basic Setting	Input 01	Door A	Door Contact 💌							
Network Setting	Input 02	Door B 🛛 🖌	Door Contact 🛩							
Other Setting	Input 03	Door C 🛛 🖌	Door Contact 🛩							
Firmware Update	Input 04	Door D 🖌 🖌	Door Contact 🛩							
Account Setting	Input 05	Normal Input 💌	Latch Disable 💌							
Advance Setting	Input 06	Normal Input 💌	Latch Disable ⊻							
Function Setting	Input 07	Normal Input 💌	Latch Disable 💌							

Figure 6-6



6.3.5 Step 5: Locating Users

To locate a user, select **Monitoring** on the menu bar and select **New Locate Person**. When the Exit or Entry reader is triggered, the GV-ASManager can tell if users follow Anti-Passback rules and then grand or deny access. When the door contact sensor is triggered, the GV-ASManager can tell the location of the user.

📲 Locate People				
Ŷ				
Cardholders	Location	Cardholder: joyce		
1	🗐 TEST85 (1)	Message	Cardholder	~
joyce	Reception	Access Granted	joyce	
		Access Granted	joyce	
		🛛 🐼 Access Denied: APB (Double Entry)	joyce	
		🛛 🛈 Access Granted	joyce	
		🛛 🔱 Access Granted	joyce	
		🛛 🔱 Access Granted	joyce	
		🛛 🔃 Access Granted	joyce	
		🛛 😣 Access Denied: APB (Wrong Area)	joyce	
				~
				>
Cards Cardholders				

Figure 6-7

To reset Anti-Passback on GV-ASManager or GV-ASRemote, right-click the **Host** or **Controller** icon on the Device View 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.

Patrol Tour Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Patrol Tour Sunday Image: Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Sunday Image: Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Sunday Image: Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Wednesday Image: Controller Door Image: Controller Door Image: Controller Image: Controler <	dd Patrol Tour	Add Patrol P	oint										
Patrol Tour Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Patrol Tour Sunday Image: Sunday Im	🕅 Patrol Tour												×
Patrol Tour 1 Controller Door Time 0 2 4 6 8 10 12 14 16 18 20 22 0 Sunday Image: Controller Image: Controler Image: Controller Im	💩 🖉 🤤 🛒 🗈	0/0											
Sunday Monday Tuesday Wednesday Thursday Fiiday Saturday	Patrol Tour		Controller	Door	Time	0 2	4 6	8 10	12 14	16 18	20	22 0	^
Monday Tuesday Wednesday Thursday Friday Saturday	Tour 1	Sunday											
Tuesday Wednesday Thursday Fiiday Saturday		Monday											
Wednesday Thursday Friday Saturday		Tuesday											
Thursday Friday Saturday		Wednesday											
Friday Saturday		Thursday											
Saturday		Friday											
		Saturday											
													V
	1	<										>	

Figure 7-1

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



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

Add Patrol Point (Sunday)	
Controller:	Controller 1
Door:	Door 1
Time:	6 💌 : 0 💌
Buffer Period:	30 💉 (05:30 - 06:30)
Extended Buffer Period:	40 🗸 (04:50 - 07:10)
Patrol Message:	Patrol Message 1 💌
	ОК

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 6-7* 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 6-7* 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.

ol Tour		Controller	Door	Time	0 :	2 4	6 8	3 10	12	14	16 18	20	22)
ampus_East Side		Controller 1	Door 1	[05:30 - 06:30] [04:50 - 07:10]			0	5:00						
	Sunday	Controller 2	Door 1	[08:30 - 09:30] [07:50 - 10:10]			[09:00					
		Controller 1	Door 1	[17:30 - 18:30] [16:50 - 19:10]								18:00	1	
	Monday	Controller 1	Door 3	[20:30 - 21:30] [19:50 - 22:10]									21:00)
	Tuesday	Controller 1	Door 3	[20:30 - 21:30] [19:50 - 22:10]									21:00)
	Wednesday	Controller 1	Door 3	[20:30 - 21:30] [19:50 - 22:10]									21:00)
	Thursday	Controller 1	Door 3	[20:30 - 21:30] [19:50 - 22:10]									21:0)
	Friday	Controller 1	Door 3	[20:30 - 21:30] [19:50 - 22:10]									21:00)
		Controller 1	Door 1	[05:30 - 06:30] [04:50 - 07:10]			0	5:00						
	Saturday	Controller 1	Door 2	[08:30 - 09:30] [07:50 - 10:10]			[09:00					
		Controller 1	Door 1	[17:30 - 18:30] [16:50 - 19:10]								18:00	1	

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.

Patrol Tour Setup				×
 Notification 				
Pass	📃 Early	🗌 Late		Absence
Mapping				
Card List:		E-Mail		
		BCC:		
		Country Code:	e Mobile:	
				<u> </u>
		3.		
				DK Cancel

Figure 7-4

2. Click the **Add** button 2 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 remained 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.



Mapping Card List: (026) 123-45678 (026) 234-56789] E-Mail o: C: CC:			
	Short Message Se Country Cod	ervice e: M	obile:	
	1.	×		~
	2.	~		~
	3.	▼		~
			Apply	Cancel

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



- **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.

Pat	rol Tour Setup				×
	Active				
	Notification				1
	Pass 🗌 Pass	Early	🔽 Late	Absence	
					-

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.



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.

🔋 Patrol Tour Monitor											
9											
	Controller	Door	Time	12 16	20	0	4	8	12	1	~
										1	~
<										>	

Figure 7-7

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

🚚 ASManager - [Da	ay Patrol]			-	1	-					-		-		-]	X j
👔 File Monitor	ring View S	etup Persor	nnel Langu	lage	Tool	s 1	Window	w H	elp										-	Ð	×
🗐 🍯 🌼 🍒	- 🔜 🖷 😏	19 😫 🕅	8 🔊 🚨			27	0														
Day Patrol																				4	×
7																					
	Controller	Door	Time		8	9	10	11	12	13	14	15	16	17	18	19	20	21			~
Rick (067-06644)	GV-AS210	Door 1	14:55									1	4:49								
Paul (084-27443)	GV-AS210	Door 1	14:55									1	4:50								
Curry (228-31386)	GV-AS210	Door 1	14:55																		

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 Patrol Log. This window appears.

Patrol Log								_ 🗆 🗙
	Patro	L	og					
Filter			~	🗄 Expand All 📄 Collapse All			Export: TXT	This Page OK
Log			^	Name 🔺	User	Time	Punch Time	Status 0 2
Tour:	Campus_East Side	~		4 🕈 Campus_East Side				<u> </u>
Status:		~		2013-08-01				
Date Period:	This Month	~		a 💼 123-45678				
Start Date:	08/01/13			1: Controller		[20:30 - 21:30][19:50 - 22:10		Absence
End Date:	08/31/13			⊿ 💼 234-56789 (S Spik	e)			
				1: Controller	S Spike	[20:30 - 21:30][19:50 - 22:10		Absence
Card				▷ 2013-08-02				
Card Numbers		~		▶ 2013-08-04				
Card Number.		-		> 2013-08-05				
Card Code:		~		≥ 2013-08-06				
Card Type:		~		▷ 2013-08-07				
Card Status:		~		2013-08-08				
Privilege:		~		2013-08-09				
Access Group:		~	~	▷ 2013-08-10				~
Search	Clear			<				>
Search	Clear			A Page 1 of 1		2		Displaying 1 - 1 of 1

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.

GeoVision

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.

8.1.1 Adding a New User

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

ASManager					X
Co Cuest	ID:	SFUser			
Generation SFUser	Password: Level:	User			
B Supervisor	Database Tool ASManager	ASWeb	VMWeb ASRe	TAWeb mote	
	 Person Data System Settings Door Operations Stop Alarm Clear Events Monitor Live Video Playback Server Start/Stop 				
	Data Group	Read	Write	Execute	^
	Taipei branch				
	SF branch		✓		
	Tokyo branch				
	Data Group 4				
	Data Group 5				
	Data Group 6				
	Data Group 7				
	Data Group 8				⊻
Allow removing password system		OK		Cancel	

Figure 8-1



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

Add Account	×
ID:	LimaUser
Password:	••••
Password Confirmation:	••••
Level:	User 💌
ОК	Cancel

Figure 8-2

- 3. Type the user's **ID** and **Password**. Re-enter the same password in the Password Confirmation field.
- 4. Give a **Hint** (optional) that would remind you of the password.
- 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 Removing System**, you can erase all user and supervisor accounts by running **AccessPassUninstall.exe** in the folder where the GV-ASManager program was installed.



8.1.2 Editing an Exiting User

Only supervisors are allowed to edit the information of a system user.

- Select a user from the user list to display its properties. Or, right-click on a user level (User or Supervisor), and then select **Find Specific Account** for a quick search. A valid password is required to edit a supervisor.
- 2. Edit the properties as required. Check the **Account Is Disabled** option if you wish to disable this 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.

Short Message Service Configuration					
SMS Server IP Address: 127.0.0.1	Port: 6886				
Send more than one sm	ns if content is too long.				
Login					
<u>U</u> sername:	Username: 1				
Password:					
Default Mobile Phone					
<u>C</u> ountry Code:	<u>M</u> obile:				
✓ 1. 886	0939234691				
2. 886	0939234697				
✓ 3. 886	0939234692				
OK Cancel					

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, you should configure the e-mail server.

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

Mail Configuration	X
Sender	
<u>N</u> ame:	joyce
E- <u>M</u> ail Address:	fae@geovision.com.tw
Authentication:	None
∐semame:	joycechang
<u>P</u> assword:	•••••
Mail Server	
<u>H</u> ost Name / Address:	geovision.com.tw
Command Port:	25 <u>S</u> SL
Misc	
Message Priority:	None
Test	
Send to: faek@geov	vision.com.tw
	OK Cancel

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 the Access, Event, LPR or Hotlist tab to set the alert methods for different events.
- 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".
- 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.
- 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.

Options 🛛 🔀
🔽 Run at Startup
🔽 Auto Backup
D:\Access Control\ASManager\ASBackup\
Export to file
D:\Access Control\ASManager\ASExport\
At Startup
Remote Monitor Server
Web Server
GeoFinger Server
Connect to SMS Server
OK Cancel

Figure 8-6

- **Run at Startup:** Run GV-ASManager at Windows startup.
- 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 3rd party programs. The access data will be listed in the file name of the text files. Up to 5000 files can be stored.

[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-ASWeb.



- 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 14.3 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.

Note: GV-GF1911 / 1912 / 1921 / 1922 is only supported in GV-ASManager 4.0 or later.

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 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.

User Setup	
General Home Busin	ness User Define Fingerprint Scan
Field	Value
User	Simon Lim
First Name	Lim
Middle Name	
Last Name	Simon
ID ID	
Gender	Male
Birthday	1/1/1900
Address(Home)	✓
	- File Type
	Oriver License
	O Business Card
	Scan
	Extract
	Lindate
	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.



8.6 Setting Hot Keys to Quickly Control Doors

You can assign hot keys to quickly control individual or multiple doors to perform one of the commands below: Unlock door, lock down, force lock, force unlock, disable door lock operation.

Device	Hotkey
☐ @ TEST198-PC	
— 🔟 Unlock Door	
— 🔟 Lock Down	
— 🔟 Force Lock	
- Difference Unlock	
Disable Door Lock Operation	
🖵 🚊 1 : Controller 1	
Unlock Door	
Lock Down	
Force Lock	
Force Unlock	
Disable Door Lock Operation	
Door 1	
Unlock Door	F1
E Lock Down	
- D Force Lock	
Force Unlock	
🗁 🔟 Disable Door Lock Operation	
Device Hotkey	
Hotkey for the selected command:	
F1	Clear
List of hotkeys:	- Assign
Hotkey currently used by:	

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

Figure 8-10

- 2. Under the Device list, select the GV-ASManager, a controller, or a door 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.

8.7 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 **Personnel** and select **Code Format Settings**. The pre-defined card formats are listed.

Customize Card Dial	og			X
Customized Card List:				
Card Name	Card Bits	Facility Bits	CardNo Bits	Parity Bits
Wiegand26	26	8	16	2
HID32	32	16	16	0
Geo34	34	16	16	2
HID35	35	12	20	3
HID37	37	16	19	2
New	Edit	Delete		Exit

Figure 8-11



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

Customize Card Setting			
Select Card Bits: Card Name:	27 Wiegand27	• ОК	Cancel
Card Bit		Parity	
25 24	Add ->		Up
23 22 21	<- Remove		Down
20 19 18		Facility code	
17 16 15 14 13 12 11 10 9 8 7 6 5 4	Add ->		Up Down
3		Card number	
1 0	Add -> <- Remove		<u>Ц</u> р <u>D</u> own

Figure 8-12

- 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**.



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

9.1 Installing GV-ASRemote

Insert Software DVD to your computer and a window will pop up automatically. Select **Install GeoVision Access Control System**, click **GeoVision Access Control System** and follow on-screen instructions to complete the installation.

9.2 The GV-ASRemote Window



Figure 9-1



No.	Name	Function	
1	Menu Bar	The Menu Bar includes the options of File (log in / out the GV-ASManager), Monitoring (display monitor windows of alarm, access and event), View (display the function windows) and Window (arrange the display of different windows).	
2	Toolbar	The Toolbar includes the options of Connect , Disconnect , Auto Connect , Add Host , Remove Host , Settings and Resolution .	
3	Device View	Displays a list of connected doors and their current status.	
4	Alarm Monitor	Displays alarm events of doors.	
5	Event Monitor	Displays monitored events of doors.	
6	Access Monitor	Displays access activities of doors.	
7	MultiView	Displays live views of connected cameras from multiple IP devices. For details, see <i>5.4 The MultiView Window</i> .	
8	Information Window	Displays the information of doors, card readers and monitored events.	
9	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> .	
10	Live Video	Displays live views of one connected camera. For details, see the same operations in <i>5.2 Accessing Live View</i> .	
11	Camera List	Displays a list of connected cameras.	



9.2.1 Toolbar





The buttons on the Toolbar of GV-ASRemote:

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 may connect to one GV-ASManager, the GV-ASManager must allow the remote access by this procedure:

• 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:

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

Add Host		
<u>H</u> ostname:	Test1	ОК
Address:	127.0.0.1	Cancel
<u>P</u> ort:	9987	
<u>I</u> D:	1	
Pass <u>w</u> ord:	1	
Controller		
V 🗐 Test1		Add
		Bemove
		<u>I</u> IIIIIIII



- 2. 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.
- 3. Click Add. This dialog box appears.

Add Co	ntroller			×
<u>I</u> D:		1		
	OK		Cancel	

Figure 9-4

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



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





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 4-7), see *D*. *Controller Status* in Appendix.

GeoVision

Chapter 10 GV-ASWeb

The GV-ASWeb allows you to access data and settings on the GV-ASManager over the network. Connecting to one GV-ASManager at a time, users can remotely watch live video, view event data, download logs in different formats, and set up camera / cards / users / vehicles / controllers / schedule using Web interface.

To use the GV-ASWeb, the version of browser in the client PC must be **Internet Explorer 7** 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.

GeoWebServer Setting Dialog
Http Port Https Port 443 (Takes effect after you restart WebServer.)
Rule From IP To IP Up Down
Add Modify Delete

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 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 10-2a

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



Figure 10-2b

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 10-3



Accessing Live Video 10.2

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 **Live Video**. This window appears.





Figure 10-4

- 2. Click the **Device** drop-down list to select a connected GV-System 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 Accessing Logs

You can access the logs of the connected GV-ASManager, including Access Log, Daily Access, Alarm Log, Event Log and I/O Log. In addition, you can set up search criteria to view the records more efficiently.



Figure 10-5

10.3.1 Setting Search Criteria

- 1. Select a log you want to view. Here we use Access Log as an example.
- 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 AS400, and dates from November 21st to November 27th. The resulting filter window may look like this.

Access Log							
	Access	Log]				
Filter		«			Export: T	XT This Page	ок
🕒 Log			Access Message	Door	Local Time	Snapshot 1	Snapsho
Message:	Access Granted	•					
Door:	AS400 - Gate A	•					
Direction:	In	•					
Date Period:	Date Range	-					
Start Date:	11/21/10	3					
End Date:	11/27/10	3					
Card							
Card Number:	120-38620	-					
Card Code:		- 🗸					
Searc	ch Clear		<				>
			III IIII Page 1 of 1 ▶ ▶	2		No data	to display

Figure 10-6

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



10.3.2 Log Window Icons

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

EXECUTE: Indicates the availability of the recorded video.

image. 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 information are 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.

10.3.3 Exporting Logs

You can download the logs of the connected GV-ASManager to the current computer in four formats: .txt, .html, .xls and html (zip).

- Use the Export drop-down list on the top-right corner and select the file format TXT, HTML, Excel and HTML (ZIP).
- 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.

10.3.4 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 10-7

- 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.

Access Log							I	Employee ID Job Title
Filter			~					Department
Log			^		Message	▼ Door	Lo	Office
Message:		~		1	Access Granted	A Sort Ascending	1	Phone (Business)
Door:		~	=	2	Access Granted	Z↓ Sort Descending		Ext (Business)
50011				3	Access Granted			Fax (Business)
Direction:	In/Out	*		4	Access Granted	Columns		Web Page (Business)
Date Period:	Today	~		5	Access Granted	Controller 1 - Doo	9/	F-Mail Address (Business)
Start Date:				6	Access Granted	Controller 1 - Doo	9/	Notes (Business)
				7	Access Granted	Controller 1 - Doo	9/	Notes (busiless)
End Date:		L ²		8	Access Granted	Controller 1 - Doo	9/	Parking Space Number
				9	Access Granted	Controller 1 - Doo	9/	User Define 02

Figure 10-8

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:

Access Log							
Filter		~			E	xport: TXT	This Page OK
Log		-		Message	Card Number	User	Parking Space Number
Message:	Duress Active						
Door:	v						

Figure 10-9


10.4 Adding and Deleting Controllers

You can use GV-ASWeb to remotely add or delete controllers to the GV-ASManager.

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

Controller List	- C X
Controlle	er List
🖪 🗟 🐡 🗾	Information
Door	No items for display.
1: Controller 1 (1/4 Doors) GV-A5400	
Door 1	
Door 2	
. Door 3	
Door 4	
🛛 🖣 Page 1 of 1 🕨 🕅 🖑 Displaying	

Figure 10-10

- 2. Click the **Add** button **b** 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.

Controller List			- - ×
Controlle	er List		
2 I 🐉 🗾	Door		
Door	General		
1: Controller 1 (1/4 Doors) GV-AS400	Set Door Info		_
Door 1	Name:	Door 1	=
Door 2	Password:	●●●● 4~8 digits(0~9)	
Door 3	Lock Reset Time:	5 Sec(1~255)	
Door 4		12 (Handicap Card)	
	Held Open Time:	10 Sec(5~9999)	
		15 (Handicap Card)	
	Fire Action:	Unchange 🗸	
II I Page 1 of 1 ▷ ▷ ② Displaying	Revert		Save



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

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



10.5 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:



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

🖹 New a Card			×
-Card			
User:		2 &	
Card Number:	<u>.</u>	Card Code: [26] Wiegand26	
Card Status:	Active	Card Type: Normal	
Activation Date: 1	12/24/13	3	
📃 Deactivation Date:	12/24/13		
Pin Code:		Privilege: No Privilege 💙	
Data Group:	No Groups	Disable Lock Card	
Access Group:	Default	•	
Door		Schedule	
🗉 🗐 Controller 1 (4 D	oors)		
🗔 Door 1		24-hour restricted	
Door 2		24-hour restricted	
Door 3		24-hour restricted	
Door 4		24-hour restricted	
🗄 📋 Controller 2 (2 D	oors)		
			×
		OK Cancel	

Figure 10-12

- 3. Fill out the required information. Refer to 4.3 Setting Cards for more details.
- 4. Click **OK** to save the settings.
- If you have a GV-PCR310 Enrollment Reader installed, you can click Card Reader to add a card using GV-PCR310.

٢	New 🖉 Edit 🎯 Delete 🎑	ard Reader		Exp	ort: TXT	This Page	ок
	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	-	-	



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 User List. The User List window appears.
- 2. Click the **New** button. This dialog box appears.

😰 User Setting				×
General Home	Business User Defined Finge	erprint		
First Name: Display: Employee ID:	Bill	Middle Name: Data Group: Photo:	No Groups	Last Name: Lumbergh
Cards: Card Number	🗿 🎲 👄 Card Code			
Vehicles: License Plate	Brand Model			
🗌 Send SMS 🖉	2			
		ОК	Cancel	

Figure 10-14

- 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 led 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 **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*.



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.



Searching, Adding and Deleting IP Cameras 10.6

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

On GV-ASWeb, click the **Camera List** icon **Camera List**. The Camera List window appears. 1.



To search for available IP devices under LAN, click the Search button 🖾 and select 2. Search DVR and NVR or Search IP Device. This dialog box appears.

💼 Camera List						
200	🦻 Camera List					
	ଷ୍ଟ 🔾 🤤 🐇	earc	h IP Device			\$ X
Camera	Location		Host Name		Address	
🗄 🎒 www (1 C	Camera)	5 🕅	DVR-IPCAM V1(1	92.168.2.4)	192.168.2.4	^
		6 🕅	GVLX4(RL2.235)	(192.168.2.235)	192.168.2.235	
		7 🔽	GV-IPSpeedDome	e(192.168.3.222)	192.168.3.222	
		8 🔽	GV-VS02A(192.1	168.3.228)	192.168.3.228	
		9 🔽	Demo-GV-VPv1(192.168.1.167)	192.168.1.167	
		10 🔲	Leo-GPS(192.168	3.1.62)	192.168.1.62	
		11 🔳	Joe-IPCAM1.3M(1	92.168.1.116)	192.168.1.116	
		12 🔽	VS-02(192.168.1	.115)	192.168.1.115	
		13 🔽	GV-IPSpeedDome	e(192.168.3.188)	192.168.3.188	~
		Network A	dapter:	IP(192.168.0.171)	Intel(R) PRO/1000 🗸	Q.
		Port:		15000		
🕅 🖣 Page	1 of 1 🕨 🕅 ಿ Displaying 1 - 1 of	1			Add	Cancel

Figure 10-15

- A. Select the GV-Systems 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-System or IP device is added to the camera list on the left.
- D. To login, select the GV-System or IP device, click the Edit Mode button 🐲, and type the User ID and password.



Camera List	🕞 Camera L	.ist			- 0
	ଜ୍ୟି • 📀	۵ 🍪	New Host		
Camera	Location		Host Setting		-
🗄 🎒 www (1	Camera)		Туре:	IP Camera 💌	
			Host Name:	fish	
			Address:	192.168.3.199	
			User:	admin	
			Password:	••	
			VSS Port:	10000 Default	
			Brand:	GeoVision_GV-FE420_Series	
			Number of Cameras:	1 💌	
A Page	1 of 1 🕨 🕅 ಿ Displaying	1 - 1 of 1	Revert		Save

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

Figure 10-16

- 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-Systems, 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 is 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.



10.7 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.

10.7.1 Setting Daily Schedule

1. On GV-ASWeb, click the **Time Zone Setup** icon



Time Zone Setup

. This dialog box appears.

Figure 10-17

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

🚱 Tim	e Zone Setup																-	
0) 😨 😨 💽 🤅	0																
D	Name	0 1 	2 3	4 5	6 7	, s 11111	9 11111	10 11 II.	12 13	14 1111	15 16 	17 	18 19 	20 1111	21 22	2 23 24	Data Group	
	New Time Zone																No Groups	~
U	Deny Access								Cance	el							NO Groups	
255	Full Access																No Groups	
14 4	Page 1 of 1		2														Displaying 1 -	5 of 5

Figure 10-18

- 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 (a) and drag the mouse across the selected time.



- You can use the **Data group** drop-down list to assign the time zone to a data group. You 5. can then allow or forbid a user to read/write the functions listed under the data group. Refer to Adding a New User in Chapter 8 for more details.
- Click **Update** to save. 6.

10.7.2 Setting Weekly Schedule

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

_
-
3 3 3
Schedule
Setun

87 9	ichedu	e Setup										X
0	0		ID:	0	Name:	2	4-hou	ur res	tricted			
	ID Name				Data Groups			No.(Found			-1
1	0	24-hour restricted			Data Group.				sioups			
2	255	24-hour access	Name									
			Monday	Deny Access			'	1	1	1	1	
			Tuesday	Deny Access	1 1		1		1	1	'	
			Wednesday	Deny Access	1 1		1		1	1	'	
			Thursday	Deny Access			'	Т	1	1	1	
			Friday	Deny Access			1	Т	1	1	1	
			Saturday	Deny Access			1	Τ	1	1	1	
			Sunday	Deny Access			1	Т	1	1	1	
			Holiday	Deny Access	1 1		1		1	1	1	
14	≪ p	age 1 of 1 🕨 🕅 🧟									Close	

Figure 10-19

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



Specifying Holiday 10.7.3

On the main page of GV-ASWeb, click the Holiday Setup icon

day Setup. To specify holidays, click Add Holiday and click the dates of the Holiday. To remove holidays, click Remove Holiday and click the dates.

I Holiday Setup																																_ ×
🕑 Ac	ld Ho	liday]0	Rem	ove H	loliday	/ 🗮	Clea	r All I	Holida	iys																					
		De	cemb	er 20	10					Ja	anuar	y 201	1		~			Fe	bruar	y 20	11					ſ	March	201	1			~
Wk.	s	М	т	W	т	F	S	Wk.	S	М	т	W	т	F	S	Wk.	S	М	т	W	т	F	S	Wk.	s	М	т	W	т	F	S	
48				1	2	3	4	52							1	5			1	2	3	4	5	9			1	2	3	4	5	
49	5	6	7	8	9	10	11	1	2	3	4	5	6	7	8	6	6	7	8	9	10	11	12	10	6	7	8	9	10	11	12	
50	12	13	14	15	16	17	18	2	9	10	11	12	13	14	15	7	13	14	15	16	17	18	19	11	13	14	15	16	17	18	19	
51	19	20	21	22	23	24	25	3	16	17	18	19	20	21	22	8	20	21	22	23	24	25	26	12	20	21	22	23	24	25	26	Ξ
52	26	27	28	29	30	31		4	23	24	25	26	27	28	29	9	27	28						13	27	28	29	30	31			
1								5	30	31						10								14								
			April	2011							May	2011							June	2011							July	2011				
Wk.	s	М	т	W	т	F	S	Wk.	s	М	т	W	т	F	s	Wk.	s	М	т	W	т	F	S	Wk.	s	М	т	W	т	F	S	
13						1	2	17								22				1	2	3	4	28						1	2	
14	3	4	5	6	7	8	9	18	1	2	3	4	5	6	7	23	5	6	7	8	9	10	11	27	3	4	5	6	7	8	9	
15	10	11	12	13	14	15	16	19	8	9	10	11	12	13	14	24	12	13	14	15	16	17	18	28	10	11	12	13	14	15	16	
16	17	18	19	20	21	22	23	20	15	16	17	18	19	20	21	25	19	20	21	22	23	24	25	29	17	18	19	20	21	22	23	
17	24	25	26	27	28	29	30	21	22	23	24	25	26	27	28	26	26	27	28	29	30			30	24	25	26	27	28	29	30	
18								22	29	30	31					27								31	31							
August 2011 September 2011 October 2011 November 2011																																
OK Cancel																																

Figure 10-20

10.8 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.

93 I	Access Groups Setup						- - ×
0	O	Name:	Access	Group 01			
	Name 🔺	Data Group:		Data Group 1	~		
1	Access Group 01	Data Gloup.					
		Door			Schedule		
		🗉 📋 Controller 1	l (1 Doo i	r)			
		Door 1			24-hour restricted		
		N A Page 1	of 1	> N 2			Displaying 1 - 1 of 1
						Save	Close
	🖣 Page 1 of 1 🕨 🕅 🍣 No data to						

Figure 10-21



. For details on

Setting Door Groups 10.9

Using GV-ASWeb, you can remotely organize controllers into different door groups, allowing you to quickly upload fingerprints to all controllers in a door group at once.

Controllers Using Door Groups in Chapter 3 of GV-GF Fingerprint Reader User's Manual.

On the main page of GV-ASWeb, click the **Door Group Setup** icon how to set up door groups and upload fingerprints, refer to Uploading Fingerprints to



Figure 10-22



10.10 Configuring Areas for Anti-Passback

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

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

Area Settings		
🛂 Add 🛛 🙀 Remove 🎾 Rename	Doors	
Name	Controller 1 (3 Doors)	
Global Area	Door 1 goes from Lobby to Global Area	
📑 Lobby	Door 2 goes from Reception to Meeting Room B1	
Reception	Door 4 goes from Demo Room to Lab	
Demo Room		
👪 Meeting Room B1		
👪 Lab		
na ta kutoka ana	A Page 1 of 1 D D 2	Displaying 1 - 3 of 3

Figure 10-23

- 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.

Area Settings		- DX
🛃 Add 📓 Remove 🖉 Rename	Doors	
Name	□ □ Controller 1 (3 Doors)	
📑 Global Area	Door 1 goes from Lobby to Global Area	
Lobby	Door 2 goes from Reception to Meeting Room B1	
Reception	Door 4 From : Demo Room To : Lab	~
Demo Room B Meeting Room B1	Update Cancel Global Area Lobby	
Lab Area 7	Reception Demo Room Meeting Room B	31
	Lab	
	Area 7	
4 4 Page 1 of 1 ▶ ▶	III → Page 1 of 1 → FI 2 Displayi	ng 1 - 3 of 3

Figure 10-24

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.



10.11 **Creating Maps**

1.

You can place the icons of connected controller, LPR lanes, and LPR cameras 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.



鸄 Map ~ 6 F

- **-** × 📀 Add Map 🛭 🎲 Edit View -~ Device Мар Map Satellite 🚞 Map Ŷ 4 🔄 Controller + Controller 1 Controller 2 United State d 🔜 LPR 1 Þ 🚍 LPR 2 🖌 😋 Camera ⊳ 🗐 LPR 1 Mexico ⊳ 🗐 LPR 2 Map data ©2013 Google, INEGI, MapLink - Terms of Use

Figure 10-25

- 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.

🚉 Add Map		×
Name:	Mall_1F	
Map:	Level 1.bmp	
	Upload Cancel	

Figure 10-26

- Type a name for the map and click the **Add** button **I** to locate the file of the map. 4.
- 5. Click Upload. A pin is placed on the map.
- 6. Click Edit in the top-right corner. If you have uploaded your own map, click the pin to open the map.

GeoVision

- 7. Drag the controller, LPR lane, and LPR camera icons from the left menu onto the map according to their location.
- 8. Click **Edit** again when you are finished. You can click the icon of the controllers, LPR lanes or LPR cameras to access their information.



Figure 10-27

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

					🔘 Add Map	e 🍪 Edit	View •
Tracking							»
Type:	Card	~					^
User:	Parker	¥					
Card Number:		¥					
Date Period:	This Month	~					
Start Date:	07/01/13						=
Time:		~					
End Date:	07/31/13	•					
Time:		~					
	Route Planning b	y Google					
		Search	Clear				
		Search	Cical				
Records Informat	tion						
Message	Door	Local Time	Camera 1	Camera 2	Card Number	User	
∃ 1:GV-A5210 - Doc	or 1 7/18/2013 11:43	:13 AM (10 Items)					^
Access Granted	GV-AS210 - Door 1	7/18/2013 11:43:13 AM	ii	iii III	131-19618	Parker	
Access Granted	GV-AS210 - Door 1	7/18/2013 12:00:10 PM	iii III	iii ::::	131-19618	Parker	
Access Granted	GV-AS210 - Door 1	7/18/2013 12:00:30 PM		÷	131-19618	Parker	
Access Granted	GV-AS210 - Door 1	7/18/2013 1:34:42 PM	<u>ii</u>		131-19618	Parker	
Access Granted	GV-AS210 - Door 1	7/18/2013 1:47:36 PM	÷	iii ::::	131-19618	Parker	~
🗐 🖣 🕴 Page 👥 1	of 2 🕨 🔰 ಿ					Displaying 1	- 32 of 11

Figure 10-28



- 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 / LPR cameras to another.

- 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 10-29



10.12 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.

ASManager					×
Guest Guest User Gupervisor	ID: Password: Level:	Guest Guest			
	ASManage Database Tool V Log Export Image/Playback Access Setup V Person Data	ar ASWeb	ASRi VMWeb	emote TAWeb	
	Data Group Data Group 1 Data Group 2 Data Group 3 Data Group 4 Data Group 5 Data Group 5 Data Group 7	Read	Write	Execute]
Allow removing password system		ОК		Cancel	

Figure 10-30

- 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.
- 7. Click OK.



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:** Looks up workforce schedule, attendance records, and employee payroll.
- **TA Shift:** Sets up different types of daily work schedules.
- TA Template: Arranges schedules of up to 45 days with daily schedules from TA Shift.
- TA Holiday: Designates which dates are holidays.
- **TA Schedule:** Assigns work schedule to individual or a group of employees.
- **TA User:** Specifies employee salary.

To use the GV-TAWeb, the browser in the client PC must be Internet Explorer 7 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.

 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 Gate tab and select Time Clock.

General Setup Gate 1 Gate 2 Gate 3 Gat	e 4
General Set Door Info	
Name:	Gate A
Password :	•••• 4~8 digits(0~9)
Lock Reset Time :	5 Sec(1~255)
	5 (Handicap Card)
Held Open Time :	10 Sec(5~9999)
	10 (Handicap Card)
Fire Action	Unchange 🗸
Reader's Keypad	Anti-Passback
Entrance	📃 Local Anti-Passback
💌 Exit	Globe Anti-Passback
GeoFinger	Two-Person Rule
Time Clock	Entrance
Auto Check Out	Exit

Figure 11-1

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

GeoWebServer Setting Dialog
Http Port Https Port 443 (Takes effect after you restart WebServer.)
IP Filter
Rule From IP To IP Up Down
Add Modify Delete
OK Cancel

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 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.

Add Shift 🤤	Remove Shift	🌮 Edit Shift				
Name	Start Time	End Time	Break time start (1)	Break time end (1)	Break time start (2)	Break time end (2

Figure 11-5

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

lame:		
tart Time:	9:00	0
ind Time:	17:00	0
dvance Period:	02:30	0
xtended Period:	04:00	0
Vertime Buffer Period:	00:30	0
Break Time (1)		
Start Time:	12:00	0
Start Time: End Time:	12:00 13:30	0
Start Time: End Time: Break Time (2)	12:00 13:30	0
Start Time: End Time: Break Time (2) Start Time:	12:00 13:30 15:00	0

Figure 11-6

GeoVision

- 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.
- 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.

ttings
Weekday
e: 9:00 O
:: 18:00 🙂
Period: 02:00 0
Period: 04:00 0
Buffer Period: 00:30 O
Time (1)
ime: 12:00 O
ne: 13:00 O
Time (2)
ne: 15:30 O
Save Cancel

Figure 11-7



Using the above figure as an example, an employee working 4 hours passed the 18:00 pm regular end time will receive overtime pay for 4 hours (18:00 - 22:00), while an employee working 20 minutes passed 18:00 will not receive overtime pay.

07:00 - 9:00	Start Time 09:00			End Tim 18:00	e	18:00 - 22:00	[
Advance Period	R	egular W	ork Hours		E	xtended Period	
	12	Break Time :00 - 13:	00		Overtime Buffer Period 18:00 - 18:30		-



9. Click **OK** to save 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 11-9

2. Click Add Template. This dialog box appears.

Day1 Day2 Day3 Day4 Day5 Day6 Day7 -	Name: Period:			7									
Day1 Day2 Day3 Day4 Day5 Day6 Day7 - v -	With Holidays:												
- v - v - v - v - v -	Day1		Day2		Day3		Day4	Day5		Day6		Day7	
Description:	-	~	-	v	-	~	- •	-	~	-	v	-	
	Description:												~

Figure 11-10

- 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.



6. 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 De	sk-PT									
Period:	14										
With Holidays:											
Day1 C	Day2	Day3		Day4		Day5		Day6		Day7	
morning 🗸 m	norning 🔪 🥆	afternoon	~	special event	~	special event	~	special event	~	-	~
Day8 E	Day9	Day10		Day11		Day12		Day13		Day14	
morning 🗸 m	norning	afternoon	~	afternoon	~	morning	~	-	~	-	~
Description:	Part-time	work schedule	for fr	ont desk (2 wee	ks)						
				Save C	anc	el					

Figure 11-11

7. Click Save.

11.2.3 TA Holidays: Setting Certain Dates as Holidays

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

•	ТА	Но	liday	/																												- X
0	Ad	ld H	olida	y 🧲	Ren	nove	Holida	ay 💡	😕 Edi	t Holic	day																					
													Ja	nuai	ry 20	10 -	Dece	embe	er 20	10												
•	1		Ja	anuar	y 201	10					Fe	brua	y 20	10						March	2010							April	2010			
W	k.	s	М	т	W	т	F	s	Wk.	S	М	т	W	т	F	s	Wk.	s	M	т	W	т	F	s	Wk.	s	М	т	W	т	F	5
5	3						1	2	5		1	2	3	4	5	6	9		1	2	3	4	5	6	13					1	2	1
	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 1	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
3	4 2	24	25	26	27	28	29	30	9	28							13	28	29	30	31				17	25	26	27	28	29	30	
	5 3	31							10								14								18							
				May	2010	j.						June	2010	i.						July	2010						A	ugus	t 201	D		
W	k.	s	М	т	W	т	F	s	Wk.	s	М	т	W	т	F	s	Wk.	s	М	т	W	т	F	s	Wk.	s	М	т	W	т	F	5
1	7							1	22			1	2	3	4	5	26					1	2	3	30							~
<						_										Ш																>

Figure 11-12

- 2. Select a date and click **Add Holiday**.
- 3. Type a name for the holiday.
- 4. 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 department, open the employees' user information in User List and select the **Business** tab. In the **Department** field, type the department of the employee and all employees with the same department name will be grouped into one department in GV-TAWeb.

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



Figure 11-13



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.

Shift:	FAE Schedule	*
Date:	2014/04/24	
Apply to		
Oroup:	FAE	
Only Se	lected Users	

Figure 11-14

- 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.

λA	Assign Shift 📎 A	ssign Template (Remove Schedul	le				
	Employee	01/02 (Sun)	01/03 (Mon)	01/04 (Tue)	01/05 (VVed)	01,06 (Thu)	01/07 (Fri)	01/08 (Sat)
1	Angeline Tay	-	Orientation	Night	Day Time	Night	Special Event	Special Event
2	Grace Chong	-	Day Time	Orientation	Morning	-	Special Event	Special Event

Figure 11-15



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.

Template:	-	~
emplate Day of Start Date:		~
tart Date:		
nd Date:		
- Schedule Overlapping Sche	eme	
 Overwrite the original sch 	edule	

Figure 11-16

- 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.

mplate:	FAE Sched	~
nplate Day of Start Date:		~
tart Date:	1 : FAE Schedule	
nd Date:	2 : FAE Schedule	
Oshadula Quarlanning Oshama	3 : FAE Schedule	
-schedule overlapping scheme -	4 : FAE Schedule	
⊙ Overwrite the original schedule	5 : FAE Schedule	
○ Keep the original schedule	6 : -	
	7:-	

Figure 11-17

- 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.
- 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.

at)
-
-

Figure 11-18

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.

TA Template Setting	js											×
Name:		FAE scl	hed	tule								
Period:		7										
With Holidays:	[
Day1	Day2			Day3		Day4		Day5	Day6		Day7	
FAE Schedule 👻	FAE Sch	iedule	~	FAE Schedule	Y	FAE Schedule	~	FAE Schedule	-	*	-	~

Figure 11-19

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

Assign Template (Admin)			A	ssign Template (Admin)								×
Template:	FAE schedule	~		Template: Template Day of Start Date:	FAE	: sche	edule	1				*
Template Day of Start Date:	6:-	~		Start Date:	201	.1/01	/15					
Start Date:	1 : FAE Schedule			End Date:			Janua	ry 20	11 🔻			
End Date:	2 : FAE Schedule			Schedule Overlapping Scheme	s	М	т	w	Т	F	S	
	3 : FAE Schedule			• Overwrite the original schedu	26	27	28	29	30	31	1	
Schedule Overlapping Scheme	4 : FAE Schedule			Keen the original schedule	2	3	4	5	6	7	8	
 Overwrite the original sched 	ι 5 : FAE Schedule				9	10	11	12	13	14	15	
○ Keep the original schedule	6:-				16	17	18	19	20	21	22	
	7:-			ок	23 30	24 31	25 1	26	3	28 4	29 5	

Select the first non-working day

Select a Saturday for Start Date

Figure 11-20

GeoVision:

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.





- 2. Select an employee from the list.
- 3. Type the Hourly Regular Pay and the Hourly Overtime Pay.
- 4. 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 11-22

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. 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.
- 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.



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

Daily Time Card	d						
🚽 Save 下 Run	Export CSV						
Date Name	Department	Job Title F	Punch In Time	Punch Out Time	Punch Out Time (Lun	Punch In Time (Lunch)	Work Time
:)		Ш					[
4 4 Page	1 of 1 🗼) 2º				No	data to displ
Report Settings							3
Exception							
A: In Late E: Over Hours	B: F:	In Early Unschedule	d Absence		C: Out Late G: Missed Punch	D: Out H: Not S	Early Schedule
Title:	Dai	ly Time Card	i				
Date:	20	13/06/25	•				
<							>

Figure 11-23

- 4. Select the **Date** and **Department** to look up the employees' scheduled shift and actual attendance record.
- 5. 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 T	Time	Punch Ou	t Time	Work Time	Start Time	End Time	Duty Work Time	Exception
	Guiry	10.00		10.00		00.71	11.00	10.00	01.20	-, v, ii
	Irving	18:00	TA	19:00	TA	00:47	17:35	19:00	01:20	A, C, H
	lverson	17:52	TA	18:16	TA	00:18	17:35	19:00	01:20	A, D, H
	Parker	10:01	TA	16:56	TA	06:55	09:00	17:00	08:00	A, D
5	Paul	10:01	TA	16:56	TA	06:55	09:00	17:00	08:00	A, D
;	Rick	-		2		2	-	2	23	2
	Rondo	17:52	TA	18:16	TA	00:19	17:35	19:00	01:20	A, D, H
		1 of 1		2						Displaying 1 -
ep	ort Settin	igs								
	B: Ir F: U	n Early nscheduled	Absence			C: Out Lat G: Missed	te Punch	D: (H: N	Out Early Iot Scheduled	

Figure 11-24



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

📄 TA Report				
Report Template	~	×	Delete Report 😁 Open Report	Searching reports by the title 🔎
🖃 😋 All Templates			Title	Template
Griedule Templates Employee Schedule Upscheduled Employee		1	Daily Time Card	📖 Daily Time Card
Cirischeutred Employee				
i Daily Time Card Employee Time Card				
Exception				
Exception Summary				
🖃 😋 Payroll Templates				
📰 Employee Payroll		14	4 Page 1 of 1 ▶ ▶ 22	Displaying 1 - 1 of

Figure 11-25

- 8. Click **Export CSV** to export the data in an excel file.
- 9. To select which data to display, click the arrow next to the column title and click **Column**.

	Name	Punch In Time	 Punch Out Time 	Wo	ork Ti	me Start Time
1	Lydia Ching	09:56	Ag↓ Sort Ascending		40	09:00
2	Ng Koh Sheng	09:57	Z Sort Descending		40	09:00
3	Edmund Lau	09:57		. [00.00
4	Lance Yeo	09:57	Columns		1	Name
5	Tony Tey	09:57	-	-	V	Punch In Time
6	Vivien Lee	09:57	18:37	08	V	Punch Out Time
7	Jeslin Poh	09:56	18:37	08	V	Work Time

Figure 11-26

Note: The **Export CSV** function is only available after you have saved the report by clicking the **Save** button.



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.

ASManager					
Contraction Contra	ID: Password: Level:	HRstaff • User			
	ASManager		۵SBe	note	
	Database Tool	ASWeb	VMWeb	TAWeb	
	 ✓ Report Viewing ✓ Payroll Setup 				
	Data Group	Read	Write	Execute	
	Data Group 1				
	Data Group 2				
	Data Group 3				
	Data Group 4				
	Data Group 5				
	Data Group 6				
	Data Group 7				
Allow removing password system		OK		Cancel	

Figure 11-27

- 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 7 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.

GeoWebServer Setting Dialog
(Takes effect after you restart WebServer.)
Rule From IP To IP Up Down
Add Modify Delete
OK Cancel

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 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.

VMWeb - Microso	oft Internet Explo	rer									- 7 ×
File Edit View Fa	rvorites Tools He	lp									A
🚱 Back 🔹 🛞 -	💌 🗟 🐔	🔎 Sea	rch s	📩 Favorites 🚱 🔗 -	🍓 🔜 4	8					
Address 🕘 http://192.	168.0.205/VMWeb/V	MWeb.html								*	🔁 Go Links 🏾
- P. e		Visit	or	Management						💡 Logout	💞 Themes 🔹 🎆 🔹
Filter			~	🚨 Visitors							
Visitor				🙈 New 🐉 Edit 🗙 Delete							
Name:		~		Name	Gender	Cardholder	Company	Employee ID	Job Title	Department	Office
Company:		*		All Visitors							
Employee ID:											
Job Title:		*									
Department:		*									
Liser Define 01:											
User Define 02:		_									
User Define 03:		_	~								
Searc	h Clear										
				A Page 1 of 1	ы 🖓						Displaying 1 - 1 of 1
Demands For Vis	iit - [All Visitors	1									*
💿 New 🗙 Delete							Search	Card Numb	er	¥	9
Visit Date	Visit Time	Destinatio	n	Notes	Permission	Card Number	Che	eck In		Check Out	Deactivatio
<											Na data ta sfanlari
Director											No data to display
neauy											
E Done			_							🔮 Inte	met

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.

ASManager				X		
Guest Guest User BrRstaff Cupervisor	ID: Password: Level:	ID: Security Password: Level: User				
	Database Tool	ASWeb	VMWeb	TAWeb		
	View Visit Record Edit Visit Record Permit Visit Issue Card System Settings			_		
	Data Group	Read	Write	Execute		
	Data Group 1					
	Data Group 2					
	Data Group 3					
	Data Group 4					
	Data Group 5					
	Data Group 6					
	Vata Group 7					
Allow removing password system		OK		Cancel		

Figure 12-5



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

A	dd Account 🛛 🛛
	ID:
	Password:
	Password Confirmation:
	Level: Supervisor 🗸
	OK Cancel

Figure 12-6

- 3. 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 as shown in Figure 11-6. Click OK. To grant limited access, select User and click OK.
- 5. Click the **VMWeb** tab.
- 6. 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
- 7. 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.

Visitor Settings		
General Home	Business User Defined	
First Name:		Middle Name: Last Name:
Displays		
Display:		
		Photo: Browse 🙆 🗶
Cards:		
Card Number	Card Code	
		OK Cancel

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 is 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 *4.6.4 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.

Note: You need to first 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*.

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

	Demands For Visit - [Slydell Bob]											
\odot	New 💢 Delete 🖳	Export CSV					Search:	Card Number	~			9
	Visit Date	Visit Time	Destination	Notes	Approval	Permit	Card Number	Check In	Check Out	Deactivation Date	User	
	01/13/2014 📑	16:05 🕓	Initech	Baord Meeting		✓	255-4567 ×	•				
					Update	C	ancel					
14	4 Page 1 o	f1 🕨 🕅	2							No	data to disp	olay

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.

				1	ege card no
	Card Number	Card Type	Card Status	Activation Date	Deactivation Date
1	255-32465	Visitor	Active	12/24/2013	2
2	255-45785	Visitor	Active	12/24/2013	12/26/2013 12:0
3	255-45678	Visitor	Active	12/24/2013	12/27/2013 12:0
4	4 Page	1 of 1 🕨	N 2		Displaying 1 - 3
۹ 5e	4 Page	1 of 1)	≥ 2		Displaying 1 - 3
۹ 5e	Page etting Deactivation	1 of 1 🕨	× 2	▼	Displaying 1 - 3

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** is 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.
- 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.

	Demands For Visit - [Slydell Bob]										
O New X Delete B Export CSV Se							Search:	Card Number		•	Q
	Visit Date	Visit Time	Destination	Notes	Approval	Permit	Card Number	Check In	Check Out	Deactivation Date	User
	01/13/201	16:05	Initech	Baord Meeting	admin		255-45 6	01/13/2014 16:06:57		01/13/2014 23:5	9 Slydell Bob
					Update	•	Cancel				
<											
14	Page 1	of 1 🗼 🖡								Dis	playing 1 - 1 of 1

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 or User.

Filter		~	8	Visitors								
- 🔺 Visitor		^	8	New 🐉	Edit 🔀 Del	ete						
Name:			Name 🔺	C	èender	Cardholder	Company	У	Employee ID	Department		
Company:		~	All	All Visitors								
Employee ID:			1	B Michae	el		Visitor	1900-1900-1		-	engineering	
Job Title:		~	2	G Peter			Visitor			-	engineering	
				N Samir			Visitor			-	Engineering	
Dopardinoridi	chighteening											
Sear	rch Clear		M	🖣 🕴 Page	e 1 of 1		2			C	visplaying 1 - 3 of 3	
Demands For Vis	iit - [G Peter]										*	
💿 New 💢 Delete						Search:	Card Number		~		Q	
Visit Date	Visit Time	Destination	Notes	Per	rmission	Card Numb	Card Number			Chec	k Out	
				Destination		- 1						
							Notes					
							Cardholder		_			
🚺 🖣 Page 🚺 o	if 1 🕨 🕅 🍣										No data to display	

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.

	:0		
Servers	Confirmation E-Mail	Password E-Mail	
— Mail Se	erver Information		
SMTP Se	erver Address:	geovision.com.tw	
Login Na	ime:	admin	
Login Pa	ssword:	•••••	
SSI:		Port: 25	
		1014	
Web S	erver Information	192.168.0.171	
Web S	erver Information	192.168.0.171	
Web S	erver Information	192.168.0.171	
Web S	erver Information	192.168.0.171	

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.
- 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.

n E-Mail Password E-Mail
Geo Admin
admin@geovision.com.tw
Visitor Account Confirmation
Thank you for registering a visitor account. To activate your account, A click the link below.

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



Registe	a Visitor Account
E-Mail Account:	Lumbergh@geovision.com.tw
Password:	•••••
Re-type Password:	•••••
Word Verification:	Type the characters you see in the picture below.
	QQPkHaAFB2
	QQPkHaAFB2

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

Figure 12-17

- 4. Type the e-mail address and type a password for the visitor account.
- 5. Type the characters for word verification.
- 6. Click **Submit**. A confirmation e-mail will be sent to the 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.

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

	Visit Red	quest 🔠	Lumbergh@geovision.com.	tw [] 🔓 Password Change	🐉 Visitor Setting 🛛 💡 Logout
🕑 Add Visit 🥥 Remove Visit					
Visit Date	Visit Time	Notes	Permit	Check In	Check Out
Page 1 of 1 🕨					No data to display

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.

Add Visit		×
Visit Date:	2011/07/27	
Visit Time:	10:00 💿	
Notes:	Board Meeting	
	~	
	Save Cancel	

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.

	Demands For Visit - [Lumbergh Bill]											
•	New 🔀 Del						Search:	Card Numb	er	~		٩
	Visit Date 4	Visit Time	Destination	Notes	Approval	Permit	Card Number	Check In	Check Out	Dea	activation Date	Cardholder
1	08/29/2011	10:00		Board Meeting		8						Lumbergh Bill
14	4 Page	1 of 1		þ								Displaying 1 - 1 of 1
Rea	dy											

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-DSP LPR and GV-DVR 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-DSP LPR and / or GV-DVR LPR, which can recognize license plates detected in the connected cameras.



Figure 13-1



Main Screen



Figure 13-2

13.1 Installing GV-DVR LPR

A GV-System V8.5.5.0 or later can be turned into a GV-DVR LPR simply by installing the LPR Plugin supplied in the Software DVD and by inserting an LPR Dongle.

13.1.1 System Requirements

Before setting up GV-DVR LPR, make sure the PC meets the minimum system requirements.

Number of LPR Channels	1-4 Channels	5-8 Channels		
OS	64-bit Windows 7 / 8 / Server 2008 / Server 2012			
CPU	Core i5 2400, 3.1 GHz Core i7 2600, 3.4 GHz			
Memory	2 x 2 GB Dual Channels			
Hard Disk	500 GB			
VGA	AGP or PCI-Express, 1280 x 1024 , 32-bit color and support			
	DirectX 10c			
DirectX	End-User Runtimes (November 2008)			
Software	.NET Framework 3.5			
	SQL Server 2005 Express (optional)			
Browser	Internet Explorer 7.0 or later			
GV-System	GV-ASManager 4.0: V8.5.5.0	or V8.5.6.0		
	GV-ASManager 4.1: V8.5.7.0			
	GV-ASManager 4.2: V8.5.8.0			
	GV-ASManager 4.2.1: V8.5.9.0			

Note:

- 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 in the supplied software DVD.
- 2. It is recommended to use separate PCs for GV-ASManager and GV-DVR LPR.



13.1.2 Installing LPR Plugin

1. Insert the supplied Software DVD to your computer and a window pops up automatically.



Figure 13-3

2. Select Install LPR Plugin and follow on-screen instructions to complete the installation.

13.1.3 Inserting LPR Dongle

To see recognition results, an LPR Dongle needs to be inserted to the computer of the GV-System. 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-System (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 GV-DVR 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-System and click **TestRecogPicView.exe**. This dialog box appears.



Figure 13-4

2. Click **Show**. 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 are displayed under the snapshots.

(XXF2LD)	LIXIFILD	LIXEFULS	LYXFLIG	Switch Page Cur Page : 1
CXXF6L9	COFUS	Connect CXXF(L)	LIXEFLIO	1 2 3 4 5 6 7 8
4XXF449	4XXF449	4XXF449	4XXF449	Close

Figure 13-5

- 3. To see the results from channels 5 to 8, click **Switch Page** to switch to page 2.
- To manually force the GV-DVR LPR to detect license plates, click the channel number buttons on the right. You may need to switch to the correct page first to see the recognition results.



13.2 Setting Up GV-DVR LPR

To set up GV-DVR LPR, follow the requirements listed in *12.1 Installation* and then follow the steps below:

• Step 1 Enabling LPR Functions on GV-DVR LPR

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

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

Establish the communication between GV-ASManager and GV-DVR 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 <u>GV-LPR Cam 20A</u>, <u>GV-LPR Cam 10A</u>, and <u>GV-Hybrid LPR Cam 10R</u>. For more information, visit GeoVision's website at: <u>http://www.geovision.com.tw/english/3 1 LPR.asp</u>.

13.2.1 Step 1: Enabling LPR Functions on GV-DVR 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.

		System Configure 🔹 🕨
	License Plate Recognition 🔹 🕨 🕨	Enable LPR Service
	Camera Popup Setting Object Index/Monitor Setting Privacy Mask Setting	Enable Overview Camera Service
		Auto Start LDD Service
		Auto Start Overview Camera Service
	Advanced Motion Detection Setting	
Scene C	Scene Change Detection Setting	Configure 🕨
	Video Lowpass Filter Setting	LDD Dapalay & parks
_		LPR Dongle: o ports

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-System as overview camera.
- Auto Start LPR Service: Automatically start LPR Service at GV-System Startup.
- Auto Start Overview Camera Service: Automatically start Overview Camera Service at GV-System 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-System.



13.2.2 Step 2: Adding GV-DVR LPR to GV-ASManager

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





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





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

1 Type:	DVF	R-LPR		Name	Value
LPB 1				Version	6016
				Max. number of logs per folder	999
No Groups	~			Max. number of lines per log file	999
				Log: API	Enable
				Log: Recognition	Disable
100,100,0.0				Log: Recognition upon 1/U trigger	Disable
192.168.0.2	ID	Camera		Log: Result export	Disable
admin	1	Camera 1		Log: FPS	Disable
admin	2	Camera 2		Saving image: Unidentifiable image	Disable
•••••	4	Camera 3		Saving image: Identifiable image	Disable
	5	Camera 5		Saving image: Min. free space(MB)	2048
3388	6	Camera 6		Saving image: Number or images	1000
	7	Camera 7			
5611	8	Camera 8			
EEE2	9	Camera 9			
5552	11	Camera 11			
32	12	Camera 12			
32	13	Camera 13			
	14	Camera 14			
	15	Camera 15	_		
	15	Camera 15			
	18	Camera 18			
	19	Camera 19			
	20	Camera 20	~		
					Default
					Derauk
				Country	
	1 Type: LPR 1 No Groups 192.168.0.2 admin admin 3388 5611 5552 32 💌	1 Type: DVF LPR 1 No Groups Image: Comparison of the second	1 Type: DVR-LPR LPR 1	1 Type: DVRLPR LPR 1	I Type: LPR 1 No Groups 132.168.0.2 admin bit bit comera 1 comera 1 </td

5. Click OK. This dialog box appears.



- Assign the GV-DVR 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 Adding a New User in Chapter 8 for more details.
- 7. Under Connection, type the IP Address, User name and Password of the GV-DVR LPR.
- 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-System.
 - 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.

LPR Setup					
General Setup Lane 1 Lan	ne 2 Lane 3 Lane 4 Lane 5 Lane 6	Lane 7 Lane 8			
General		Recognition Region Se	etup	Recognition Engine	
🗹 Enable		Camera 1 Camera 2	2	Name	Value
Lane Name:	Lane 1	Becognition:		Recognition loop number	10
Recognition Comercy		riscognition.		Max. characters	9
riccognition camera.				Min. characters	200
	Camera 2 🗸			Min. character height(pixel)	12
				Enable rotation detection	Enable
	None			Enable fast rotation detection	Disable
	None		//B *	Max. rotation detection angle	18
	None			Min. rotation detection angle	-18 Factor
Overview Camera:	Camera 3			Enable Slant detection	Enable 10
				Min. Slant detection angle	-10
	Camera 4 👻		5A0 9651	Detect 2 line license plate	Disable
				Detection number of license	1
	None			Default plate background co	Light
				Invert plate background color	Enable
				Replace I with 1	Disable
Drive Direction				Replace zero with U	Disable
Drive Direction:	Incoming			License plate rule 1	Disable
				License plate rule 2	
				License plate rule 3	
				License plate rule 4	
Recognition Setting				License plate rule 5	
Recognition:	By motion detection	[License plate rule 6	
-					
Matching Mode:	All Characters Match 🔽				
Sensitivity:		Barrier Control:	Module 1 - Output 1		
-	5		·		
		Do not record unto	econical results		
1	10		cognized results		Default
					Derduit
Sync from D	Sync from DVR-LPR DK Cancel				

Figure 13-10

2. Select Enable.

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

3. Select up to four cameras connected to the GV-System 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 that the resolution of the recognition camera needs to be at least D1.

- 4. Select up to three **Overview Cameras** to capture the overall appearance of the vehicle. The overview camera must be connected to the GV-System.
- 5. Configure the Recognition Settings:
 - Recognition: Select to start license plate recognition upon motion detection or I/O trigger.
 - Matching Mode: To open 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 order of the characters will be ignored. For example, license plate ABC-123 will be considered matching with ZZC-321 when Allow 2 mismatched characters is selected.
 - **Sensitivity:** Adjust the sensitivity level for motion detection.
- 6. Adjust the **Recognition Region Setup** for each camera if needed: Only license plates inside the area drawn will be recognized.
- 7. 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.
- 8. Select **Do not record unrecognized results** to omit unrecognized results from LPR log.
- 9. 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.

GeoVision

- 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 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.
- 10. 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 example below.

If the icon 💂 appears, it indicates the connection between the GV-DVR 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.

LPRs	×
16x16 🔽	
LPR	Status
👻 🛒 TEST68-A256A280	
 LPR 1 1: Lane 1 2: Lane 2 3: Lane 3 4: Lane 4 5: Lane 5 6: Lane 6 7: Lane 7 8: Lane 8 	

Figure 13-11

Note:

- 1. The Overview Cameras need to be set to round-the-clock recording on GV-System.
- 2. To ensure optimal performance, the total number of Overview Cameras supported in a GV-System 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 (Configure button > Accessories > I/O Device > I/O Device Setup). Refer to 6.1 I/O Device Setup on 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 equipments, 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. On GV-DVR LPR, click the **Configure** button, select **Video Analysis**, select **License Plate Recognition**, select **Configure** and click **Export Setting**.



Figure 13-12

Export through RS-232

 If you are connecting the computer to your equipment using RS-232 connection, click the Export Through RS232 tab and select Enable Export through RS232.

port Setting		
Export through RS232 Export to Fil	e	
🗹 Enable Export through RS232		
RS232 Setup		
Select Port	COM 8	 Ø
Select Recognition Items to Exp	port	Recognition Time Export Format
Select All		Export Item
Export Item	Length (Bytes) 12 12 24 2 1 1 1 Not configurable Not configurable 2	 ✓ Year ✓ Month ✓ Day ✓ Hour ✓ Minute ✓ Minute Export Content Format Export Item Content ✓ Add prefix { ✓ Separate items by _ ✓ ✓ Add suffix }

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 your equipment, click the **Export to File** tab and select **Enable File Export**.

port Setting	Σ
Export through RS232 Export to File	
☑ Enable File Export Path	
D:\GV-800\LPR\Export	
File Extension Image: Select Export Item Image: Add data to the end of the existing export file	File Name Setting Fixed File Name LPR_EventLog User Define Define File Name
	OK Cancel

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.

Select Export Item	
Select Recognition Items to Export	Recognition Time Export Format
Select All	7/30/2013 21:59:17
Export Item Recognized Plate Plate Region Recognition Confidence Messages Lane Drive Direction UTC Local Time Lane Camera	Plate Region Export Format Width and Height
	OK Cancel

Figure 13-15

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

- 5. Under File Name Setting,
 - You can use a **Fixed File Name**.
 - To define your own file name, select **User Define** and click the **Define File Name** button. Next, select the data you want listed in the file name.

File Name Setting		
		Recognition Time Export Format
Export Item	Sample Value	Export Item
 Recognized Plat License Plate Plate Region Recognition Co Messages Lane Drive Direction UTC Local Time Lane Camera 	ate GEO789 GEO689 160147 21 2 0 20130814035159390 20130814115159390 1	Export Item Year Month Day Hour Minute Second Plate Region Export Format Width and Height Auxiliary Information Setting Add prefix EVENT Separate items by Add suffix
Preview	EVENT_GE0789_GE0689_160147_099098	097096095094_21_2_0_20130814035159390_201308141151
		OK Cancel

Figure 13-16

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



13.2.5 Recognition Engine Version

No.	Country	Engine Version	No.	Country	Engine Version
1	Argentina	6.0.1.6	23	Italy	6.0.0.2
2	Australia	4.2.1.1	24	Malaysia	6.0.0.3
3	Austria	6.0.1.6	25	Mexico	4.4.5.6
4	Belgium	6.0.1.6	26	New Zealand	6.0.1.6
5	Brazil	6.0.1.6	27	Norway	6.0.1.1
6	Bulgaria	6.0.1.6	28	Poland	6.0.1.6
7	Canada	4.0.4.0	29	Portugal	6.0.1.6
8	Channel Islands	4.0.3.8	30	Qatar	3.1.2.2
9	Chile	3.2.0.9	31	Russia	6.0.1.7
10	China	4.2.1.3	32	Serbia	4.0.3.8
11	Columbia	4.2.1.5	33	Slovakia	6.0.1.6
12	Croatia	4.0.3.8	34	Slovenia	4.0.3.8
13	Cyprus	4.0.3.8	35	South Africa	6.0.0.9
14	Czech	6.0.1.6	36	Spain	6.0.1.6
15	France	6.0.1.6	37	Taiwan	4.5.5.7
16	Germany	6.0.1.6	38	Thailand	2.3.0.8
17	Global	6.0.1.6	39	Turkey	4.0.3.8
18	Hong Kong	6.0.1.2	40	UAE	2.3.0.8
19	Hungary	6.0.1.5	41	UK	6.0.1.6
20	India	4.2.1.1	42	USA	4.2.1.2
21	Ireland	6.0.1.5	43	Vietnam	4.2.1.0
22	Israel	3.1.2.2			

GV-DVR LPR V4.2.1 only supports the following versions of recognition engines:

13.3 Setting Up GV-DSP LPR

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

Note:

- GV-ASManager V4.1 is only compatible with GV-DSP LPR firmware V2.0 and V2.0.1.
- GV-ASManager V4.2 is only compatible with GV-DSP LPR firmware V2.0.2.
- GV-ASManager V4.2.1 is only compatible with GV-DSP LPR firmware 2.0.3
- Step 1 Enabling Connection with GV-ASManager on GV-DSP LPR Enable connection with GV-ASManager on GV-DSP LPR.
- Step 2 Adding GV-DSP LPR to GV-ASManager

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

• 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 on GV-DSP LPR

To enable connection with GV-ASManager on GV-DSP LPR, first make sure a mini or micro SD card is inserted to the GV-DSP LPR and formatted. Next, log in the Web interface of the GV-DSP LPR and follow the steps below.

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

Registry Database Setting
Registry Database
In this section you can set registry database and compared mode.
Enable Registry Database
Registry Database Comparison Complete (All Characters Match)

Figure 13-17



- 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*.

To open a gate when the detected license plate is recognized as a registered vehicle, refer to *4.2.2 Output Setting* on the *GV-DSP LPR User Manual* to see how to set the gate as the output device.

13.3.2 Step 2: Adding GV-DSP LPR to GV-ASManager

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





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

Please Enter ID		X
ID:	2	
Name:	LPR 2]
Туре	DSP-LPR	ОК
		Cancel

Figure 13-19

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



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

	T	0.001.00	
Device ID:	2 Type:	DSP-LPR	
Device Name :	LPR 2		
Data Group:	No Groups	~	
Connection			
Address :	192.168.0.53		
User:	admin		
Password :	•••••		
Https Port :	443		
VSS Port :	10000		
Number of Cameras :	1 🗸		

Figure 13-20

- 6. Assign the GV-DSP 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 *Adding a New User* in Chapter 8 for more details.
- 7. Under Connection, type the IP Address, User name and Password of the GV-DSP LPR.
- 8. 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

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

eneral		Recognition Region Setu	p	
Enable		Camera 1		
Lane Name:	Lane 1	Recognition:		
Recognition Camera:	Camera 1	-		
	None		Statistics of the local division in the loca	
	None			
	None			
Overview Camera:	DVR -2, Camera 2	-		
	DVR -2, Camera 3	- 1	EL 6269E	
	None	-		
Playback Camera	None	•	Control of	
Drive Direction:	Incoming	•	BAAT 1.CM	

Figure 13-21

- 2. Select Enable.
- Select up to three Overview Cameras to capture the overall appearance of the vehicle. The overview camera must be connected to a GV-System and the GV-System needs to be added to the camera list:
 - a. Right-click the GV-System in the Camera List and select Settings.
 - b. Click the Add button and select Add DVR Mapping.
 - c. Type the connection information of the overview camera and click **OK**.
- 4. Select a Playback Camera, usually the same camera as the Recognition Camera. The playback camera also needs to be connected to a GV-System and the GV-System needs to be added to the camera list. You can select an event in the monitor 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.
- 5. Click **OK** to apply the settings.

GeoVision:

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

Note:

- 1. The Playback Cameras need to be set to recording on GV-System 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-System.
- 3. To ensure optimal performance, the total number of Overview Cameras supported in a GV-System 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 GV-DVR LPR or GV-DSP 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 13-23).
 - On the menu bar, click **Personnel** and select **Vehicles**. This dialog box appears.

🖨 Vehicle List									
New	Edit	Delete	mport	Export	Refres	h			
Search by Licen:	se Plate		*				Auto Select	Filter View	
License Plate	User	Brand	Model	Color	Ticket	Vehicle Sta	Activation Date	Deactivation Date	Access Group
						Total Vehicles:	0		.;;

Figure 13-22



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

Adding a New Vehicle	
User:	
License Plate:	AB-1234
Brand:	
Model:	
Color:	Black
Ticket:	
Vehicle Status:	Active
Activation Date:	9/19/2012
Time:	19:44
Deactivation Date:	9/19/2012
Time:	19:44
Access Group:	Default
E LPR 1	
Lane 1	24-hour restricted
Data Group:	No Groups OK Cancel

Figure 13-23

- 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.

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 Adding a New 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.

User Setup		×
General Home Business	User Define Fingerprint Sca	an
First Name:	Middle Name:	Last Name:
Nombre		Apellido
Display:	Employee ID:	
Apellido Nombre	0121634587	
Card List:		
[032] 3469554359		
Vehicle List:		
Send SMS		
Data Group:		
No Groups	*	
	(OK Cancel

Figure 13-24

You can also import and export vehicle data in mdb or xls format. Refer to 4.3.3 Importing / *Exporting Card Data* for similar settings.

GeoVision

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**.

LPRs		×
16x16 💌		
LPR	Status	
👻 🛒 TEST68-A256A280		
 ✓		



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

Name	Function
Reconnect	Reconnects with the LPR.
Sync LPR	After modifying the LPR settings, clicking Sync LPR 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 GV-DVR LPR, refer to the Barrier Control option in
	13.2.3 Step 3: Configuring a Channel. For GV-DSP LPR, see the
	Output Setting section in Chapter 4 of the GV-DSP LPR User Manual.
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.

Steps In the second sec						X
🌱 🖾 🔒						
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		~
Lists Tiles Thumbnails						

Figure 13-26

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 13-27

For detailed settings, refer to 8.2 Notification Setup.

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.

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 veh	nicle hotlis	st.					
	Source Database :	Excel	Excel					
	Select a source table :	[Sheet	:1\$]				~	
	Field Name	Fi	eld Type	<>	Field Name		Field Type	
	📃 License Plate	n\	/arChar	<>	[Plate]		VarChar	
	🚍 Group Name	n∖	/arChar	<>	[Group]		VarChar	
	📜 Memo	n\	/arChar	<>	[Memo]		VarChar	
	<							
	Immediate View	10	_(0 ~	100)			Refresh	
	License Plate			Grou	p Name	Memo		
,						ОК	Cano	;el

Figure 13-28

GeoVision

- 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.

Adding Vehicles to the Hotlist

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

🕾 Vehicle Hotlist				
Group	Vehicle Hotlist		License Plate	?
Name	License Plate 🔺	Memo		
Default				
Oakland				
San Francisco				
· · · · · · · · · · · · · · · · · · ·				
	Vehicle			
	License Plate:			
	Memo:			
				Update
	L			
Auto-update hotlist program will not execute when I	notlist is opened.		0.8-0	(-)
			Uiter	n(s)



2. Under the Group section, click the **Add** button (2) to create a hotlist group if needed. If you have imported data from an external database using ASDBManager, the vehicles will be listed under the **Default** group already.

3. To add vehicles to the hotlist manually, click the **Add** button index which which we hotlist and type the **License Plate**. You can add a **Memo** to note the stolen time and location.

Adding a New Vehicle		Ì
License Plate:	F1234567	
Memo:		
Stolen 2013/12/7. M	acArthur Blvd and San Pablo Ave.	
		Add

Figure 13-30

- 4. Click Add.
- 5. To import an existing license plate from the vehicle list, click the **Import** button \square .

🖨 Import licens	e plates fi	rom vehic	e list						
Search by License	Plate		-	~			Auto Select Filter V	liew	Select
License Plate	User	Brand	Model	Color	Ticket	Vehicle Sta	Activation Date	Deactivation Date	Access Group
🚐 A98765432				Orange		Active	12/24/2013 2:53:00 PM		
🚐 A2345678				Black		Active	12/24/2013 2:52:00 PM		
🚐 A3456789				Gray		Active	12/24/2013 2:53:00 PM		
🚐 A76543129				Orange		Active	12/24/2013 2:59:00 PM		
	Total Vehicles: 4								



6. Select the vehicles you want to add and click **Select**.

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



Figure 13-32



13.8 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 GV-DVR LPR or GV-DSP 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.
- 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.

13.8.1 LPR List

You can use LPR List to remotely add and delete a GV-DVR LPR or a GV-DSP LPR to GV-ASManager, set up channels and delete an LPR.

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

🚊 LPR List	
LPR I	List
0 🗢 🍪	Information
Lane	No items for display.
🛖 1: DSP LPR 01 (1/1 Lane) DSP_LPR	
Lane 1	
🕅 🖣 Page 1 of 1 🕨 🕅 🦿	



- 2. Click the **Add** button is to add an LPR. For details on the settings, see 13.2.2 Adding GV-DVR LPR to GV-ASManager and 13.3.2 Adding GV-DSP 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 *13.2.2* and *13.3.2* 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.



13.8.2 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 **O**. This dialog box appears.

Add a Vehicle				
Cardholder:	Rohit Zutshi		2 &	
License Plate:	12345678		Photo:	
Brand:		~		
Model:		~		
Color:		~		
Ticket:		~		
Vehicle Status:	Active	~		
Activation Date:	09/20/12	•		
Time:	12:00	~		
Deactivation Date	09/20/12			
Time:	12:00	~		
Data Group:	No Groups	~		
Access Group:	Default	~		
Lane	:	Schedule		
🖻 🛖 DSP LPR 01 (1 Lane)				
Lane 1	3	24-hour restric	ted	
		ОК	Cancel	

Figure 13-34

- 3. Fill out the required information. Refer to 13.4 Adding Vehicles for more details.
- Click **OK** to save the settings. 4.
- 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.

13.8.3 LPR Log

Using LPR Log, you can set search criteria to look up a record, see snapshots of detected license plates and play back recorded videos.

Setting Search Criteria

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 this month. The resulting filter window may look like this.

🚔 LPR Log							- • ×
	LPR Log						
Filter		~			Export: T	XT This Pag	е ок
Message:	Plate Recognized: Unr 🕶		Message	Recognized	License Plate	Lane	Local Time
Lane:	LPR 1						
Date Period:	This Month 💌	=					
Start Date:	09/01/12						
End Date:	09/30/12						
Vehicle —							
	Fuzzy Matching						
Recognized Plate:	FM0505						
License Plate:	~	~					
Search	Clear						>
Courter			Page 1 of 1			No da	ata to display

Figure 13-35

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

- Letter B will become 8
- Letter O and D will become 0 (Zero)
- Letter S will become 5

- Letter Z will become 2
- Letter I will become 1
- 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.



Search Results Window

Below is an example of a search results window.

-	LPR L	og										- 🗆 X
(LPR	Log	J							
>>									Export:	ТХТ	This Page	ок
		Message	Recognized	Licens	Lane	Local Time	Plate Number's Photo	Recognition Camera	Overview Camera 1	Overvi	Over User	
	1	Plate Recog	0I2NP	0I2NP	LPR 1 - Lane 1	9/21/2012 3:	012 NP				-	
	2	Plate Recog	012NP	012NP	LPR 1 - Lane 1	9/21/2012 3:	012 NP				2	
	3	Plate Recog	012NP	012NP	LPR 1 - Lane 1	9/21/2012 3:	012 NP	1			2	
	4	Plate Recog	0P9885	0P9885	LPR 1 - Lane 1	9/21/2012 3:	OP-9885				2	
	5	Plate Recog	0P9885	0P9885	LPR 1 - Lane 1	9/21/2012 3:	OP-9885				2	~
	M	A Page 1	of 429 🕨	S N						D	isplaying 1 - 30 o	of 12842

Figure 13-36

A snapshot of the detected license plate will be displayed.

E: Indicates the availability of the recorded video.

image.

You can right-click each search result to access more information such as vehicle information en or user information en .

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.

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.

13.8.4 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



Access oups Setup. For details on how to set up access groups, refer to Setting Access Groups in

Chapter 4.

93 A	ccess Groups Setup				- - ×
\odot	0	Name:	Default		
	Name 🔺	Data Group:	No Groups		
1	Default	baca oroup.	No oroups		
2	FAE	Door		Schedule	
		🗉 📋 Controller A	A_Reception (2 Doors)		
		Gate A		24-hour restricted	
		Gate B		24-hour restricted	
		A Page 1	of 1 🕨 🕅 🖓		Displaying 1 - 2 of 2
		Lane		Schedule	
		🖃 🚊 LPR 1 (8 La	nes)		<u>^</u>
		👔 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	
		4	of 1 🕨 🕅 🧬	Of being analyisted	Displaying 1 - 9 of 9
14	4 Page 1 of 1 ▶ ▶ 2 Displ				Save Close

Figure 13-37

GeoVision

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. The following functions are supported:

- Watch camera live view from GV-System or GV-DVR LPR mapped with a door or lane
- Lock or unlock a door
- Check door status to see if alarm events have occurred
- Open an LPR lane

Supported Operating Systems:

- Android version V4.1.2
- iOS version V6.14

14.1 Installing GV-Access

To install GV-Access on your mobile devices, search and download **GV-Access** in Android Play Store or Apple App Store. The GV-Access icon will appear on the desktop of your mobile device.





14.2 Connecting to GV-ASManager

(A)

Tap the **GV-Access** icon on the desktop of your mobile device. There are three tabs on the bottom: **Controller**, **LPR** and **Config**.

1. Tap the **Config** tab and tap the **Add** button **+**.

< Ado	d GV-ASMan	ager
Name	ASManager-HQ	
IP	192.168.0.10	
Port	80	
Account	admin	
Password	••••	
	Test Login	
	Add	
	Version 1.05	
Controller	LPR	ද် <u>လ</u> ှိန် Config

Figure 14-2

- 2. Type a **Name** to help you identify the GV-ASManager and type the **IP** address, **Port**, login **Account** and **Password**.
- 3. Tap **Test Login** to test the connection with GV-ASManager.
- 4. Tap **Add** to add the GV-ASManager.



14.3 Managing Controllers

After adding GV-ASManager to GV-Access, the controllers and doors associated with the GV-ASManager will be listed under the **Controller** tab.

1. Tap the **Controller** tab.



Figure 14-3

The authentication mode is listed under each door: card mode, card or password mode, card and password mode, and release mode. When you remotely control the doors using GV-Access, the action taken will be listed instead until Disable Door Operation is selected.

The following icons are available.

lcon	Description	lcon	Description	
	Connected		Camera(s) available	
	Disconnected	2	Control door(s)	
Note: To access camera live view, the camera(s) associated with the door must be connected to a GV-System or GV-DVR LPR.				

The following alert icons are available. When alert conditions occur, the alert icon will light up in red. To clear the alert, tap the red icon and select **OK**.

lcon	Description	lcon	Description
Å	Alarm	B	Fire Alarm
	Force Open	5	Held Open
	Duress		Tailgating
ET.	Tamper	G	Access Denied

Note:

- 1. GV-EV48 Elevator Controller only supports the Duress alert icon. The remaining alert icons are not functional for GV-EV48.
- 2. The Tailgating function is currently not functional.
- 2. To remotely control the door(s), tap the **Control** button $\xrightarrow{\sim}$ and select one of the

following options. If you use the Control button next to a GV-ASManager, the command will apply to all connected doors.

- Unlock Door: Unlock door temporarily.
- **Force Unlock:** Unlock door until Disable Door Operation is selected.
- **Force Lock:** Lock door until Disable Door Operation is selected.



- Disable Door Operation: Cancel Force Unlock, Force Lock or Lock Down command.
- Lock Down: Lock the door, and the door can only be opened by presenting the correct access card.

Note: The Lock Down function is not supported in GV-EV48 Elevator Controller.

3. Tap a door to access its live view if available. You can tap **Switch Camera** if there are multiple cameras connected to the door.



Figure 14-4

14.4 Managing LPR

After adding GV-ASManager to GV-Access, the GV-DVR LPR and GV-DSP LPR associated with the GV-ASManager will be listed under the **LPR** tab.

1. Tap the **LPR** tab. The connected LPR and lanes appear.

e	GV-Access	
🗸 🚰 A	SManager-HQ	2
🗸 🎘 L	PR 1	2
L	ane 1	2
	ane 2	2
Controller	LPR	င်္သြန် Config

The following icons are available.

lcon	Description	lcon	Description		
	Connected		Camera(s) available		
	Disconnected	2	Control door(s)		
Note: To access camera live view, the camera(s) associated with the lane must be					
connected to a GV-System or GV-DVR LPR.					

Figure 14-5



- 2. To remotely unlock the LPR lane, tap the Control button $\stackrel{\frown}{\longrightarrow}$ and select Unlock Gate.
- 3. Tap a lane to access its live view if available. You can tap **Switch Camera** if there are multiple recognition cameras connected to the lane.



Figure 14-6

Chapter 15 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 exits, the GV-ASManager provides you the **Source Database** function to convert various database formats to be the GV-ASManager's (Access or SQL Server).

15.1 Starting the Database Tools

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

- 1. If 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.
- 2. If you have run the GV-ASManager, run **ASDBManager.exe** from the program folder to access the Database Tools.

🚮 Database Too	als	
Please Select D Which tool do	atabase Tools : o you use for database?	
	ASManager Database Setting : Setup, upgrade, deletion, backup and recovery.	
	Settings from Source to ASManager Database : Set the connection of Source Database, the mapping relative tables betweem Source and ASManager database, the autor request, and the manual update request.	ons of the p-update
	Re-login	Exit

Figure 15-1



15.2 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 15-1).
- 2. Click the **Setup MDB/MSSQL Database for ASManager** button. This dialog box appears.

Create Database	
Database Type	
O Microsoft Office Access Databas	e
 Microsoft SQL Server 	
SQL Database Setting	
Data Source:	VINCENTYU_SQLSE\SQLEX
Authentication: Windows Authentication SQL Server Authentication	
Login:	vincent
Password:	
Database	
ASConfig Name:	ASConfig
ASLog Name:	ASLog
	Test connection
C	OK Cancel

Figure 15-2

- 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 the 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 the 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.



15.3 Other Database Settings

You can upgrade, delete, back up and remove the database of GV-ASManager. Click **ASManager Database Setting** button on the Database Tools dialog box (Figure 15-1) to display the following dialog box and have further settings.

🖬 ASManager	Database Setting
	Setup MDB / MSSQL Database for ASManager
AS BO	Upgrade to latest database version
	Delete ASManager Database
	Backup Database
	Recovery Database
Database versio	un: 2.1.0.0

Figure 15-3

[Upgrade to latest database version] If an old database exits on the local computer, select this option to upgrade the version of the old database to the latest.

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

[Backup Database] Backs up the Configuration file.

[Recovery Database] Restores the backup **Configuration** file to the current computer or import it to another computer.

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



15.4 Mapping Source Database

The Source Database function can convert **OLE DB** and **Active Directory** database into GV-ASManager (Access or SQL Server) database. Click the **Setting from Source to ASManager Database** button on the Database Tools dialog box (Figure 15-1). This dialog box appears.



Figure 15-4

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.



15.5.1 Converting Data from the Active Directory Database

- 1. Click the **Set Connection** button on the Options dialog box (Figure 15-4). The Source Database dialog box appears.
- 2. Select Active Directory. This dialog box appears.

🚚 Set up a connecti	on to active directory		×
Server Server name:	192.168.220.128	Port: 389	
Account User Name: Password:	Administrator	Bind type C Bind as currently logged on user C Bind with credentials	
Distinguished name (Connect to the C Default	DN) or naming context following node: Root Node de		
Test Connection		S	ave

Figure 15-5

- 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.
- Click the Update Cardholder Data manually button in the Options dialog box (Figure 15-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
- 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.
- To update the database automatically later, click the Input/Modify the Auto-update time setting button in the Options dialog box (Figure 15-4) and specify the time in minutes.

15.5.2 Converting Data from the OLE Database

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

- Connect an OLE database
- Map the cardholder data
- Map the card data
- Convert the data from the source database

To connect an OLE database:

- 1. Click the **Set Connection** button on the Options dialog box (Figure 15-4). The Source Database dialog box appears.
- 2. Select Other Database. This dialog box appears.



Figure 15-6

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.

🗒 Data Link Properties 🔀
Provider Connection Advanced All
Specify the following to connect to SQL Server data:
DYLAN\SQLEXPRESS Refresh
2. Enter information to log on to the server: C Use Windows NT Integrated security
User <u>n</u> ame: fae
Password:
Blank password Allow saving password
3. Select the database on the server:
AdventureWorks
Attach a database file as a database name:
AdventureWorks
Using the filename:
[est Connection]
OK Cancel Help



 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.

To map the cardholder data:

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



Figure 15-8

- 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** filed as example. lick the 🖼 button in the Name field. This dialog box appears.

Set the mapping fields							×
Destination Field :IName Select the source fields for mapping.							
Fields			1	Mapping Fields			
Field Name	Field Type			Field Name	Field Type		
🗒 EmployeeID	Integer			💽 ContactID	Integer		
📜 NationallDNumber	VarWChar						
📃 LoginID	VarWChar						
🚍 ManagerID	Integer		Add ->				
📜 Title	VarWChar			1		Cancel	
🚍 BirthDate	DBTimeStamp			1			
🚍 MaritalStatus	WChar		<- Delete				
🚍 Gender	WChar					LIP	
🚍 HireDate	DBTimeStamp						
🚍 SalariedFlag	Boolean					DOWN	
📜 VacationHours	SmallInt						
🔄 SickLeaveHours	SmallInt					Set Foreign Key	
🗐 CurrentFlag	Boolean	•				Sochologintoy	

Figure 15-9

- 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 15-9), the **Contact ID** field of the source database corresponds to the **Name** filed 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.

Foreign Key Table:			Primary Key Table:		
HumanResources.[Em	ployee]	_	Person.[Contact]		-
Foreign Key Field:		=>	Primary Key Field:		
ContactID			ContactID		•
All Primary Key Fields			Mapping Fields		
Field Name	Field Type 🔺		Field Name	Field Type	
ContactID	Integer		📃 FirstName	VarWChar	
🔄 NameStyle	Boolean		🔤 MiddleName	VarWChar	
🚍 Title	VarWChar	Add >	📜 LastName	VarWChar	UK
🚍 Suffix	VarWChar				Cancel
🗏 EmailAddress	VarWChar				Calicel
📰 EmailPromotion	Integer				
Phone	VarWChar	< Delete	1		UP
🛒 PasswordHash	VarChar	(* Delete			DOM: 01
🚍 PasswordSalt	VarChar				DOWN
AdditionalContactInfo	LongVa/WCha _1				

Figure 15-10

- 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.
- 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 15-10), 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.
- Click OK. In the Mapping Setting window, you can see the mapping results. In the example (Figure 15-8), 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).

To map the card data:

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

Using field mapping to establish Select a source table : dbo.[(relation between fie Card_Data]	lds from	the Card and Source.		Select a
Field Name	Field Tune	<>	Field Name	Field Tune	Source table
	Integer	(-)	Card Holder => Name	VarWChar ⇒ nVarChar	
Card Number	nVarChar	<->	Card No		
	Integer	<->			
Activation Date	DateTime	<->			
Deactivation Date	DateTime	<->			
Deactivate (Yes/No)	Bool	<->			
🚍 Pin Code	nVarChar	<->			
			Clear (DK Cancel	
The fields of the	e GV-		The fields of the		

Figure 15-11

- 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.

To convert the data from the source database:

- Click the Update Cardholder Data manually button in the Options dialog box (Figure 15-4) to convert the cardholder data from the source database to the GV-ASManager database immediately.
- 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.
- To update the database automatically later, click the Input/Modify the Auto-update time setting button in the Options dialog box (Figure 15-4) and specify the update time.

GeoVision

Chapter 16 Net Module Utility

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

- Insert Software DVD, select Install GeoVision Access Control System, click Net Module Utility and follow the onscreen instructions to install the program.
- 2. Run Net Module Utility. This window appears.

🐔 GvNetMod	ule Utility									
Search	Set Login Sett	ing Advanced	OT Contraction Con	It Firmware	Update to (Cancel qu				
Module Name	Version	Controller Name	MAC Address	IP Address	Subnet Mask	Default Gate	Network A	Action	Status	~
GV-A5200	V2.0.0-20090204	Controller 1	00:13:E2:01:1A:69	192.168.3.42	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗍 GV-AS200	V2.0.0-20090313	Controller 1	00:13:E2:01:1A:4F	192.168.3.227	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗍 GV-AS400	V1.0.0-20090924	Controller 2	00:13:E2:01:07:5D	192.168.0.224	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗍 GV-AS100	V1.0.2-2009093x	Controller 1	00:13:E2:01:00:84	192.168.2.160	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗍 GV-AS100	V1.0.2-20091005	Controller 2	00:13:E2:01:07:57	192.168.0.109	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗐 GV-IOBOX	V1.0.0-20090929	IOBOX-01	00:13:E2:01:00:A9	192.168.2.97	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗍 GV-IOBOX	V1.0.0-20090929	IOBOX-01	00:13:E2:01:00:A7	192.168.0.199	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	
🗐 GV-IOBOX	V1.0.0-20090904	IOBOX-01	00:13:E2:01:00:BC	192.168.0.14	255.255.252.0	192.168.0.1	Intel(R) PR		Set Login first	~
< .				IIII				1		>

Figure 16-1

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 17 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 17-1

- 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

	Network Configuration	
	Machine Name	
Basic Setting	Machine Name	Controller 1
Network Setting	DHCP Client:	
 Other Setting Firmware Update 	○ Enable	
Account Setting Advance Setting	● Disable	
Function Setting Parameter Setting	IP Address:	192 . 168 . 0 . 100
Time Setting	Subnet Mask:	255 . 255 . 252 . 0
Input Setting	Default Gateway:	192 . 168 . 0 . 1
Output Setting	Domain Name Server:	192 . 95 . 1 . 1

Figure 17-2

- 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

		Controller Setup	
🚚 ASServer		General Setup Gate 1 Gate 2 Gate 3 Gate 4	
File Monitorin	g View Setup Persons Tools Window Help 🖻 🙀 🐺 🥦 🖙 📾 🚑 🥑	Controller Name : Controller_Taipei Controller ID : 1	
Device View	Controller List	Interlock : DoorA - DoorB DoorC - DoorD	
TEST151	a a a a a a a a a a a a a a a a a a a	GMT: • 08 • : 00 •	
	Controller ID Door A Door B	Data Group: Data Group 4	
	Please Enter ID	Connection COM Port:	
	ID: OK Name: Controller 1 Cancel	IP: 192.168.0.100 Port: 4000 User: admin	
		Password : ••••• Crypto Key : ••••••	

Figure 17-3


7. The connection between the GV-ASManager and the controller should be established, and the connection icon $\stackrel{\texttt{P}}{=}$ 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 17-4

- 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 17-2.
- 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 17-3.

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 $\stackrel{2}{\twoheadrightarrow}$ 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, GV-AS120 and GV-AS400, 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, insert the supplied Software DVD to your computer, and select **Install DirectX End-User Runtimes (November 2008)**.

Q9: How can I find more help?

Visit our website at <u>http:///www.geovision.com.tw</u> Write to us at <u>support@geovision.com.tw</u>

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/english/4_21.asp

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

Туре	Description
Force Open	Door <name> is forcibly open.</name>
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 5 in <i>4.2.2 Step 2: Configuring the Doors</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.</name>
	See Step 2 and 5 in <i>4.2.2 Step 2: Configuring the Doors</i> .
Access Denied	The access is rejected.

• "Access" events

Туре	Description
Access Granted	The access from User <name> and Card <number> is granted.</number></name>
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.</number>
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.</number>
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 (Duplicate Entries)	The access is rejected because the Anti-Passback rule is violated. Card <number> is recorded as successive entries, without exit, to a secure area.</number>
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.</number>
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.</number>
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.</number>
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</i> <i>a Controller</i> .

• "Event" events

Туре	Description
Force Open	Door <name> is forcibly open.</name>
Duress	Duress function is triggered.
	See "Duress" in 1.2 Concepts.
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 5 in <i>4.2.2 Step 2: Configuring the Doors</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 5 in <i>4.2.2 Step 2: Configuring the Doors</i> .
Held Open	Door <name> is held open over the specified time.</name>
	See Step 2 and 5 in <i>4.2.2 Step 2: Configuring the Doors</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.
Clear Fire Event Failed-I/O Still Unclear Door Open	Fail to clear Fire alarm because Fire Inputs remain triggering. Door <name> is open.</name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close	Fail to clear Fire alarm because Fire Inputs remain triggering. Door <name> is open. Door <name> is close.</name></name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock	 Fail to clear Fire alarm because Fire Inputs remain triggering. Door <name> is open.</name> Door <name> is close.</name> Door <name> is unlocked.</name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock Door/Gate Lock	Fail to clear Fire alarm because Fire Inputs remain triggering.Door <name> is open.Door <name> is close.Door <name> is unlocked.Door <name> is locked.</name></name></name></name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock Door/Gate Lock Two Person Rule-Active	Fail to clear Fire alarm because Fire Inputs remain triggering.Door <name> is open.Door <name> is close.Door <name> is unlocked.Door <name> is locked.Two-person A/B rule is active when Card <number> is presented.</number></name></name></name></name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock Door/Gate Lock Two Person Rule-Active Two Person Rule-Confirm	Fail to clear Fire alarm because Fire Inputs remain triggering.Door <name> is open.Door <name> is close.Door <name> is unlocked.Door <name> is locked.Door <name> is locked.Two-person A/B rule is active when Card <number> is presented.Two-person A/B rule is confirmed when Card <name> is presented after the other AB card.</name></number></name></name></name></name></name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock Door/Gate Lock Two Person Rule-Active Two Person Rule-Confirm Two Person Rule-Inactive	Fail to clear Fire alarm because Fire Inputs remain triggering.Door <name> is open.Door <name> is close.Door <name> is unlocked.Door <name> is locked.Door <name> is locked.Two-person A/B rule is active when Card <number> is presented.Two-person A/B rule is confirmed when Card <name> is presented after the other AB card.Two-person A/B rule is violated when Card <name> is presented successively or the other AB Card isn't presented within 20 seconds.</name></name></number></name></name></name></name></name>
Clear Fire Event Failed-I/O Still Unclear Door Open Door Close Door/Gate Unlock Door/Gate Lock Two Person Rule-Active Two Person Rule-Confirm Two Person Rule-Inactive Keypad Code Confirm	Fail to clear Fire alarm because Fire Inputs remain triggering.Door <name> is open.Door <name> is close.Door <name> is unlocked.Door <name> is locked.Door <name> is locked.Two-person A/B rule is active when Card <number> is presented.Two-person A/B rule is confirmed when Card <name> is presented after the other AB card.Two-person A/B rule is violated when Card <name> is presented successively or the other AB Card isn't presented within 20 seconds.On the Card or Common mode, the password entered is correct.</name></name></number></name></name></name></name></name>



Release Mode	Door <name> is on the Release Mode. See Step 4 in <i>4.2.2 Step 2: Configuring the Doors</i>.</name>
Card or Common Mode	Door <name> is on the Card or Common Mode. See Step 4 in <i>4.2.2 Step 2: Configuring the Doors</i>.</name>
Card and PIN Code Mode	Door <name> is on the Card and PIN Code mode. See Step 4 in <i>4.2.2 Step 2: Configuring the Doors</i>.</name>
Card Mode	Door <name> is on the Card mode. See Step 4 in <i>4.2.2 Step 2: Configuring the Doors</i>.</name>
Fire Unlock Mode	Door <name> is unlocked after Fire Inputs are triggered. See "Fire Action" at Step 2 in <i>4.2.2 Step 2: Configuring the Doors</i>.</name>
Fire Lock Mode	Door <name> is locked after Fire Inputs are triggered. See "Fire Action" at Step 2 in <i>4.2.2 Step 2:</i> <i>Configuring the Doors</i>.</name>
Force Unlock Remotely	Door <name> is unlocked remotely from the control of GV-ASManager or GV-ASRemote server.</name>
Force Lock Remotely	Door <name> is locked remotely from the control of GV-ASManager or GV-ASRemote server.</name>
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.</name>
Force Lock Locally	Door <name> is locked on the site of Door Controller.</name>
Disable Local Door Lock Operation	The event of "Force Unlock Locally" or "Force Lock Locally" is cleared.
Reset	Door Controller <name> is reset.</name>

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.
1224	%N (Card Number): include card number.
	%H (User Name): include user name.
89	%G (Gender): include user's gender.
	%E (Employee ID): include employee ID.
(REC)	%Y (Company): include company name.
	%P (Department): include department name.
1980 1990	%F (Office): include office name.
rê -	%C (Photo): include user photo.
<u> </u>	%S (Snapshot): include snapshot.



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.