GV-AS1620 Controller

User's Manual

Before attempting to connect or operate this product, please
read these instructions carefully and save this manual for future use.

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

October 2019

Contents

Optional Devices

Optional devices can expand the capabilities and versatilities of your controller. Consult our sales representative for more information.

GV-CR420	GV-CR420 is a card reader with a built-in 4MP wide angle IP camera. The card reader recognizes identification cards and transmits live view through network connection.
GV-CR1320	GV-CR1320 is a card reader with a built-in 2MP wide angle IP camera. The card reader recognizes identification cards and transmits live view through network connection.
GV-DFR1352	GV-DFR1352 is a card reader that uses a 13.56 MHz frequency. The reader has both Wiegand and RS-485 outputs that can be connected to any standard access control panel.
GV-FWC	GV-FWC can integrate GV-Face Recognition Cameras (GV-FD8700-FR / GV-VD8700) into access control systems by sending access card data, paired to Face IDs, to controllers either through TCP/IP or Wiegand connection.
GV-FR2020	GV-FR2020 is a 13.56 MHz face recognition reader. The reader supports two operation modes for access control: Face Recognition and Card.
GV-IB25 / 65 / 85 Infrared Button	The GV-IB25 / 65 / 85 Infrared Button detects infrared movement within 3 to 12 cm and allows you to open the door with a wave of hand.
GV-Reader 1251	GV-Reader 1251 is a card reader that uses a 125 kHz frequency. The reader has both Wiegand and RS-485 outputs that can be connected to any standard access control panel.
GV-R1352	GV-R1352 is a card reader that uses a 13.56 MHz frequency. The reader has both Wiegand and RS-485 outputs that can be connected to any standard access control panel.
GV-RK1352	GV-RK1352 is a card reader with keypad that uses a 13.56 MHz frequency. The reader has both Wiegand and RS-485 outputs that can be connected to any standard access control panel.
GV-RU9003	GV-RU9003 is a Radio Frequency Identification (RFID) reader of ISO 18000-6C (EPC GEN2) standard. Designed for parking lot management, the reader can read RFID tag within 10 m (32.8 ft).
GV-SR1251	GV-SR1251 is a card reader that uses a 125 kHz frequency. It has both Wiegand and RS-485 outputs that can be connected to any standard access control panel.
GV-GF Fingerprint Readers	GV-GF1921 / 1922 is a fingerprint reader, supporting three operation modes: Fingerprint Only, Fingerprint + Card and Card Only. Readers with optical and capacitance sensors are available.
GV-AS ID Card / Key Fob & GV-UHF Tag	GV-AS ID Card and GV-AS ID Key Fob are ideal for business and residential environment, where access control is important for security reasons. 125 KHz and 13.56 MHz cards and key fobs are available. GV-UHF Tag is ideal for parking lot management. 900 MHz UHF Tag is available.
GV-POE Switch	The GV-POE Switch is designed to provide power along with network connection for IP devices. The GV-POE Switch is available in various models with different numbers and types of ports.
GV-WTR	GV-WTR is a converter designed to support Wiegand interface to RS-485 interface, thereby enabling 3rd party readers to be connected to RS-485 GV-Controllers. Through the GV-WTR, Wiegand-interface readers can be easily combined to access control systems for improved versatility.
Electric Lock	Three types of electric locks are available: electromagnetic lock, electric bolt and electric strike.
Power Adapter	Contact our sales representatives for the countries and areas supported.
Push Button Switch	The push button switch can be integrated with access control system, allowing door exit by momentarily activating or deactivating the electric locking device. Both American standard and European standard push buttons are available.

Chapter 1 Introduction

GV-AS1620 is a single door controller with three types of interfaces, Wiegand, RS-485 and TCP/IP, to accommodate various readers for entry and exit management. Through its I/O pins, it provides not only basic door operations but also alarm, tamper and fire senor applications, as well as allowing LEDs connected to indicate an access granted and denied.

1.1 Key Features

- One door IP controller (entry and exit)
- 3 types of interfaces, Wiegand, RS-485 and TCP/IP, supporting 2 readers for each interface.
- 4 digital inputs for door contact, exit button, fire contact and tamper contact
- 4 relay outputs for lock, alarm, 2 LED for an access granted and access denied
- DC 12V, 3A / PoE+ (IEEE 802.3at)
- Suitable for door, parking lot and elevator controls
- Stores up to 100,000 cards

1.2 System Requirements

GV-ASManager V5.2.0 or later

1.3 Packing List

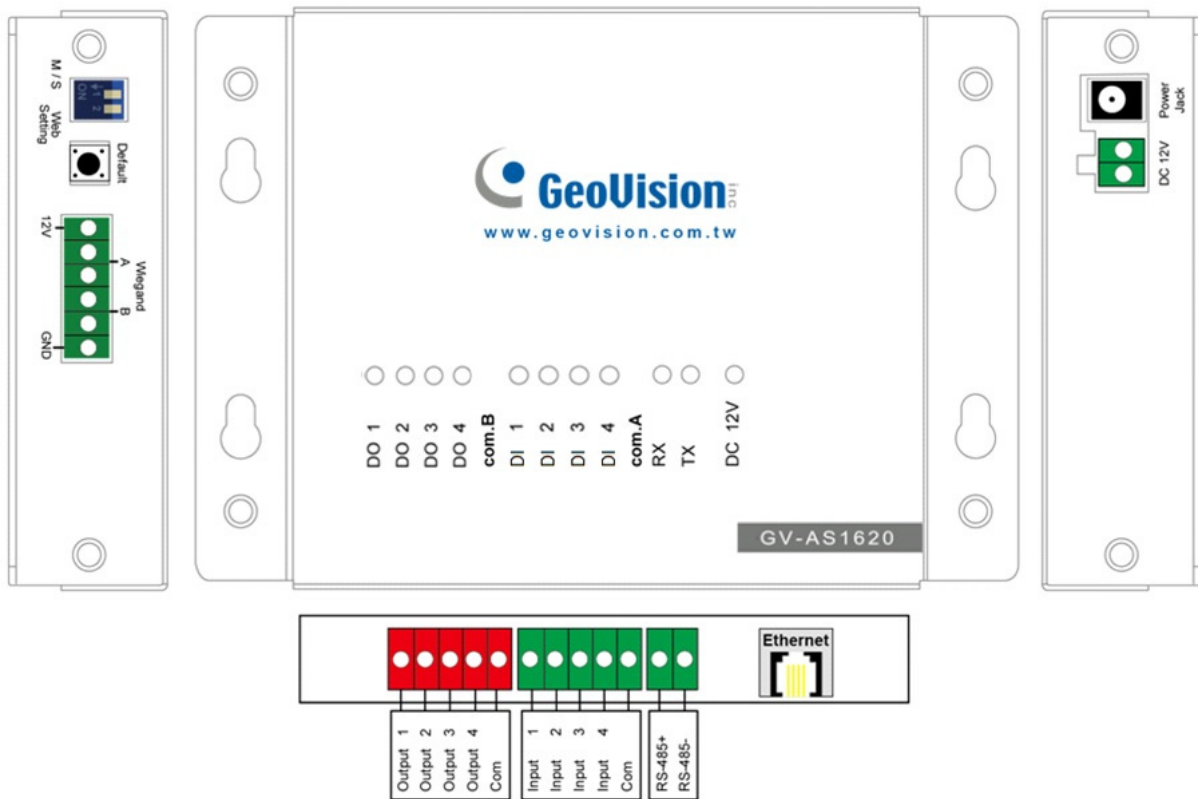1. GV-AS1620
2. Warranty Card
3. Download Guide

1.4 Overview

Figure 1-1

Pin	Definition	Pin	Definition	Pin	Definition
DO 1	Lock	DI 1	Door Contact	Wiegand A	Entry Reader
DO 2	Alarm	DI 2	Exit Button	Wiegand B	Exit Reader
DO 3	LED for Access Granted	DI 3	Fire Contact	RS-485 +/-	RS-485 Readers
DO 4	LED for Access Denied	DI 4	Tamper Contact		

Control	Definition
DC 12V	Power output for compatible devices connected
Web Setting Switch	GUI security lock. Switch on to lock all system configurations on the Web interface of the controller.
Default Button	Reset the controller to factory default if it is not functioning correctly. To do this, hold down the **Default** button with a pointy object such as the tip of a pen for 3 to 5 seconds.

Chapter 2 Installing on a Network

Through network connection, you can access the Web interface of the controller and connect it to GV-ASManager for more comprehensive management. There are three ways to set up the controller on network.

1. By default, when the controller is connected to a network with a DHCP server, a dynamic IP address will be assigned to the controller. See *2.1 Checking the Dynamic IP Address* to look up its IP address.

2. When the DHCP server on your network is unavailable or disabled, the controller is accessible by its default IP address **192.168.0.100**. See *2.2 Configuring the Static IP Address*.

3. You may also use a DDNS (Dynamic Domain Name System) server to access the controller. For details on domain name service, see *2.3 Configuring DDNS Connection*.

2.1 Checking the Dynamic IP Address

Follow the steps below to look up the IP address and access the Web interface of the controller.

1. Download and install **GV-IP Device Utility** from our website.

Note: The PC installed with GV-IP Device Utility must be under the same LAN as the controller you wish to configure.

---

2. On the GV-IP Utility window, click the 🔍 button to search for the IP devices connected in the same LAN.

3. Click the **Name** or **Mac Address** column to sort.

4. Find the controller with its MAC address, click on its IP address and select **Web Page**.
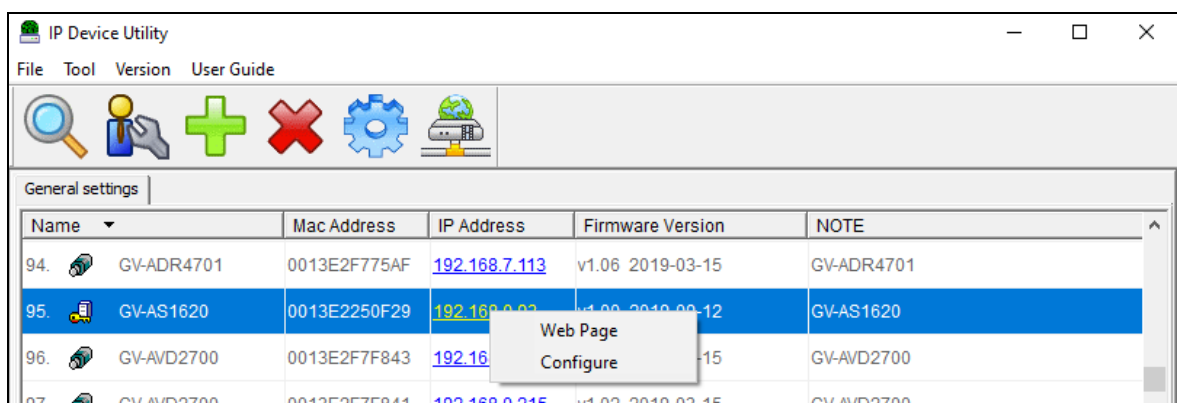

Figure 2-1

5. When the login dialog box appears, type the default **admin** for both username and password and click **OK** to log in.

2.2 Configuring the Static IP Address

By default, the controller uses a DHCP connection. However, you can follow the instructions below to configure a static IP address.

1. Open an Internet browser, and type the default IP address https://192.168.0.100 or the dynamic IP address. The login dialog box appears.

2. Type default value **admin** for both username and password, and click **OK**. This page appears.

Network Configuration

Machine Name				
Machine Name:	Controller 2			

DHCP Client

○ Enable
⦿ Disable

IP Address:	192	168	2	168
Subnet Mask:	255	255	248	0
Default Gateway:	192	168	0	1
Domain Name Server:	0	0	0	0

Figure 2-2

3. In the **DHCP Client** section, select **Disable**. Type the static IP address information, including IP Address, Subnet Mask, Default Gateway and Domain Name Server.

4. Click **Submit**. When the setting is complete, the Status field will indicate *Register Success*. Then the controller can be accessed with this fixed IP address.

2.3 Configuring DDNS Connection

DDNS (Dynamic Domain Name System) provides another way of accessing the controller when using a dynamic IP. DDNS assigns a domain name to the controller, so GV-ASManager can always access the controller by using a static domain name. The controller supports two DDNS services: GeoVision DDNS Server and Dynamic Network Services Inc. (DynDNS).

Note:

1. Dynamic DNS uploads IP addresses over the Internet through ports 80 and 81. If your controller is connected behind a router or firewall, make sure ports 80 and 81 are enabled. Dynamic DNS will only upload global IP addresses. If your controller is using virtual IP, NAT port mapping should be done first.

2. The DDNS service is provided purely as a favor to you. We hope it simplifies the process of trying to connect an IP video device to the network. GeoVision does not and cannot warrant that the DDNS service will be uninterrupted or error free. Please read Terms of Service carefully before using the service.

To enable the DDNS function, you first should register a domain name from one of the two supported DDNS service provider's websites.

GV-AS1620

Internet
(DDNS Server)

GV-ASManager

Two DDNS servers supported:
(1) GV Dynamic DNS Server
and (2) DynDNS.
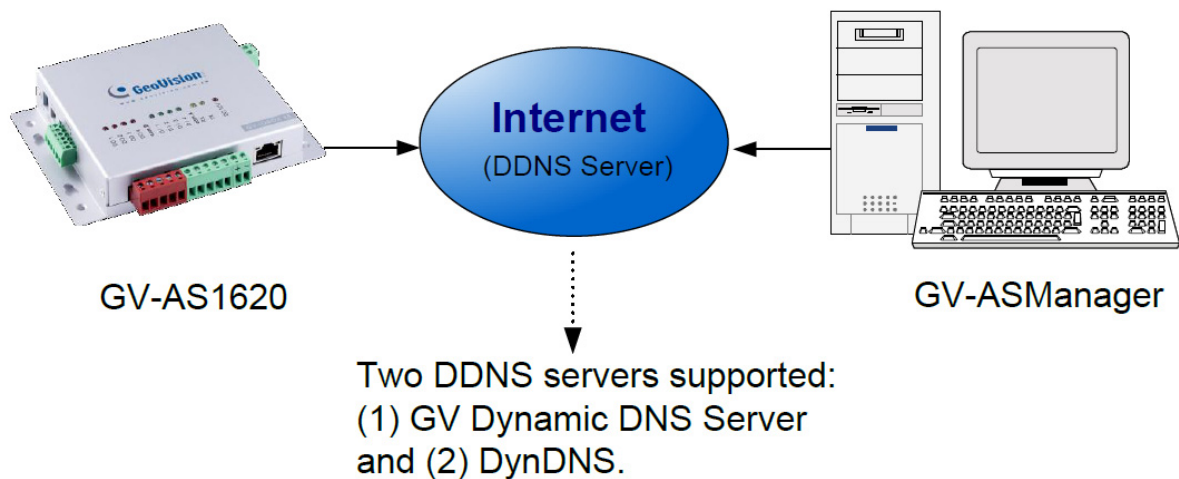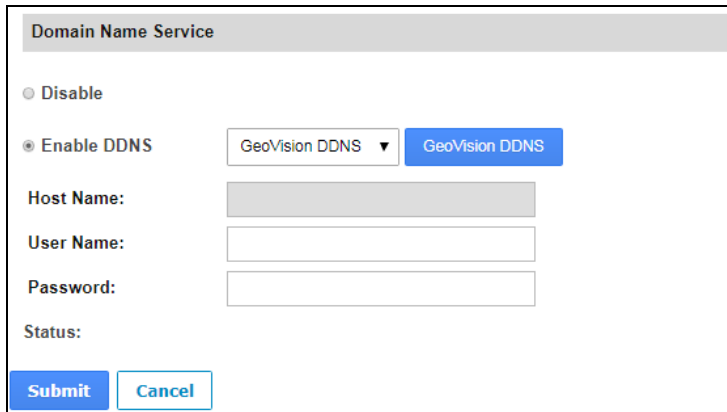
Figure 2-3

2.3.1 Registering a DDNS Domain Name

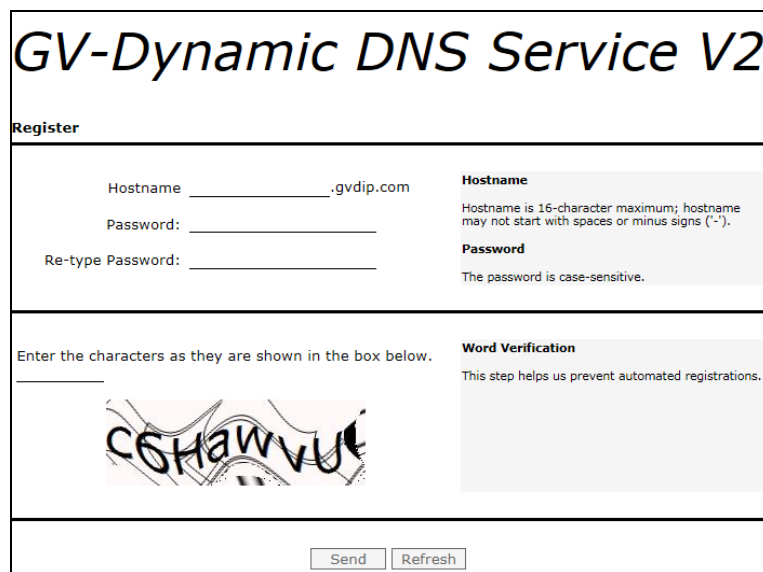To obtain a domain name from the GeoVision DDNS Server:

1. Click the **GeoVision DDNS** button on the **Network Configuration** page (*Figure 2-2*). Or open an Internet browser, and type the Web address **http://ns.gvdip.com/register.aspx**. The GV-Dynamic DNS Service V2 page appears.

Figure 2-4

Figure 2-5

2. Type a **Hostname** and **Password** based on the requirements noted on the page.

3. Type the characters or numbers shown for word verification, and click **Send**.

4. When the registration is complete, this page will appear. The **Hostname** is the domain name, consisting of the registered username and "gvdip.com", e.g. somerset02.gvdip.com.

Figure 2-6

Note: The registered username will be invalid when it is not used for three months.

2.3.2 Configuring the Controller on Internet

After acquiring a domain name from the DDNS Server, you need to configure the registered domain name on the controller in order to access the unit by the domain name on Internet.

1. Open an Internet browser, and type the controller's IP address**.** The login dialog box appears.

2. Type the username and password of the controller, and click **OK**. The Network Configuration page appears.

3. Select **Enable DDNS**.

4. Type **Host Name**, **User Name** and **Password** that are registered on the DDNS Server. If **GeoVision DDNS** is used, the system will automatically bring up the Host Name.
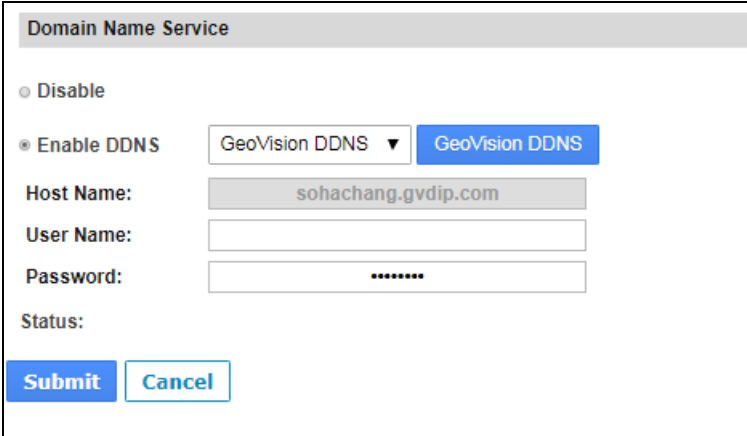

Figure 2-7

5. Click **Submit**. When the setting is complete, the Status field will indicate: *Register Success*. Then the controller can be accessed with the domain name.

Chapter 3 The Web Interface

After installing the controller on the network, you can configure the controller's settings on the Web interface. The left menu of the Web interface is divided into three sections: **Basic Setting**, **Advanced Setting** and **Extended Device**.
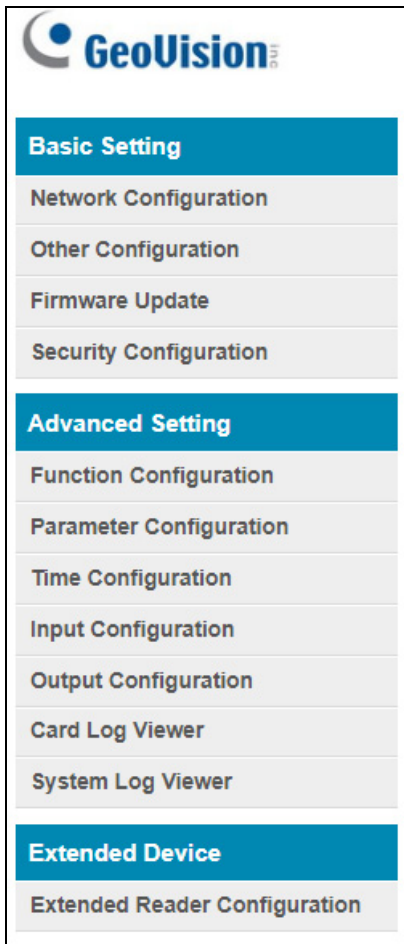

Figure 3-1

3.1 Basic Settings

The Basic Settings section covers general system settings, firmware update and user account settings. For details on Network Configuration, refer to *Chapter 2 Installing on a Network*.

3.1.1 System Setup

In the left menu, click **Other Configuration**. This page appears.

Figure 3-2

- **3DES Code 1-3:** Stands for Triple DES (Data Encryption Standard). Type up to three different keys for data encryption. The default 3DES Code1 is **12345678**.

- **Device Port:** Keeps the default value **4000**. Or modify it to match that of GV-ASManager.

- **GV-ASManager Connection Status**: If the controller is successfully connected to GV-ASManager, the IP address of GV-ASManager will be automatically brought up here.

- **Mac Address:** Indicates the MAC address of the network medium.

- **Firmware Version:** Indicates the current firmware version of the controller.

- **Reboot System:** Performs a warm boot of the controller. This operation will keep the current system configuration.
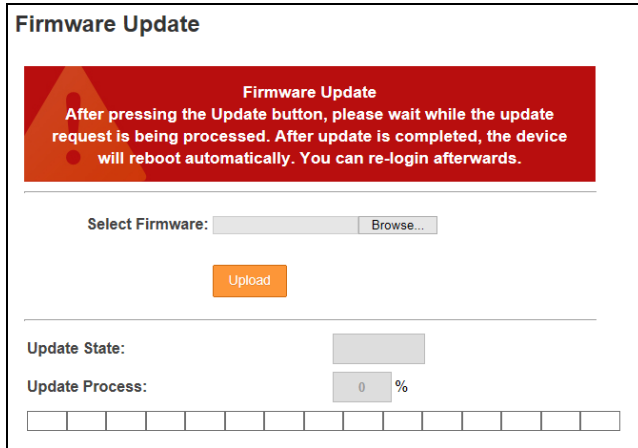
[Configuration Control]

- **Default Value:** Resets all configuration parameters to factory settings. This may take 5 seconds to complete.

- **Backup Configuration:** To backup controller settings, click **Download Backup**. A .bin file will be exported. You can then import the file to other controllers to avoid setting each controller individually. Note that network settings such as IP address and hardware ID will NOT be included in the backup file.

- **Restore Configuration:** To import controller settings, click **Browse** to select the .bin file previously exported, and click **Upload**.

3.1.2 Firmware Update

Follow the steps below to update the firmware of the controller.

1. In the left menu, click **Firmware Update**. This page appears.

Firmware Update

> **Firmware Update**
> After pressing the Update button, please wait while the update request is being processed. After update is completed, the device will reboot automatically. You can re-login afterwards.

Select Firmware: [   ] Browse...

Upload

Update State: [   ]
Update Process: [0] %

Figure 3-3

2. Click **Browse** and select the firmware file.

3. Click **Upload**. This update process may take 60 seconds to complete.

4. When the Update is complete, you will be asked to reboot the system.

5. Click **OK** to restart the controller.

Note:
1. Make sure the controller remains powered on during the firmware upgrade.
2. It is required to reboot the controller after firmware update. Without rebooting, the firmware update is not complete.

3.1.3 Security Configuration

Follow the steps below to change the login ID and password.

1. In the left menu, click **Security Configuration**.

2. Modify the login name and password. The password is case sensitive and is limited to alphabets and numbers.

Figure 3-4

3.2 Advanced Settings

Under Advanced Settings, you can configure the door settings, turn on Alarms, set the device time, edit the input function and view logs.

Changes in some of the Advanced Settings pages will affect the options available on other pages. Below is a diagram drawing the relationships between each Advanced Settings page.

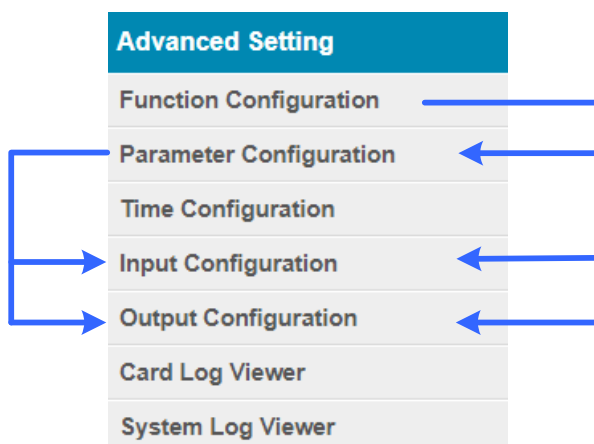The Relationship Diagram between each Advanced Setting Page

Figure 3-5

3.2.1 Function Configuration

In the left menu, click **Function Configuration**. This page appears.

Figure 3-6

[ID]

Enter the ID number for the controller. This ID is used by GV-ASManager to differentiate among multiple units of controllers. ID number can only be between 1 and 1000.

[Door/Gate A]

Select the function type and authentication mode for the use of the door/gate.

- **Function:** Define the function of the controller connected to the door/gate which is used for door, parking lost or elevator access control.

- **Authentication Mode:** Select the authentication mode for the door/gate.

  - **Local Unlock Mode:** Remains open. The held-open state cannot be cleared through GV-ASManager.

  - **Local Lock Mode:** Remains locked. The locked state cannot be cleared through GV-ASManager.

  - **Fixed Card Mode:** Grants access after the card is presented or a passcode is entered, and ignores the authentication schedule of GV-ASManager.

  - **Fixed Card Mode + PIN Mode:** Grants access after the card is presented and the card's PIN code entered too. Ignores the authentication schedule of GV-ASManager.

  - **Fixed Card/Common Mode:** Grants access after the card is presented or after the door/gate's password is entered. Ignores the authentication schedule of GV-ASManager.

  - **Authentication Schedule Mode:** Follows the authentication schedule set on GV-ASManager.

  - **Local Lock Down:** Locks down the door and denies access when the card is presented. Ignores the Lock Time setting and APB setting.

Note: To grant access to a card in **Local Lock Down** mode, click the **Access Monitor** button on GV-ASManager, right-click on the card to select **New/Edit Card** and select **Disable Lock Card / Disable APB / Allow Access during Lockdown Mode**.

[Series Function (APB & Fire)]

You can set Anti-Passback and fire sensor functions across multiple controllers. The Anti-Passback means that a card used on an entry door/gate cannot access the same entry door/gate again unless it has been used on a corresponding exit door/gate. For details on setup, see *Chapter 6 Anti-Passback* on *GV-ASManager User's Manual*.

For the fire sensor function, when the fire sensor of the associated controller is triggered, the fire sensor on GV-AS1620 will also be activated.

- **Enable/Disable:** Enables or disables Anti-Passback and fire sensor functions.
- **Info IP:** Enter the IP address of the next corresponding controller.

[Wiegand Card Filter Setting]

- **Wiegand A/B Filter:** Enable to avoid recording repeated access logs, from the same card via Wiegand port A or B, within the duration set.
  - ☉ **Wiegand A/B Filter Duration:** Set the duration of filter, from 3 ~ 60 seconds.

[Camera Mapping]

You can assign a camera to capture snapshots upon card presented. The captured snapshots will be saved to the built-in flash drive of GV-AS1620 and then transferred to the Access Log on GV-ASManager whenever GV-ASManager resumes connection after it has been disconnected.

- **Enable/Disable:** Enables or disables the camera mapping function.
- **First Camera:** Type the IP address of the assigned camera to take snapshots.

Type the **User Name** and **Password** of the camera to complete the mapping process.

Note: This function is supported only on GV IP cameras except GV-EBD / ABL / ADR / AVD / TDR / TBL / TVD series, GV-VD8700 and FD8700-FR.

[HTTP Event (Card Log Notification)]

Select **Enable** to send access and event logs of the controller to the configured **event IP** address and **Port** number.

3.2.2 Parameter Configuration

In the left menu, click **Parameter Configuration**. This page appears.

IMPORTANT: Once connected to GV-AS1620, GV-ASManager will load its parameters to the controller. That means some of the Parameter Settings you have configured here may be overwritten by GV-ASManager later.

Figure 3-7

[Events]

Set the parameters for the events. The options available vary depending on **Door Control**, **Parking Control** and **Elevator Control** selected in the **Function Configuration** page (*Figure 3-6*):

Option	Description
Anti-Passback	Enables or disables the Anti-Passback function.
Lock Reset Time	Sets the time (1 to 600 sec.) that a door remains open after which the door will automatically be locked.
Held Open Time	Sets the time (5 to 9999 sec.) that a door can be held open before an alarm is generated.

Fire Action	Locks or unlocks the door when a fire condition occurs. Otherwise, remains the door's current state by selecting *Unchanged*.
Alarm Continuous Time	Sets the time (1 to 10 sec.) that the alarm will continuously go off before it ends.
Relay On Time	Sets the time (1 to 600 sec.) that a gate remains open after which the gate will automatically be closed.

[Alarm]

Select **Yes** or **No** to enable or disable the alarm function. The options available vary depending on **Door Control**, **Parking Control** and **Elevator Control** selected in the **Function Configuration** page (*Figure 3-6*):

If you have defined the alarm conditions in the **Input Configuration** (*Figure 3-9*) and **Output Configuration** (*Figure 3-10*) pages, remember to activate the corresponding alarms here; otherwise, even though the alarm conditions are met, the expected alarm will not be triggered. The default settings for all the alarms are set to **NO**.

Option	Description
Held Open	This alarm activates whenever the door is held open over the specified time period.
Forced Open	This alarm activates whenever the door is opened by force.
Fire Alarm	This alarm activates whenever fire is detected.
Access Denied	This alarm activates whenever entry is denied due to invalid card or password presented.
Tamper	This alarm activates whenever the sensor for tampering alarm is triggered. The tampering alarm sensor needs to be installed separately and the triggering conditions depend on the type of sensor installed, e.g. opening of the controller's cabinet.

[Common Password]

When **Fixed Card/Common Mode** is selected as **Authentication Mode** in the **Function Configuration** (*Figure 3-6*) page, you can gain access by using a card or entering this Common Password (door's password).

3.2.3 Time Configuration

In the left menu, click **Time Configuration** to set up system time, local time and daylight saving time period.

Figure 3-8

[System Local Time] Displays the current data, time and time zone of the controller.
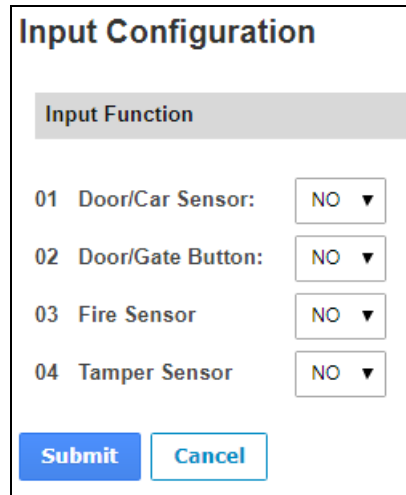
[Local Time]

- **Disable:** Disable the manual configuration of time and date.

- **Setup:** Configure the time and date of the controller manually. You can click **Current local time** to synchronize the controller's date and time with those of the local PC.

[Daylight Savings Time (DST)]

- **Disable:** Disable the manual configuration of DST.

- **Time Zone:** Enable the manual configuration of DST by setting **Start Time** and **Stop Time** for the DST period.

3.2.4 Input Configuration

In the left menu, click **Input Configuration** to define the input devices connected to the controller. You set the input status to either NO (normally open) or NC (normally close).
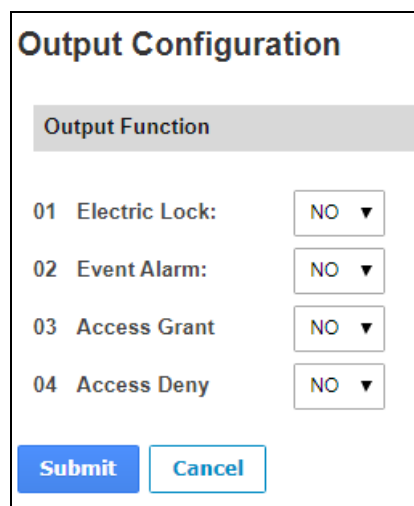

Figure 3-9

3.2.5 Output Configuration

In the left menu, click **Output Configuration** to define the output devices connected to the controller. You set the input status to either NO (normally open) or NC (normally close).

Figure 3-10

3.2.6 Log Viewer

In the left menu, click **Card Log Viewer** to search for the log data. The log entries are only created when the controller is disconnected from GV-ASManager. Only up to 100 log entries of Event Log / Access Log on the Web interface can be retrieved at a time.

Figure 3-11

3.2.7 System Log Viewer

In the left menu, click **System Log Viewer** to view the current system status and dump data that can be used by service personnel for analyzing problems.

3.3 Extended Device

In the left menu, click **Extended Reader Configuration** to define the readers connected to the controller through RS-485 or network connection.
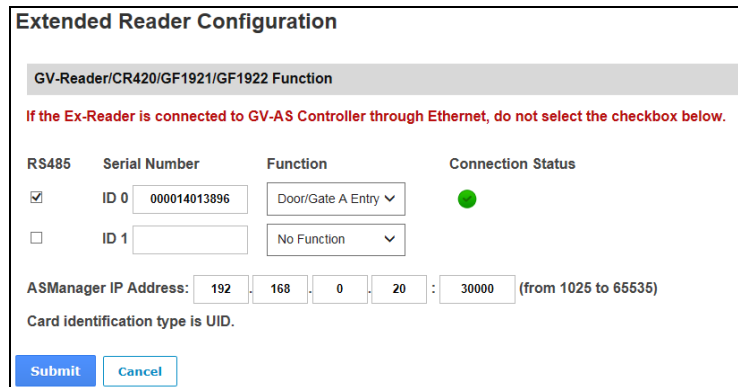

Figure 3-12

[GV-Reader / CR420 / GF1921 / 1922 / CR1320 / FR2020 Function] Define the readers connected to the controller, and then use the **Function** drop-down list to select the door associated with the reader.

- **GV-RK1352 / R1352 / DFR1352:** Select the **RS-485** checkbox and type the **Serial Number** of the reader. The ID number located next to the serial number field will be assigned to the reader.

- **GV-Reader 1251 / Reader 1352 V2:** Select the **RS-485** checkbox and leave the serial number field blank. Note that the ID number located next to the serial number field needs to match the reader's ID number defined by the dip switches on the reader.

- **GV-GF1921 / GF1922 / CR1320 / FR2020:** Type the **MAC address** of the fingerprint reader or camera and do not select the RS-485 checkbox.

- **GV-CR420:** Select the **RS-485** checkbox only if the GV-CR420 is connected to the controller through RS-485 connection. If the reader is using network connection, do not check the RS485 box. Type the **MAC address** of GV-CR420 if you using the latest GV-CR420 firmware.

[ASManager Server IP Address] To allow GV-ASManager to receive data from the GV-AS1620, type the IP address and port of the GV-ASManager's Server.

Click **Submit**. If the reader is detected, the **Connection Status** field will be green.

Chapter 4   Troubleshooting

Q1: GV-ASManager cannot connect to the controller over the Internet.

There are several causes for this problem such as IP address conflict, incorrect connection settings and network failure. Follow the steps below to assign a fixed IP to the GV-ASManager and the controller respectively. This procedure can determine if the problem is caused by faulty devices and incorrect network settings.

1. Disconnect the hub or switch, which connects both the GV-ASManager and the controller, from the Internet.

2. Give the GV-ASManager a fixed IP address that is NOT used by another device under the LAN, e.g. 192.168.0.154.
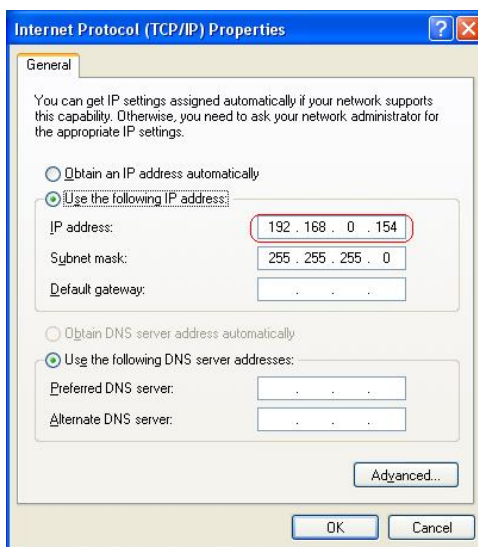

Figure 4-1

3. Reset the controller to factory defaults. For details, see *3.1.1 System Setup*.

4. Log in the controller using the default IP: http://192.168.0.100

5. In the IP address fields, give the controller an IP address that is NOT used by another device under the LAN, e.g. 192.168.X.XXX.

Figure 4-2

6. On the GV-ASManager, type the following settings:

Controller ID: 1

Network: TCP/IP

IP: 192.168.X.XXX

Port: 4000

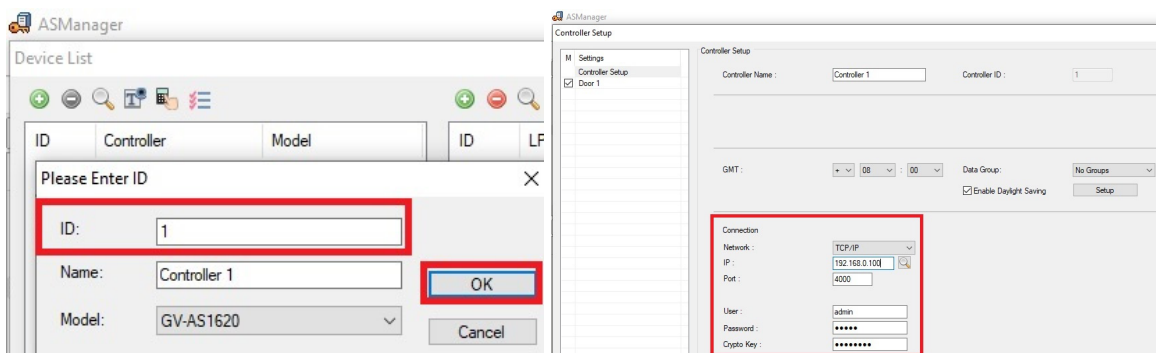**User:** admin

Password: admin

Crypto key: 12345678

Figure 4-3

7. The connection between the GV-ASManager and controller should be established under the LAN with the connection icon ![icon] appearing. If disconnection happens soon after you connect the hub or switch back to the Internet, then it should be other network problems. Please contact your network administrator.

4 **Troubleshooting**

Q2: The connection established between the GV-ASManager and the 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 both the GV-ASManager and the 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 4-4

4. Give the GV-ASManager a fixed IP address that is NOT used by another device under the LAN. See *Figure 4-1*.

5. Log in the controller The Network Configuration page appears.

6. In the IP address field, give the controller an IP address that is NOT used by another device under the LAN.

7. On the GV-ASManager, enter the following settings. See *Figure 4-3*.

   Controller ID: 1

   Network: TCP/IP

   IP: 192.168.0.XXX

   Port: 4000

   User: admin

   Password: admin

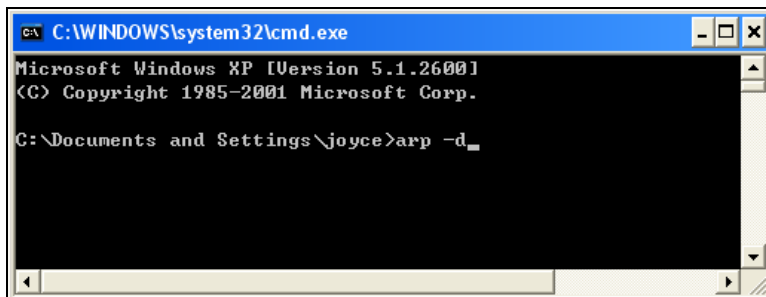   **Crypto key:** 12345678

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

25

Q3: GV-ASManager cannot receive card messages but the reader accepts the card when the connection between the GV-ASManager and GV-AS1620 is well established.

It may be due to memory failure in the controller. Reset the controller module to factory settings. For details, see *3.1.1 System* Setup.

Q4: After I added a card on GV-ASManager and then presented it to the reader, the message "*Access Denied Invalid Card"* still appears.

It may be the card format is not compatible with the controller. Make sure the card format is 64 bits. Otherwise, send us the related information of your card format so that we can customize the setting for you.

Q5: GV-ASManager cannot receive card messages from the reader connected to the controller through RS-485 interface.

1. Make sure the reader is correctly wiring to the controller.

2. Make sure the reader has been defined on the controller. See *3.3 Extended Device* for details.

Q6: How can I find more help?

Visit our website at http://www.geovision.com.tw/products.php?c1=25

Write to us at support@geovision.com.tw