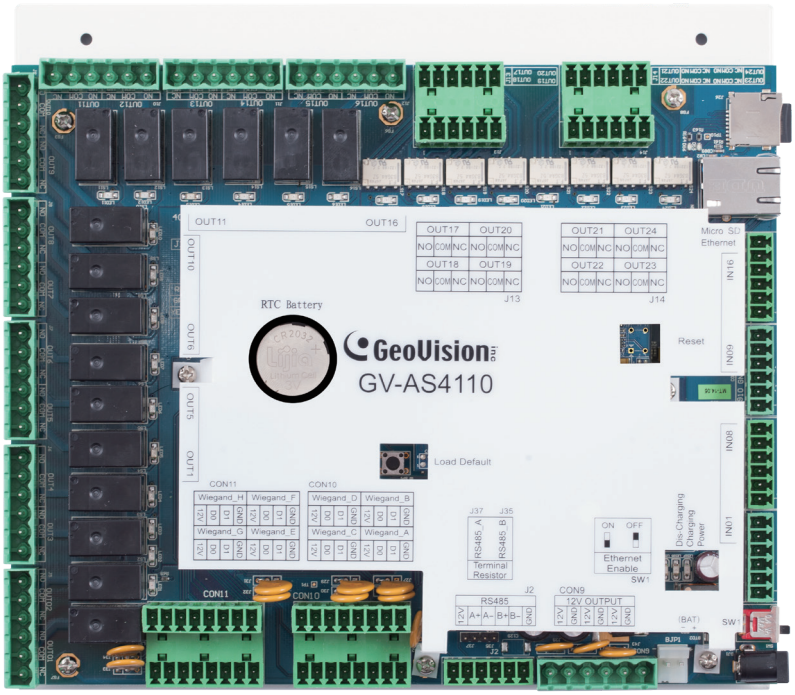
GeoVision inc
The Vision of Security

GV-AS4110 Cloud Controller

User's Manual



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

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

October 2025

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

[Warranty]

[Technical Support Policy]

Contents

Chapter 1 Introduction 1

1.1 Overview 2

Chapter 2 Installing on a Network 3

2.1 Checking the Dynamic IP Address 3
2.2 Configuring the Static IP Address 4
2.3 Configuring DDNS Connection 5

Chapter 3 The Web Interface 8

3.1 Basic Settings 9
3.1.1 System Setup 9
3.1.2 Firmware Update 11
3.1.3 Security Configuration 12
3.2 Advanced Settings 14
3.2.1 Function Configuration 14
3.2.2 Parameter Configuration 15
3.2.3 Time Configuration 17
3.2.4 Input Configuration 18
3.2.5 Output Configuration 18
3.2.6 Wiegand Configuration 19
3.2.7 System Log Viewer 19
3.4 Extended Devices 20
3.4.1 Extended Reader Configuration 20
3.4.2 Extended Camera Configuration 21

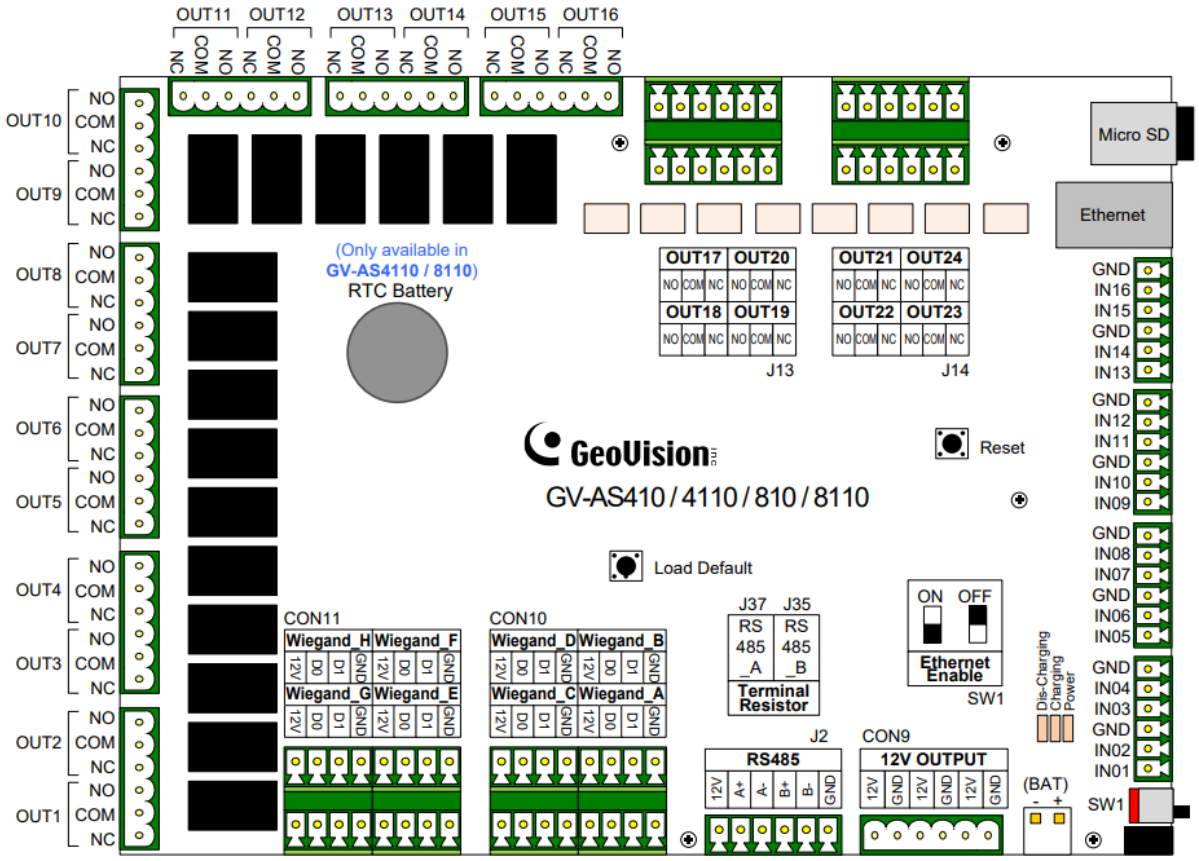
Chapter 1 Introduction

GV-AS4110 Cloud is a four-door controller with three types of interfaces, Wiegand, RS-485 and TCP/IP—to support various readers for entry and exit management. In addition to basic door control, its I/O pins support applications such as alarm, tamper detection, and fire sensor integration.

When connected directly to IP cameras or via the GV-Cloud Bridge, the GV-AS4110 Cloud can transmit snapshots, live view, or recordings (requires GV-Cloud Bridge) to GV-Cloud Access Control following an access event.

1.1 Overview

For details on how to connect readers, I/O devices, a backup battery, and power, see *Chapter 5 GV-AS410 / 4110 / 810 / 8110 Controller* in *GV-AS / EV Controller User's Manual*.



Note: The **Reset** button is not functional in the GV-AS4110 Cloud.

Chapter 2 Installing on a Network

Through a network connection, you can access the controller's Web interface and connect it to access control software for more comprehensive management. There are three ways to set up the controller on network.

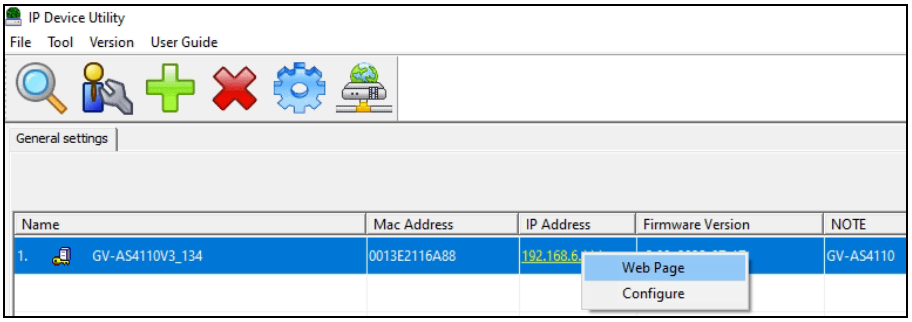
1. By default, when the controller is connected to a network with a DHCP server, a dynamic IP address will be assigned to the controller. See *2.1 Checking the Dynamic IP Address* to look up its IP address.
2. When the DHCP server on your network is unavailable or disabled, the controller is accessible 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*.

Note: The **DHCP** function on the controller is enabled by default. The controller's default ID and password are **admin** and **admin**.

2.1 Checking the Dynamic IP Address

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

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

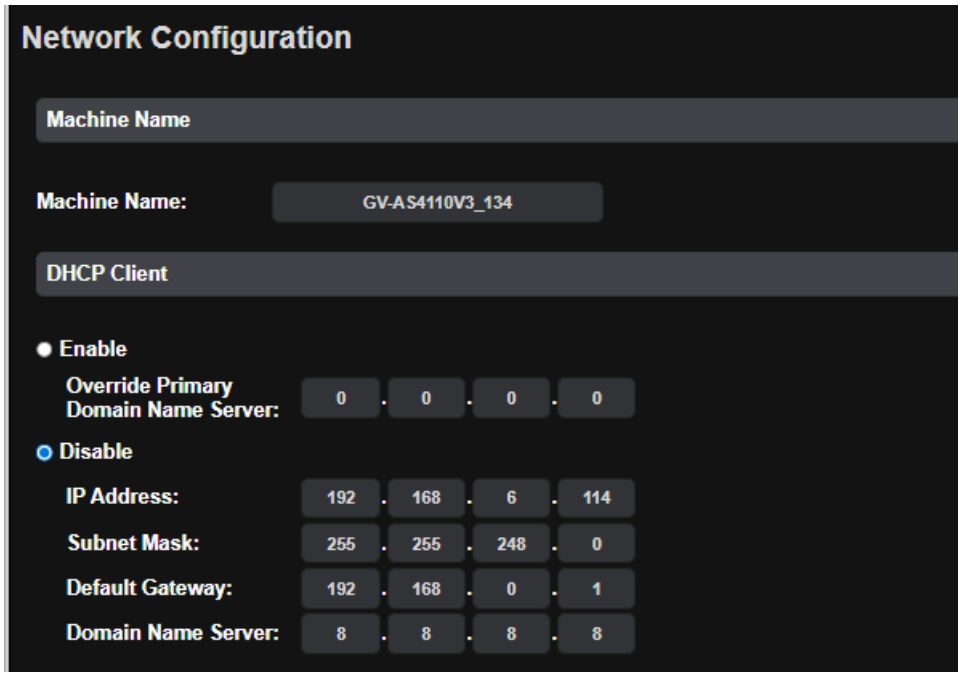


5. When the login dialog box appears, enter the default **admin** for both username and password and click **OK** to log in.

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 a dynamic IP address. The login dialog box appears.
2. Type default value **admin** for both the username and password, and click **OK**.
3. In the left menu, select **Network Configuration**. This page appears.



4. Under **DHCP Client**, select **Disable**. Type the static IP address settings, including IP Address, Subnet Mask, Default Gateway and Domain Name Server.
5. Click **Submit**. When the settings are saved, the Status field will indicate *Register Success*. You can now access the controller using the fixed IP address.

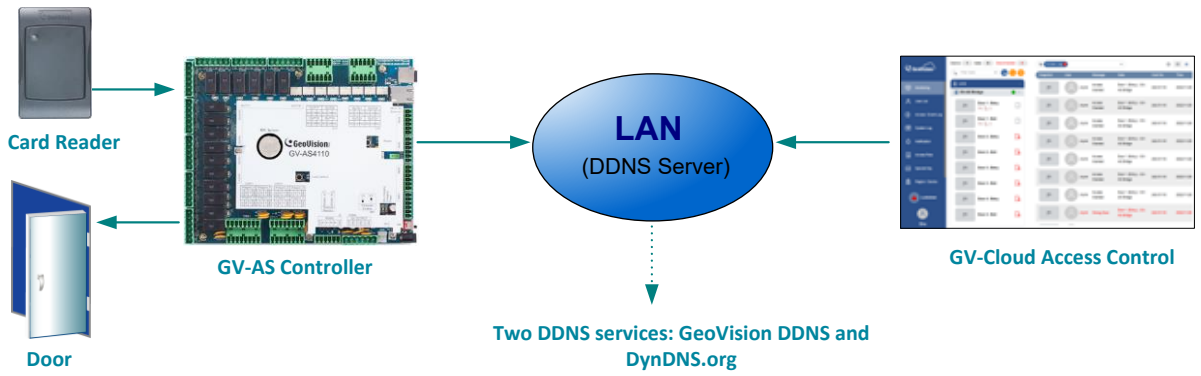
2.3 Configuring DDNS Connection

DDNS (Dynamic Domain Name System) provides an alternative way to access the controller when using a dynamic IP address. It assigns a domain name to the controller, allowing it to be accessed consistently using the domain name, even if the IP address changes. The controller supports two DDNS services: **GeoVision DDNS** and **DynDNS.org** (Dynamic Network Services Inc.).

Note:

1. Dynamic DNS uploads IP addresses over the Internet through ports 80 and 81. If your controller is behind a router or firewall, make sure the two ports are enabled. Dynamic DNS will only upload global IP addresses. If your controller uses virtual IP, NAT port mapping should be done first.
2. The DDNS service is provided solely as a convenience to assist with connecting IP video devices to the network. GeoVision makes no guarantees that the service will be uninterrupted or error-free. Please read Terms of Service carefully before using the service.

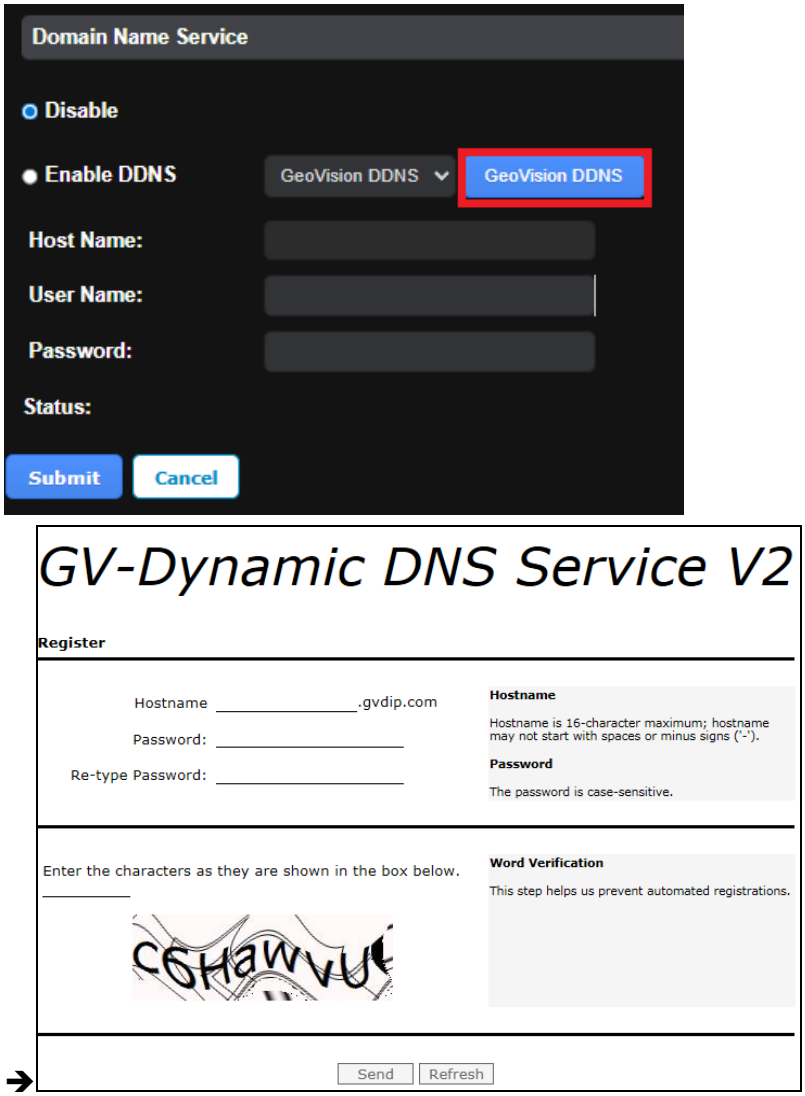
To use the DDNS function, first register a domain name through one of the two recognized DDNS service providers' websites.



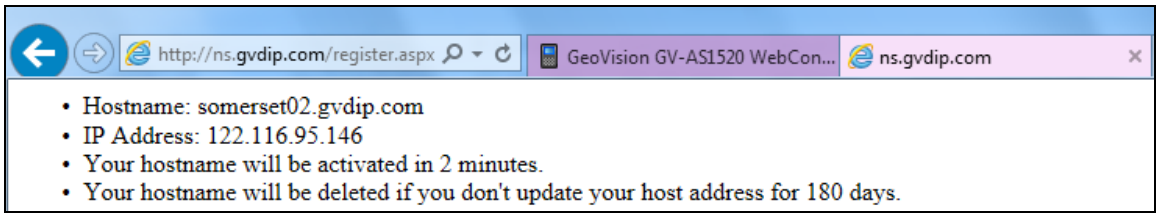
2.3.1 Registering a DDNS Domain Name

To obtain a domain name from the GeoVision DDNS Server, follow the steps below.

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



3. Type a **Hostname** and **Password** based on the requirements noted on the page.
4. Type the characters or numbers shown for word verification, and click **Send**.
5. When the registration is complete, this page appears. The **Hostname** is the domain name, consisting of the registered username and “gvdip.com”, e.g. somerset02.gvdip.com.



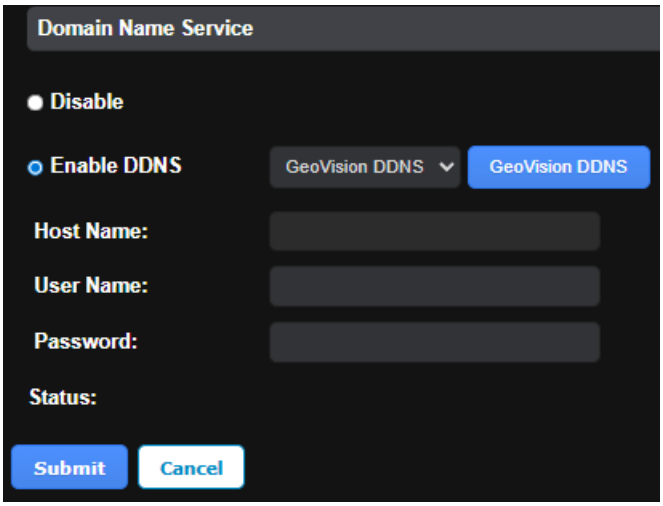
Note:

1. The registered username will be invalid when it is not used for three months.
2. Optionally, you can type the backup DNS next to **Override Primary Domain Name Server** under the **DHCP Client** section to prevent the malfunction of the set DNS.

2.3.2 Configuring the Controller on Internet

After obtaining a domain name from the DDNS Server, configure the registered domain name on the controller to enable access via the domain name on the Internet.

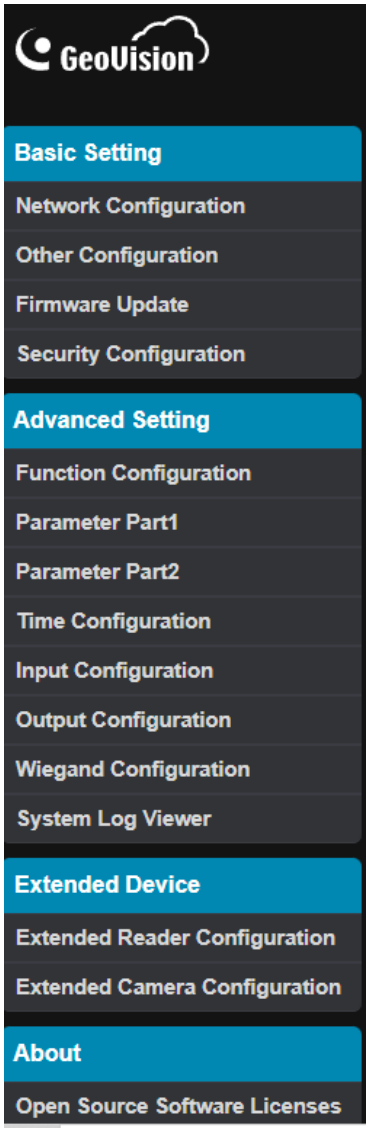
1. In the left menu, select **Network Configuration**. The Network Configuration page appears.
2. Select **Enable DDNS**.
3. Type **Host Name**, **User Name** and **Password** that are registered on the DDNS Server. If **GeoVision DDNS** is used, the system will automatically bring up the Host Name.



4. Click **Submit**. When the settings are saved, the Status field will indicate: *Register Success*. You can now access the controller using the domain name.

Chapter 3 The Web Interface

After installing the controller on the network, you can configure its settings via the Web interface. The left menu of the Web interface is separated into three sections: **Basic Settings**, **Advanced Settings**, and **Extended Device**.

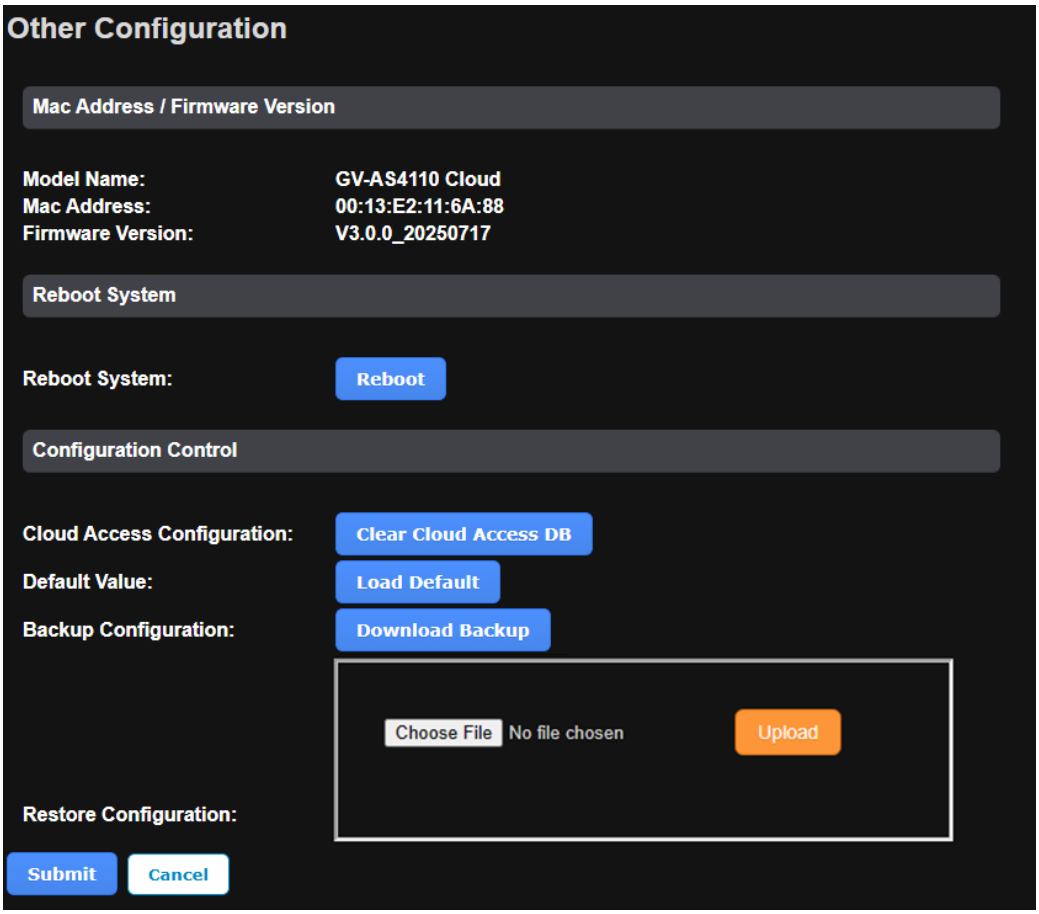


3.1 Basic Settings

The Basic Settings section covers general system settings, firmware update, and GV-Cloud Access Control connection settings. For details on Network Configuration, see *Chapter 2 Installing on a Network*.

3.1.1 System Setup

The Other Configuration page allows you to perform actions such as system reboot, restoring default settings, back up configurations, and more.



[Mac Address / Firmware Version]

- **Mac Address:** Indicates the MAC address of the controller.
- **Firmware Version:** Indicates the current firmware version of the controller.

[Reboot System]

- **Reboot System:** Performs a warm boot of the controller. This operation maintains current system setup.

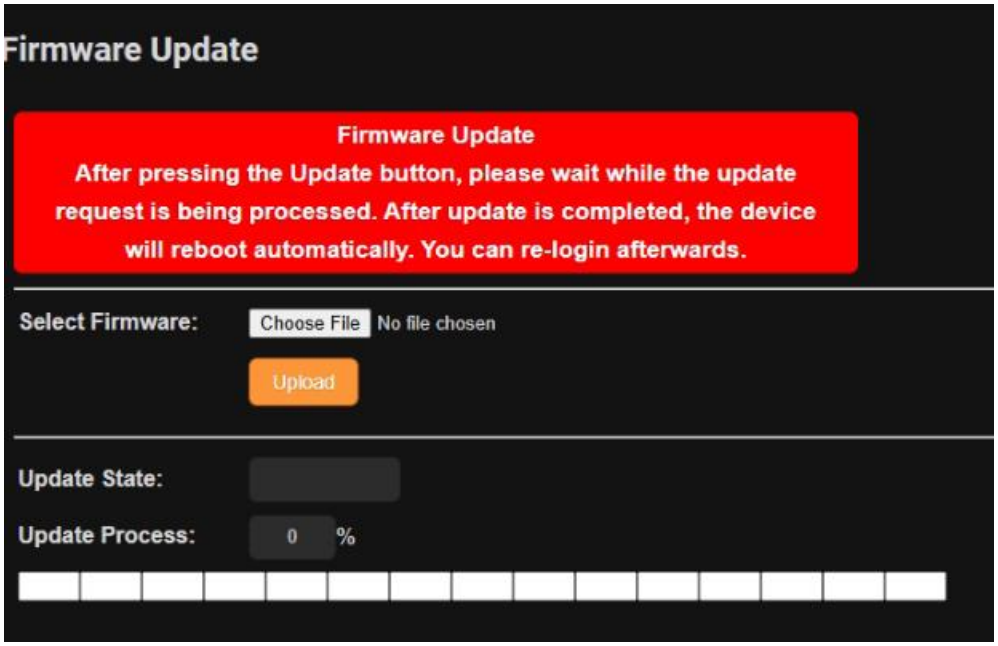
[Configuration Control]

- **Cloud Access Configuration:** Click **Clear Cloud Access DB** to clear the controller database. After reconnecting to GV-Cloud Access Control, the system will automatically synchronize the user and card data from GV-Cloud Access Control with the controller.
- **Default Value:** Click **Load Default** to reset all configuration parameters to factory defaults. This may take 5 seconds to complete.
- **Backup Configuration:** Click **Download Backup** to backup controller settings. A .bin file will be exported. You can then import the file into another controller to avoid configuring 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**, select the .bin file previously exported, and click **Upload**.

3.1.2 Firmware Update

The Firmware Update page allows you to update the controller's firmware to the latest version.

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



2. Click **Choose File** 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**. The controller is rebooted.

IMPORTANT:

GV-AS4110 firmware versions **V1.xx** and **V2.xx** are designed for **GV-ASManager** applications, while version **V3.xx** is intended solely for **GV-Cloud Access Control**. Firmware for GV-AS4110 Local and GV-AS4110 Cloud are not interchangeable and cannot be upgraded across platforms.

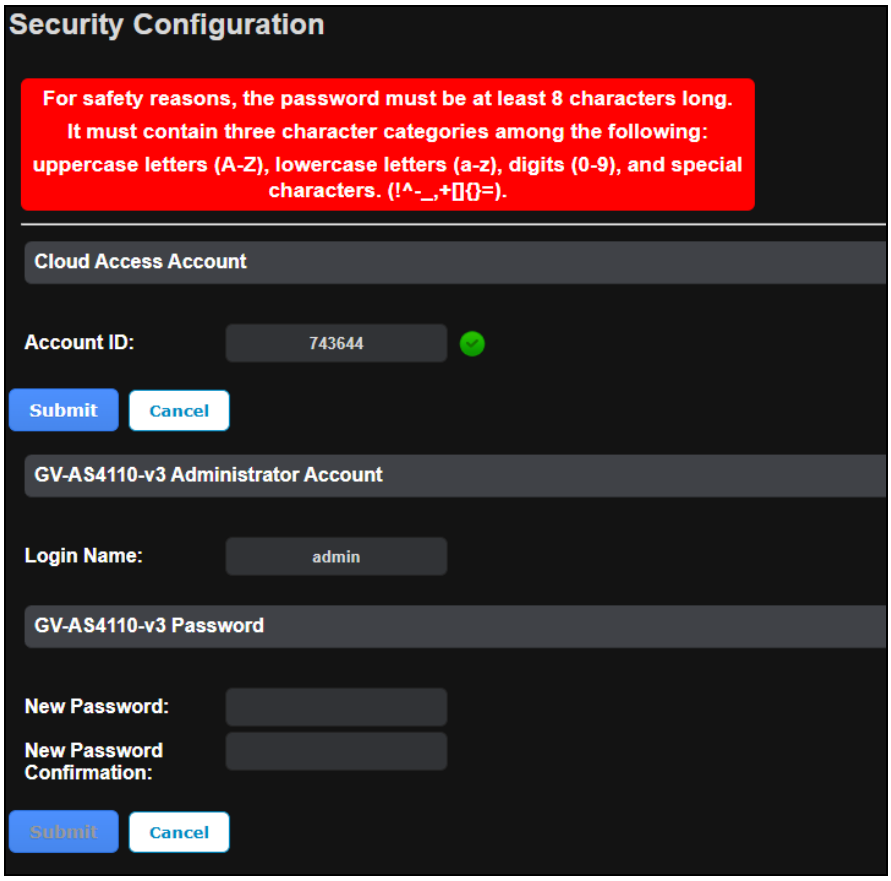
- GV-AS4110 local is the GV-AS4110 controller.
- GV-AS4110 Cloud is the GV-AS4110 controller with GV-AS41 Series Cloud Net Module.

Note:

1. Make sure the controller remains powered on during the firmware upgrade.
2. The controller must be rebooted following the firmware update. Without a reboot, the firmware update is not complete.

3.1.3 Security Configuration

The **Security Configuration** page allows the controller to connect to GV-Cloud Access Control for cloud-based centralized access management. You can also modify the controller's login ID and password on this page.



[Cloud Access Account]

Follow the steps below to connect the controller to GV-Cloud Access Control

1. Before connecting, you must first create an account on the GV-Cloud Access Control platform.
2. Type the **Account ID** you created on the GV-Cloud platform.
3. Click **Submit** right under the **Cloud Access Account** section.

Once the controller is connected, a green status appears next to the **Account ID** field. After the connection is established, add the controller on the **Device List** of GV-Cloud Access Control for centralized access control. See *4.2.1 Adding a Device* in *GV-Cloud Access Control User's Manual*.

[GV-AS4110-v3 Administrator Account] This is to create the login ID of the controller's Web interface.

[GV-AS4110-v3 Password] This is to create new password for the controller's Web interface.

Note:

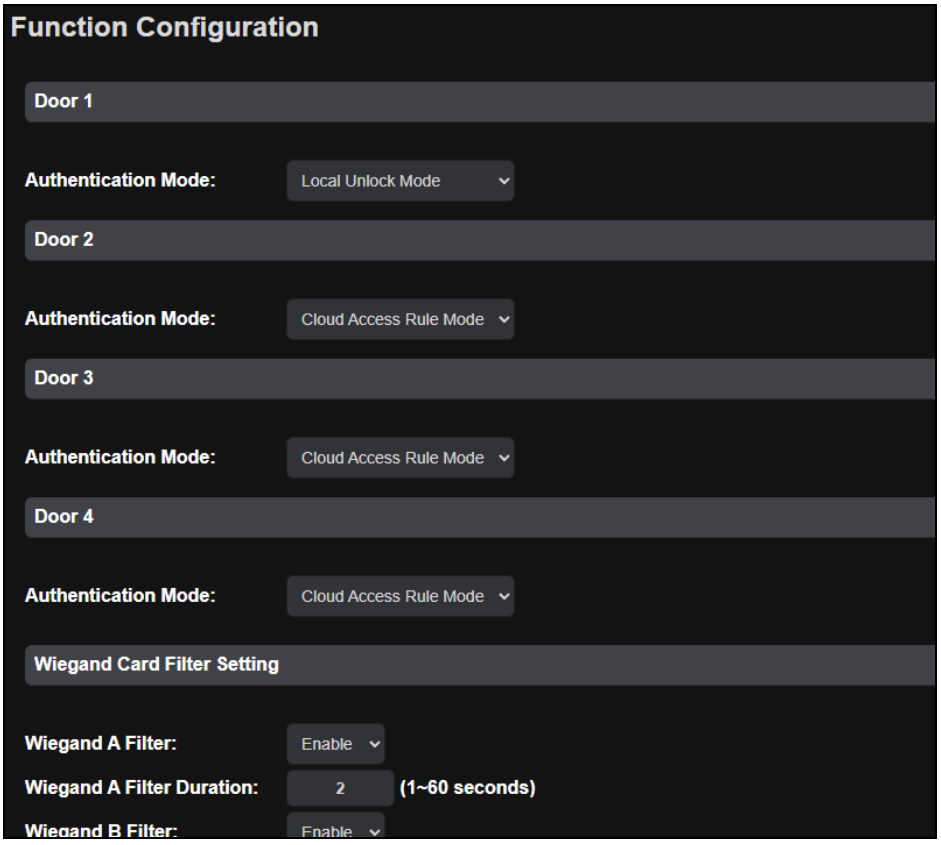
1. If the controller's password changes, ensure to update it on GV-Cloud Access Control to maintain the connection.
2. To switch to a different GV-Cloud Access Control account, type the Account ID under the **Cloud Access Account** section and click **Submit**.

3.2 Advanced Settings

Under Advanced Settings, you can configure door settings, enable alarms, set the device time, and view system logs.

3.2.1 Function Configuration

The Function Configuration page defines the access authentication mode for each door, and configures the filtering function for Wiegand card readers.



[Door 1 ~ Door 4]

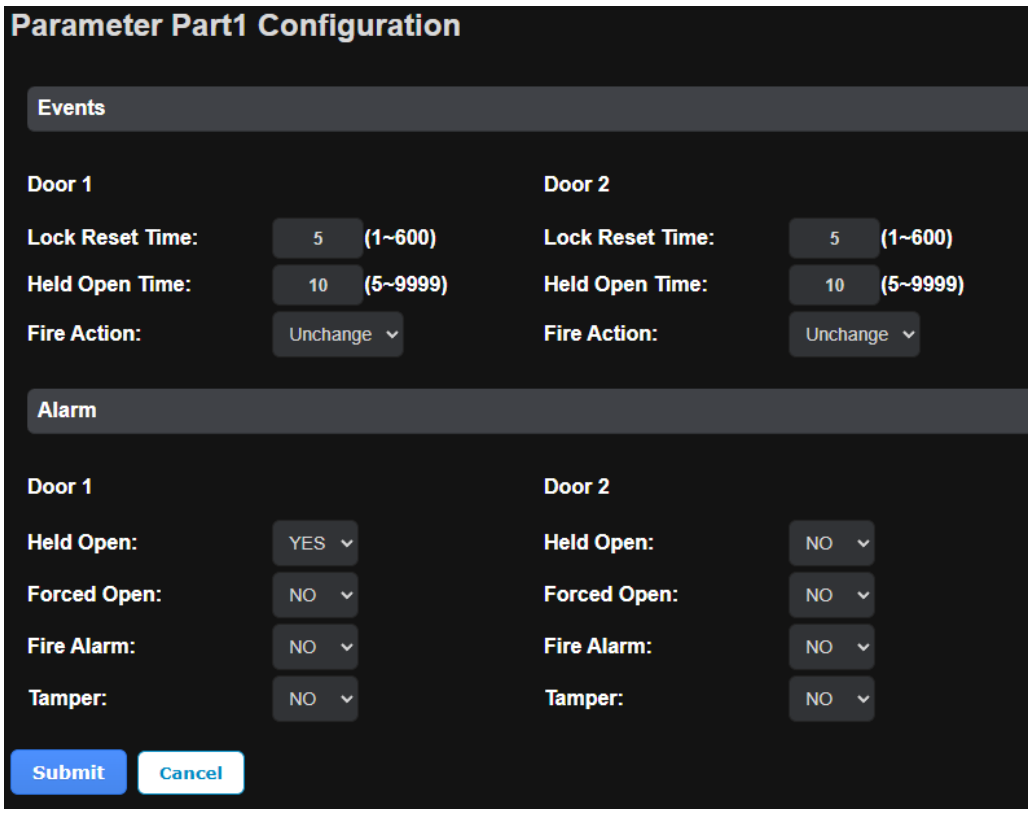
- **Authentication Mode:** Select the desired access rule.
  - **Local Unlock Mode:** Select this option to open the door immediately. The held-open state cannot be cleared using GV-Cloud Access Control.
  - **Local Lock Mode:** Select this option to lock the door immediately. The locked state cannot be cleared using GV-Cloud Access Control.
  - **Cloud Access Rule Mode:** Select the mode to follow the access rules set on GV-Cloud Access Control.

[Wiegand Card Filter Setting]

- **Wiegand A Filter ~ Wiegand H Filter:** Enable to prevent recording multiple access logs, from the same card, via the specified Wiegand card reader within the set duration.
- **Wiegand A Filter Duration ~ Wiegand H Filter Duration:** Set the duration of filter, from 1 ~ 60 seconds.

3.2.2 Parameter Configuration

The Parameter Part 1 Configuration defines **Doors 1 and 2** actions, and the Parameter Part 2 Configuration defines **Doors 3 and 4** actions.



[Events]

- **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, remain the door's current state by selecting *Unchanged*.

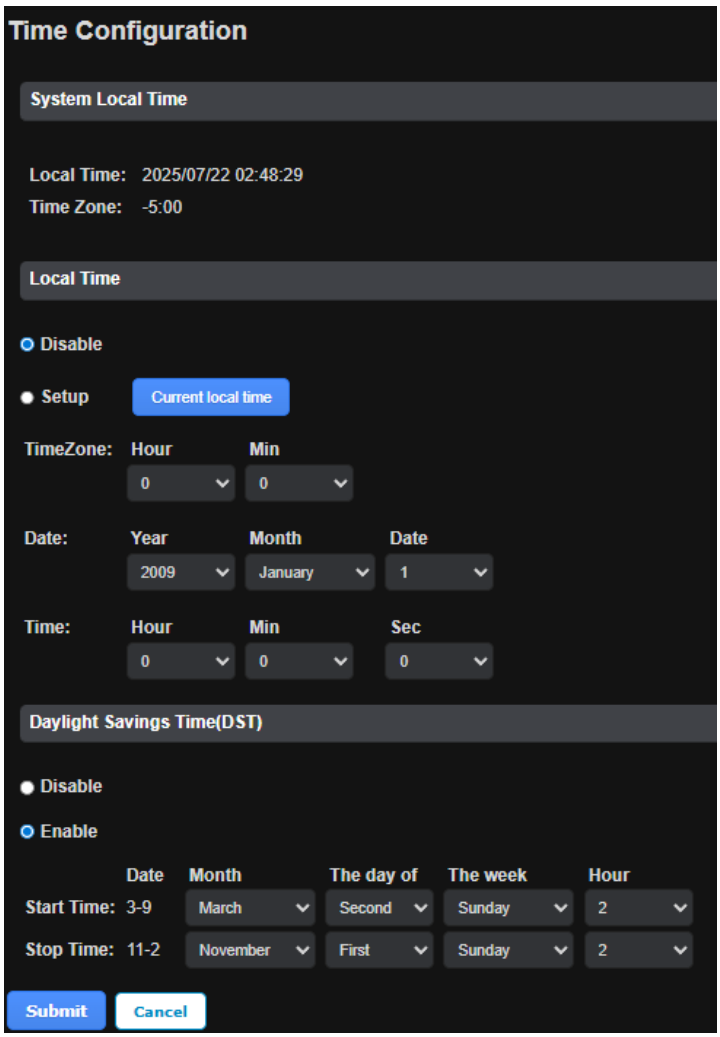
[Alarm]

- **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.
- **Tamper:** This alarm activates whenever the sensor for tampering alarm is triggered. The tampering alarm sensor must be installed separately and the triggering conditions depend on the type of sensor used, such as the controller's cabinet being opened.

Note: If you have defined the alarm conditions in the **Input Configuration** and **Output Configuration** pages, make sure to activate the corresponding alarms on this page. Otherwise, even though the alarm conditions are met, the expected alarm will not be triggered. The default setting for all alarms is **NO** (disabled). To enable them, select **Yes**.

3.2.3 Time Configuration

The Time Configuration page allows you to view and modify the system time, as well as enable daylight saving time.



[System Local Time] Displays the controller's current time and time zone.

[Local Time]

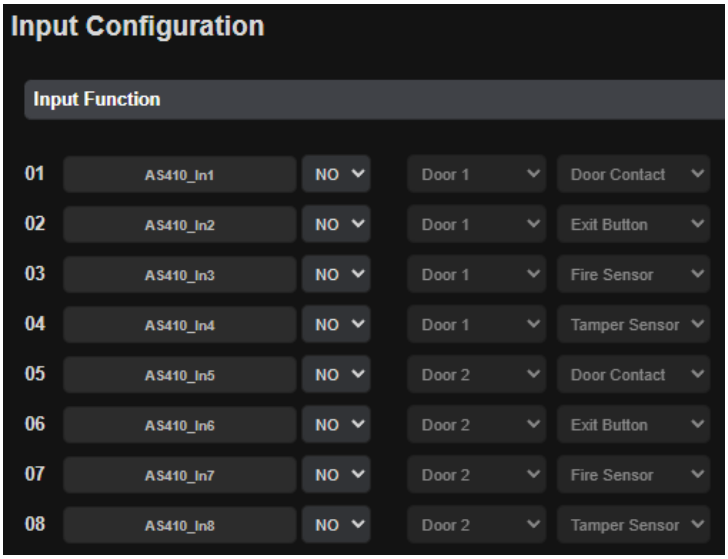
- **Disable:** Disable manual configuration of time and date.
- **Setup:** Configure the controller's time and date manually. You can click **Current local time** to synchronize the controller's time and date with those of the local PC.

[Daylight Savings Time (DST)]

- **Disable:** Disable manual DST configuration.
- **Enable:** Enable manual DST configuration and set up **Start Time** and **Stop Time** of the DST period.

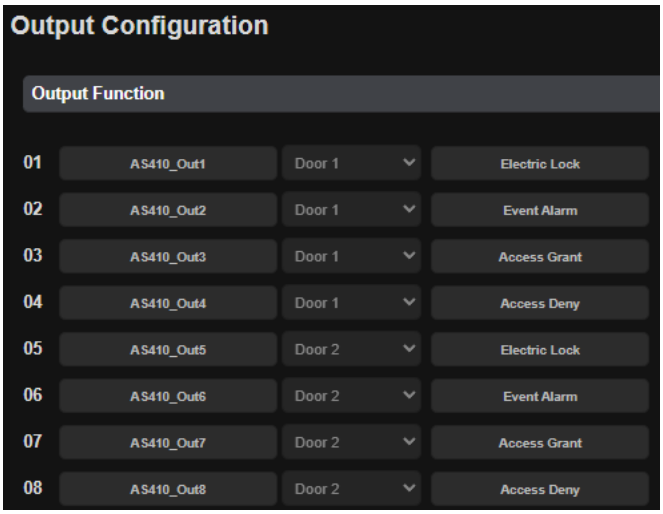
3.2.4 Input Configuration

The Input Configuration page defines the status of input devices connected to the controller. Set the input status to either **NO (normally open)** or **NC (normally close)**.
Up to **16 input devices** are supported, including door contacts, exit buttons, fire sensors, and tamper sensors.



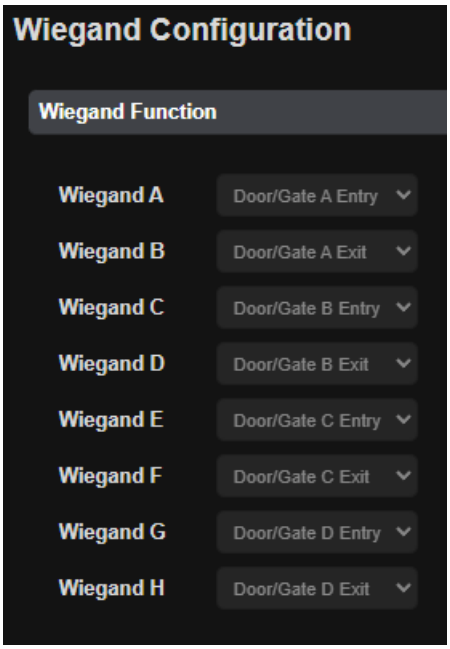
3.2.5 Output Configuration

The Output Configuration page defines the output devices connected to the controller. Up to **16 output devices** are supported for applications such as electric locks, event alarms, access granted, and access defined. **Each output function is predefined and cannot be modified.**



3.2.6 Wiegand Configuration

The controller supports up to **8 Weigand readers**. **Each Wiegand function is predefined and cannot be modified.**



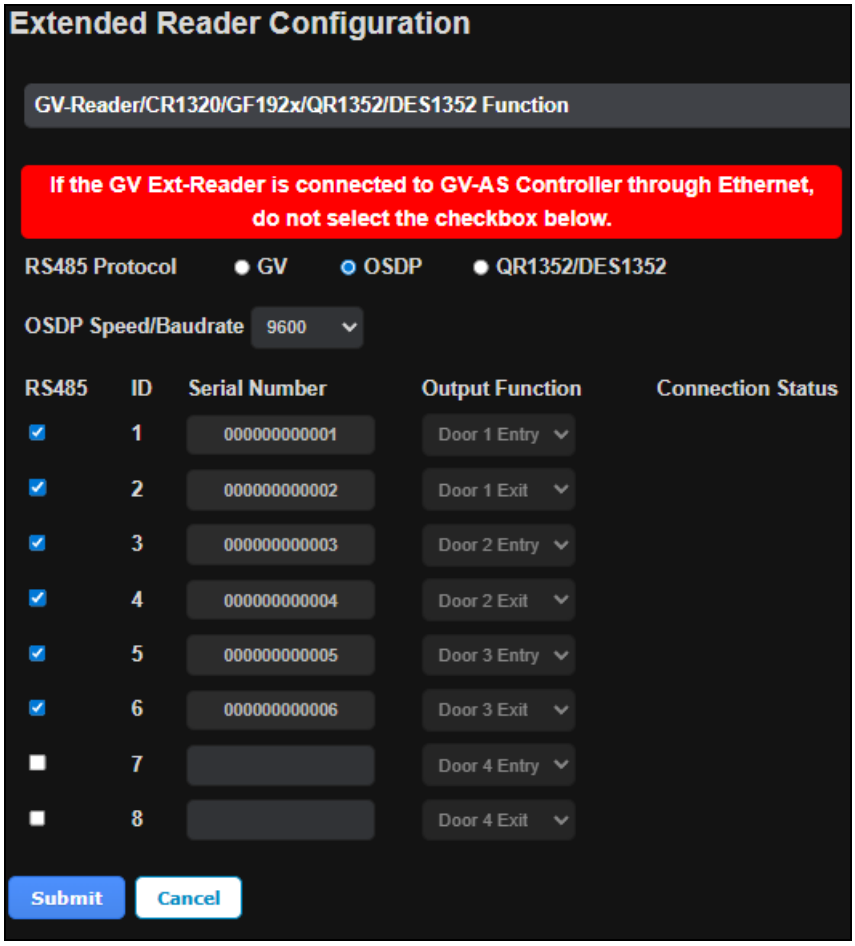
3.2.7 System Log Viewer

The System Log Viewer allows service personnel to export data for troubleshooting and analysis.

3.4 Extended Devices

3.4.1 Extended Reader Configuration

The Extended Reader Configuration page defines the readers connected to the controller via RS-485 or network. **The Output function for each reader is predefined and cannot be modified.**



[Protocol] Select only one of the following reader protocols to connect to GV-AS4110 Cloud: GV, OSDP, and QR1352/DES1352

- **GV:** For the following GeoVision readers, select the **GV** protocol.
  - **GV-RK1352 / R1352 / DFR1352:** Select the **RS-485** checkbox and type the **Serial Number** of the reader.
  - **GV-GF1922 / CR1320 / FR2020:** Type the **MAC address** of the fingerprint reader or the camera and *do not* select the RS-485 checkbox.
- **OSDP:** For OSDP compliant readers, e.g. GV-RKD1352, select the **OSDP** protocol, and select the checkbox before the paired ID No. of the reader (ID #1 ~ #8) to activate it.

- **QR1352/DES1352:** For GV-QR1352 / DES1352 / R1354 reader, select the **QR1352/DES1352** protocol, and select the checkbox before the paired ID No. of the reader (ID #0 ~ #7) to activate it.

Click **Submit**. The green Connection Status indicates the successful connection between the controller and the reader whereas a red status indicates otherwise.

Note: When the RS-485 checkbox is not selected, the Extended Reader Configuration page is used to configure network readers, such as GV-GF1922 / CR1320 / FR2020.

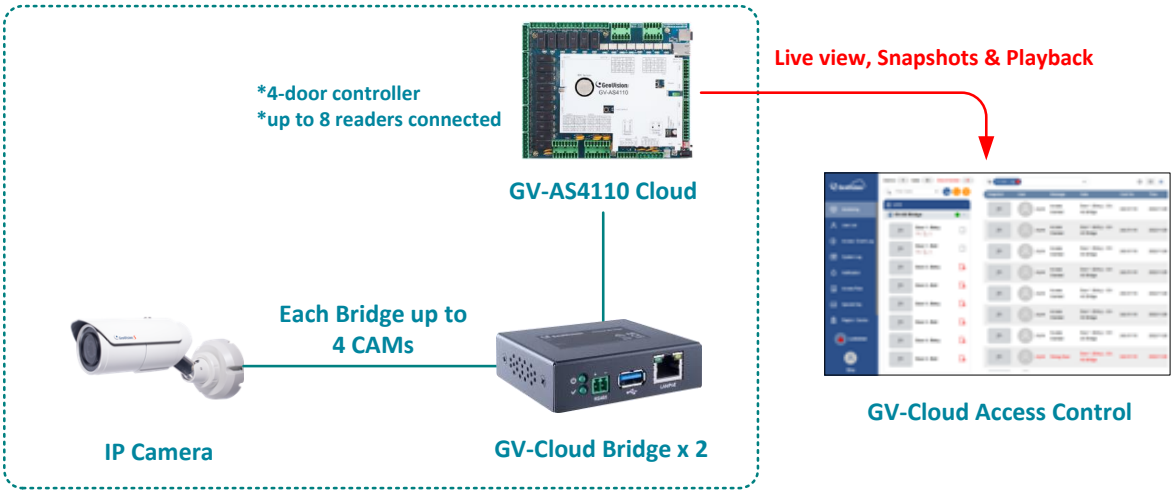
3.4.2 Extended Camera Configuration

By combining a GV-Cloud Bridge with the controller, the **live view**, **snapshots**, and **recordings** of IP cameras installed near readers can be transmitted to the GV-Cloud platform in response to access events.

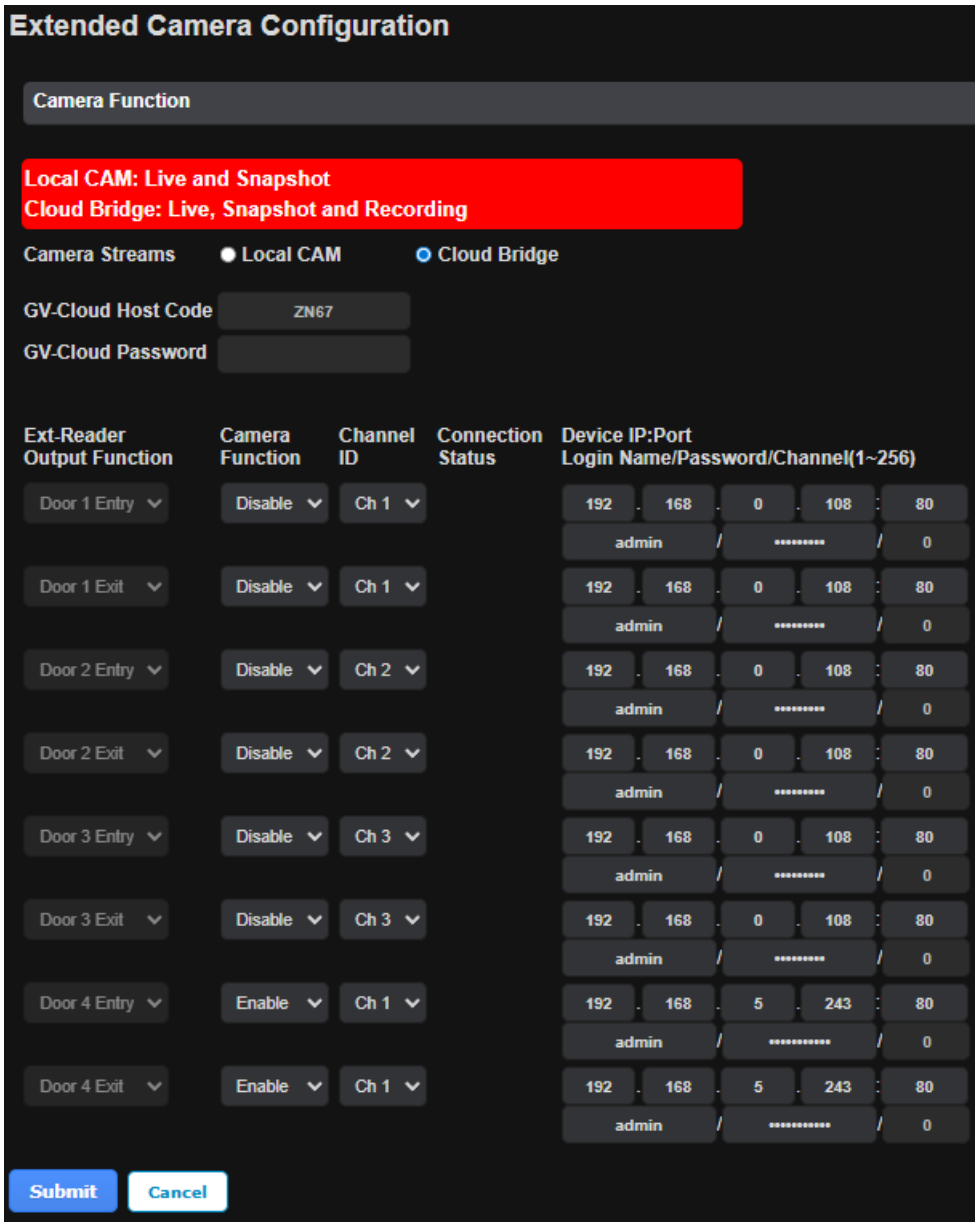
Alternatively, you can connect IP cameras directly to the controller, which will transmit **live video** and **snapshots** to the GV-Cloud platform – recordings are not supported in this setup.

3.4.2.1 Connecting GV-Cloud Bridge to GV-AS4110 Cloud

For entry and exit video monitoring, you can connect up to **8 IP cameras** to the controller using **2 GV-Cloud Bridge units**, as illustrated below.

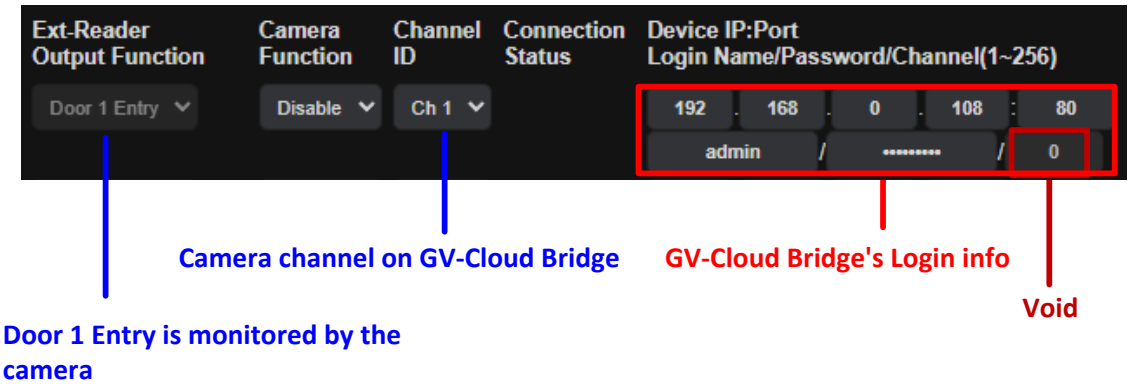


1. In the left menu, click **Extended Camera Configuration**. This page appears.

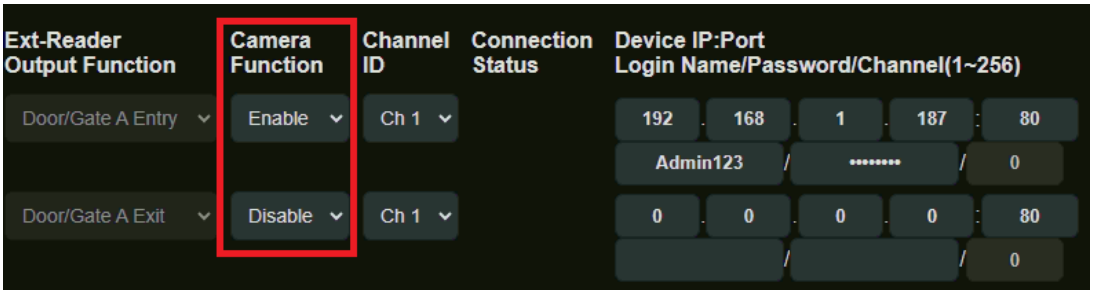


2. Select **Cloud Bridge** from the **Camera Streams** options.

3. Type the GV-Cloud Bridge's IP address, ID and password to log in.



4. Select **Channel ID** (CH1 ~ CH4) corresponding to a camera channel from the GV-Cloud Bridge.
5. Select **Enable** from the **Camera Function** dropdown list to enable snapshots and live views of the camera from the GV-Cloud Bridge.



6. Click **Submit.** The green Connection Status indicates a successful connection between the controller and the IP cameras from the GV-Cloud Bridge, while the red status indicates an unsuccessful connection.

[GV-Cloud Access Control Settings]

In addition to the settings described above in *Connecting GV-Cloud Bridge to the Controller,* the following settings must be completed to gain access to the GV-Cloud platform for not only live view and snapshot but also playback. The entire settings can be found in *6.2 Accessing Playback* in *GV-Cloud Access Control User's Manual*.

6.2.1 Adding a Playback License

6.2.2 Creating a Host on GV-Cloud VMS

6.2.3 Configuring GV-Cloud Bridge and a Controller

6.2.4 Accessing Playback

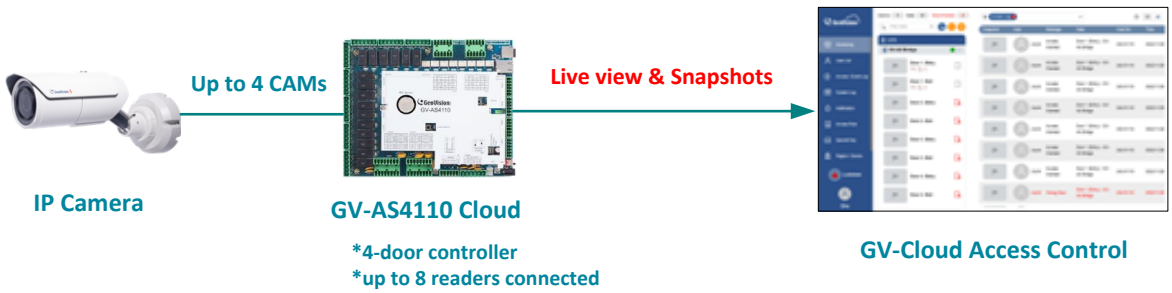
Note:

1. The **GV-Cloud Access Control License** is required for accessing access control activities, event logs, snapshots, and live view on GV-Cloud Access Control.
2. The **Playback License** is required for accessing recordings on the GV-Cloud platform.

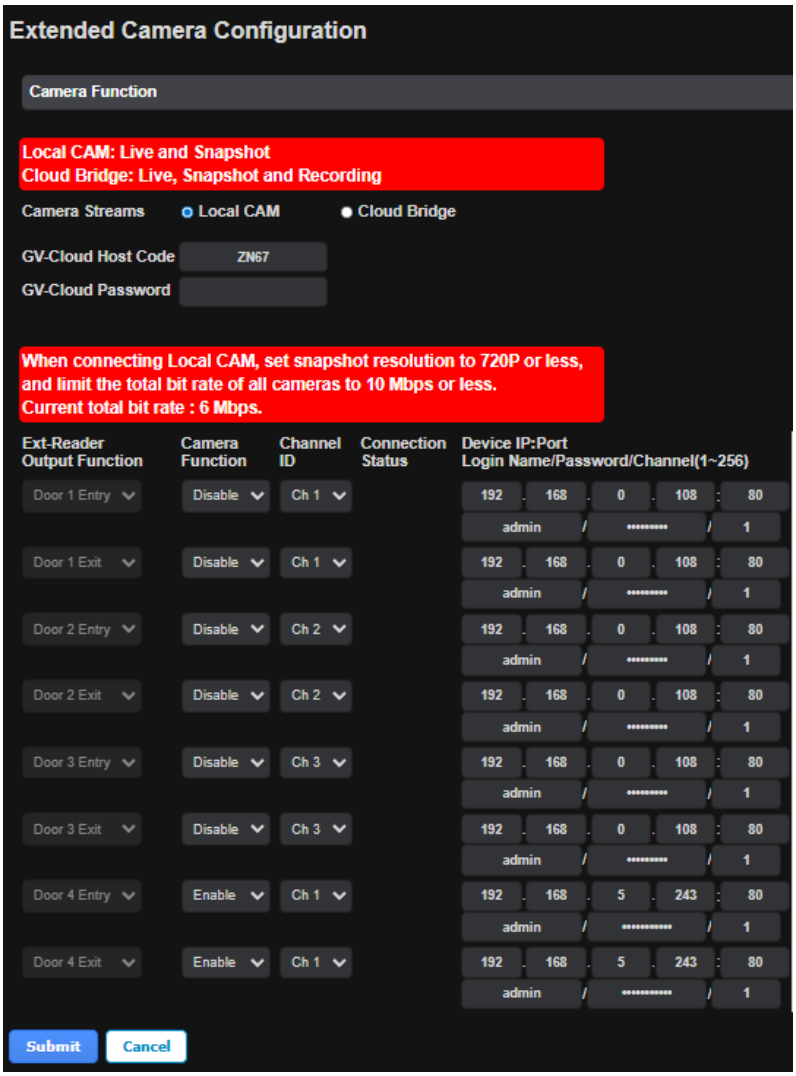
3.4.2.2 Connecting IP Cameras to GV-AS4110 Cloud

For entry and exit video monitoring, connect up to **4 IP cameras** to the GV-Cloud platform via the controller, as illustrated below.

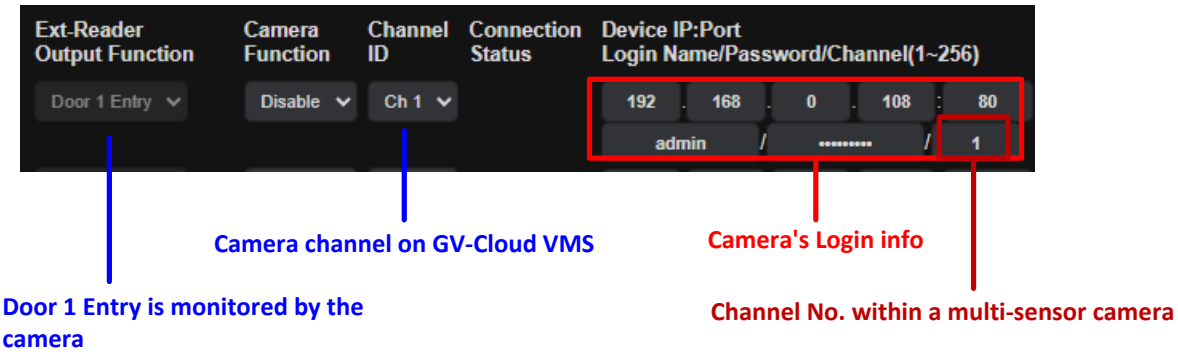
For the integration, it is required to add the controller as a host on the GV-Cloud VMS first. See *6.1.1 Creating a Host on GV-Cloud VMS* in *GV-Cloud Access Control User's Manual*.



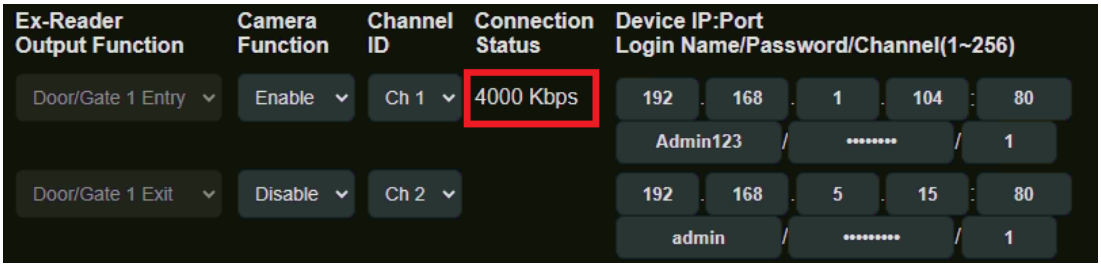
1. In the left menu, click **Extended Camera Configuration**. This page appears.



2. Select **Local CAM** from the **Camera Streams** options.
3. Type **GV-Cloud Host Code** and **Password** created on GV-Cloud VMS.
4. Based on the door being monitoring, type the IP camera's IP address, ID and password to log in. If the camera has multi sensors, specify the channel number of the corresponding sensor.



5. Select **Enable** from the **Camera Function** dropdown list to enable snapshots and live streaming from the camera.
6. Select **Channel ID** (CH1 ~ CH4) corresponding to a camera channel displayed on GV-Cloud VMS. Make sure not to select the same channel ID for different cameras connected to the controller.
7. Click **Submit**. Once the connection between the controller and the camera is successfully built, the bit rate of the camera will be displayed under the **Connection Status** column.



[GV-Cloud Access Control Settings]

In addition to the settings described above in *Connecting IP Cameras to the Controller,* the following settings must be completed to gain access to the GV-Cloud platform for live view and snapshots. The entire settings can be found in *6.1 Receiving Snapshots and Live Streaming* in *GV-Cloud Access Control User's Manual*.

6.1.1 Creating a Host on GV-Cloud VMS

6.1.2 Configuring a Controller

6.1.3 Viewing Live Stream

Note:

1. Before connecting a local IP camera to the controller, make sure to set the camera's resolution to 720P or below, and limit the total bit rate of all cameras to 10 Mbps or less.
2. If a green status icon does not appear beside GV-Cloud Host Code, make sure the Host Code and Password are consistent with those created on GV-Cloud VMS.
3. The **GV-Cloud Access Control License** is required for accessing access control activities, event logs, live view, and snapshots on GV-Cloud Access Control.