Grandstream Networks, Inc.

GDS3710

Hemispheric HD IP Video Door System

User Manual

COPYRIGHT

The latest electronic version of this user manual is available for download here:
http://www.grandstream.com/support

CAUTION

Changes or modifications to this product not expressly approved by Grandstream, or operation of this product in any way other than as detailed by this User Manual, could void your manufacturer warranty.

WARNING

Please do not use a different power adaptor with your devices as it may cause damage to the products and void the manufacturer warranty.

FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) The device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Important: Any changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Declaration of Conformity

This transmitter complies with the essential requirements and provisions of directives 2014/53/EU, 2014/30/EU, 2015/35/EU and subsequent amendments, according to standards

ETSI EN 300 330 V2.1.1 (2017-02);
ETSI EN 301 489-1 V2.1.1 (2017-02); ETSI EN 301 489-3 V2.1.1 (2017-03);
EN 60950-1: 2006+A11:2009+A1:2010+A12:2011+A2:2013: EN 62311: 2008

CE

Manufacturer:
Grandstream Networks, Inc.
126 Brookline Ave, 3rd Floor Boston, MA 02215, USA

Channel Frequency:	125 KHz
Channel Number:	1
Antenna Type / Gain:	Internal
Type of Modulation:	ASK
Operation temperature:	-30 °C ~ +60 °C
Storage temperature:	-35 °C ~ +60 °C
Humidity:	10 ~ 90% non-condensing

GNU GPL INFORMATION

GDS3710 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from: http://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download

Table of Contents

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes the basic concept and tasks necessary to use and configure your GDS3710. And it covers the topic of connecting and configuring the GDS3710, making basic operations and the call features. Please visit http://www.grandstream.com/support to download the latest "GDS3710 User Manual".

This guide covers following topics:

CHANGE LOG

This section documents significant changes from previous versions of user manual for GDS3710. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.3.34

- Added support for video live view on Chrome/Firefox with no Plugin required. [Live View Page]
- Added option to send Snapshot via Email when doorbell pressed. [Snapshot when Doorbell Pressed]
- Added RTCP/RTCP-XR for SIP Call to meet Cloud Solution Service Provider. [Enable RTCP]
- Added alarm notification of non-scheduled access users. [Non-Scheduled Access Alarm]
- Added Keep Door Open section. [Keep Door Open]
- Added MJPEG Authentication Mode. [MJPEG Authentication Mode] [Live View Page]

Firmware Version 1.0.3.32

- Added LED lighting indication pattern for firmware upgrade process. [Upgrade]
- Increased the maximum allowed whitelist numbers to 30 records with 20-digit length for each number [White List]
- Added Support for HTTP command to Open Door. [Enable HTTP API Remote Open Door]
- Added display device logs at GDS web UI. [Event Log]
- Added valid start/end dates for Card Management. [Card Management]
- Added “Test” button for Alarm Action. [Alarm Action]
- Added “Alarm IN/OUT Status” display at GDS “Status” page UI. [System Info]
- Added Self-defined Even Notification Message. [Event Notification]

Firmware Version 1.0.3.31

- Added ability to upload Trusted CA certificate files. [Trusted CA Certificates]
- Added support for multi-channel call mode. [Enable Multi-channel Call Mode]
- Added option to enable/disable certificate validation. [Validate Server Certificate]

Firmware Version 1.0.3.23

- Added Standard Mode and Broadsoft Mode in SIP Settings, Broadsoft Supported. [Special Feature]
- Added card ID number and phone number reported in event log message. [Event Notification]
- Added “Click-to-Dial” feature support. [Click-To-Dial]

Firmware Version 1.0.3.13

- Added option to disable alarm sound at phone side when event trigger SIP call to the phone [Special Feature].
- Increased maximum characters to 256 in “Number called when doorbell pressed” to allow serial hunting of SIP extensions or IP address with port or mixing of both, with each ring several seconds before going next [Number Called When Door Bell Pressed].
- Added feature to capture snapshot when doorbell pressed [Snapshot when Doorbell Pressed].
- Added feature to disable keypad input (lock keypad) and ONLY doorbell button can be pressed [Disable Keypad (except the Doorbell Button)].
- Added option to disconnect call automatically after door open event [Enable On Hook After Remote Unlock].
- Added timer to expire Card Issuing Mode automatically [Card issuing State Expire Time(m)].
- Added ability for whitelist entries to open door using remote PIN [White List].

Firmware Version 1.0.2.25

- Added if schedule disabled, GDS3710 will bypass the option to open door [Group overrides Schedule].
- Implemented the HTTP Upload (RFID card) Log Event support for 3rd party Software Integration [Event Notification].

Firmware Version 1.0.2.22

- No major changes.

Firmware Version 1.0.2.21

- Allow config and call IP address format on SIP field when dialing the Virtual Number. [SIP Number]
- Added “Silent Alarm” Mode. [Silently Alarm Mode]
- Added option Backup/Restore including all passwords like SIP/FTP/Remote Access, etc. [Data Maintenance]
- Added schedule support for Card and PIN. [Schedule]
- Added LLDP support. [Enable LLDP]
- Added database automatic backup and synchronization.
- Modified WebGUI style.
- Added card information batch delete option in the WebGUI. [Users Operation]
- Added option to enable “Motion Detection”, “Tamper Alarm” and backlight partially light. [Tamper Alarm] [Motion Detection] [Enable Background Light]
- Added card user limitation up to 2000 and group limit to 50. [Card Management][Group]
- Added Card and PIN schedule configuration Central Mode. [Central Mode]
- Added LDC Ratio Control and Adjustment. [LDC Ratio]
- Expended the range of Ring timeout. [Ring Timeout(s)]

- Added option to disable Auto Answer. [Auto Answer]
- Updated the “DingDong” tone when doorbell pressed.
- Added function to check the default value.
- Added Factory Reset via special procedures. [Hard Factory Reset]
- Added file upload and download (card information, configuration etc.) can be executed after authentication. [Card Management]
- Added enforcement that when admin password is changed via WebGUI, user has to fill in a Valid Email Account to retrieve the email before the new admin password taking effect. [User Management]

Firmware Version 1.0.2.13

- Added support of ONVIF Profile S
- Added “Privacy Mask” support in Motion Detection Setting. [Privacy Masks]
- Updated OCX plugin engine to Version 3.1.0.74
- Added DTMF Open Door control option in WebGUI [Enable DTMF Open Door]
- Added HTTP API support [GDS3710 HTTP API].
- Optimized HTTP API for Card Management.
- Added “Enable Blue Doorbell Light” option in the webGUI. [Enable Blue Light]
- Added switch on the doorbell blue light by configured time period of the day. [Enable Blue Light]
- Implemented “Silent Alarm” mode. [Silently Alarm Mode]

Firmware Version 1.0.2.9

- Added back DTMF Open Door as optional choice, with user acknowledging the security risk. [Enable DTMF Open Door]
- Revised “Alarm Output Duration(s)” choice option as 5/10/15/20/25/30 seconds. [Alarm Output Duration(s)]

Firmware Version 1.0.2.5

- Added folder creation and file arrangement if multiple GDS3710s are uploading snapshots to FTP server.
- Improved the password prompt wording.
- Added DTMF audio playing when key be pressed. [Key Tone Type]
- Separated volume control under Web GUI -> Audio Settings. [System Volume][Doorbell Volume]
- Added “Audio, Snapshot, Recording and File Path Saved” operation with icons at Live View webpage. [Live View Page]
- Added “show password” feature when the eye icon be clicked in the webGUI.
- Added prompt popup message when capture button clicked.
- Use different email title to separate the Motion Detection and Temperature Out of the Range alarm.
- Set initial value of “0” for Virtual Number and SIP number if user leaving the field empty. [Virtual Number][SIP Number]

- Added support open door remotely via GDS Manager utility (after GDS Manager version 1.0.0.78)
- Supported GXP color phone JPEG_Over_HTTP with encryption and authentication. This feature is pending on GXP/UCM6xxx firmware availability. Currently this feature does not support 3rd party PBX if SIP extension is used in Open Door configuration.
- Added SSH support with default TCP port 22. [SSH][SSH Port]
- Added GS_Wave (Android/iOS) Application support for Open Door. [CONNECTING GS WAVE WITH GDS3710 DOOR SYSTEM].
- Enhanced webGUI login process and added random default password.
- Enhance security by disable the DTMF to open door
- Added support of sending DTMF tone in SIP calling (RFC2833, SIP INFO). [Enable DTMF]

Firmware Version 1.0.1.19

- This is the initial version for GDS3710.

WELCOME

Thank you for purchasing Grandstream GDS3710 Hemispheric HD IP Video Door System, an innovative IP based powerful video door system.

GDS3710 HD IP Video Door System is a hemispheric IP video door phone with an integrated high-definition IP surveillance camera. GDS3710 is ideal for monitoring from wall to wall without blind spots. Powered by an advanced Image Sensor Processor (ISP) and state of the art image algorithms, it delivers exceptional performance in all lighting conditions. The GDS3710 IP video door system features industry-leading SIP/VoIP for 2-way audio and video streaming to smart phones and SIP phones. It contains integrated PoE, LEDs, HD loudspeaker, RFID card reader, motion detector, lighting control switch and more.

GDS3710 HD IP Video Door System can be managed by Grandstream's free windows-based management software: GDS Manager is a client/server based software which provided RFID card management and basic reports for the door entrance.

Along with Grandstream videophone, mobile Apps, and Network Video Recorder (NVR), the GDS3710 provides a powerful recording and monitoring solution. It can be managed with GSURF Pro or any ONVIF-compliant video management system. It also offers a flexible HTTP API for easy integration with 3rd party applications and other surveillance systems.

GDS3710 is ideal for entry places requiring a wide-angle monitoring, such as banks, hotels, schools, office buildings, retail stores and small warehouses, and for most small to medium sized enclosed environments.

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the GDS3710.

Table 1: GDS3710 Features in a Glance

- High-performance streaming server allowing multiple simultaneous streaming session accesses.
- 2 Megapixel Progressive Scan CMOS, 1920H x 1080V.
- Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
- 2 Channels Input/Output alarm.
- RS485, Wiegand (26 bits) Input and Output.
- RFID card reader.
- Weather proof, vandal resistant.

Technical Specifications

The following table resumes all the technical specifications including the protocols / standards supported, voice codecs, telephony features and upgrade/provisioning settings for GDS3710.

Table 2: GDS3710 Technical Specifications

Video Compression	H.264 High Profile / Main Profile / Base Profile, Motion JPEG.
Image Sensor Resolution	1/2.7”, 2 Megapixel, 1920H x 1080V.
Lens Type	1/2”, F2.5, FOV: 180°(W) x 150°(H).
Day & Night Mode	White LEDs with smart brightness control.
Max Video Resolution	1920x1080.
Max Frame Rate	30 frames per second.
Minimum Illumination	0.5Lux.
Wide Dynamic Range	Yes, up to 120dB.
Embedded Analytics	Motion detection.

Snapshots	Triggered upon events, sent via email and/or FTP.
Multi-stream Resolution	High-performance streaming server allowing multiple simultaneous accesses: • **Primary video stream**: 1920 x 1080 resolution for continuous full HD recording. • **Secondary video stream**: 640 x 480 resolution for SIP/VoIP video calls. • **Third video stream**: 320 x 240 resolution for smartphone Apps.
Network Protocols	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS local upload and mass provisioning using TR-069 (pending), ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP.
SIP/VoIP Support	Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
Voice Codecs	G.711μ/a-law, G.722, in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO), AEC.
QoS	Layer 2 QoS (802.1Q, 802.1P) and Layer 3 QoS (ToS, DiffServ, MPLS).
Security	User and administrator level access control (pending), MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
Upgrade / Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 (Pending) or AES encrypted XML configuration file.
Audio Input	Built-in Digital Microphone, up to 1.5m with AEC.
Audio Output	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.
Keypad / Buttons	12-key touchpad plus a capacitive doorbell button, each with individual LED illumination.
RFID	125KHz: EM4100 (1 RFID card and 1 RFID key fob included).
Alarm Input	Yes, 2 channels, Vin < 15V, for door sensor or other devices.
Alarm Output	Yes, 2 channels, 125VAC/0.5A, 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch or other devices.
Network Interface	10M/100M auto-sensing.
Expansion Interface	RS485, Wiegand (26 bits) input and output.
Dimensions and Weight	173mm(H) x 80mm(W) x 36mm(D). 0.6 Kg.
Power Supply	PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).
Interoperability	ONVIF (Profile S).
Ingress Protection	Weather proof, vandal resistant, with support for extra back reinforcing metal plate
Temperature and	Operation: -30°C to 60°C (-22°F to 140°F)

Humidity	Storage: -35°C to 60°C (-31°F to 140°F) Humidity: 10% to 90% Non-condensing
Protection Class	IP66 (EN60529), IK09 (IEC62262).
Compliance	**FCC:** Part 15 subpart B Class B; Part 15 C; MPE **CE:** EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311 **RCM:** AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1 **IC:** ICES-003; RSS310

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and information for obtaining the best performance using the GDS3710 Video Door System.

Equipment Packaging

Table 3: Equipment Packaging

• 1 x GDS3710 • 1 x Installation Bracket • 1 x Drilling Template • 1 x Protecting Cap • 3 x Rubber Gaskets (for sealing the back cable) • 6 x Back Panel Screws • 6 x Bracket Screws and Anchors • 4 x Anti-tamper screws • 1 x Anti-Tamper Hex Key	• 1 x Wiegand Cable • 1 x Lens Cleaning Cloth • 1 x RFID Card (more can be purchased from Partner/reseller) • 1 x Key Fob (more can be purchased from Partner/reseller) • 1 x Frame Back Cover • 1 x Quick Installation Guide • 1 x GPL License

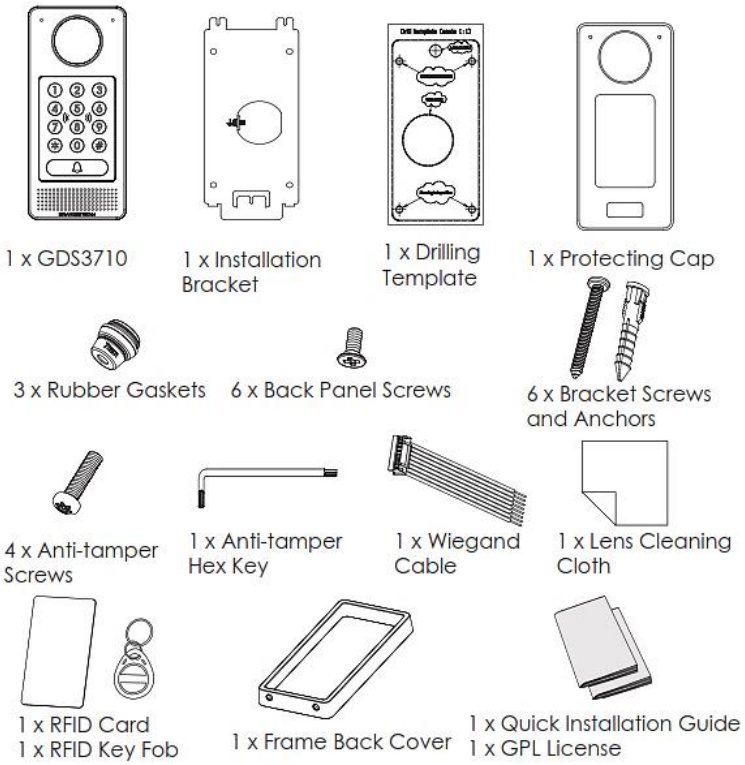


Figure 1: GDS3710 Package

Note: Check the package before installation. If you find anything missing, contact your system administrator

Description of the GDS3710

Below figures show the component of the back and front view of GDS3710 IP Video Door System:

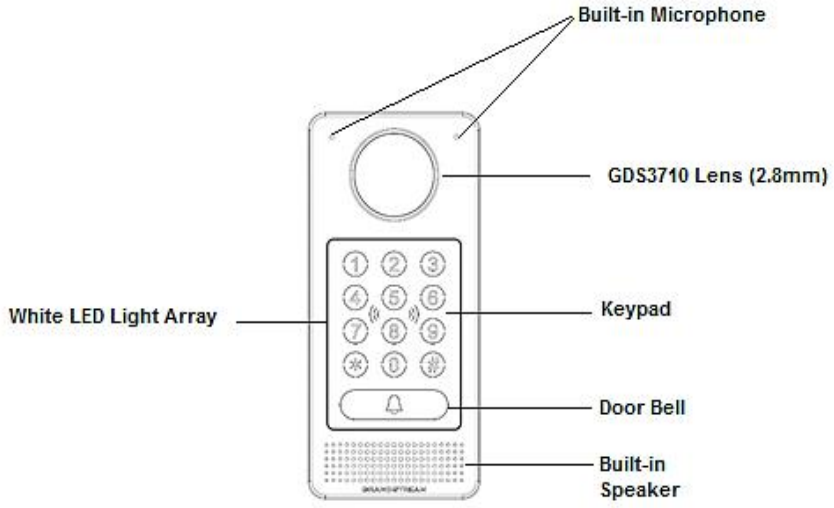


Figure 2: GDS3710 Front View

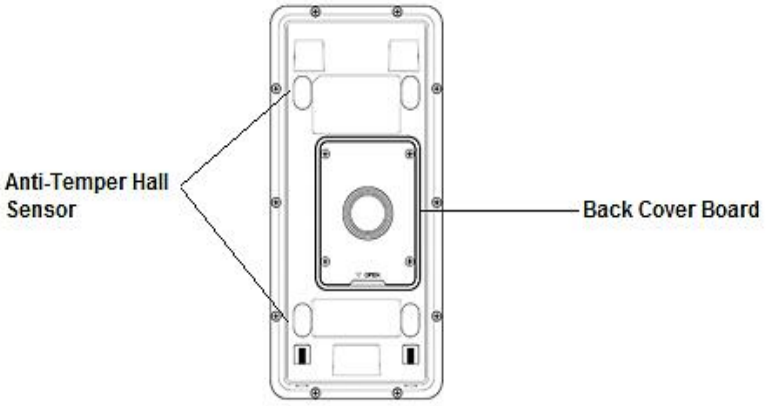


Figure 3: GDS3710 Back View

Connecting and Setting up the GDS3710

The GDS3710 can be powered using PoE or PSU:

Using PoE as power supply (Suggested)

- Connect the other end of the RJ45 cable to the PoE switch.
- PoE injector can be used if PoE switch is not available.

Using the power adapter as power supply (PSU not provided)

- Connect the other end of the RJ45 cable to network switch or router.
- Connect DC 12V power source via related cable to the corrected PIN of the GDS3710.

GDS3710 Wiring Connection

Table 4: GDS3710 Wiring Connection

Jack	Signal	Function	Note	
J2 (Basic) 3.81mm	TX+	Ethernet PoE 802.3af Class 3, 12.95W	Orange / White	Data
	TX-		Orange	
	RX+		Green / White	
	RX-		Green	
	PoE_SP2		Blue + Blue/White	Please twist these two wires together and connect to SP1, SP2 respectively even the PoE NOT used.
	PoE_SP1		Brown + Brown/White	
	RS485_B	RS485		
	RS485_A			
	GND	Power Supply	**DC 12V, 1A Minimum**	
	12V			
J3 (Advanced) 3.81mm	GND	Alarm GND		
	ALARM1_IN+	Alarm In	Vin<15V	
	ALARM1_IN-			
	ALARM2_IN+			
	ALARM2_IN-			
	NO1	Alarm Out	Relay: 30VDC/2A; 125VAC/0.5A	
	COM1			
	NO2	Electric Lock	For "**Fail Secure**" (Locked when Power Lost) Strike, connect **COM2 & NO2**. For "**Fail Safe**" (Open when No Power) Magnetic Lock, connect **COM2 & NC2**. **Relay: 30VDC/2A; 125VAC/0.5A**	
	COM2			
	NC2			
J4 (Special) 2.0mm	GND	Wiegand Power GND	Black	Both Input and Output MUST be connected
	WG_D1_OUT	Wiegand Output Signal	Orange	GDS3710 function as Output of Card Reader, Connect Pin 1, 2, 3
	WG_D0_OUT		Brown	
	LED	Wiegand Output LED Signal	Blue	For External Card Reader; Or GDS3710 as Receiver Only
	WG_D1_IN	Wiegand Input Signal	White	For External Card Reader Connect Pin 1,4,5,6,7,8
	WG_D0_IN		Green	
	BEEP	Wiegand Output BEEP Signal	Yellow	For External Reader Only
	5V	Wiegand Power Output	Red	For External Card Reader Only. 12VDC powered External Card Reader must use own power source, can NOT use this Pin.

GDS3710 Back Cover Connections

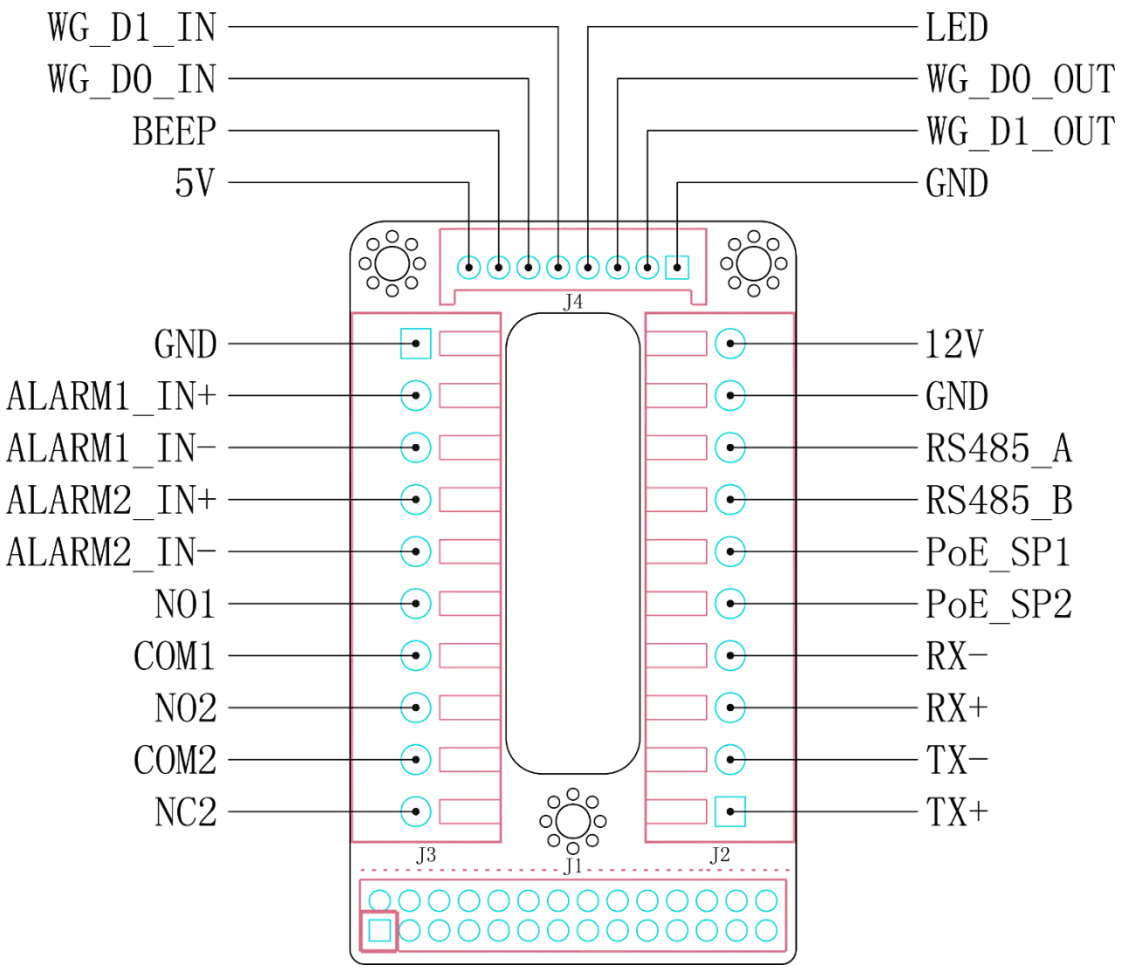


Figure 4: GDS3710 Back Cover Connections

Connection Example

To connect the GDS either by using PoE or PSU follow steps below:

- Open the Back-Cover Board of the GDS3710 which should look like following figure.

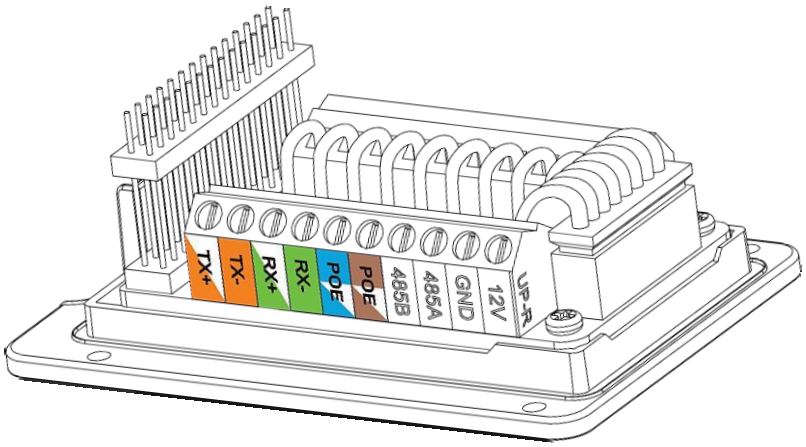


Figure 5: GDS3710 Back Cover

Power the unit using PoE

- Cut into the plastic sheath of your Ethernet cable, then Unwind and pair as shown below.
  Use the TIA/EIA 568-B standard, which define pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity.

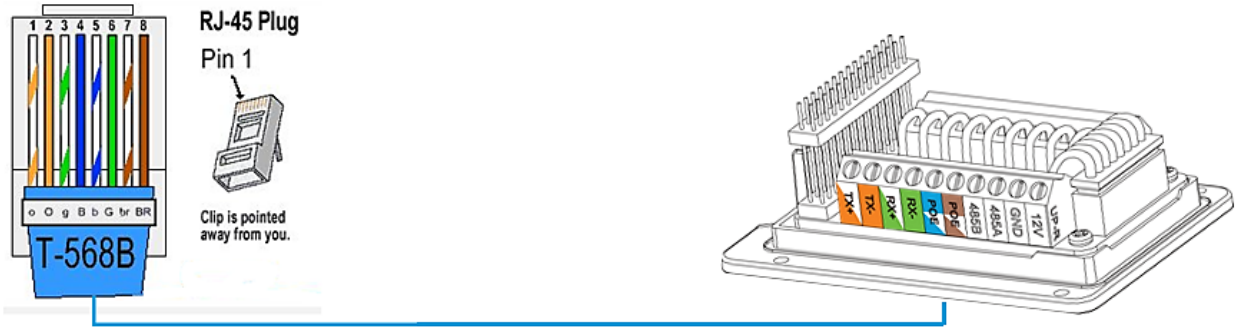


Figure 6: Connection Example

- Connect each wire of the cable to its associate on the Back Cover of the GDS3710 to power the unit using PoE.

Power the unit using PSU

- To power the unit using PSU, use a multimeter to detect the polarity of your Power Supply, then connect GND to negative pole and 12V to positive pole of the PSU.

Note: If the user doesn't have PoE switch, there is no need to connect the Blue and Brown wires to the GDS3710 since these wires are used to power the unit via Ethernet.

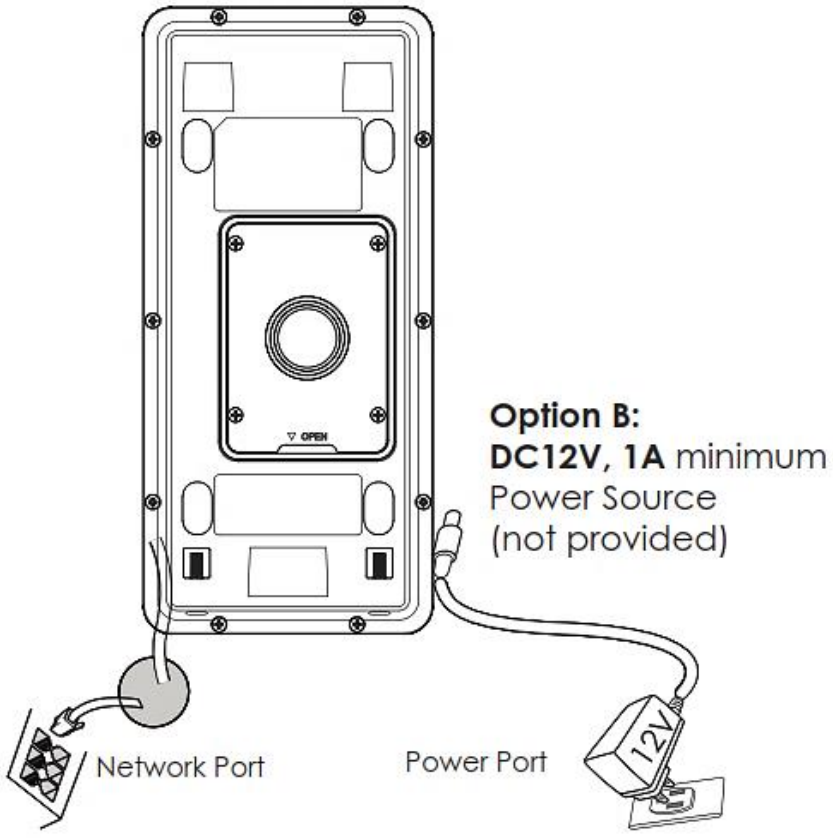


Figure 7: Powering the GDS3710

GETTING TO KNOW GDS3710

The GDS3710 has an embedded Web server to respond to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the GDS3710 through Microsoft Internet Explorer or Mozilla Firefox.

Download WebControl Plug-in from the GDS3710 WebGUI. For Apple platform OS-X, only MJPEG video codec supported currently.

Notes:

- Please disable temporarily the Antivirus or Internet Security Software when download and install the Grandstream WebControl Plug-in for Firefox/Chrome or "GSViewerX.cab" for Microsoft Internet Explorer. Please close Browser to install the downloaded Plug-in or Active-X.
- Please trust and install the file downloaded if prompted by the Antivirus or Security software.

Connecting GDS3710 to Network with DHCP Server

The GDS3710 by default has a DHCP client enabled, it will automatically get IP address from DHCP server.

Windows Platform

Two ways exist for Windows user to get access to the GDS3710:

UPnP

By default, the GDS3710 has the UPnP feature turned ON. For customers using Windows network with UPnP turned on (most SOHO routers support UPnP), it is very easy to access the GDS3710:

1. Find the "Network" icon 

on the windows Desktop.
2. Click the icon to get into the "Network", the GDS3710s will list as "Other Devices" shown like below. Refresh the pages if nothing displayed. Otherwise, the UPnP may not be active in the network.

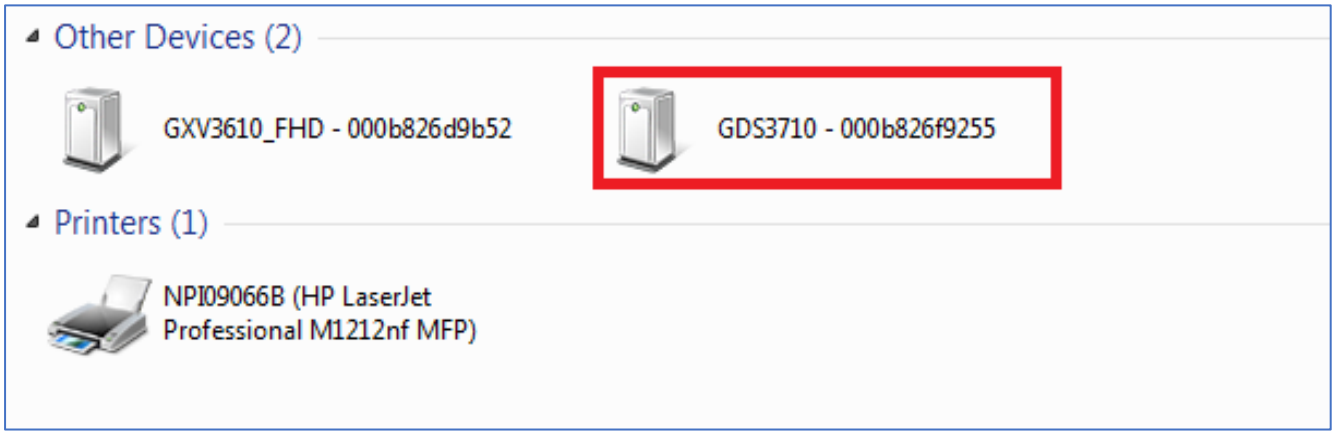


Figure 8: Detecting GDS3710 via UPnP

3. Click on the displayed icon of related GDS3710, the default browser (e.g.: Internet Explorer, Firefox or Chrome) will open and connect directly to the login webpage.

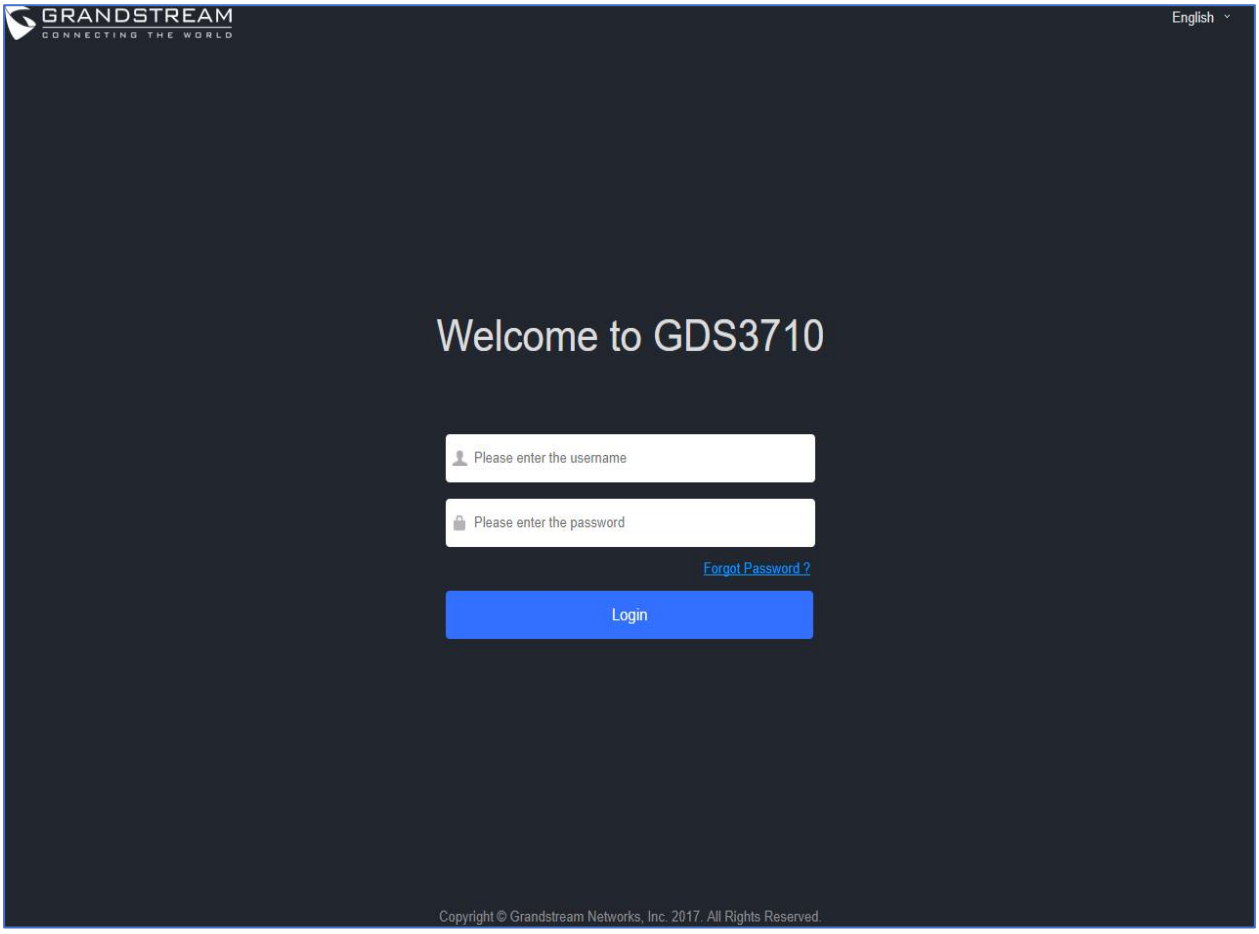


Figure 9: GDS3710 Login Page

4. Once logged in, the prompt message will display asking for plug-in installation.
5. Disable security or antivirus software, download and install the plug-in, close and open the browser again, the embedded video will be displayed if clicking the “LiveView” and pressing the stream number.

GS Search

GS search is a program that is used to detect and capture the IP address of Grandstream devices, below are instructions for using the “GS Search” utility tool:

1. Download the GS Search utility tool from Grandstream website using the following link: http://www.grandstream.com/sites/default/files/Resources/GS_Search.zip
2. Double click on the downloaded file and the search window will appear.
3. Click on 

button to start the discovery for Grandstream devices.
4. The detected devices will appear in the output field like below.

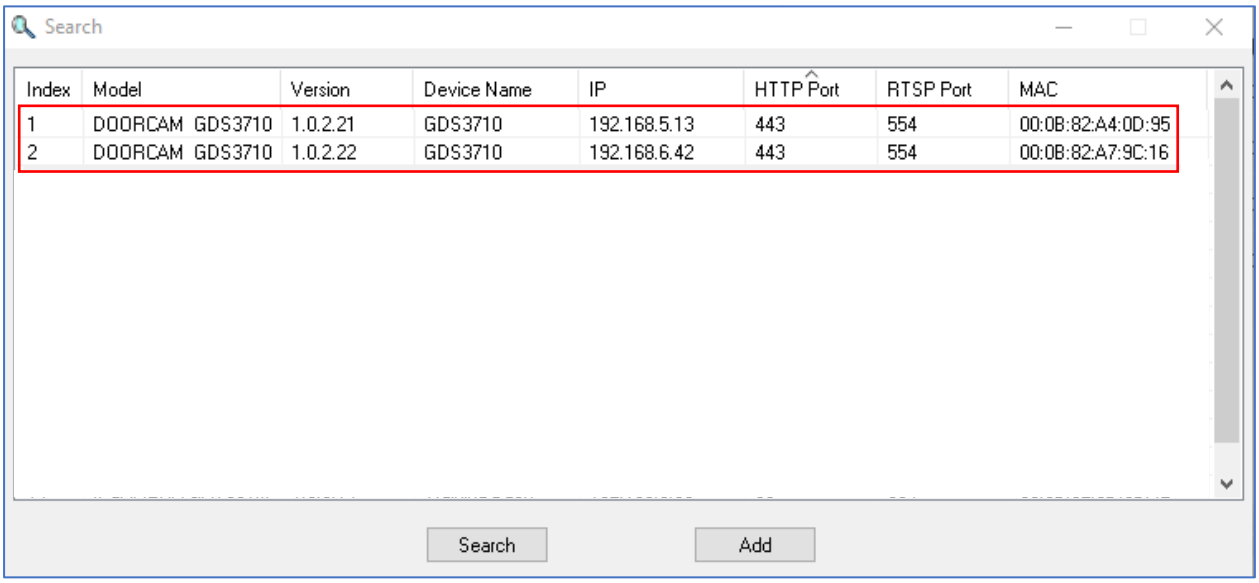


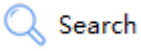
Figure 10: GS Search Discovery

5. Double click on a device to access its webGUI.

GDS Manager Utility Tool

User can know the IP address assigned to the GDS3710 from DHCP server log or using the Grandstream GDS Manager after installing this free utility tool provided by Grandstream. User can find instructions below, for using "GDS Manager" utility tool:

1. Download the GDS Manager utility tool from Grandstream website using the following link: http://www.grandstream.com/sites/default/files/Resources/gdsmanager.zip
2. Install and run the Grandstream GDS Manager, a client/server architecture application, the server should be running first, then GDSManager (client) later:

3. On the GDS Manager access to Device → Search and Click on the 

button to start device detection
4. The detected devices will appear in the output field like below:

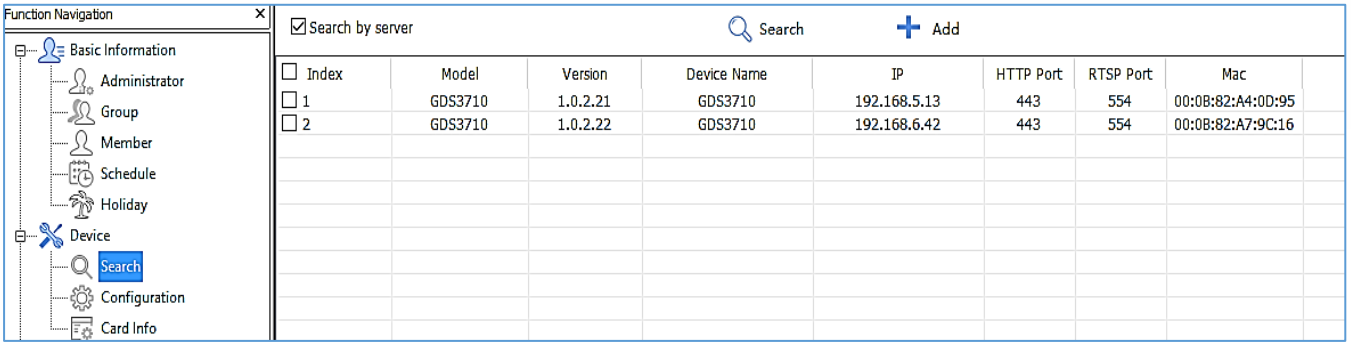


Figure 11: GDS3710 Detection

5. Double click the column of the detected GDS3710, the browser will automatically open and show the device's web configuration page.
6. The browser will ask for plug-in if not installed, please authorize the installation of the plug-in.
7. Enter the administrator user name and password to access the Web Configuration Interface, the default admin username is "**admin**" and the default random password can be found at the sticker on the GDS3710.
8. The plug-in can be downloaded from the GDS3710 Web GUI.

Apple Platform

For Apple users, please turn on Bonjour of Safari to find and access the GDS3710.

1. Open Safari, select "Advanced" to open the Advanced Setting.
2. Click "Include Bonjour in the Bookmarks menu" and "Include Bonjour in the Favorites bar" then close the setting page and back to Safari.

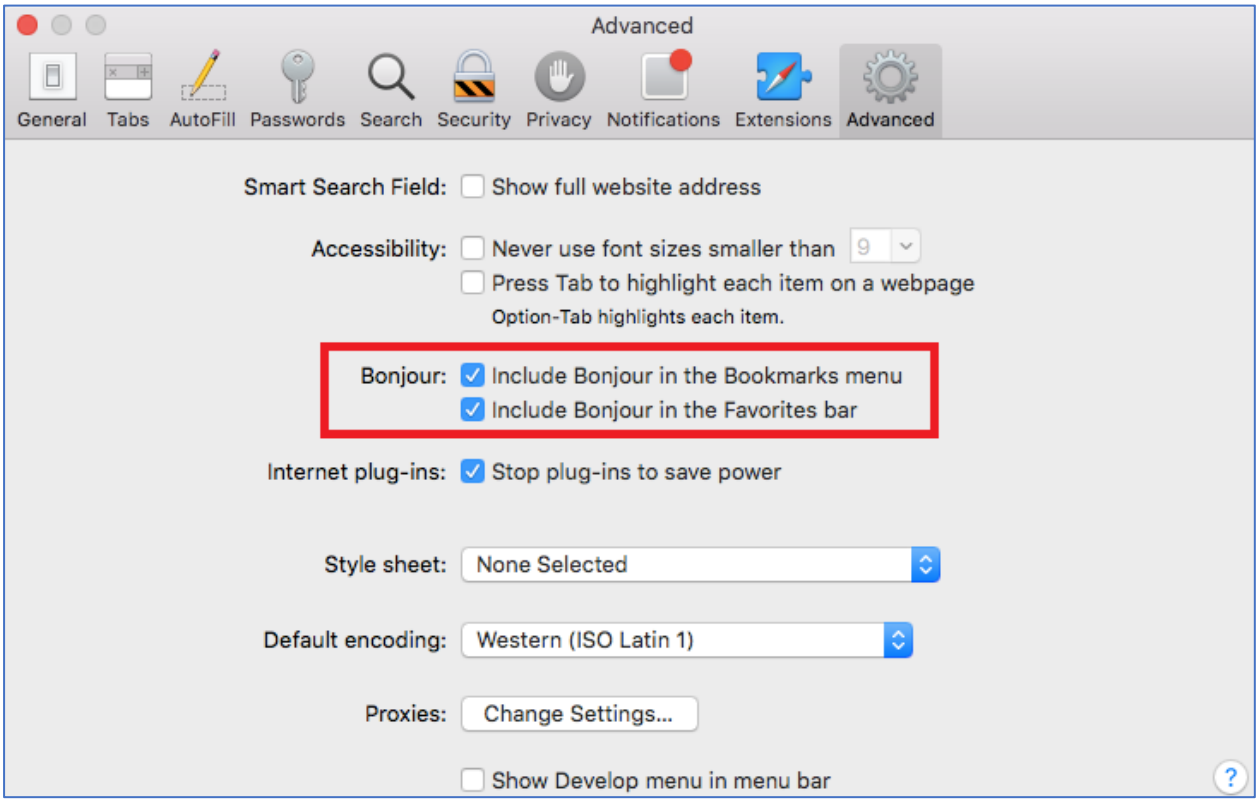


Figure 12: Apple Safari Settings Page

3. Bonjour will now display embedded at Safari. Select “Bonjour” pull-down menu and select “Webpages”, the related device like GDS3710 will be there.

Figure 13: Bonjour Setting Page

4. Click on the displayed GDS3710 to access to the configuration page of the GDS3710.
5. To see the MJPEG video stream, users should type in the browser the following URL while specifying the correct protocol (either HTTP or HTTPs and the correct port number) : http(s)://IP_address_GDS:Port/jpeg/mjpeg.html

Notes:

- The instructions provided above are based on Safari/OS-X, other Apple platform like iOS (iPhone/iPad) can use similar method.

- iPhone/iPad (iOS) users are recommended to use Applications in Apple Store.
- Free or Paid applications from Apple Store like “IP Cam Viewer” is suggested and verified working with Grandstream GDS3710.
- Apple Store applications like “IP Cam Viewer” will support H.264 video codec.

Connect to the GDS3710 using Static IP

If there is no DHCP server in the network, or the GDS3710 does not get IP from DHCP server, user can connect the GDS3710 to a computer directly, using static IP to configure the GDS3710.

1. The default IP, if no DHCP server, or DHCP request times out (after 3 minutes), is **192.168.1.168**
2. Connect the Ethernet cable from GDS3710 to the computer network port directly.
3. Configure the computer using Static IP: 192.168.1.XXX (1<XXX<255, except for 168) and configure the “Subnet mask” to “255.255.255.0”. Leave the “Default Gateway” to “Blank” like below:

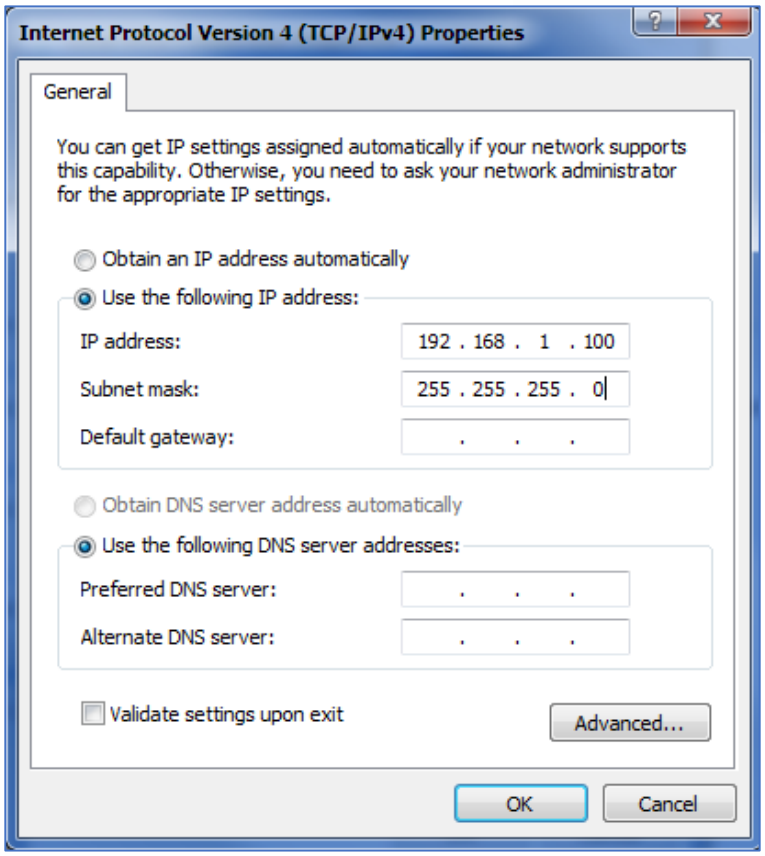


Figure 14: Static IP on Windows

4. Power on the GDS3710, using PoE injector or external DC power.

5. Enter 192.168.1.168 in the address bar of the browser, log in to the device with admin credentials. the default admin username is "**admin**" and the default random password can be found at the sticker on the GDS3710.

6. The browser will ask for plug-in or ActiveX if not installed, otherwise it will get to Home page and show web interface of GDS3710.

7. Access the Web Configuration Interface. Internet Explorer will indicate that "This website wants to install the following add-on: GSViewerX.cab from Grandstream Networks Inc.", allow the installation.

Note: Please disable temporarily Antivirus or Internet Security Software and close all browsers when download and install the Grandstream Plug-in Software.

GDS3710 APPLICATION SCENARIOS

The GDS3710 Door System can be used in different scenarios.

Peering Mode without SIP Server

For environment like remote warehouse/storage, grocery store, small (take-out) restaurants, just using static IP with PoE switch to form a LAN, using Grandstream's video phone GXV3240 or GXV3275, the GDS3710 will meet your very basic intercom, open door and surveillance requirement.

This is the solution to upgrade the traditional analogue Intercom and CCTV security system. All you need is a Power source, Switch or PoE Switch and Grandstream GXV3240 or GXV3275 video phones.

The equipment list can be found below:

- GDS3710
- GXV3240 or GXV3275
- PoE Switch with related Cat5e/Cat6 wiring

Peering using SIP Server (UCM6XXX)

For large deployment, multiple GDS3710 might be required, peered connection will not work in such case due to multiple connections. Such scenarios require an IPPBX or a SIP Proxy to accomplish the tasks.

If remote access is required, a router with internet access should be added to below needed equipment list:

- Several GDS3710
- UCM6XXX or another SIP Server
- GXV3240 or GXV3275 Video Phones
- PoE Switch with related Cat5e/Cat6 wiring
- Electronic Lock

If remote access to the GDS3710 is required for viewing live video stream, Internet access is required and more equipment such as:

- Router.
- Internet Access (Optical fiber, 3G, 4G, Cable or DSL).
- iPhone or Android phone with 3rd party applications (IP Cam Viewer for instance).

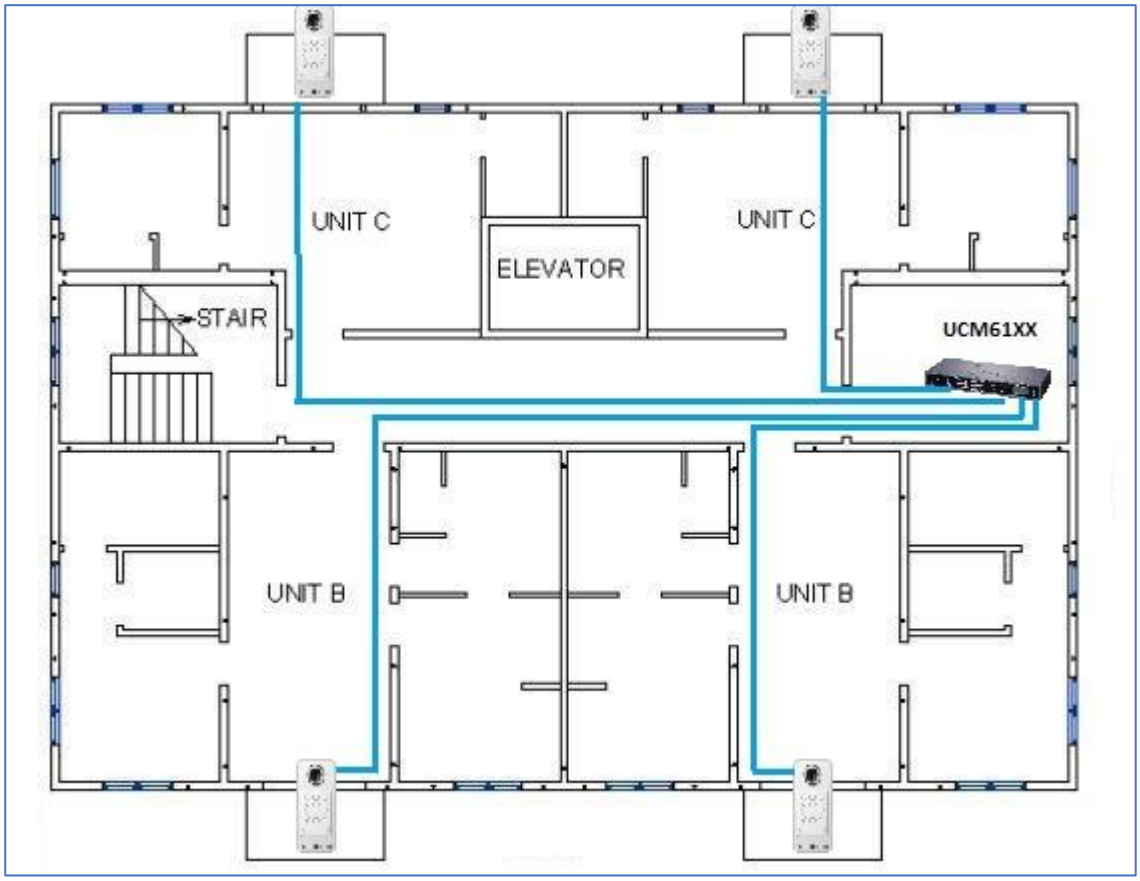


Figure 15: Peering GDS3710 with UCM6XXX

Using a Network Video Recorder (GVR355X)

For implementation with more than two GDS3710s, if local video recording is required to store the record, then an NVR like GXV355X will be added to save all the video stream when people enter the door.

Equipment List:

- Several GDS3710
- GVR355X NVR
- PoE switches with Cat5e/Cat6 wiring
- Router
- Internet Access (Optical fiber, 3G, 4G, Cable or DSL).
- iPhone or Android phone with 3rd party APP

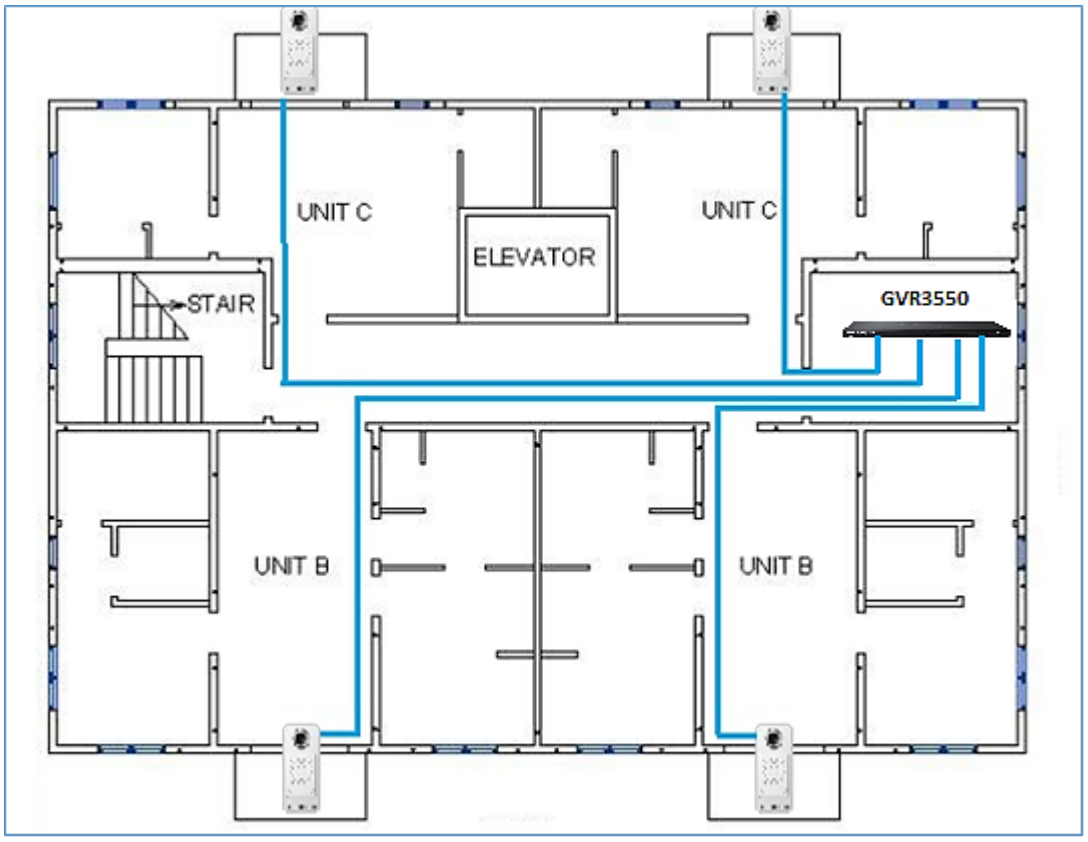


Figure 16: Peering GDS3710 with GVR3550

GDS3710 PERIPHERAL CONNECTIONS

Below is the illustration of GDS3710 peripheral connections for related applications.

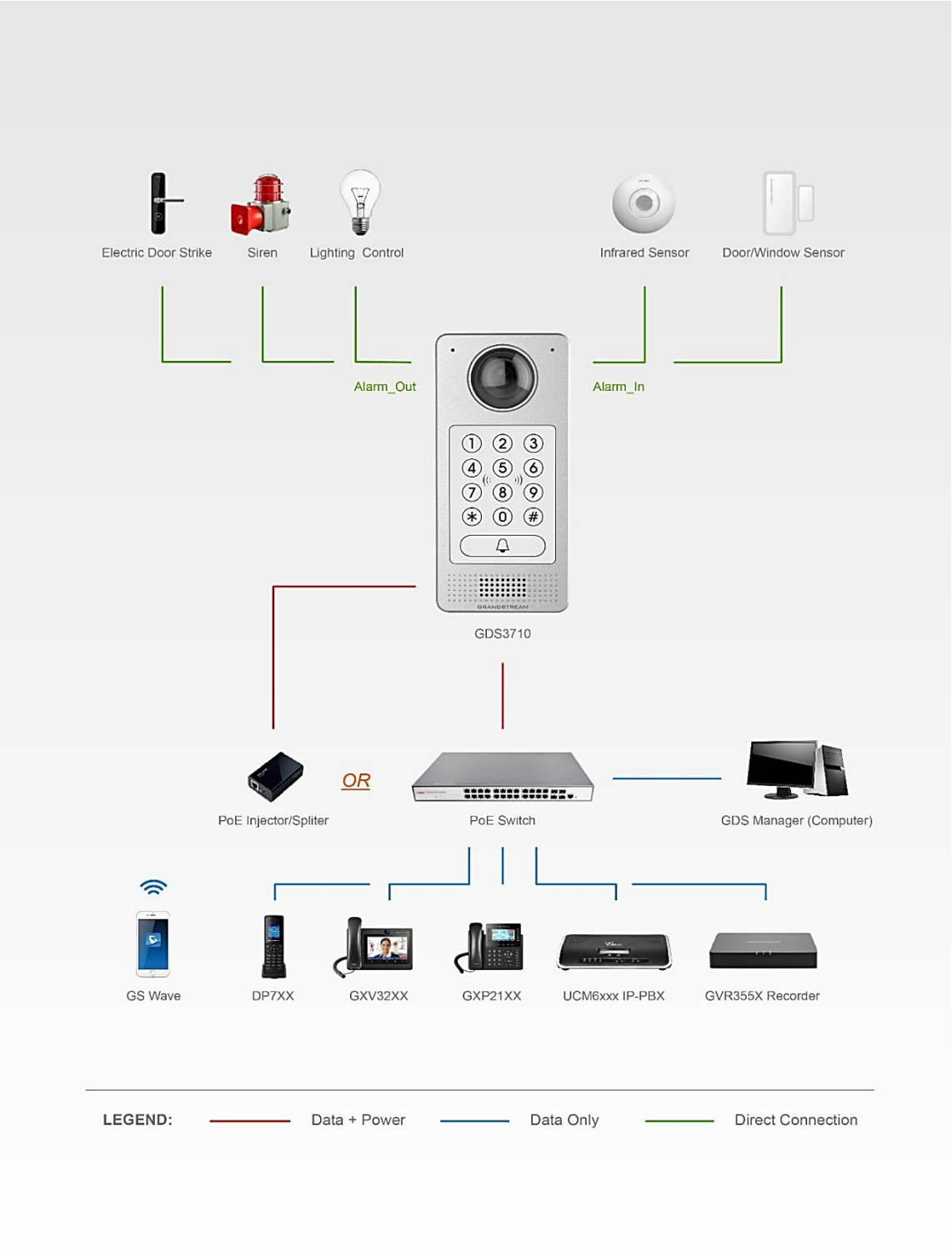


Figure 17: Peripheral Connections for GDS3710

Alarm IN/OUT

Alarm_In could use any 3rd party Sensors (like IR Motion Sensor).

Alarm_Out device could use 3rd party Siren and Strobe Light, or Electric Door Striker, etc.

The figure below shows illustration of the Circuit for Alarm_In and Alarm_Out.

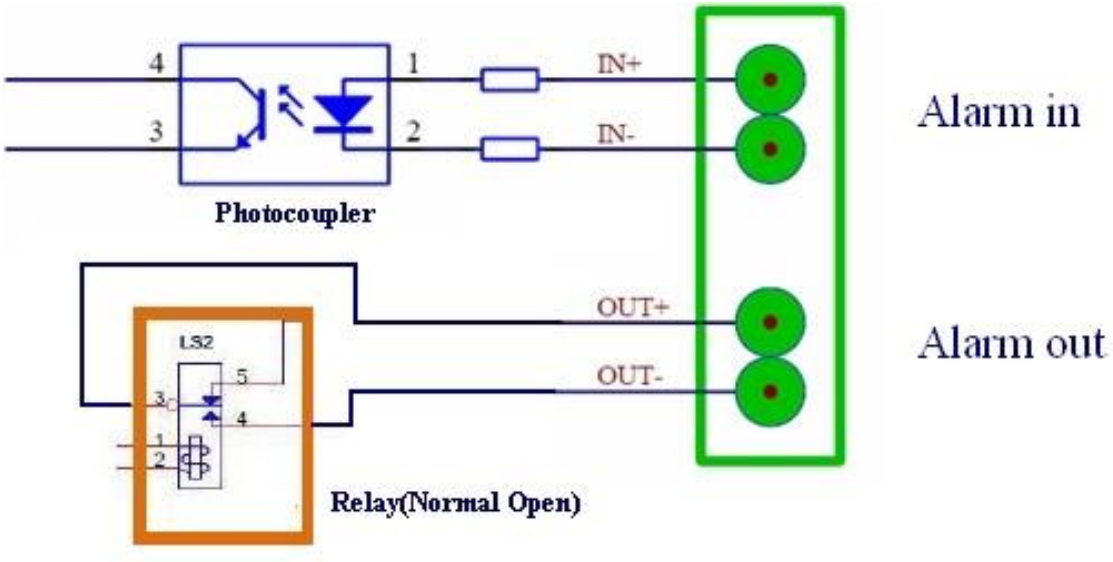


Figure 18: Alarm_In/Out Circuit for GDS3710

Notes:

- The Alarm_In and Alarm_Out circuit for the GDS3710 should meet the following requirement:

Alarm Input	3V<Vin<15V, PINs (1.02KΩ)
Alarm Output	125VAC/0.5A, 30VDC/2A, Normal Open, PINs

- The Alarm_In circuit, if there is any voltage change between 3V and 15V, as specified in the table above, the GDS3710 Alarm_In port will detect it and trigger the action and event.
- Higher voltage and wrong polarity connection are prohibited because this will damage the devices.

Protection Diode

When connecting the GDS3710 to a door strike it is recommended to set an EMF protection diode in reverse polarity for a secure use, below examples of deployment for the protection diode.

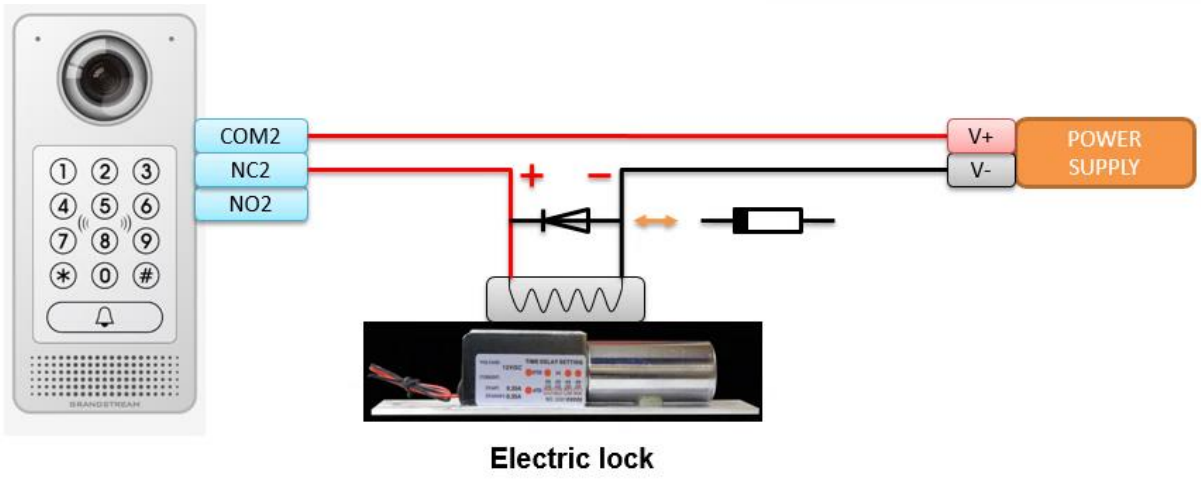


Figure 19: Protection Diode - Example 1

The reverse EMF protection diode must always be installed in reverse polarity across the door strike.

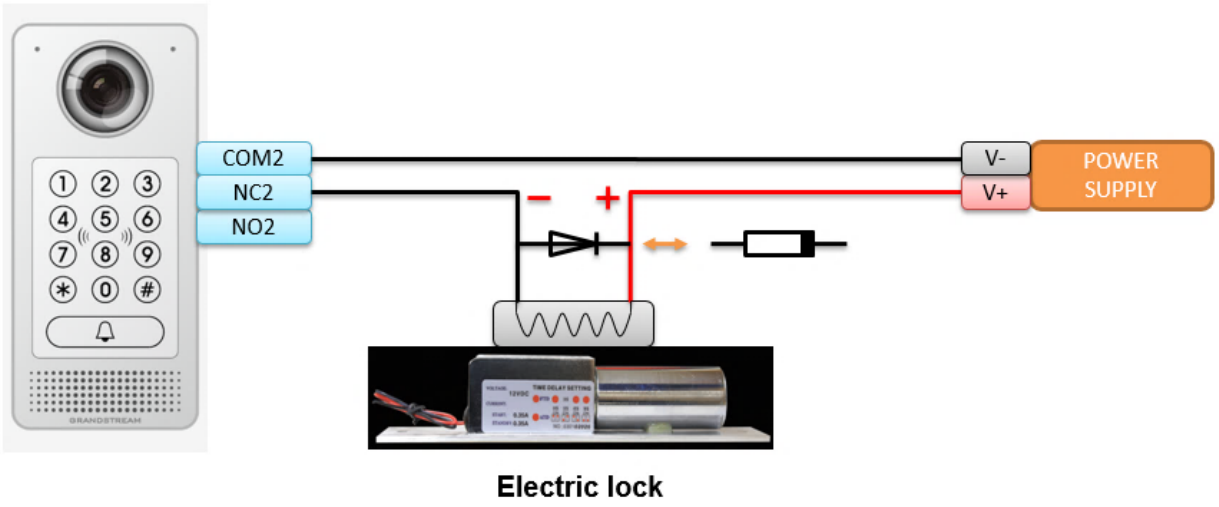


Figure 20: Protection Diode - Example 2

Connection Examples

Below examples, show how to use wiring on the back cover of the GDS3710 to connect with external devices. The “NO” (Normal Open) model strike is used as example, “NC” (Normal Closed) should be similar and users need to decide which model (NO or NC) to be used on the door.

Wiring Sample using 3rd Party Power Supply

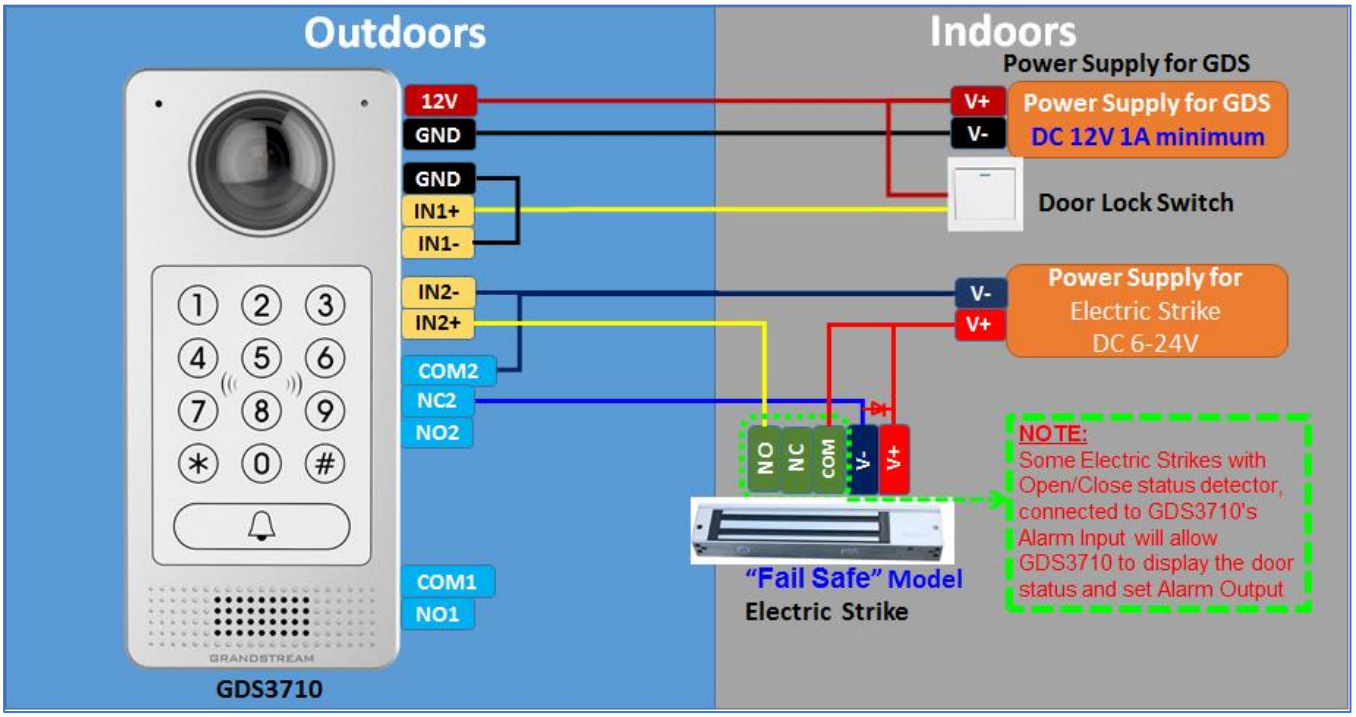


Figure 21: 3rd party Power Supply Wiring Sample

Wiring Sample using Power Supply for both GDS3710 and Electric Strike

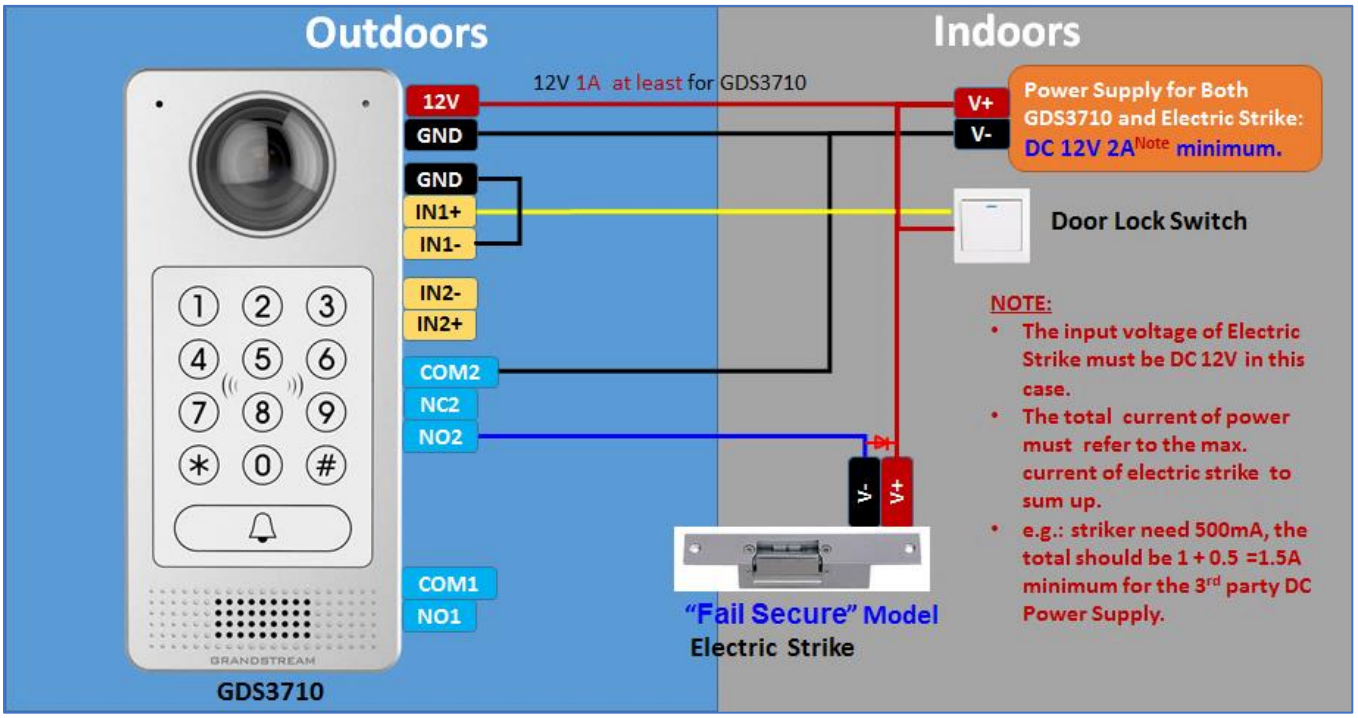


Figure 22: Power Supply used for both GDS3710 and Electric Strike

Wiring Sample using PoE to power GDS3710 and 3rd Party Power Supply for Electric Strike

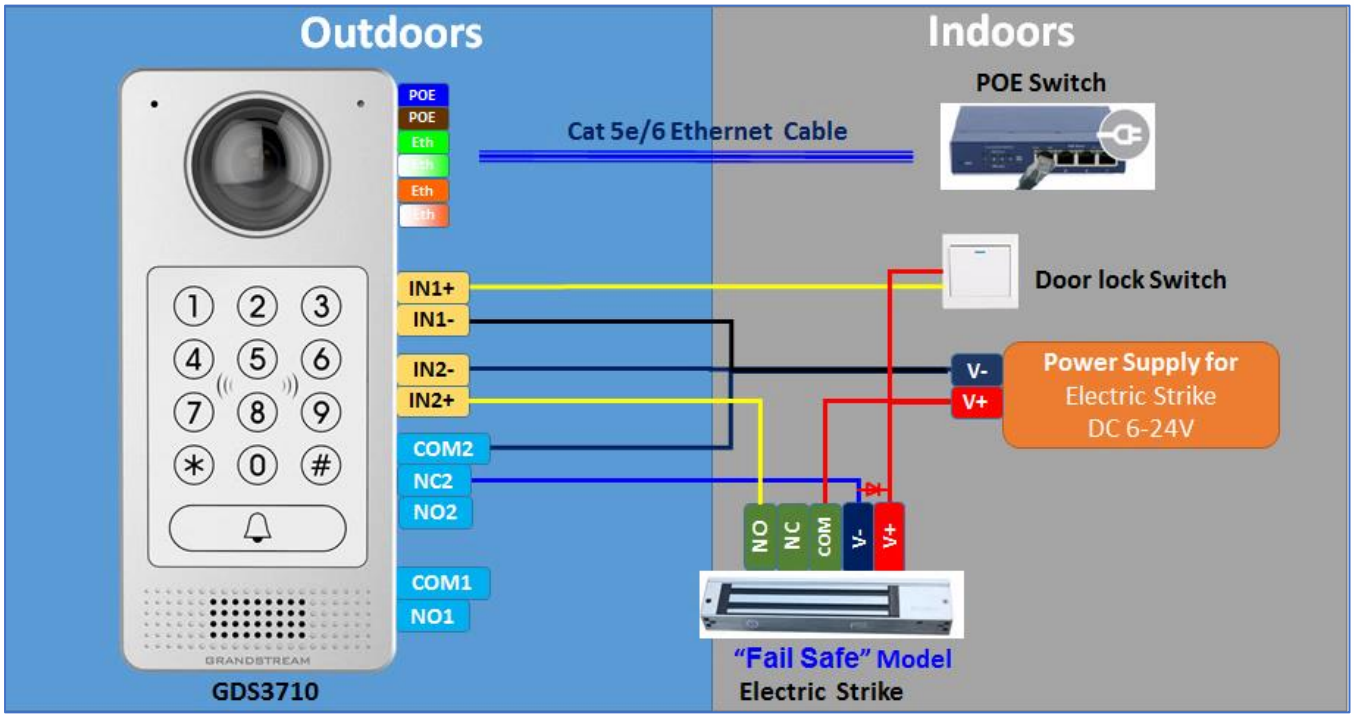


Figure 23: Wiring Sample using PoE to power GDS3710 and 3rd party Power Supply for Electric Strike

Warning: The following example should be avoided when powering the electric strike.

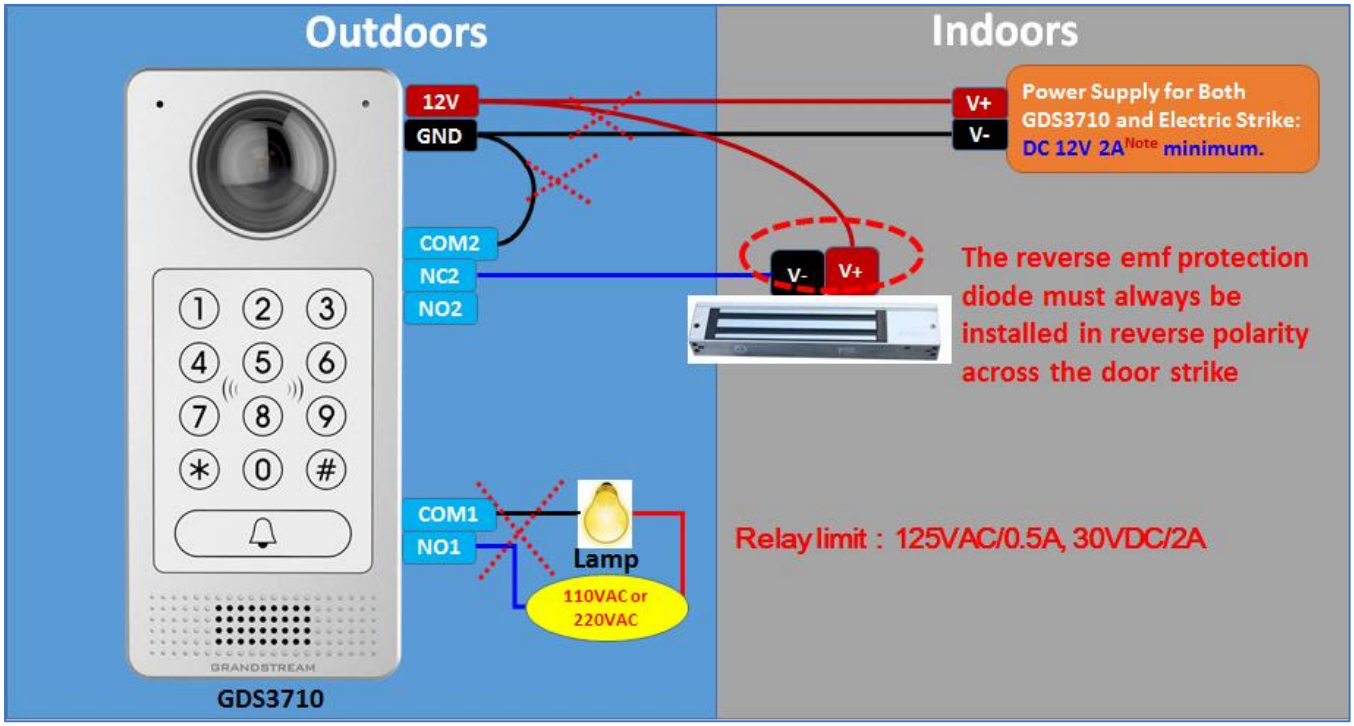


Figure 24: Example to Avoid when Powering the Electric Strike

Good Wiring Sample for Electric Strike and High-Power Device

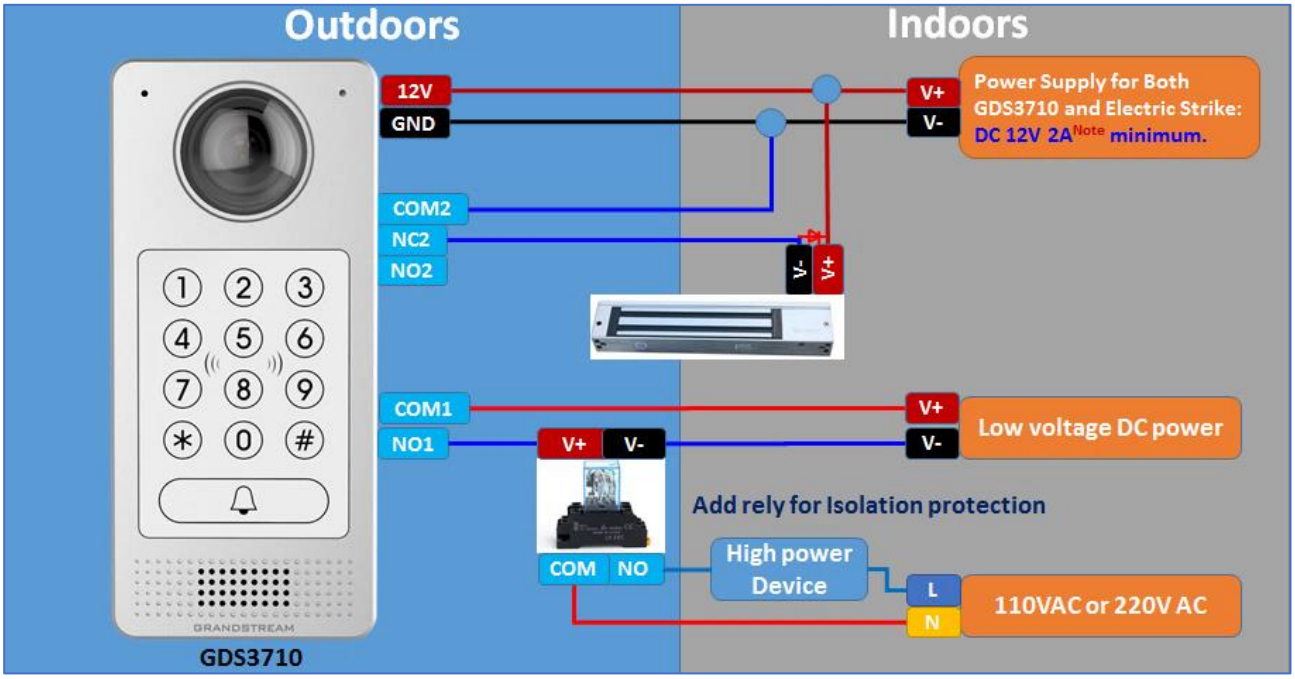


Figure 25: Electric Strike and High-Power Device Example

Wiegand Module Wiring Examples

GDS3710 package is shipped with one Wiegand cable for Input/Output Wiegand connections. The following examples shows how to connect the Wiegand Input/Output devices to the GDS3710.

Input example with 3rd party power supply for Wiegand device

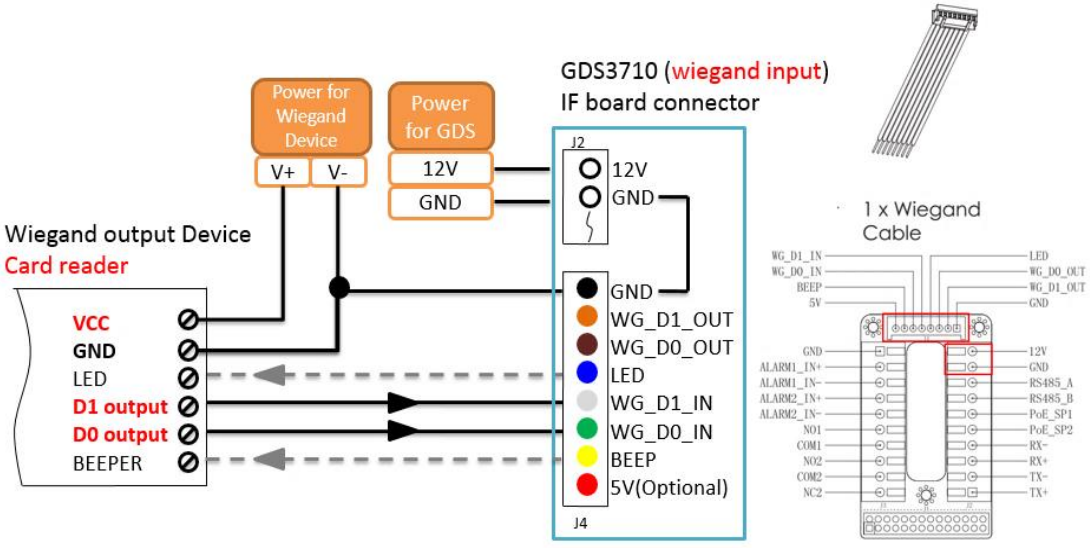


Figure 26: Wiegand Input Example with 3rd party Power Supply

Make sure to connect the GND of the Wiegand device and the GDS3710 Wiegand port.
For Wiegand input mode, LED and Beep pins require that the Wiegand device support those interfaces. These two pins will not affect the Wiegand bus when not connected.

Input example with power supply for both GDS3710 and Wiegand device

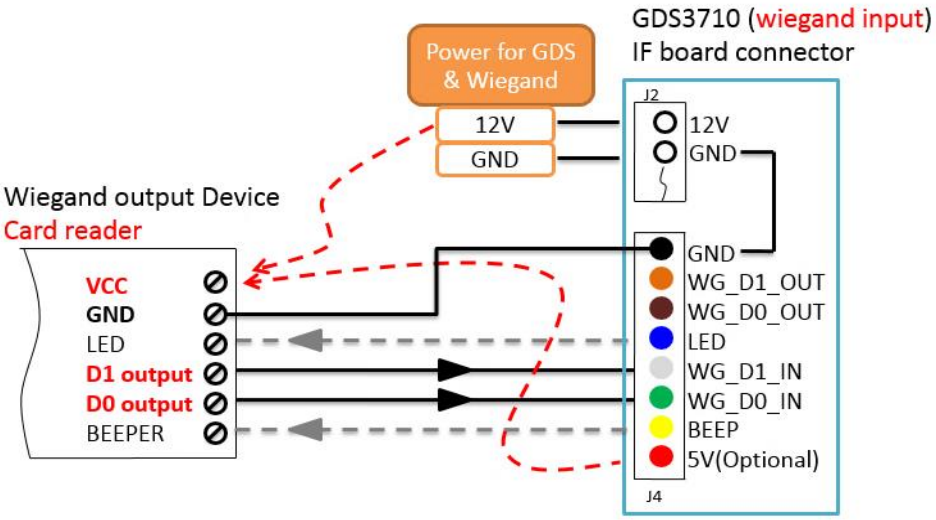


Figure 27: Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device

If power source is **12VDC**, Wiegand device can share same power source of GDS3710. However, users need to check the max power consumption and the max capability of the power source.
If Wiegand device is using **5VDC**, GDS3710 Wiegand port can provide 5VDC with max 500mA to power up Wiegand device.

Output example with 3rd party power supply for Wiegand device

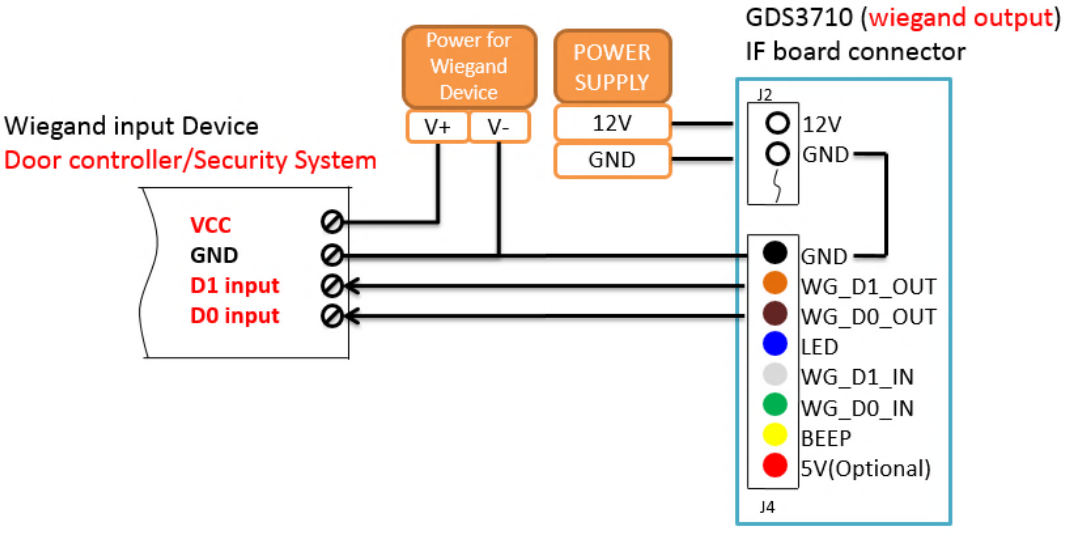


Figure 28: Wiegand Output Wiring Example

When the Wiegand output of the GDS3710 is connected, it acts as the signal receiver of the 3rd party Wiegand device, connecting to door controller. The major wiring is GND, D0, and D1. Because usually the door controller will consume big current and power, the power supply should be separated.

Wiegand RFID Card Reader Example

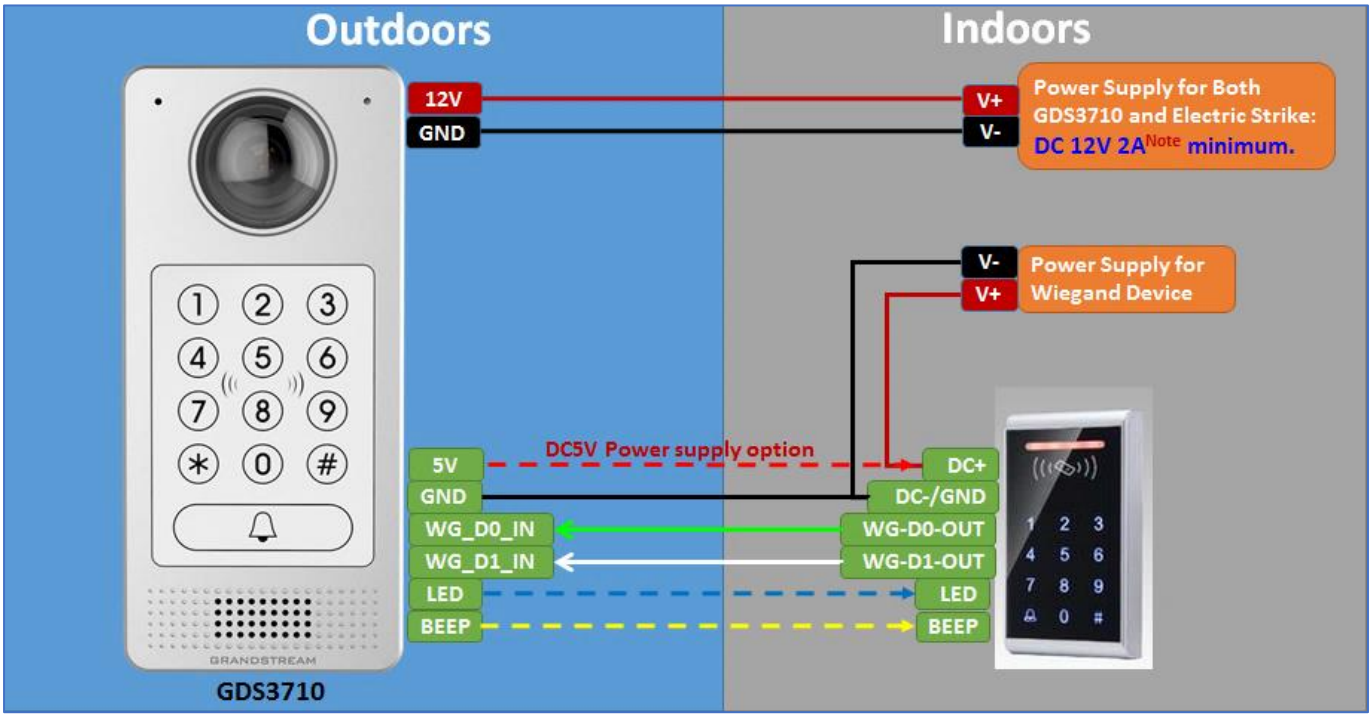


Figure 29: Wiegand RFID Card Reader Example

GDS3710 HOME WEB PAGE

Once logged in successfully to the GDS3710, user will see the following page.

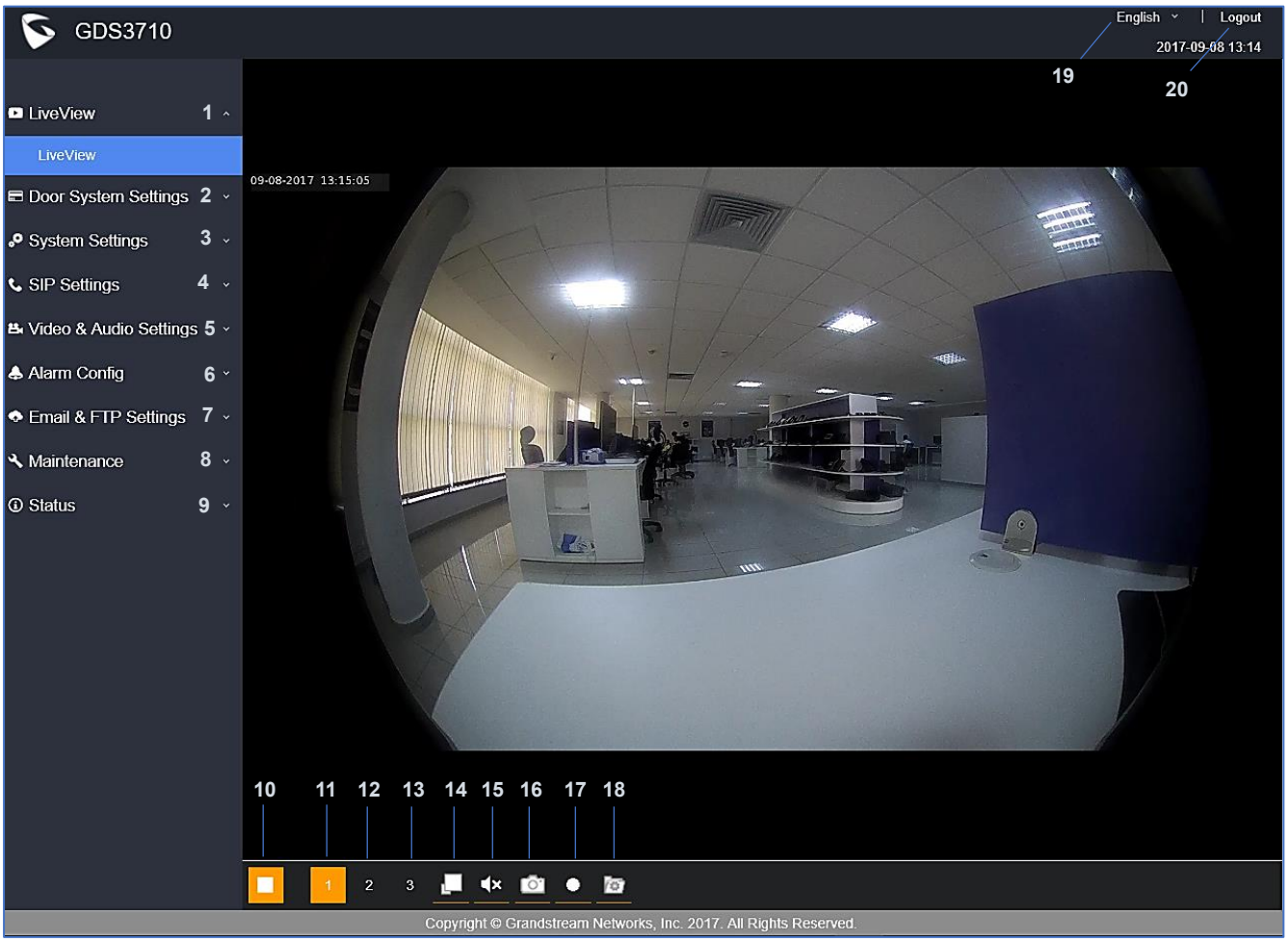


Figure 30: Home Page

Table 5: Home Page Description

Number	Fields	Description
1	**LiveView**	Access to live view stream page.
2	**Door System Settings**	Access to “Door System Settings” page.
3	**System Settings**	Access to “System Settings” page.
4	**SIP Settings**	Access to “SIP Settings” configuration page.
5	**Video & Audio Settings**	Access to “Video & Audio settings” page.

6	**Alarm config**	Access to “Alarm config” page.
7	**Email & FTP Settings**	Access to “Email & FTP Settings” page.
8	**Maintenance**	Access to “Maintenance” page.
9	**Status**	Click to enter “Status” page.
10	**Play/Stop**	Start/Stop the video stream in the web page.
11	**Stream 1**	Play the primary stream.
12	**Stream 2**	Play the secondary stream.
13	**Stream 3**	Play the third stream.
14	**Window size**	Resize the window.
15	**Audio**	Click to mute / unmute the audio.
16	**Snapshot**	Click to take a snapshot.
17	**Recording**	Click to start recording.
18	**File Path Saved**	Click to access Record and Capture paths.
19	**Logout**	Logout from the web page.
20	**Language**	Select the webpage language.

GDS3710 Configuration & Language Page

- Once the IP address of the GDS3710 is entered on the user browser, the login web page will pop up allowing user to configure the GDS3710 parameters.

- When clicking on the “Language” drop down, supported languages will be displayed as shown in Figure below. Click to select the related webpage display language.

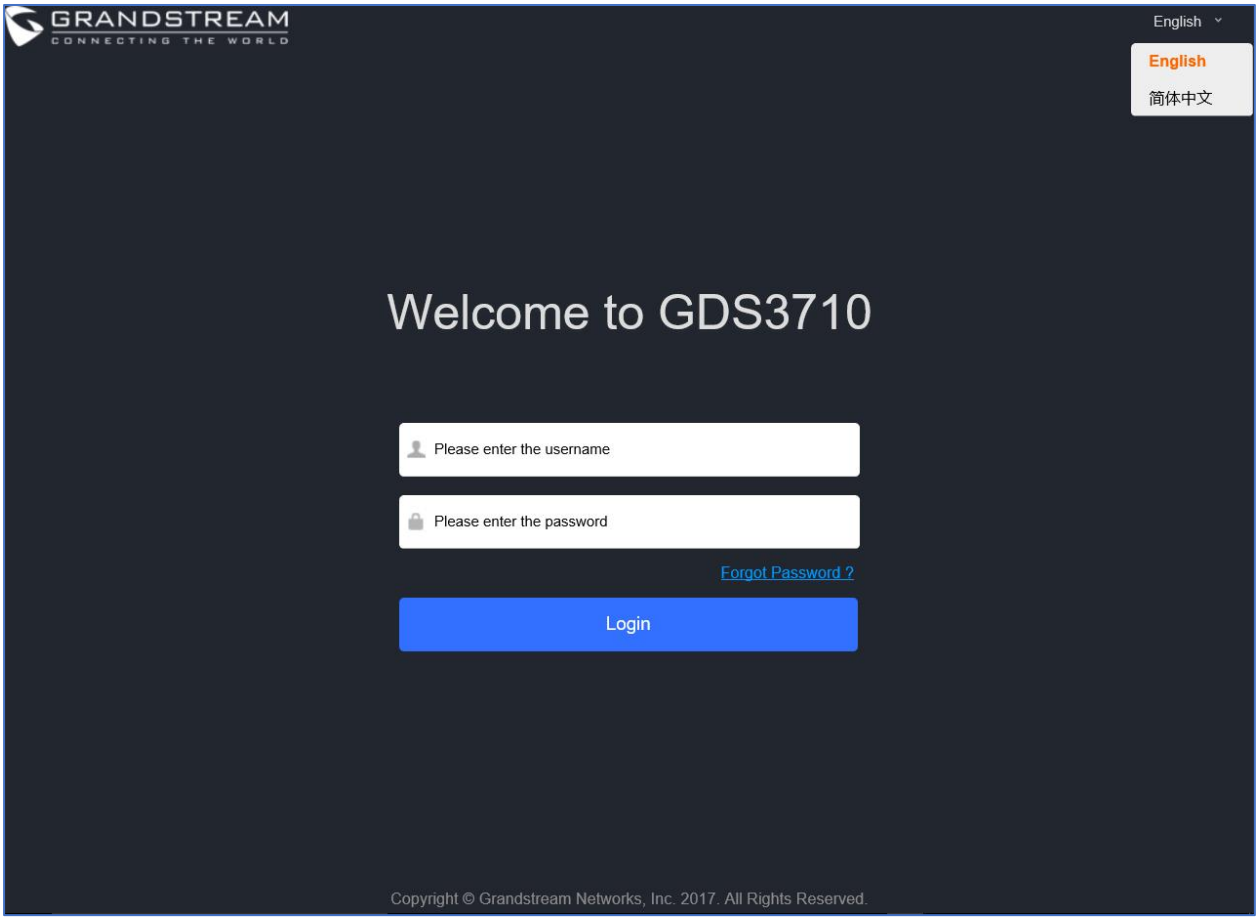


Figure 31: Switch Language Page

Note: Current firmware supports only English (default) and simplified Chinese.

GDS3710 SETTINGS

Live View Page

This page allows users to view the live video of the GDS3710 using popular browsers like Chrome or Firefox immediately without downloading and installing any plugins.

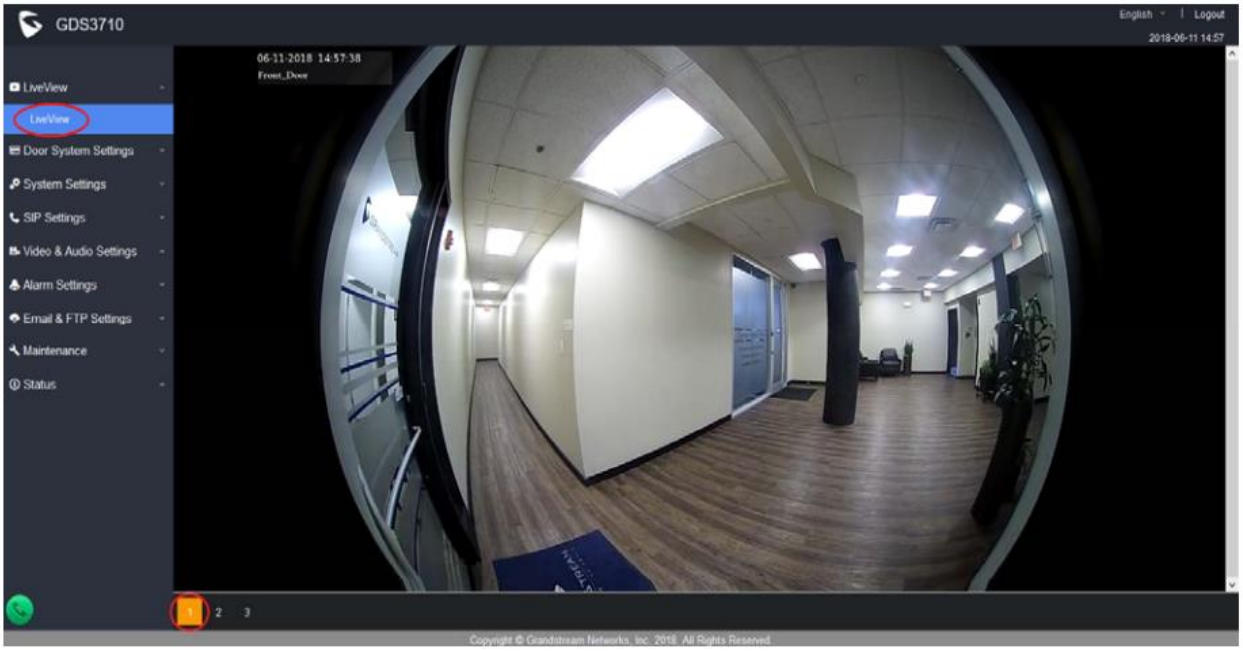


Figure 32: Live View Page

Three streams are available:

- **Primary video stream:** 1920*1080 resolution, recommended for continuous full HD recording (If used with GXV355X NVR).
- **Secondary video stream:** 640*480 resolution, recommended for SIP/VoIP video calls (if used with GXV3240/GXV3275).
- **Third video stream:** 320*240 resolution, recommended for smartphone or Tablet Apps (IP Cam Viewer for instance).

Live Snapshot

Users can take view snapshots from GDS3710 live view via HTTP API, this can be used without installing the any browser plugin. Starting from firmware 1.0.3.34, users can deploy two methods to view snapshots depending on *MJPEG Authentication Mode,* which can be set under following path:
Web UI ➔ System Settings ➔ Access Settings

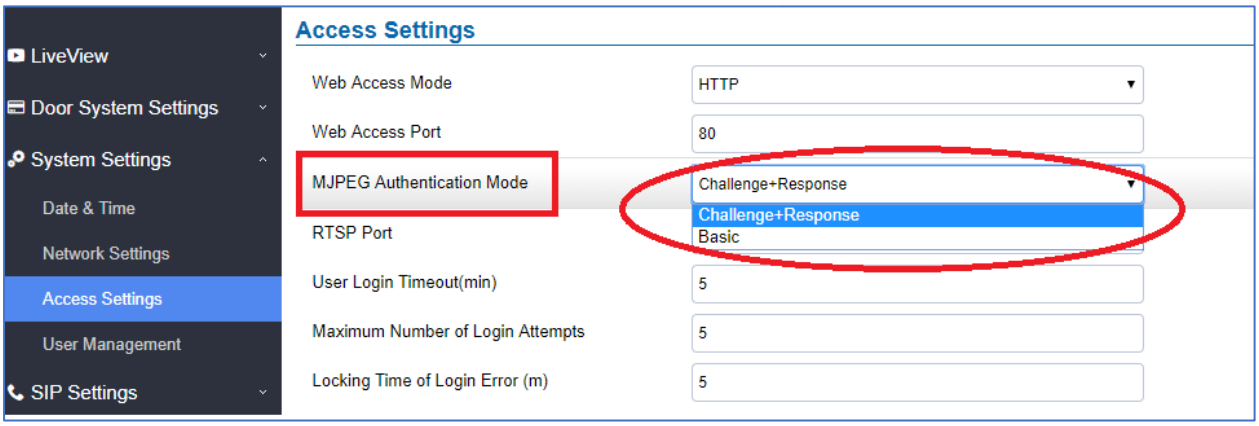


Figure 33: MJPEG Authentication Mode

1) Challenge+Response MJPEG Authentication Mode:

Please follow below steps in order to take a snapshot via HTTP commands on this mode:

1. In browser type in: **http(s)://IP_Address_GDS:Port/jpeg/view.html**
2. The browser will pop up the window above asking for credentials, user needs to enter admin credential.

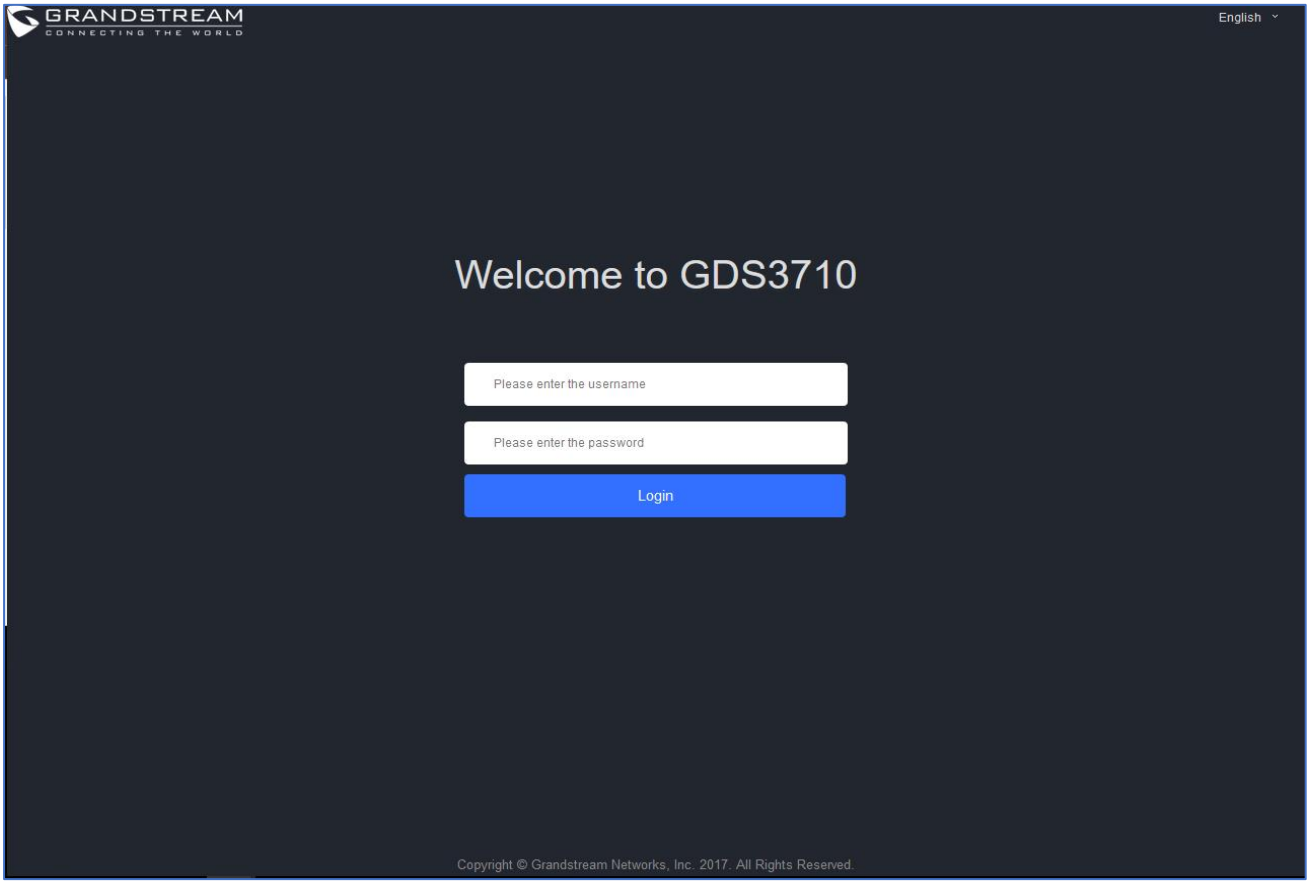


Figure 34 : Snapshot admin credential

3. The browser will show one frame of the video (720p) as a snapshot.

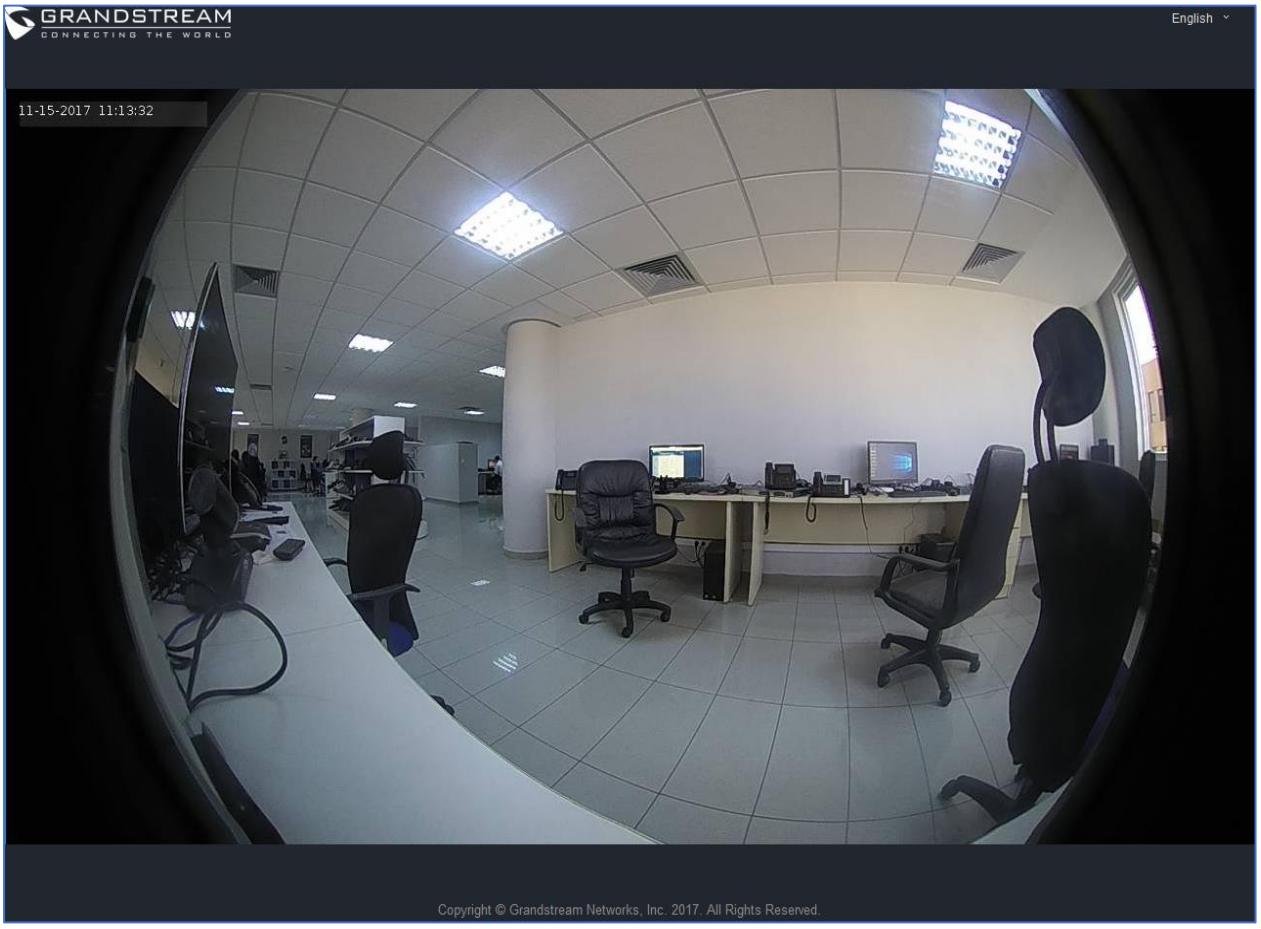


Figure 35 : Snapshot view using secured MJPEG authentication Mode

Note: This is supported on all browsers without installing any plugin and requires admin user authentication for more security.

2) Basic MJPEG Authentication Mode:

Please follow below steps in order to take a snapshot via HTTP commands:

1. In browser type in: **http(s)://admin:password@IP_Address_GDS:Port/jpeg/view.html**
2. The browser will show one frame of the video (720p) as a snapshot.

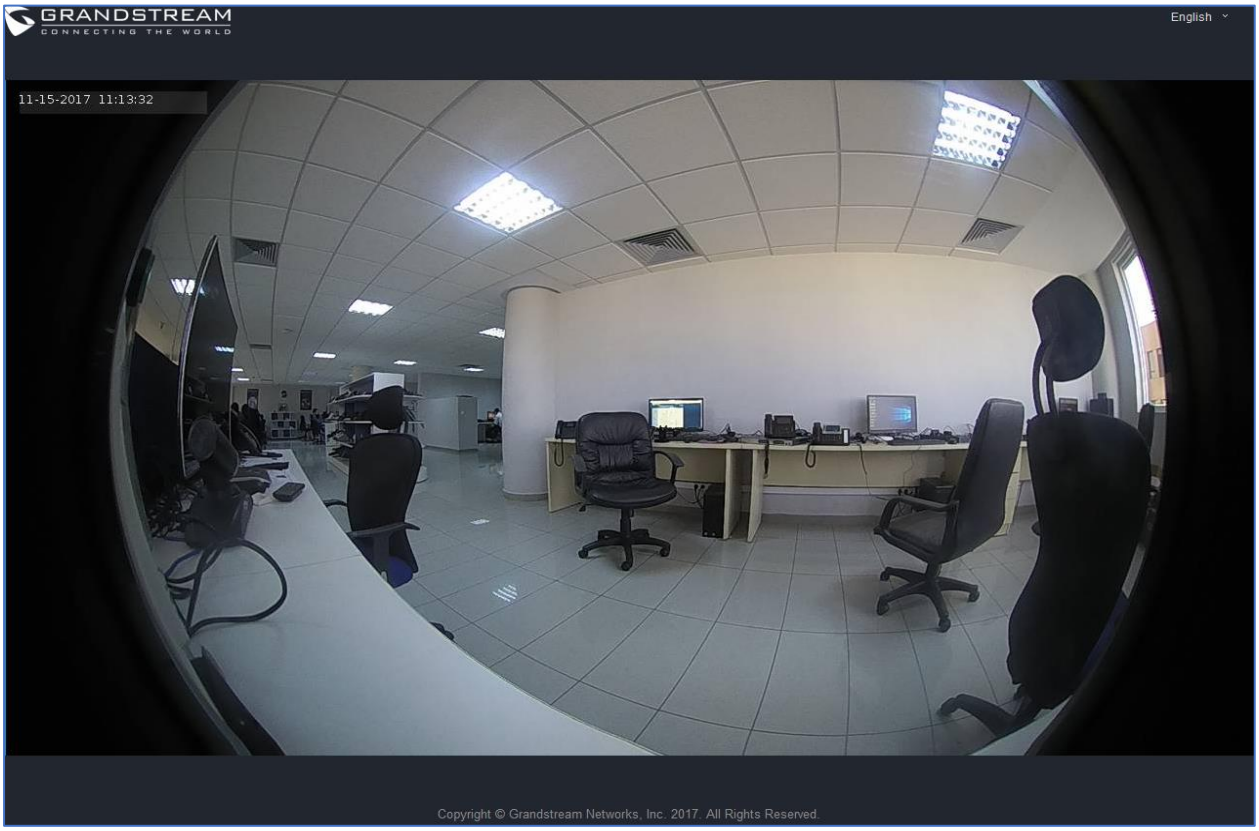


Figure 36: Snapshot view using Basic Authentication Mode

MJPEG Stream

The GDS3710 supports MJPEG Stream live viewing via HTTP API commands, this can be used without installing the Live view browser plugin. Starting from firmware 1.0.3.34, users can deploy two methods to retrieve MJPEG stream depending on *MJPEG Authentication Mode,* which can be set under following path: **Web UI ➔ System Settings ➔ Access Settings**

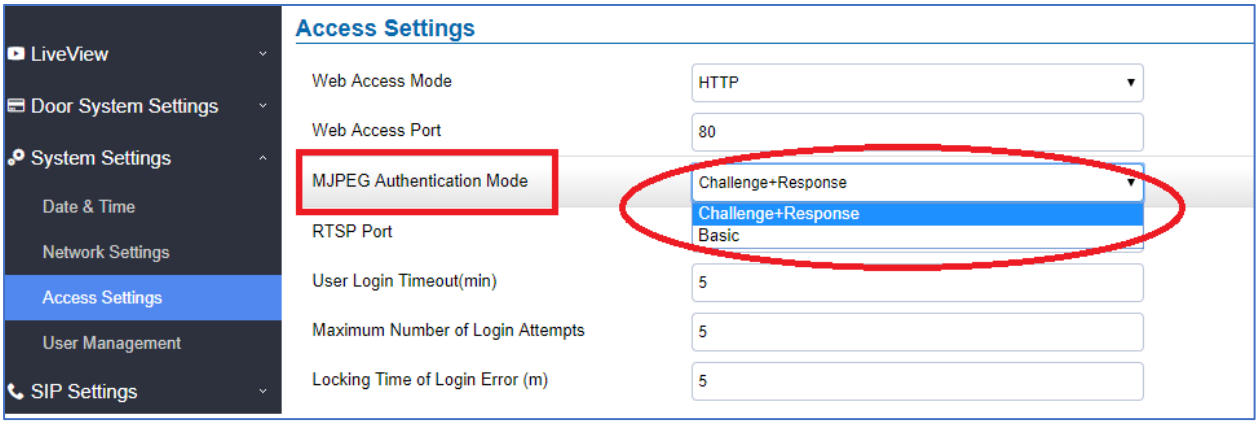


Figure 37: MJPEG Authentication Mode

1) Challenge+Response MJPEG Authentication Mode:

In order to get live view stream using MJPEG stream over HTTP command on this mode, please fellow below steps:

1. In browser type in: **http(s)://IP_Address_GDS:Port/jpeg/mjpeg.html**
2. The browser will pop up the window above asking for credentials, user needs to enter admin credential.

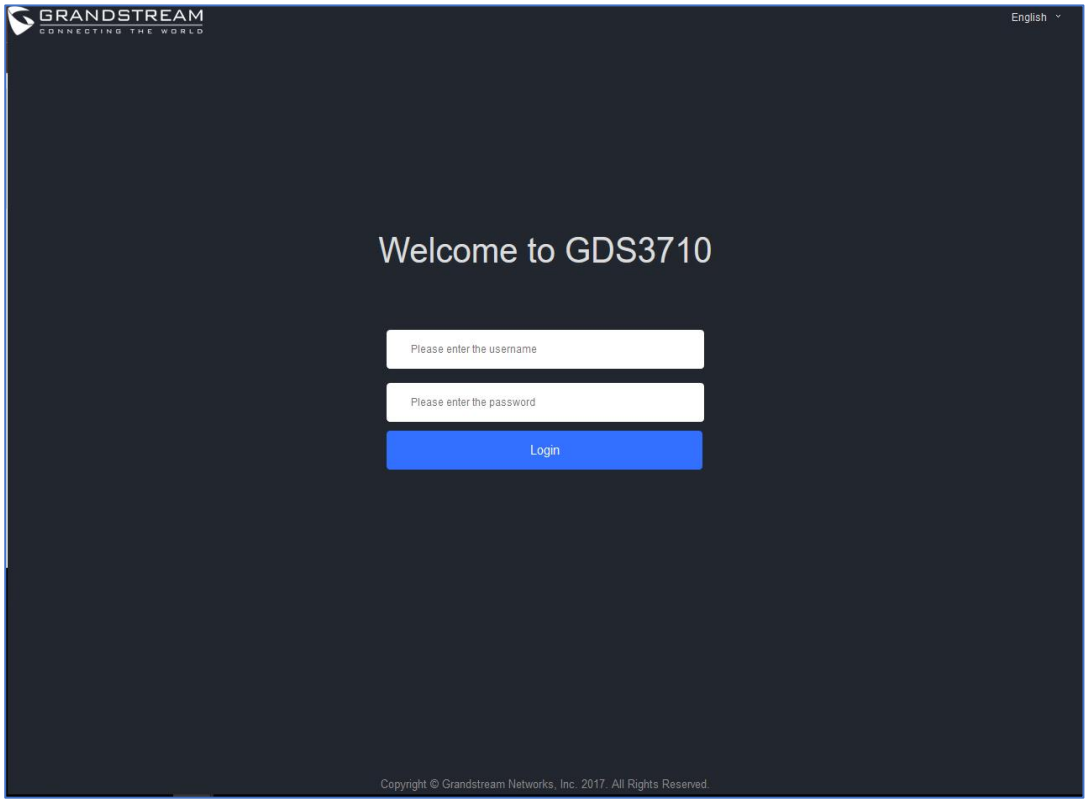


Figure 38 : MJPEG view admin credential

3. The browser will show MJPEG stream (720p).

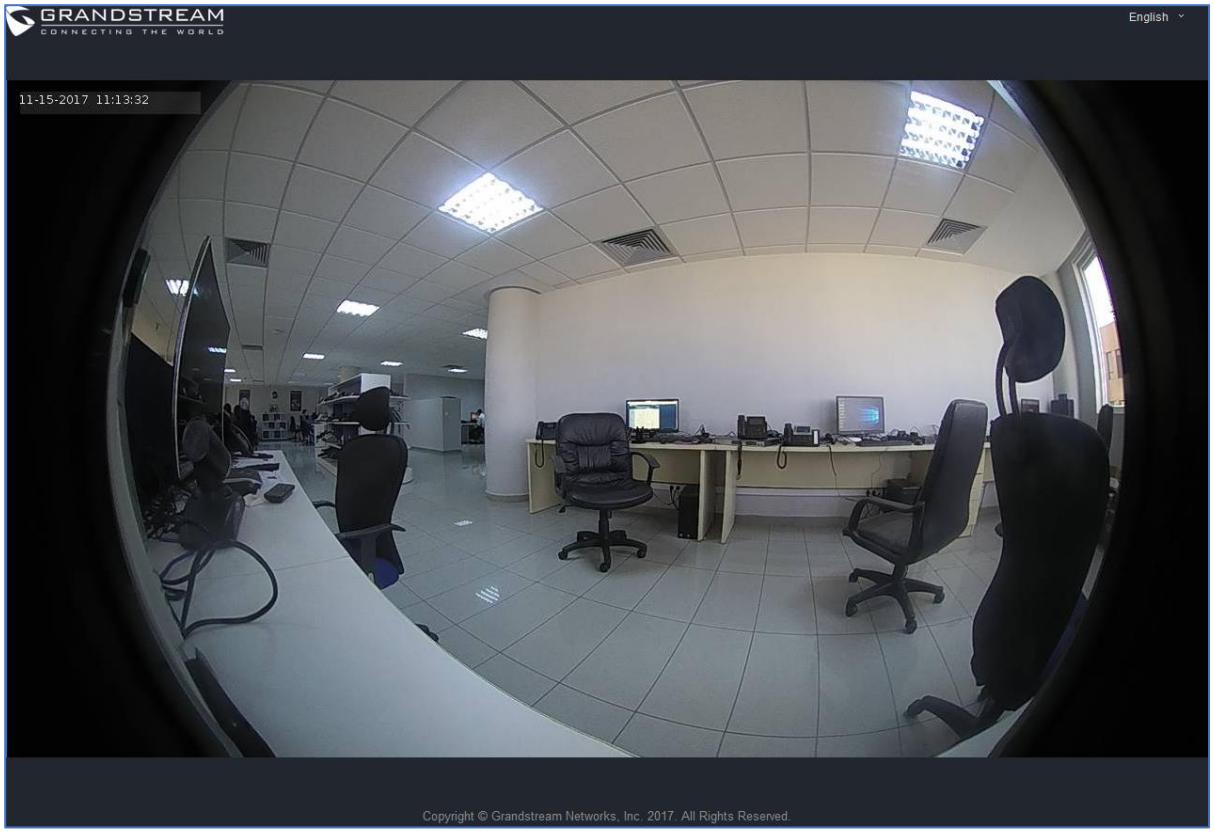


Figure 39 : MJPEG live view using secured MJPEG Authentication Mode

Note: This is supported on all browsers without installing any plugin and requires admin user authentication for more security.

2) Basic MJPEG Authentication Mode:

Please follow below steps in order to take a snapshot via HTTP commands:

1. In browser type in: **http(s)://admin:password@IP_Address_GDS:Port/jpeg/mjpeg.html**
2. The browser will show MJPEG stream (720p).

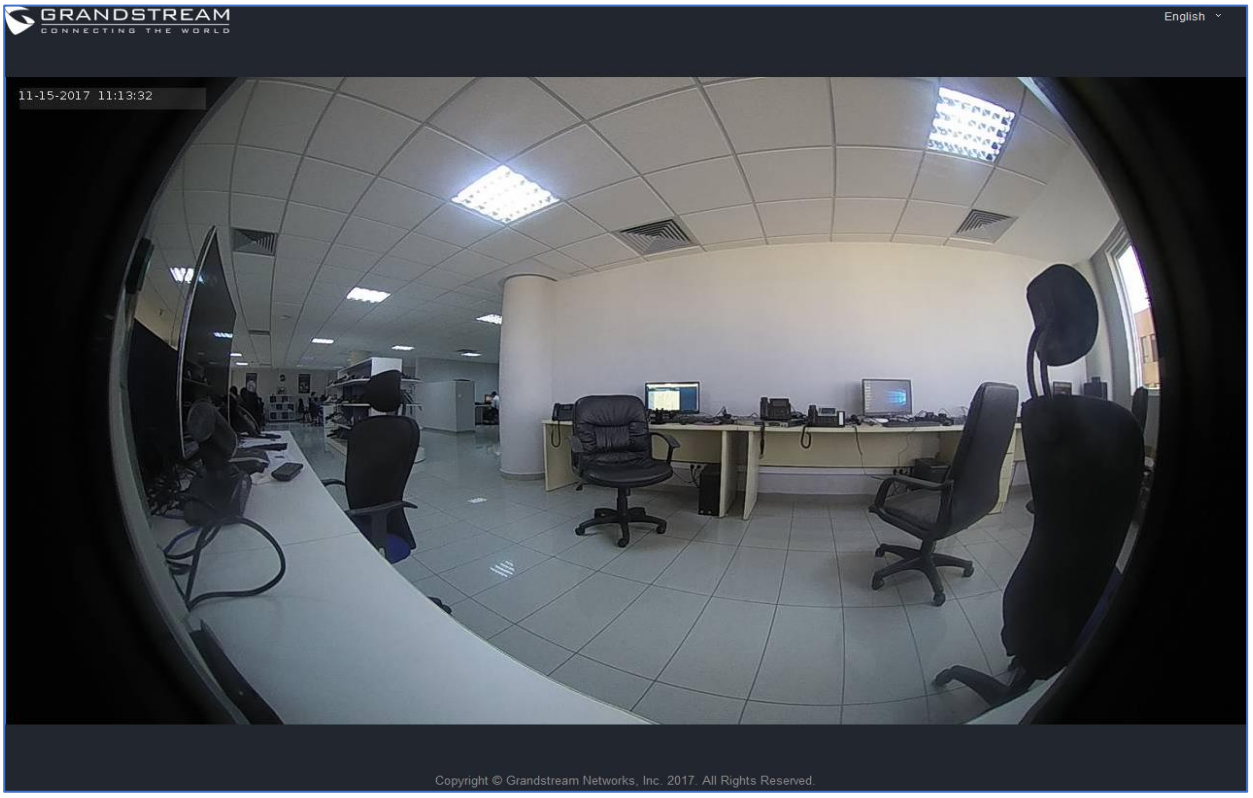


Figure 40: MJPEG view using Basic MJPEG Authentication Mode

Note: Similar command can be applied to open source application like **VLC MediaPlayer** to retrieve H.264 video stream with better quality: **rtsp://admin:password@IP_GDS3710:Port/X**

Where **X=0,4,8** corresponded to **1st, 2nd** and **3rd** video stream (**2nd** recommended).

Door System Settings

Users can configure system operations parameters, like input PIN for the door and manage users' settings.

Basic Settings

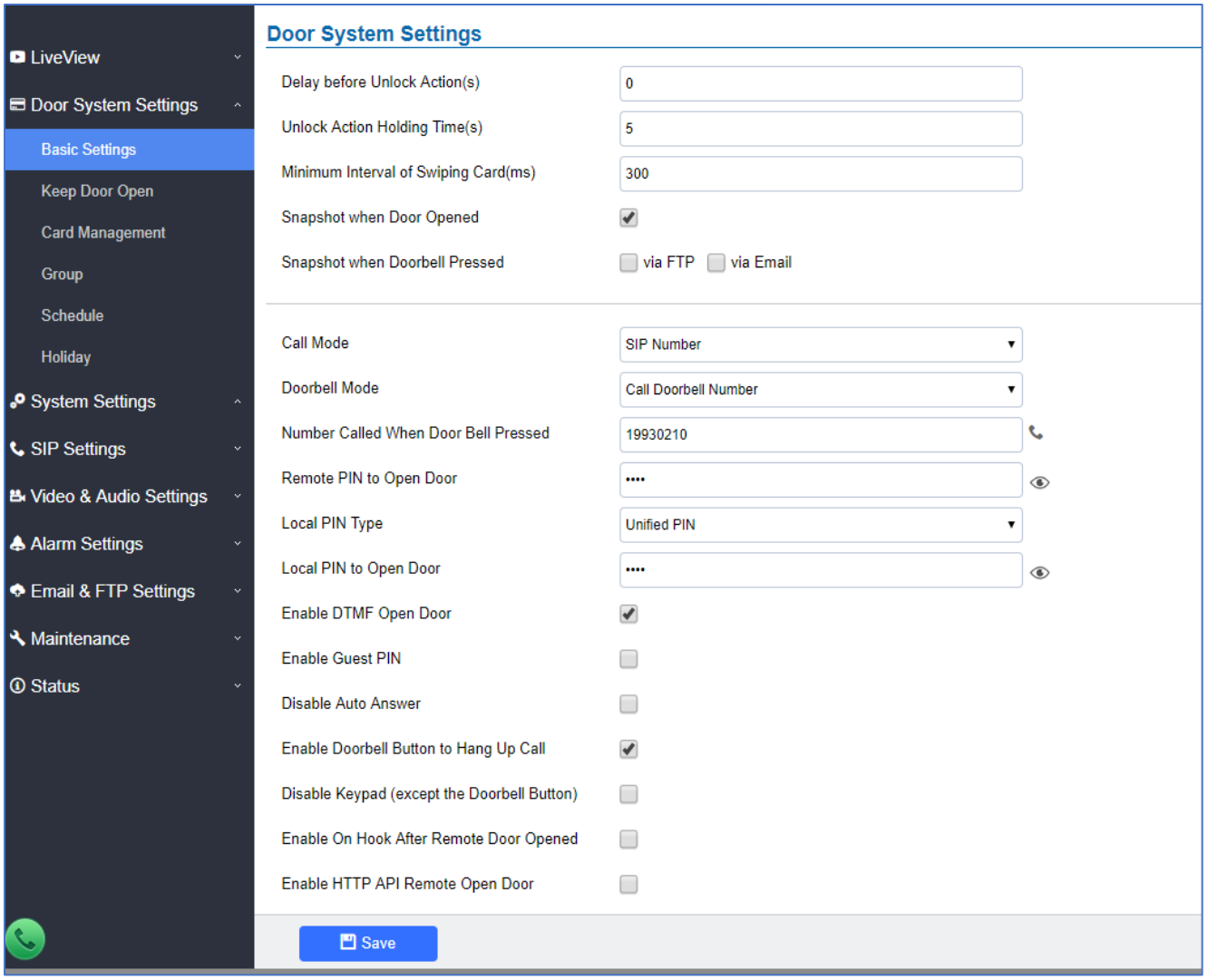


Figure 41: Door System Settings Page

Table 6: Door System Settings

Delay before Unlock Action (s)	Configures the time delay in second for the electronic lock to be triggered (default value is 0 seconds).
Unlock Action Holding Time (s)	Configures the lock holding time, in seconds (default value is 5 seconds).
Min. Interval of Swiping Card (ms)	Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms.
Snapshot when Door Opened	Enables snapshot when electronic lock operates.
Snapshot when Doorbell Pressed	User can choose to email the snapshot when doorbell pressed w/o sending the snapshots via FTP to the FTP server.
Call Mode	Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3710 keypad.
Doorbell Mode	Configures the action to be taken when the doorbell is pressed, three options are available: • **Call Doorbell Number:** when Doorbell is pressed, a call will be made to the "**Number Called When Door Bell Pressed**" • **Control Doorbell Output (Digital Output 1):** when Door Bell is pressed electronic lock for Output 1 is opened. • **Both of Above:** When selected, both Call Doorbell Number and Control Doorbell Output options are enabled.
Number Called When Door Bell Pressed	Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed: • **SIP Server mode:** - The field can be configured to store multiple one or multiple SIP extensions, if configured with multiple extensions (ex: 1001, 1002, 1003), separated with "," the GDS3710 will ring one extension after the other in a serial mode (GDS will ring each extension by default 15 seconds, this can be changed on the Ring Timeout). - When using UCM, users can also configure there a Ring Group extension (6400 for example) that will ring multiple extensions simultaneously, or one by one depending on the Ring Group ring strategy.

	- If all phones are GXP21XX, and on serial mode, the phone will stream the video frame by frame and users can open door either by pressing PIN# or by pressing Open Door button if already configured. - If early medial is enabled on phone side, user can send the PIN code using the Open-Door button before answering the call (Of course users can open the door also after answering the call). When using Parallel Mode via (Ring Group) this will not be possible since media (for DTMF) won't be included during the ringing which is required for door opening. • **Peering mode:** **-** User should configure multiple IP addresses of phones instead of SIP extensions, when Door Bell pressed the GDS3710 will ring the configured IP Addresses in Serial mode. **-** If early media is enabled, the GXV32XX will receive the video stream while it is ringing, and user can open door by pressing the Open-Door button if already configured (Of course users can open the door also after answering the call). **-** GXP21XX phones receive the GDS3710 video using JPEG streaming this means that it will receive video if early media is enabled or disabled. **Note:** This field supports a Maximum of 256 characters.
Remote PIN to Open the Door	Configures PIN code stored in the GDS3710, remote SIP phone needs to input and match this PIN (the PIN is sent via DTMF while in call) so that the GDS3710 can open the door.
Local PIN Type	Three Options are available: Private Card PIN, Unified PIN or Card and Private PIN. • **Private Card PIN**: Means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3710 to open the door [***Virtual Number*Private Door Password#**]. **Note**: When Local PIN type is set to private card PIN, users can also open the door by swiping their cards. • **Unified PIN**: Means all members share a same PIN to unlock the door. Users need to enter the following sequence from the GDS3710 keypad to open the door [***Local PIN to Open the Door#**].

	• **Card and Private PIN**: Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence **[Swipe the card + *Local PIN to Open the Door#]**
Local PIN to Open the Door	Configures PIN stored in GDS3710, input locally this PIN on the GDS3710 keypad will unlock the door. This feature needs **Private Card PIN**, means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3710 to open the door [***Virtual Number*Private Door Password#**]. **Note**: When local PIN type is set to private card PIN, users can also open the door by swiping their cards.
Enable DTMF Open Door	When enabled, remote SIP phones can open the door while in call by entering the remote PIN code configured (the PIN code is sent via DTMF). Default settings is disabled.
Enable Guest PIN	Enables password entry for guests.
Guest PIN	Configures the password that will be used by guests.
Guest PIN Start Time	Selects the start time when the Guest PIN start to take effect.
Guest PIN End Time	Selects the end time when the Guest PIN will stop working.
Disable Auto Answer	If checked, GDS3710 will not answer incoming calls automatically, users can press any key to answer the call. Default setting in unchecked.
Enable Doorbell Button to Hang up Call	If checked, Users can hang up an active call when pressing the door bell button. **Note:** Enabled by default.
Disable Keypad (except the Doorbell Button)	When checked the Keypad will be disabled, only Door Bell button can be pressed.
Enable On Hook After Remote Unlock	When checked calls will be disconnected automatically 5 seconds after the remote open door event.
Enable HTTP API Remote Open Door	Enabling this option allows to use HTTP API command to open the door remotely. **Important note:** We will not be responsible for any security problems resulting from opening the HTTP API remote function, this option is disabled by default and the user should enable it while knowing how to mitigate the risk.

Enable Card Issuing Mode	Enables RFID card issuing/program into the GDS3710. When selected sweeping an RFID card into the GDS3710 will add card information into. [Card Management]
Card issuing State Expire Time(m)	Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes).
Enable Key Blue Light	When checked, the blue light will be activated when pressing the GDS3710 Keys.
Enable Background Light	When checked, the background light will turn on once clicking the GDS3710 Keys.
Enable Blue Light	When enabled, Keypad LED will light based on the configured Start/End Time. For instance, this option can be used when GDS is deployed on dark environment, the GDS will be located easily using Keypad LED.
Central Mode	If enabled, Group/Schedule/Holiday can only be synchronized from the Central (GDS Manager), local configuration will not be allowed. If disabled, only local configuration from GDS3710 is allowed. Default setting is “Disabled”.
Key Tone Type	Configures the key tones for the GDS3710. • **Default**: Beeps will be played when pressing the GDS3710 keys. • **DTMF**: Tones will be played when pressing the GDS3710 keys. • **Mute**: No sound will be played when pressing keys.
Wiegand Input Enable	Enable Wiegand Input.
Wiegand Output Enable	Enable Wiegand Output.

Notes: Remote SIP phone needs password (digits 0-9 only, ended with # key) matching the configuration on the web page to open the door (via DTMF).

GDS3710 support RFID for multiple users to open door, therefore every user has its own PIN. For environment with 100 users and more, it’s difficult for the GDS3710 to manage all these users and a separate PC or Server should be involved for such kind of management and monitoring.

In environments with more than 100 users the GDS3710, another possibility would be to set one unified Local PIN for opening the door for all the users.

Keep Door Open

This feature allows users to set either an immediate or scheduled open door, this will allow usage scene like schools or similar private or public places where the door needs to keep open at specific time window and closed otherwise. Also handy for buildings or properties where a seminar needs to be hosted for some period or lunch breaks in a factory or company where the door keeps open and no access log required then back to locked with authorized entry after that, by default it's disabled.

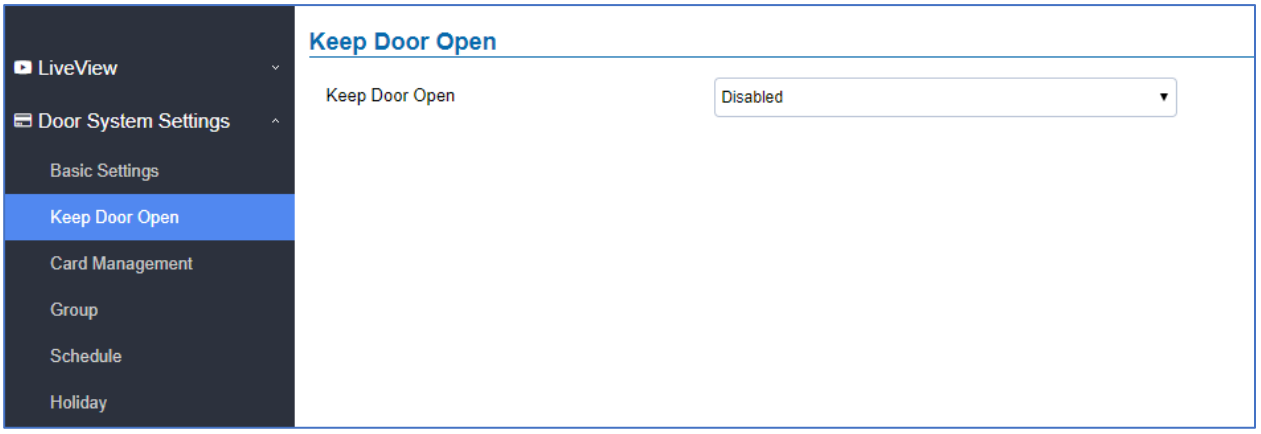


Figure 42: Keep Door Open

There are two modes under this section:

1- **Immediate Open Door (One Time Only Action)**

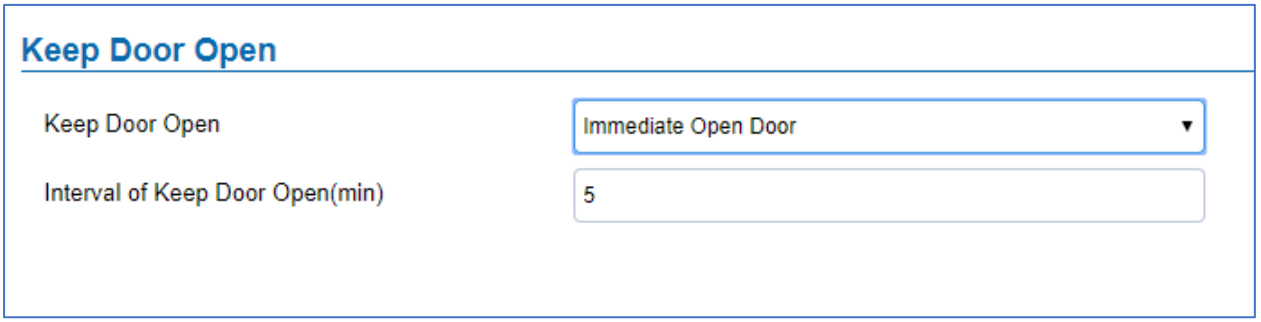


Figure 43: Immediate Open Door

Table 7: Immediate Open-Door Table

Keep Door Open	Select the Keep Door Open mode.
Interval of Keep Door Open (min)	Set the amount of time in minutes where the door will keep opened. Click Save to open door immediately.

2- Schedule Open Door (Repeated Action)

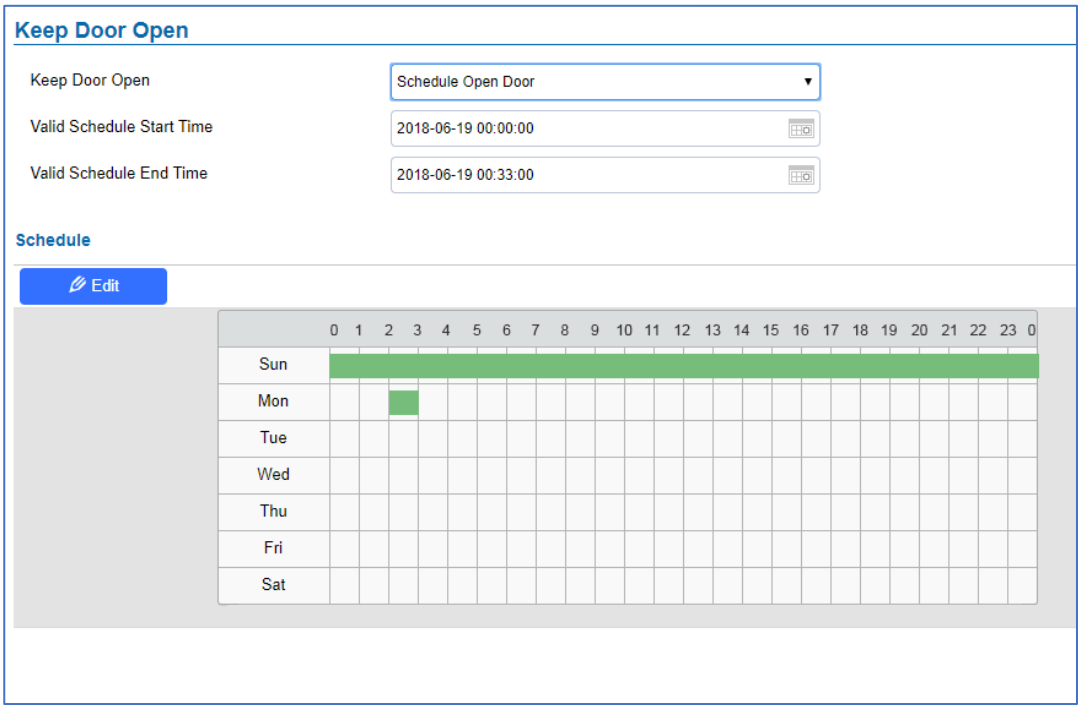
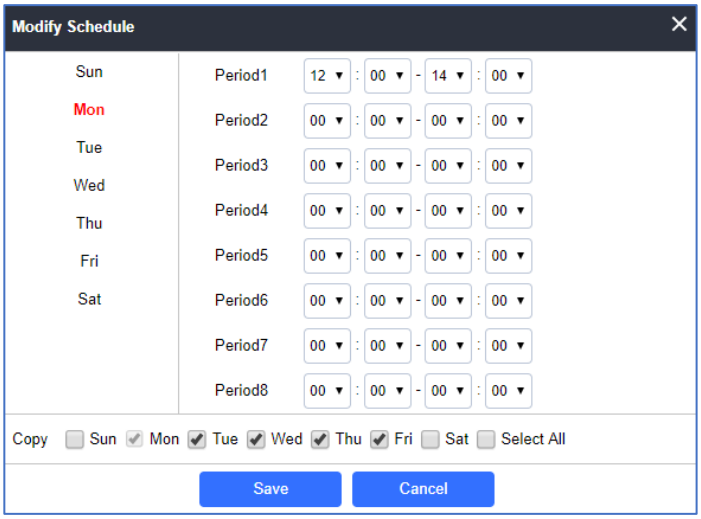


Figure 44: Schedule Open Door

Table 8: Schedule Keep Door Open

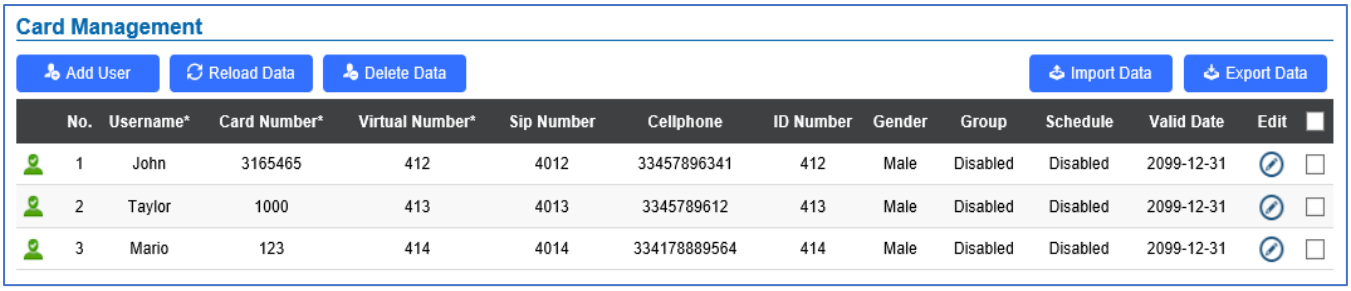
Keep Door Open	Select the Keep Door Open mode (Schedule Open Door on this case).
Valid Schedule Start Time	Selects the start time when the door will be opened.
Valid Schedule End Time	Selects the end time when the door will be locked.

Click on Edit schedule to select which periods for each day the door will remain open, as shown on below screenshot.



Card Management

This page allows users to add information about RFID cards, two options are possible either add RFID cards manually or automatically.



	No.	Username*	Card Number*	Virtual Number*	Sip Number	Cellphone	ID Number	Gender	Group	Schedule	Valid Date	Edit
	1	John	3165465	412	4012	33457896341	412	Male	Disabled	Disabled	2099-12-31	
	2	Taylor	1000	413	4013	3345789612	413	Male	Disabled	Disabled	2099-12-31	
	3	Mario	123	414	4014	334178889564	414	Male	Disabled	Disabled	2099-12-31	

Figure 45: Card Management

Notes:

- The GDS3710 can add up to 2000 user cards.
- Press Export Data or Import Data to import / export users' configuration file, information and data stored on the GDS3710.

Add Users Manually

To add users, click on Add User, the following page will pop up.

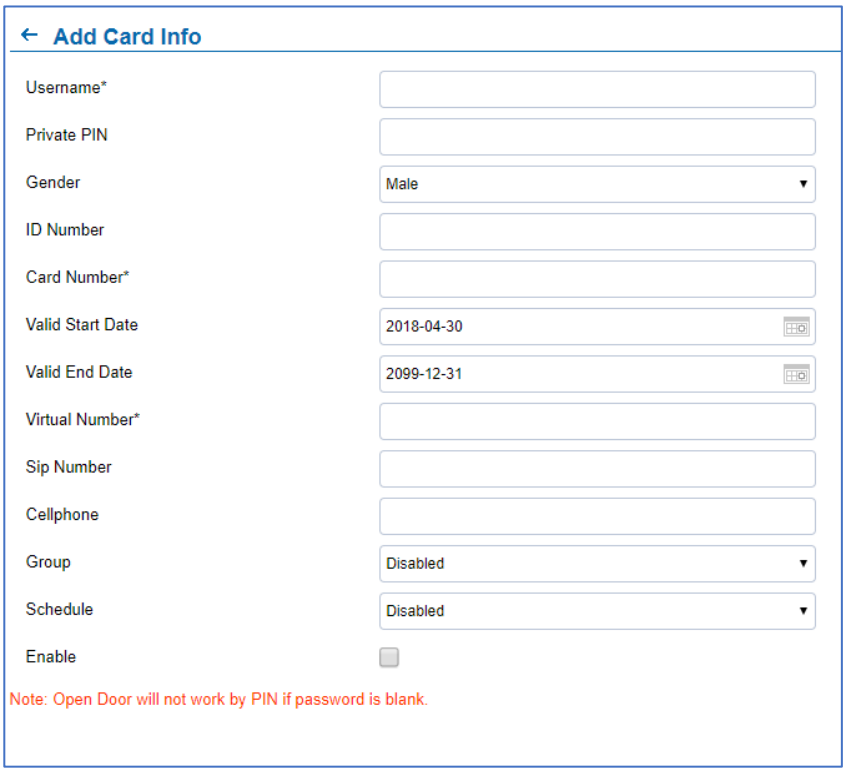


Figure 46: Card Info

Table 9: Card Info

Username	Configures the username to identify the user.
Private Door Password	Specifies a specific password to unlock the door.
Gender	Selects a gender, either Male or Female.
ID Number	Enters an ID number (This number is set by the admin to identify each user uniquely).
Card Number	Enters the RFID Card number (this is the number written on the RFID card. When "card issuing mode" is enabled, this filed will be added automatically.
Valid Start Date	Configures the start date of validity of the RFID card.
Valid End Date	Configures the End date of validity of the RFID card.
Virtual Number	When dialing directly from the keypad, the GDS accept only Virtual number to identify a user, once the Virtual number is typed followed by **#** key, the SIP Number will be dialed.
SIP Number	Configures the SIP Number which is mapped with virtual number. Once the virtual number is dialed the GDS3710 will send an INVITE to the SIP Number. **Note:** The SIP Number can be configured with an extension/phone number or IP address. Example: 192.168.5.124
Cellphone	Configures cellphone of the user.
Group	Specifies to which group the user will be added.
Schedule	Specifies the schedule that will be assigned to the user.
Enable	Enable/Disable the RFID card.

Note:

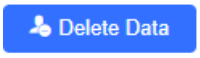
- Group overrides Schedule.

- If Schedule is set as "Disabled" the RFID Card will be accepted when swiped.

Add Users Automatically

If *[Enable Card Issuing Mode]* is checked, the GDS3710 keypad will start blinking and once an RFID card is swiped, data stored on the card will be added into the GDS3710 card management page, user can still edit the entry added automatically by modifying some fields.

Users Operation

- Click on  to edit the entry or show details of the entry.
- Select the entries and click on 

to delete the selected users.

- Click Reload Data to refresh the data entered to the GDS3710.
- Users can use Go to: to navigate through User Management pages.

Group

The Group page permits to manage the groups which will contains multiple users, click on + Add to create new groups or to edit existing groups or to delete the group.

Note: Users can create up to 50 groups.

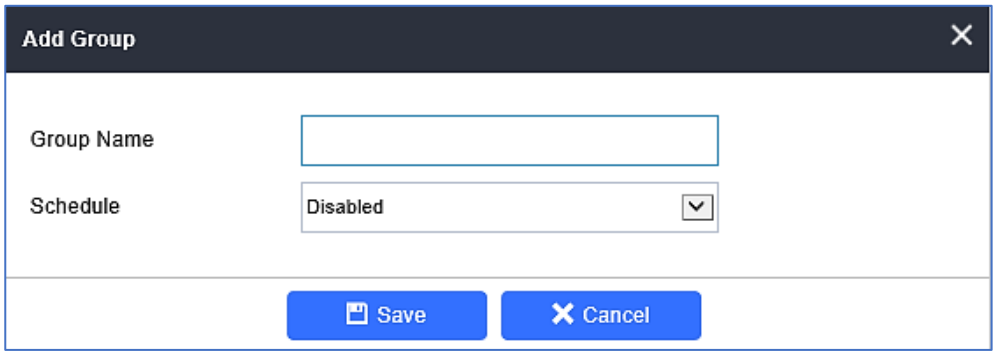


Figure 47: Add Group

Table 10: Add Group

Group Name	Configures the name to identify the group.
Schedule	Specifies the schedule that will be used by the group.

The following screenshots display the list of the created groups.

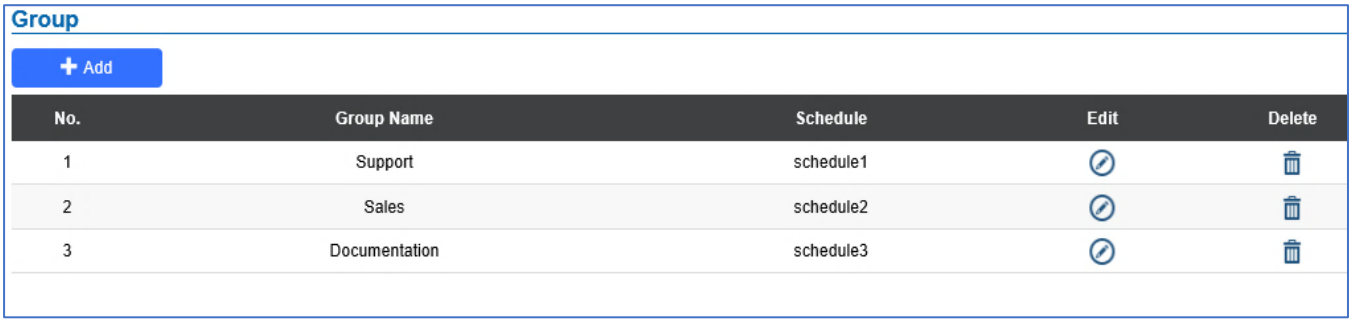


Figure 48: Groups List

Schedule

The Schedule page allows to manage schedule time frames which will be assigned to the users for door system usage. Out of the configured time intervals, GDS3710 will not allow users to access.

Click on to edit a schedule or for schedule details.

Note: The GDS3710 supports up to 10 schedules.

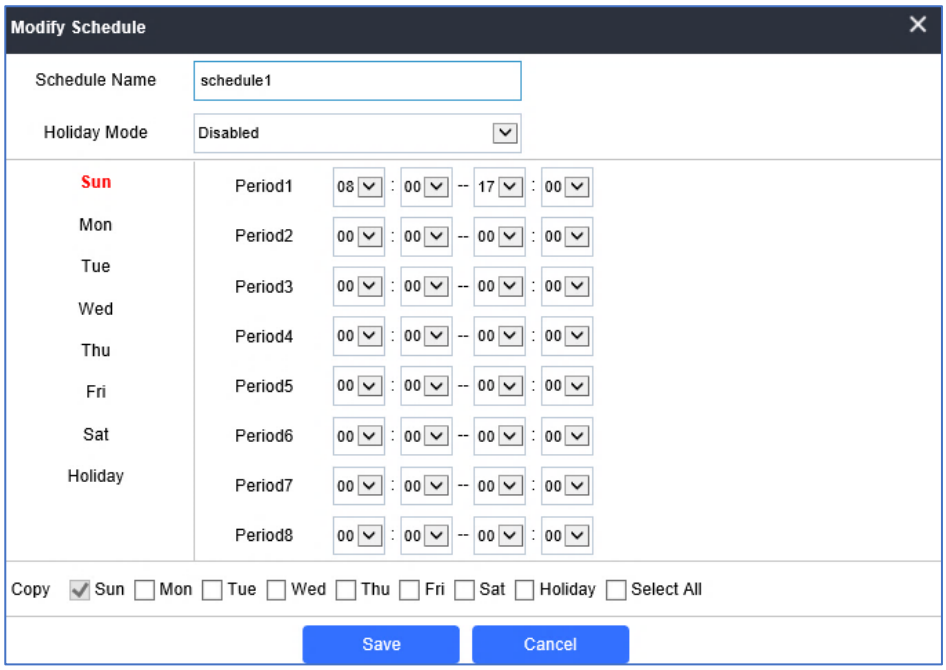


Figure 49: Edit Schedule Time

Holiday

The Holiday page allows to manage holidays which will be assigned to the users for door system usage.

Click on to edit the holidays or for holiday details.

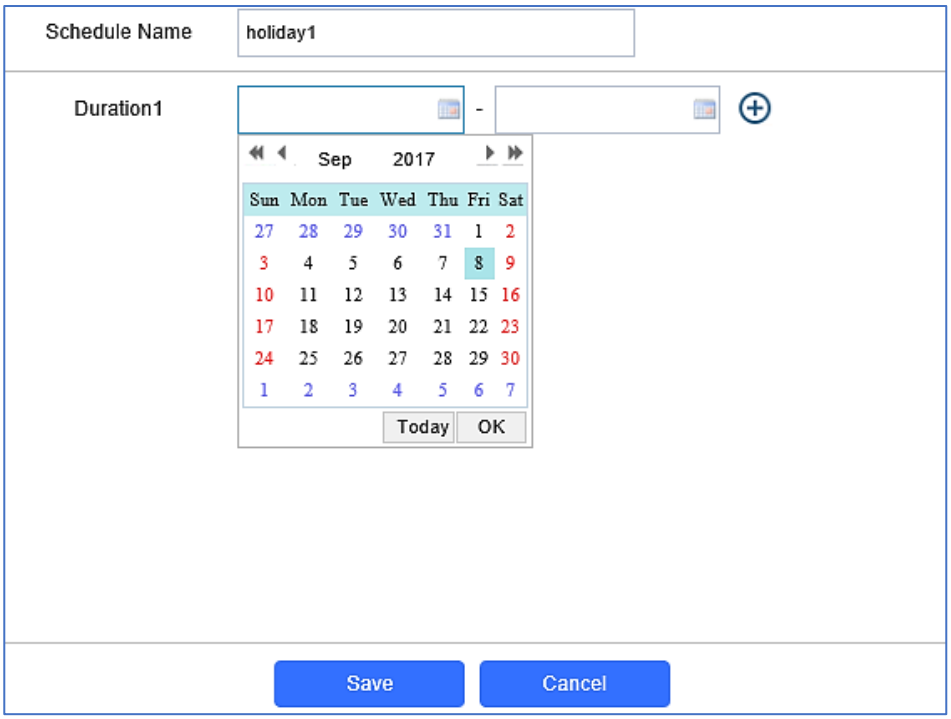


Figure 50: Edit Holiday Time

System Settings

This page allows users to configure date and time, network settings as well as access method to the GDS3710 and password for accessing the Web GUI.

Date & Time Settings

This page allows users to adjust system date and time of the GDS3710.

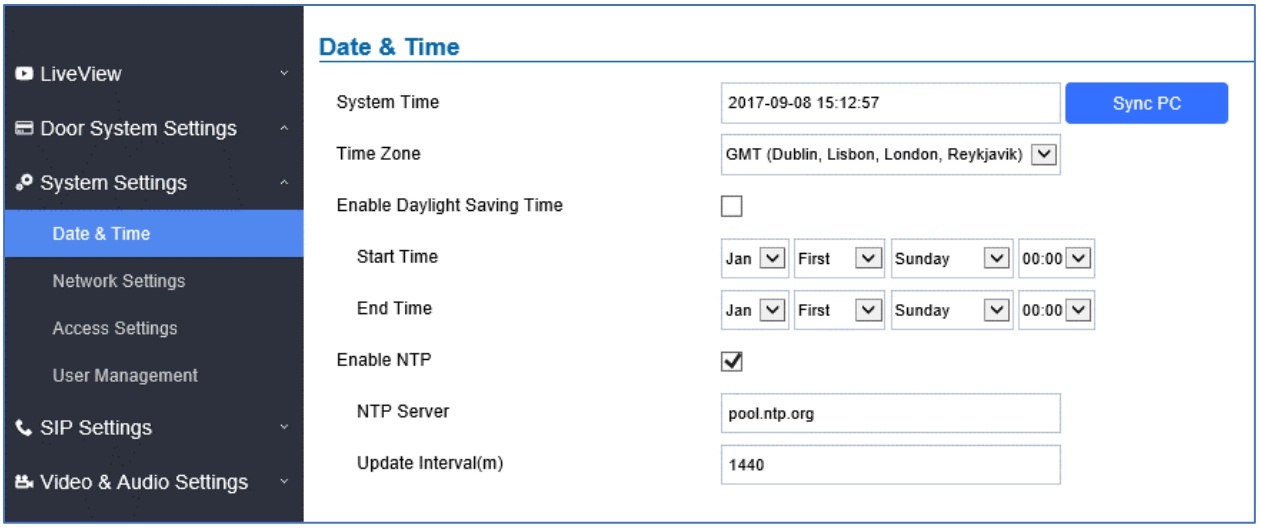


Figure 51: Date & Time Page

Table 11: Date & Time

System Time	Displays the current system time.
Sync PC	Clicks to synchronize current time with the computer.
Time Zone	Selects from drop down menu the preferred time zone.
Enable Daylight Saving Time	Enables Daylight Saving Time.
Start time	Selects the Start time of DST.
End Time	Selects DST end time.
Enable NTP	Enables NTP to synchronize device time.
NTP Server	Configures the domain name of NTP server.
Update Interval	Configures the Interval (in minutes) to retrieve updates from the NTP server.

Network Settings

This page allows users to set either a static or DHCP IP address to access the GDS3710.

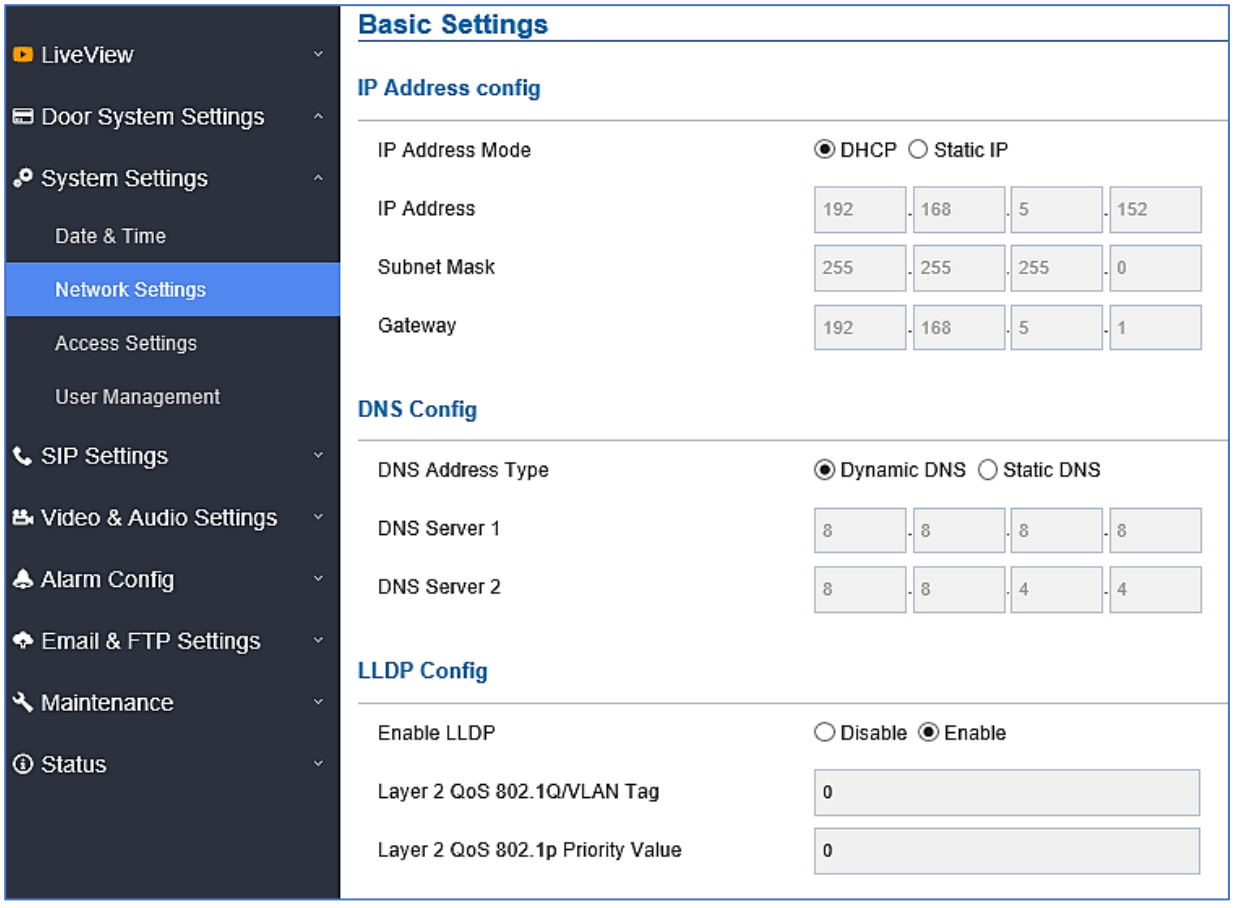


Figure 52: Basic Settings Page

Table 12: Basic Settings

IP Address Mode	Selects DHCP or Static IP. Default DHCP. (Static recommended)
IP Address	Configures the Static IP of the GDS3710.
Subnet Mask	Configures the Associated Subnet Mask.
Gateway	Configures the Gateway IP address.
DNS Address Type	Specifies the DNS type used: Dynamic DNS or Static DNS.
DNS Server 1	Configures DNS Server 1 IP address.
DNS Server 2	Configures DNS Server 2 IP address.
Enable LLDP	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is "Enabled".
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets. Default value is 0.
Layer 2 QoS 802.1p Priority Value	Assigns the priority value of the Layer2 QoS packets. Default value is 0.

Notes:

- If the GDS3710 is behind SOHO (Small Office Home Office) router with port forwarding configured for remote access, static IP should be used to avoid IP address changes after router reboot.
- TCP port above 5000 is suggested to Port forward HTTP for remote access, due to some ISP would block port 80 for inbound traffic. For example, change the default HTTP port from 80 to 8088, to make sure the TCP port will not be blocked.
- In addition to HTTP port, RTSP port is also required to configure via port forwarding, so that the remote party can view the video stream.
- If the default TCP port 80 is changed to port "A", then RTSP port should be "2000+A" (changed from default TCP 554). Both TCP port "A" and "2000+A" should be configured for port forwarding in the router. For example, of the HTTP port is changed to 8088, the RTSP port should be 10088, both TCP ports 8088 and 10088 should be configured for port forwarding to have remote GDS3710 access: 8088 for web portal, and 10088 for video streaming.

Access Settings

This page configures the GDS3710 access control parameters.

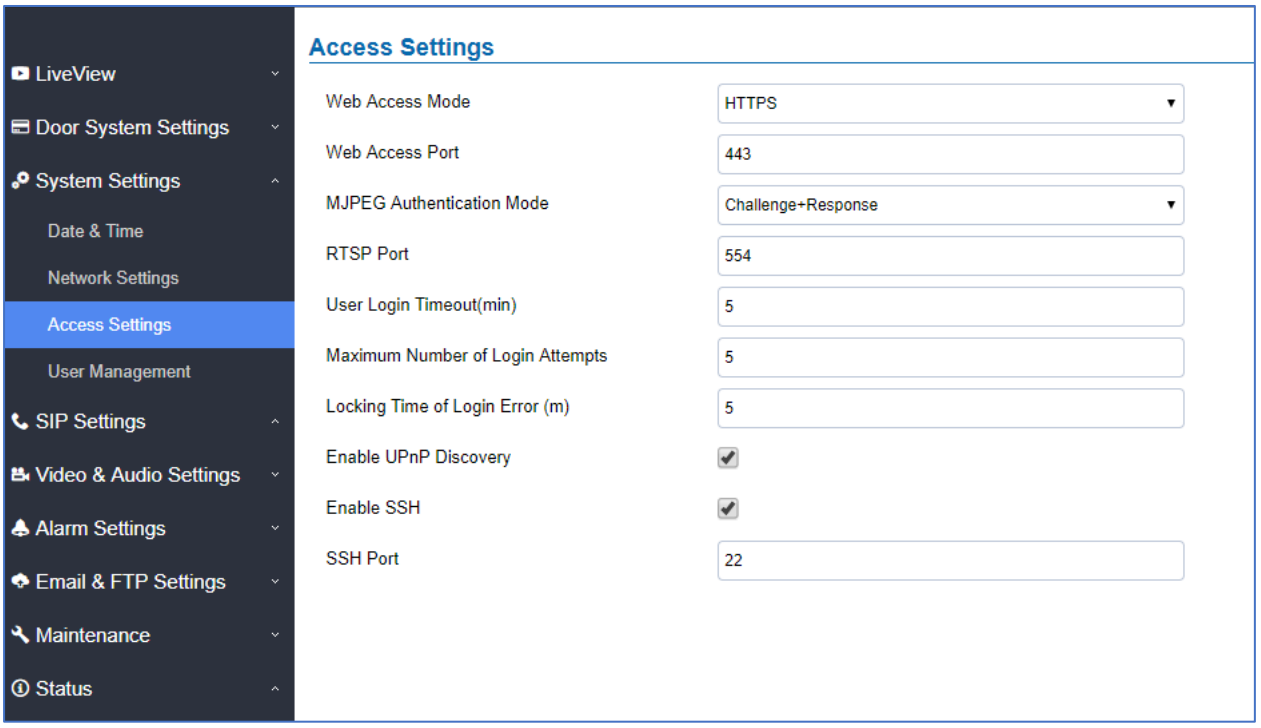


Figure 53: Access Settings Page

Table 13: Access Settings

Web Connection Mode	Selects the access mode to the webGUI either HTTP or HTTPS.
Web Access Port	Specifies the TCP port for Web Access, default 443.
RTSP Port	Specifies RTSP port for media stream, default TCP port 554.
MJPEG Authentication Mode	Allows 3rd party system integrator or developers to implement related application for users. By default, this feature is disabled and use more secured "Challenge+Response" mode. If enabled, user can send HTTP API with correct credentials to retrieve MJPEG video stream or JPEG snapshot from GDS3710. Notes: 1- The MJPEG stream can be retrieved via the following URL HTML based ➔ http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html Stream ➔ http(s)://admin:admin@ip:port/jpeg/stream 2- The MJPEG stream retrieved via the methods above is running on the background and cannot be tuned. If users want more flexibility they can use the three configurable video streams as shown on [**Retrieving Video Streams**]
User Login Timeout(min)	If no action is made within this time the GDS3710 will logout from the Web GUI, range is between 3 and 60.

Max Times Consecutively Login Error	Specifies the allowed login times error limit, if the unsuccessful login attempts exceed this value, the GDS3710 webGUI will be locked for the time specified in Login Error Lock Time.
Login Error Lock Time(m)	Specifies how long the GDS3710 is locked before a new login attempt is allowed.
Enable UPnP Discovery	UPnP (or mDNS) function for local discovery. Default setting is enabled.
Enable SSH	Selects to Enable/Disable SSH access. Default setting is enabled.
SSH Port	Specifies the SSH port. Default setting is 22.

User Management

This page allows users to configure the password for administrator. Since this is a door system which must be a secure product, the use is only limited to administrator.

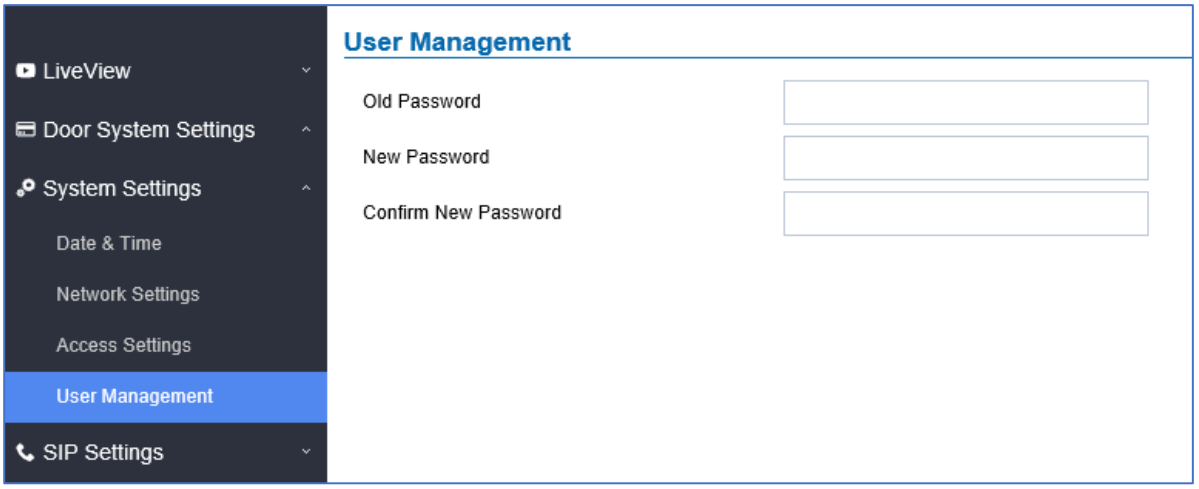


Figure 54: User Management Page

Table 14: User Management

Old Password	Old password must be entered to change new password.
New Password	Fill in the revised new password in this field.
Confirm User Password	Re-enter the new password for verification, must match.

Note:

When trying to change the password, users need to set the "**Password Recovery Email**" which is a valid Email account configurable under "**Email & FTP Settings →Email Settings**" to retrieve the email before the new admin password take effect as displayed on the following screenshot.

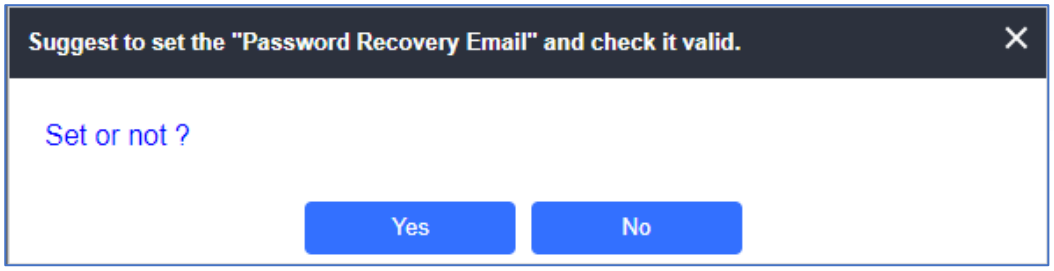


Figure 55: Password Recovery Email

SIP Settings

SIP Basic Settings

Basic Settings allow users to configure their SIP account.

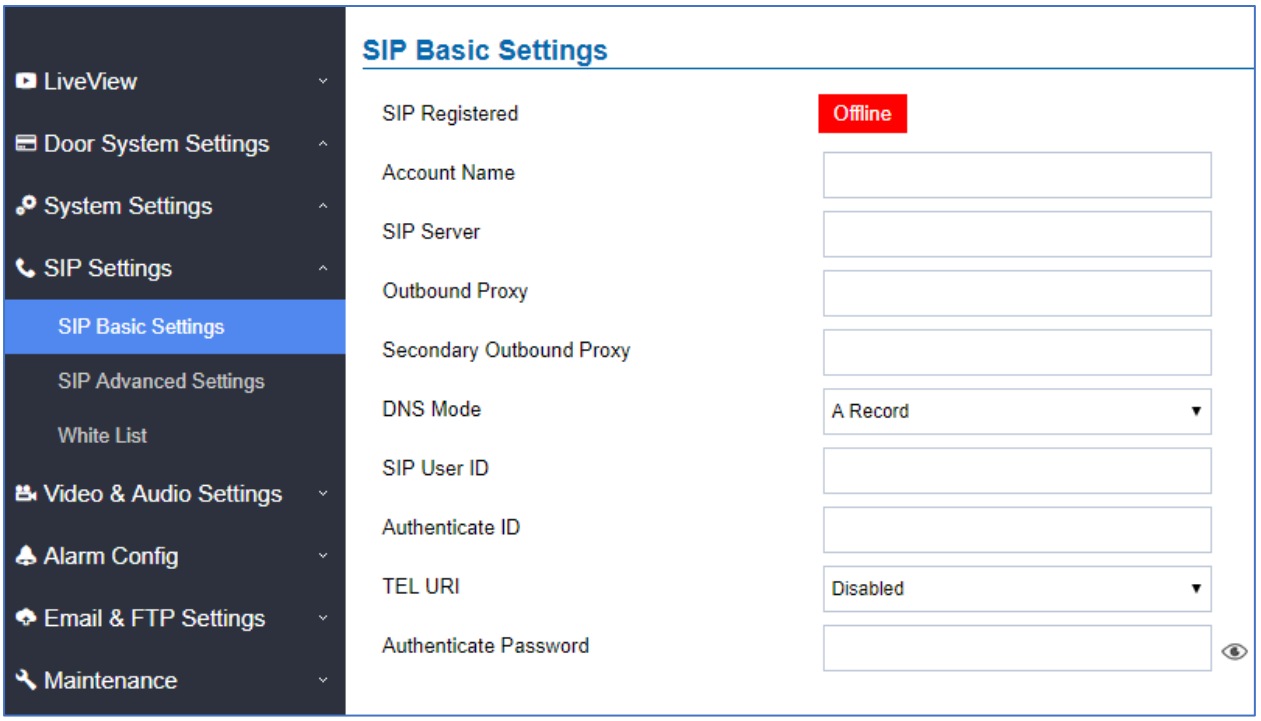


Figure 56: SIP Basic Settings Page

Table 15: SIP Basic Settings

SIP Registered	Displays the SIP registration status. Display "Online" or "Offline".
Account Name	Configures the SIP account name used for identification.
SIP Server	Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.
Outbound Proxy	Configures the IP or FQDN of Outbound proxy server.
Secondary Outbound Proxy	Configure the IP or FQDN of secondary Outbound Proxy Server.

SIP User ID	Configures the SIP username or telephone number from ITSP.
Authenticate ID	Configures the Authenticate ID used by SIP proxy.
TEL URI	Select “User=Phone” or “Enabled” from the dropdown list. If the SIP account has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable".
Authenticate Password	Sets the Authenticate password used by SIP proxy.

SIP Advanced Settings

This page allows Advanced SIP parameters to be configured.

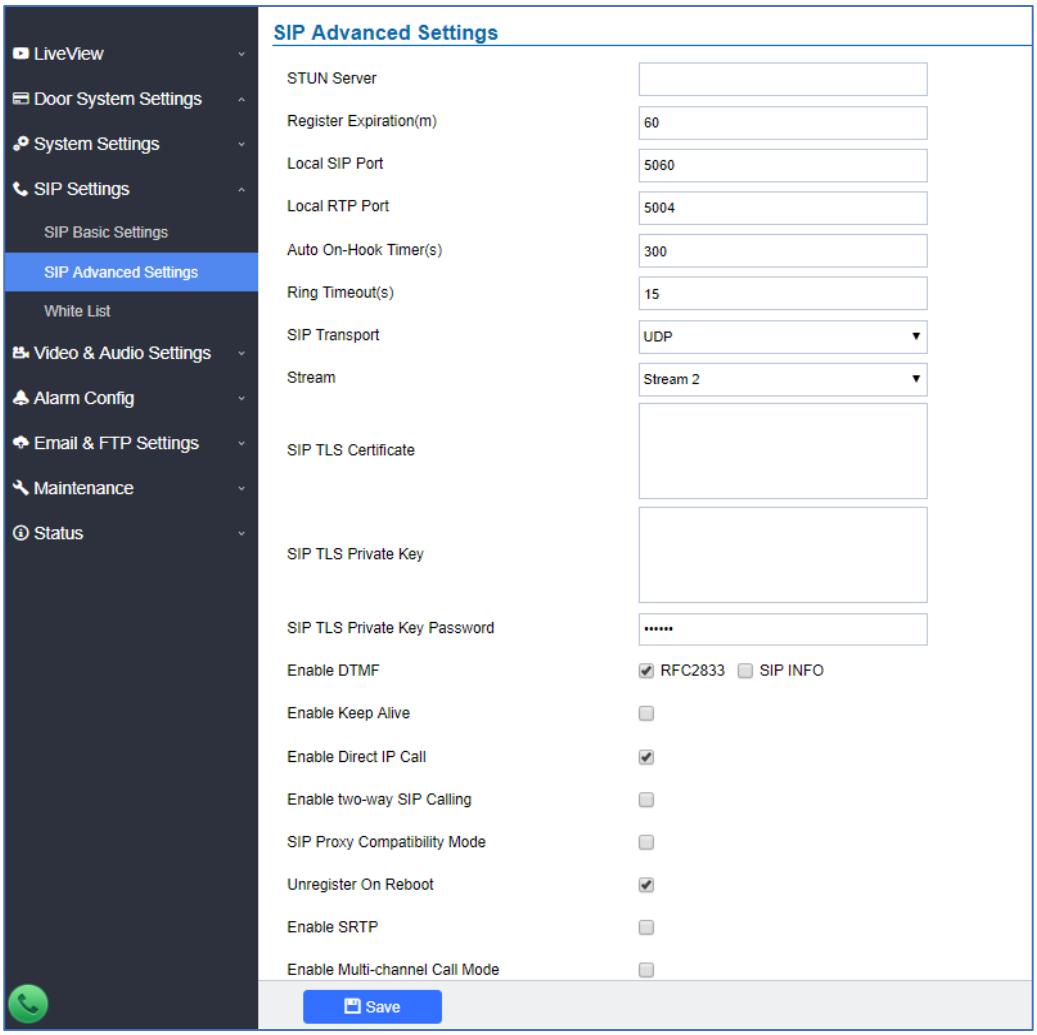


Figure 57: SIP Advanced Settings Page

Table 16: SIP Advanced Settings

STUN Server	Configures the STUN server FQDN or IP. If the device is behind a non-symmetric router, STUN server can help to penetrate & resolve NAT issues.
Register Expiration	Sets the registration expiration time. Default setting is 60 minutes.
Local SIP Port	Sets the local SIP port. Default setting is 5060.
Local RTP Port	Sets the local RTP port for media. Default setting is 5004.
Auto On-Hook Timer	Configures the auto on-hook timer (in seconds) for automatic disconnecting the SIP call. Default setting is 300.
Ring Timeout(s)	Specifies the Ring timeout, when no reply is returned from the called party after exceeding this filed, the GDS3710 will hang up the call. The value is in the range of 0s – 60s. By default; it is “15” seconds.
SIP Transport	Chooses the SIP transport protocol. Default settings is UDP.
Stream	Selects which stream to use for SIP calls. Default 2nd stream, strongly recommended 2nd or 3rd stream due to bandwidth utilization.
SIP TLS Certificate	Copy/Paste the TLS certificate here for encryption.
SIP TLS Private Key	Input private key here for TLS security protection.
SIP TLS Private Key Password	Specifies the password for SIP TLS private Key.
Enable DTMF	Specifies the mechanism to transmit DTMF digits. There are 2 supported modes: • **RFC2833** sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. • **SIP INFO** uses SIP INFO to carry DTMF. Default setting is "RFC2833"
Enable Keep Alive	Checks to help NAT resolution, sending alive packets.
Enable Direct IP Call	Accepts peer-to-peer IP call (over UDP only) without SIP server. Default is “Enabled”.
Enable two-way SIP Calling	Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.
SIP Proxy Compatibility Mode	Enables more proxy compatibility with cost of bandwidth, the SIP call will send both audio and video no matter what.

Unregister on Reboot	Allows the SIP user's registration information to be cleared when the GDS3710 reboots. The SIP REGISTER message will contain "Expires: 0" to unbind the connection **Note:** This Option is enabled by default.
Enable SRTP	Enable SRTP mode. By default, it's disabled.
Enable Multi-channel Call Mode	This feature allows the device to receive multiple calls at the same time, with one active and others on hold (up to 4 calls maximum). The first call the blue LED light will light up keypad digit "1", 2nd call will light up keypad digit "2", and so on. On hold call will have related digit blinking while active call will have the digit blue LED solid light up. Call can be switched by pressing the blinking digits.
Special Feature	Configures GDS's settings to meet different vendors server requirements. Users can choose from Standard, Broadsoft. The default settings is "Standard"
Enable RTCP	This option allows 3rd party Service Provider or Cloud Solution to monitor the operation status of the GDS3710 by using related SIP Calls. By default, it's disabled. Users can choose either RTCP or RTCP-XR.

Click-To-Dial

The GDS3710 allows users to manage their calls using the Click to Dial feature which permits to initiate calls using the Web GUI by pressing the Click to dial button to access the call menu as displayed on the following screenshot.

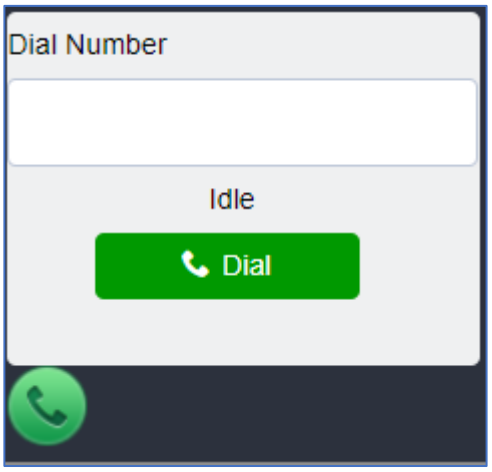


Figure 58 : Click-To-Dial

White List

This page allows users to configure the white list, which is a phone number or extension list that can call the GDS3710. (the call will be automatically answered when calling from a phone set on the white list).

The white list can contain up to 30 numbers, and each number can contain up to 20 digits.

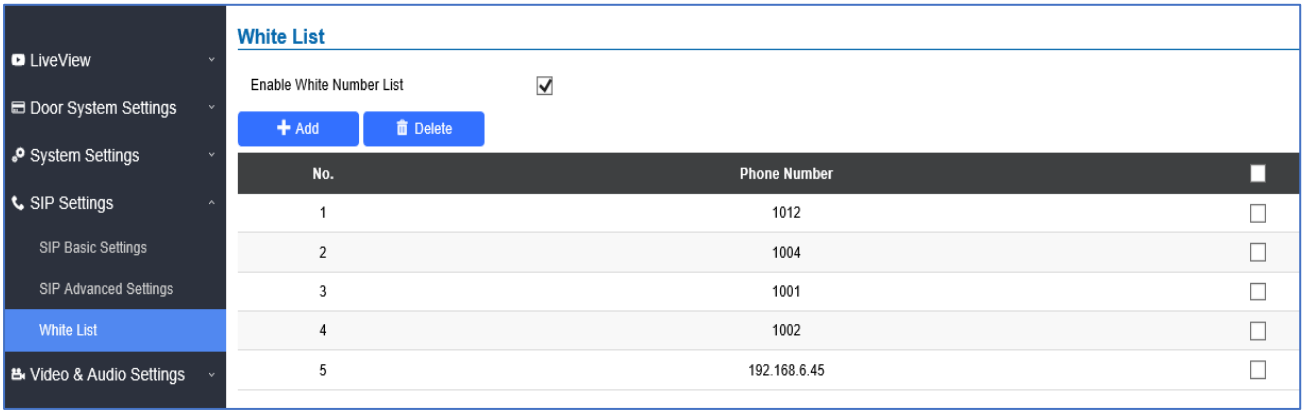


Figure 59: White List Page

The table below gives a brief overview of the options:

Table 17: White List

Enable White Number List	Enables the White List feature.
Add	Adds a new phone number to the white list.
Delete	Deletes a number from the white list.

Note: All whitelisted numbers can open door remotely using PIN Code when calling GDS.

Video & Audio Settings

The audio and videos settings allow users to configure the video / audio codecs, videos resolution, CMOS settings and audio related settings.

Video Settings

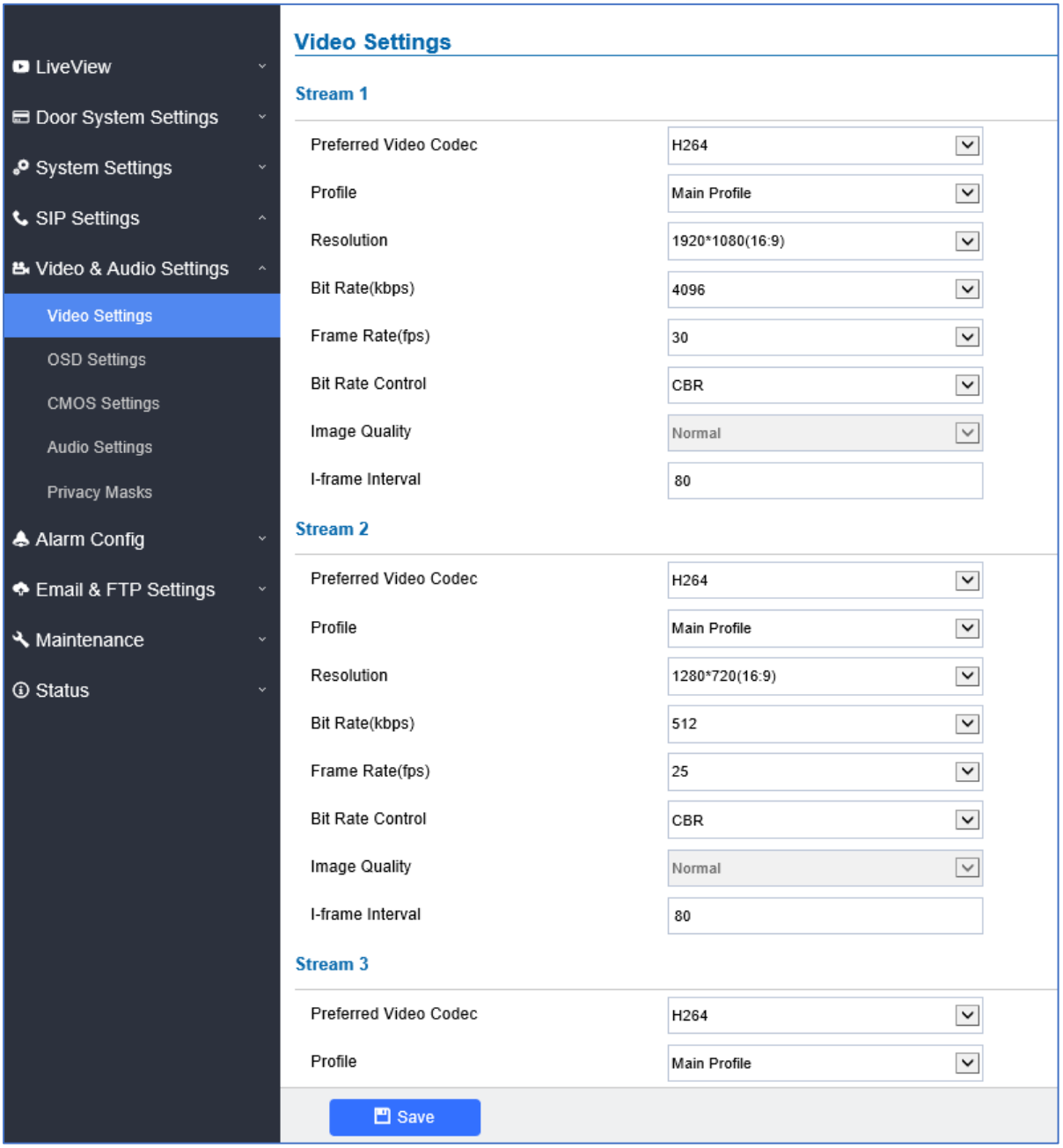


Figure 60: Video Settings Page

Table 18: Video Settings

Preferred Video Codec (Stream1)	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
Profile	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is “Main Profile”.

Resolution	Specifies the resolution in pixels used at video image, 1080p or 720p.
Bit Rate(kbps)	Selects the video bit rate or bandwidth used.
Frame Rate(fps)	Selects the maximum frame rate used (more data if big frame used).
Bit Rate Control	Selects the constantly bit rate, or variable bit rate.
Image Quality	Selects the image quality used when Variable Bit Rate used.
I-frame Interval	Configures the I-frame interval (suggested 2~3 times of frame rate).
Preferred Video Codec(Stream2)	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
Profile	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is “Main Profile”.
Resolution	Specifies the resolution in pixels used at video image, 1080p or 720p.
Bit Rate(kbps)	Selects the video bit rate or bandwidth used.
Frame Rate(fps)	Selects the maximum frame rate used (more data if big frame used).
Bit Rate Control	Selects the constantly bit rate, or variable bit rate.
Image Quality	Selects the image quality used when Variable Bit Rate used.
I-frame Interval	Configures the I-frame interval (suggested 2~3 times of frame rate).
Preferred Video Codec(Stream3)	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
Profile	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is “Main Profile”.
Resolution	Specifies the resolution in pixels used at video image, 1080p or 720p.
Bit Rate(kbps)	Selects the video bit rate or bandwidth used.
Frame Rate(fps)	Selects the maximum frame rate used (more data if big frame used).
Bit Rate Control	Selects the constantly bit rate, or variable bit rate.
Image Quality	Selects the image quality used when Variable Bit Rate used.
I-frame Interval	Configures the I-frame interval (suggested 2~3 times of frame rate).

Notes:

- H.264 suggested if the GDS3710 needs to be viewed via Internet.
- For definition of Baseline, Main Profile and High profile of H.264 please refer to: H.264 Profiles
- If MJPEG is selected, reduce the frame rate to the minimal value to save bandwidth and get better image.
- Grandstream GDS3710 provides three video streams, users can use them with flexibility. For example, the high-resolution stream for local recording, another low or high resolution for SIP video phone call or remote smartphone monitoring application, or vice versa depending application scenarios.

- Use below link to calculate bandwidth and storage before installation
  http://www.grandstream.com/support/tools/bandwidth-storage-calc

Retrieving Video Streams

- To retrieve video stream via RTSP, users can use the following format：
  rtsp://admin:password@IP_GDS3710:Port/X where X=0,4,8 for 1st, 2nd, 3rd streams respectively
- To retrieve MJPEG video stream via http, users can use the following format:
  http(s)://admin:password@IP:port/jpeg/streamX (X=Stream channel 0,1,2)

Important note: MJPEG is uncompressed video and it can consume a lot of bandwidth and hardware resources, it is recommended to use it while taking this into consideration that it might slow down network and device.

OSD Settings

OSD Settings (On Screen Display) allow the users to Display time stamp and text on the video screen.

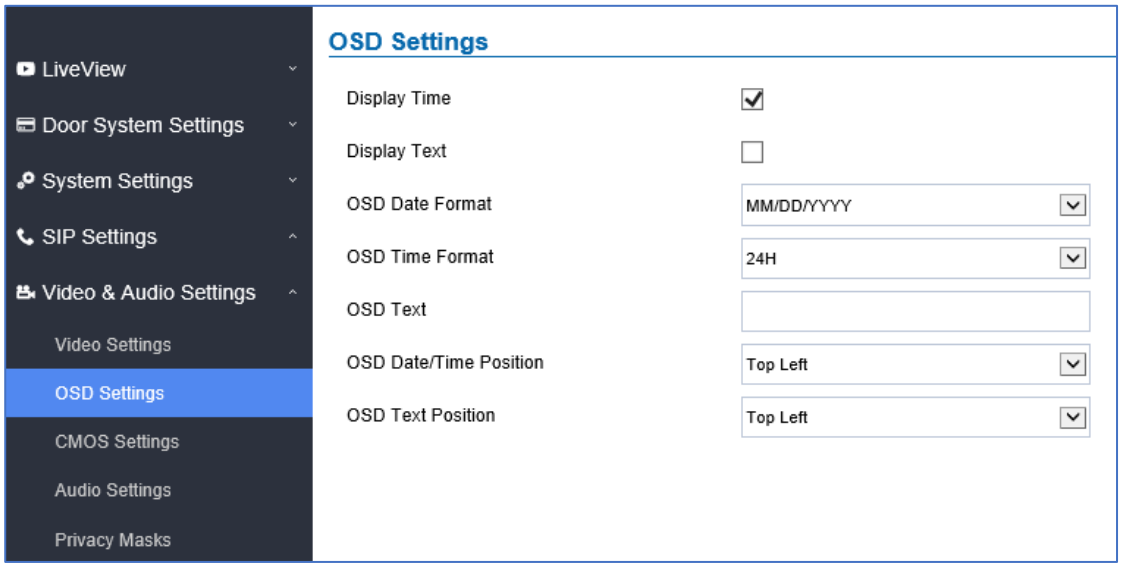


Figure 61: OSD Settings Page

Table 19: OSD Settings

Display Time	When checked, time will be displayed inside the video image.
Display Text	When checked, inputted text on “OSD Test” will be displayed on the video image.
OSD Date Format	OSD Date format, choose based on user preference.
OSD Time Format	OSD Time format, choose based on user preference.
OSD Text	Input a text (to identify the GDS3710) it will be shown on the screen.
OSD Date/Time Position	Show the Date/Time position on the screen.
OSD Text Position	Show the text position on the screen.

CMOS Settings

This page configures the CMOS parameters for different scenarios.

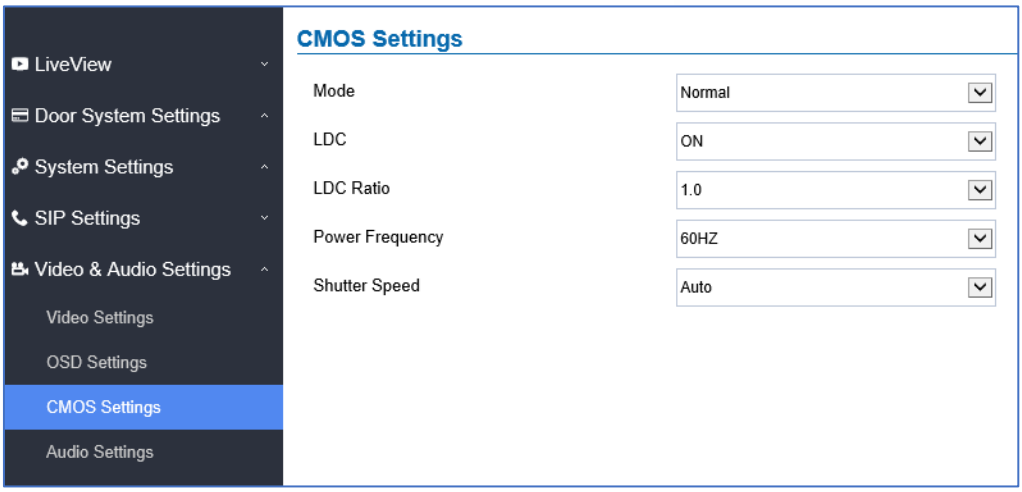


Figure 62: CMOS Settings Page

Table 20: CMOS Settings

Mode	Pull down to choose “Normal, Low Light, WDR” for different light condition. Default “Normal”.
LDC	Default “OFF”. When “ON” the display will take a normal shape, but will lose some details located at corner of the original view.
LDC Ratio	Select LDC Ratio. Available options: 0.7 ; 0.8 ; 0.9 ; 1.0 ; 1.1 ; 1.2 ; 1.3 Default value is 1.0
Power Frequency	Select the frequency power. 50Hz or 60Hz.
Shutter Speed	Defines how much time the shutter of the camera or exposed to the light, when taking a screenshot.

Audio Settings

This page allows users to configure the audio settings.

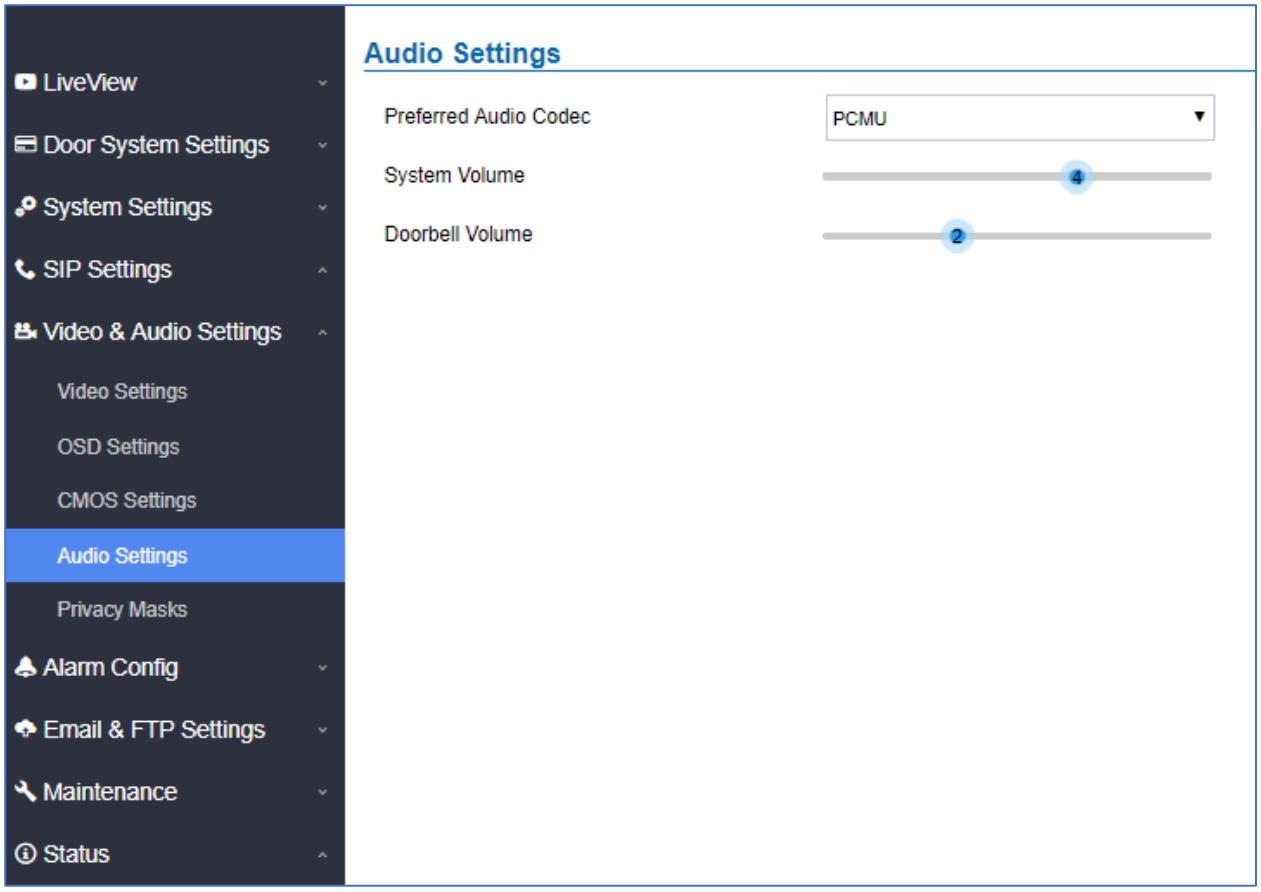


Figure 63: Audio Settings Page

Table 21: Audio Settings

Preferred Audio Codec	Configures the audio codec. Three codecs are available: PCMU, PCMA and G.722 are supported.
System Volume	Adjusts the speaker volume connected.
Doorbell Volume	Adjusts the doorbell volume.

Privacy Masks

This page allows users to configure privacy masks up to 4 different regions by selecting different regions requiring privacy mask as displayed on the following figure.

When privacy mask enabled, the video at related region will be masked by black color and no video displayed inside that mask.

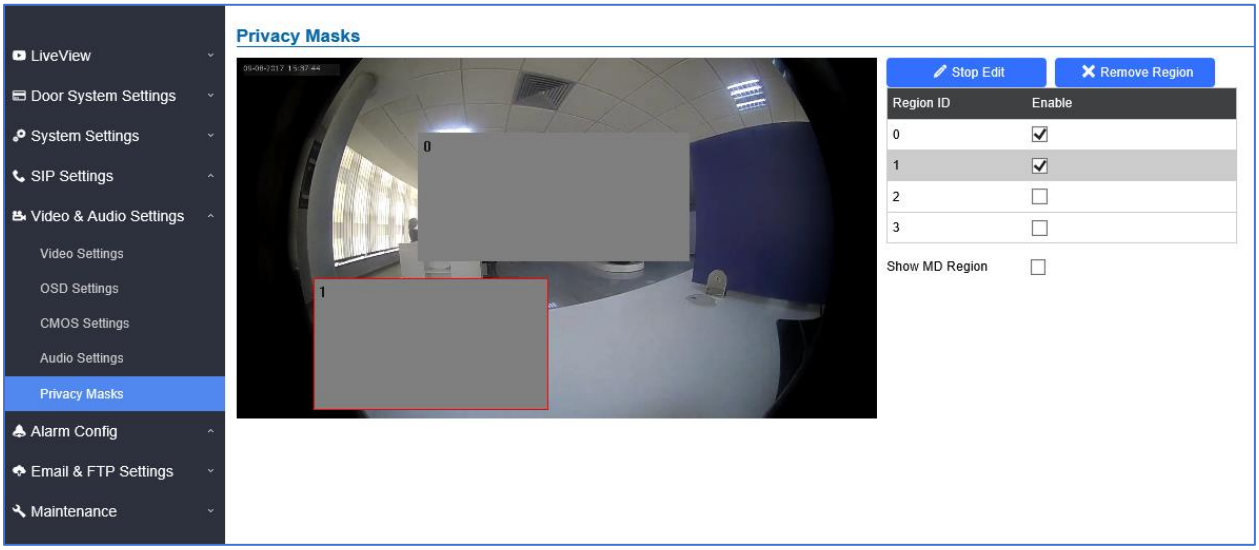


Figure 64: Privacy Masks Configuration Page

Alarm Config

This page allows users to configure alarm schedule and alarm actions.

Alarm Events Config

This page allows users to configure GDS3710 events to trigger programmed actions within predefined schedule.

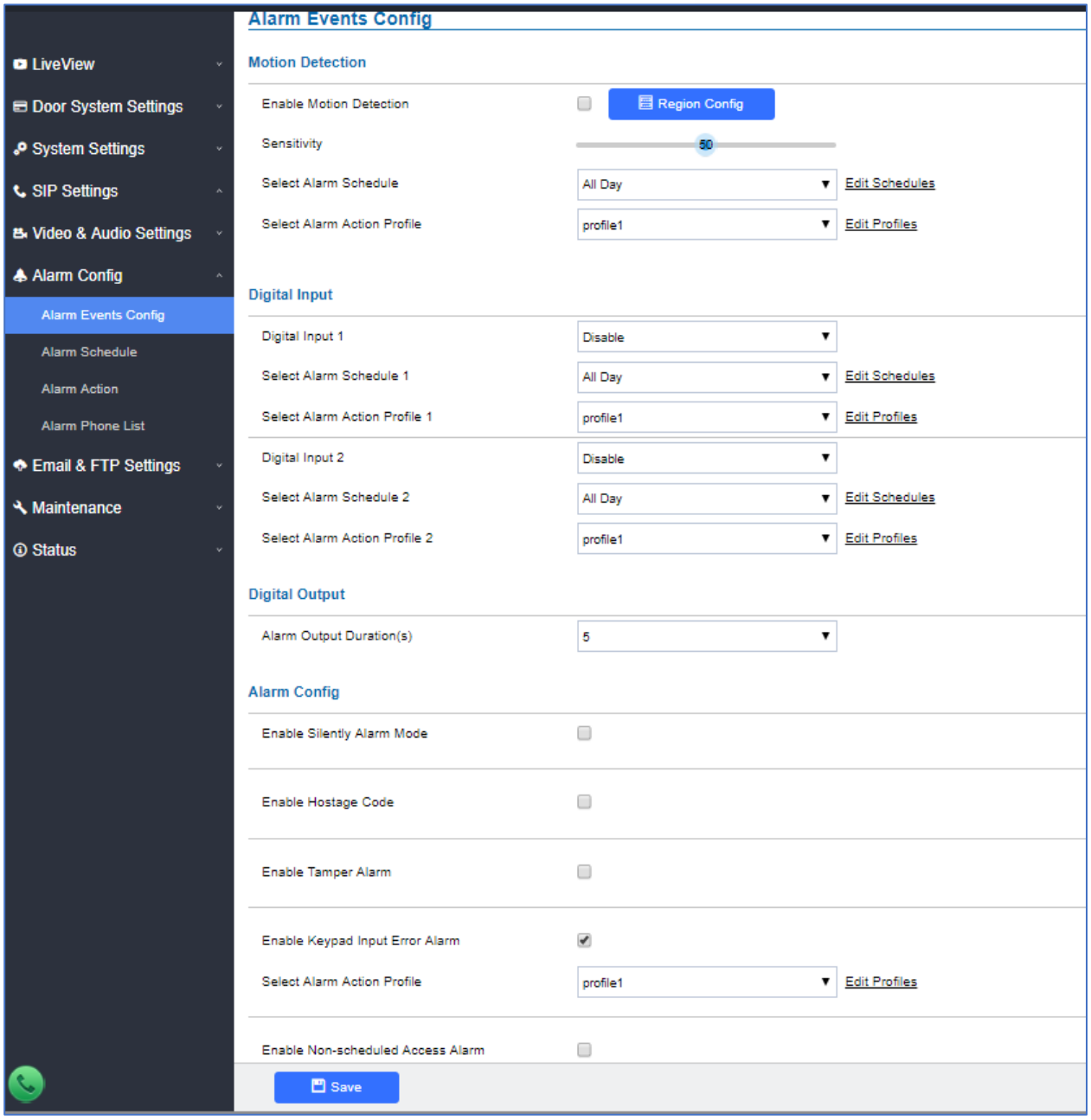


Figure 65: Events Page

Alarm can be triggered either by motion detection or by GDS3710 input.

Motion Detection

Users can select a specific region to trigger the alarm using motion detection.

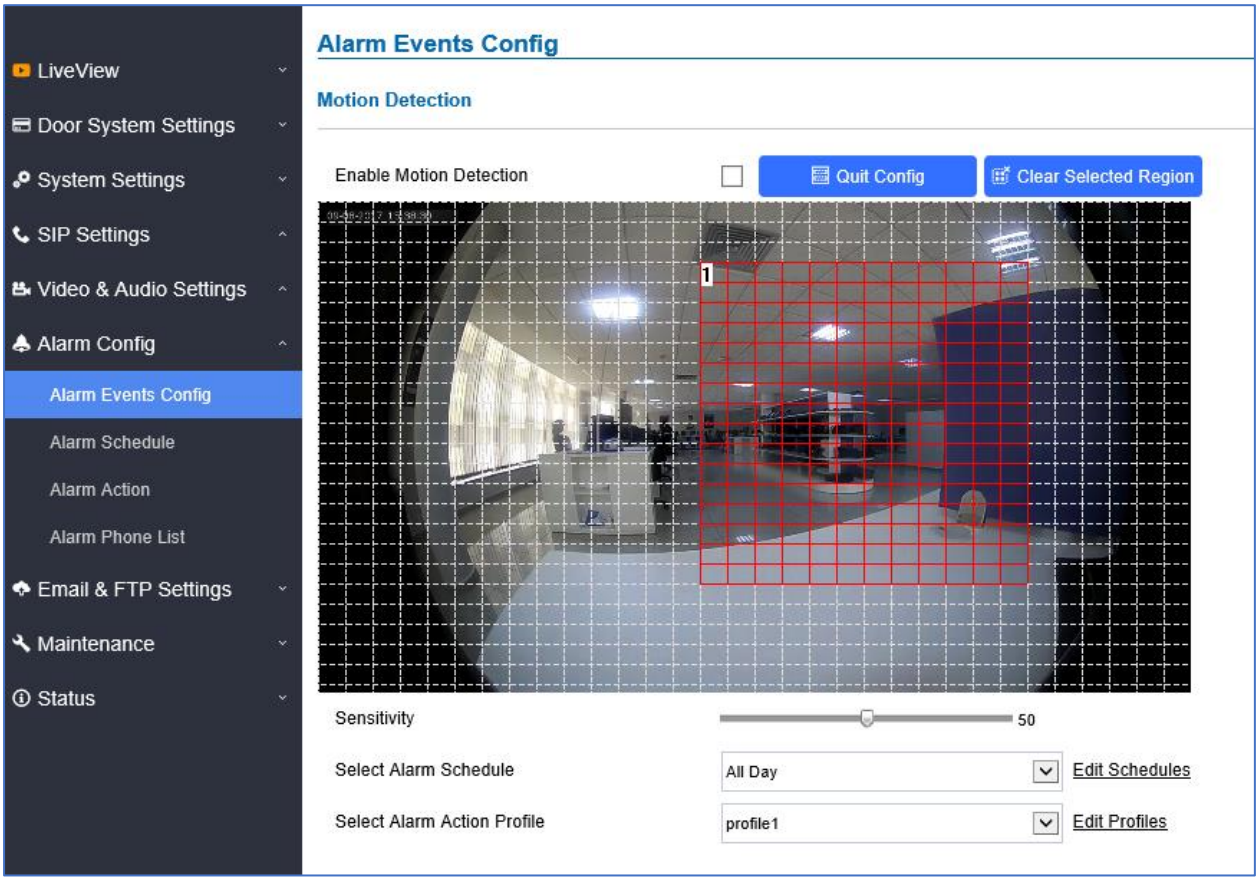


Figure 66: Region Config

Table 22: Motion Detection

Enable Motion Detection	Enables the motion detection feature.
Region Config	Configures the motion detection region.
Quit Config	Exits the motion detection region config menu.
Clear Selected Region	Selects a zone on the screen then click on “Clear” to delete the region.
Sensitivity	Specifies the region sensitivity (value between 0-100%).
Select Alarm Schedule	Selects the alarm schedule.
Select Alarm Action Profile	Selects the programmed Alarm Action profile.

Digital Input

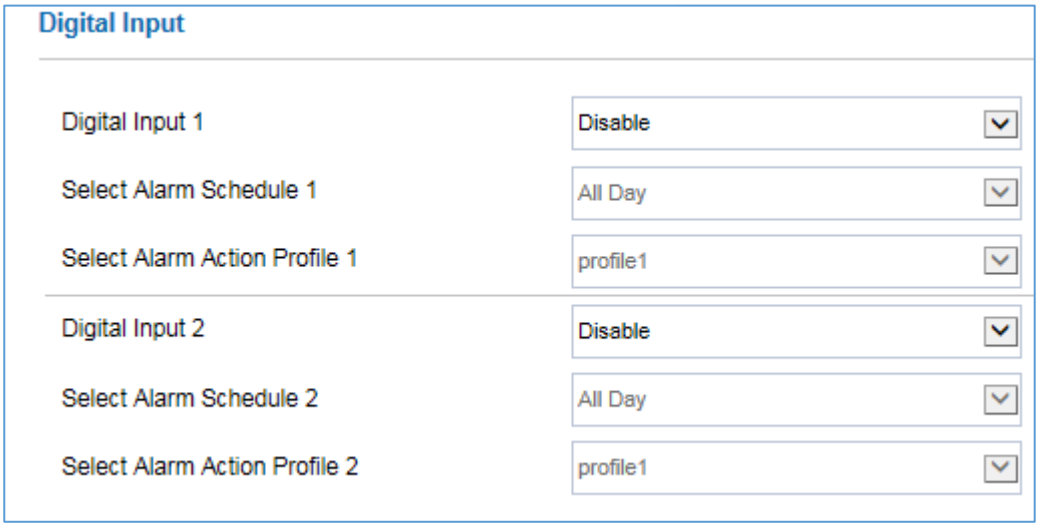


Figure 67: Digital Input

Table 23: Digital Input

Digital Input 1	Selects the Input method (alarm Input or Door Open).
Select Alarm Schedule 1	Selects the predefined Alarm Schedule.
Select Alarm Action Profile 1	Selects the predefined Alarm Action for Profile 1.
Digital Input 2	Selects the Input method (alarm Input or Door Open).
Select Alarm Schedule 2	Selects the predefined Alarm Schedule.
Select Alarm Action Profile 2	Selects the predefined Alarm Action for Profile 2.

Alarm Output

Alarm Output Duration(s) specifies how long the alarm output will take effect. The available values are: 5,10,15,20,25 and 30 seconds.

Silently Alarm Mode

If Silently Alarm Mode is enabled, GDS3710 will disable alarm sound and background light for specified alarms types (Digital Input, Motion Detection…) when they are triggered.

Note: This option affects only alarm sound/light, other actions will still be applied.

Table 24: Silently Alarm Mode

Enable Silently Alarm Mode	Enable/Disable silent alarm mode.
Silently Alarm Options	When the silently alarm mode is enabled, users can specify to which alarm options the silently mode will be applied to. The available options are: Digital Input, Motion Detection, Tamper Alarm, and Password Error.

Hostage Code

Hostage password can be used in a critical situation for instance a kidnaping or an emergency, users need to enter the following sequence to trigger the actions set for the Hostage Mode: "*** HostagePassword #**".

Table 25: Hostage Code Alarm

Enable Hostage Code	Enable/Disable the Hostage password mode.
Hostage Code	Configures the password for the hostage mode.
Select Alarm Action Profile	Select the Alarm action to be taken when the hostage password is typed on the GDS3710 keypad. **Note:** No sound alarm will be triggered in this mode.

Tamper Alarm

Tamper alarm is anti-hack from Hardware level. When this option is checked, if the GDS3710 is removed from the installation board, it will trigger configured alarm actions. There is an embedded mechanism on the GDS3710 that allows it to detect when the it is removed.

Table 26: Tamper Alarm

Enable Tamper Alarm	When activating this mode, GDS3710 will keep alarming until the alarm is dismissed.
Select alarm Action Profile	Select the type of alarms actions to be triggered for the tamper alarm mode.

Keypad Input Error Alarm

Table 27: Keypad Input Error Alarm

Enable Keypad Input Error Alarm	Enable/Disable the Input Error Alarm, GDS3710 will trigger alarm actions at every 5 incorrect attempts.
Select Alarm Action Profile	Select the type of alarms actions to be triggered after 5 incorrect attempts.

Non-Scheduled Access Alarm

Table 28 : Non-Scheduled Access Alarm

Enable Non-Scheduled Access Alarm	When enabling this feature, GDS3710 will trigger alarm to related administrator to be aware when legitimated users access the door out of the allowed configured schedule
Select Alarm Action Profile	Select the type of alarms actions to be triggered.

Alarm Schedule

This page specifies the configuration of Alarm Schedule.

Note: Schedule must be configured first to allow the alarm to take the related action.

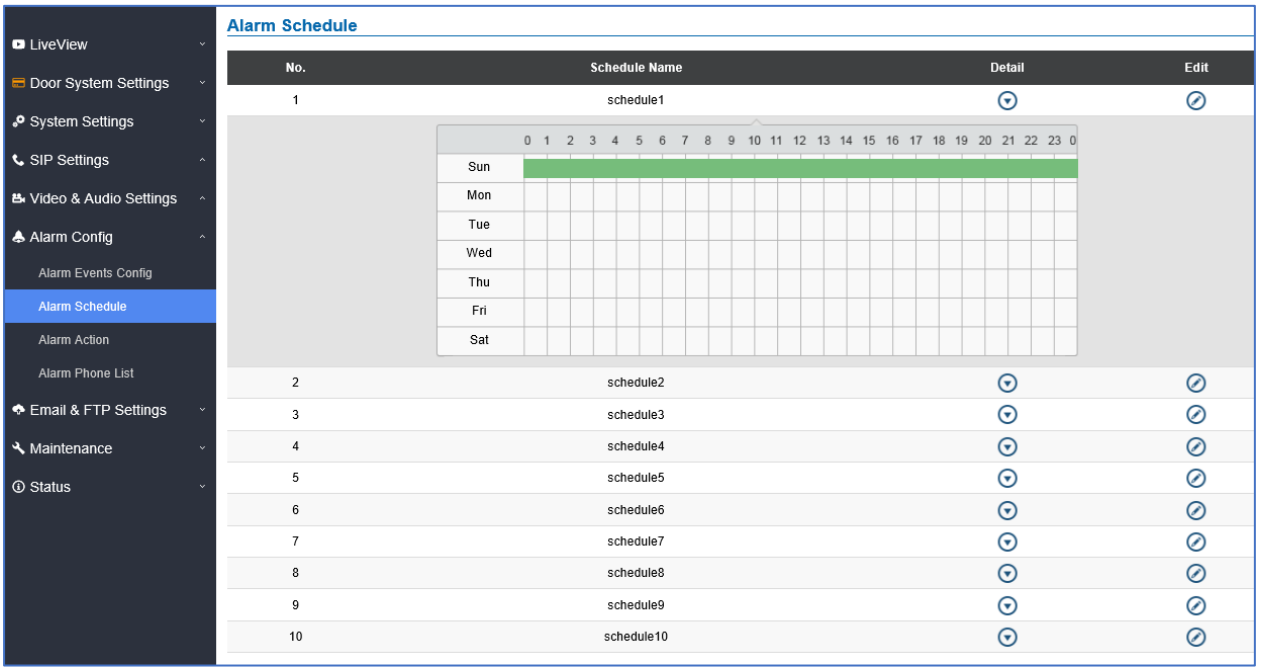


Figure 68: Alarm Schedule

GDS3710 supports up to 10 alarm schedules to be configured, with time span specified by users. User can edit the alarm schedule by clicking button. Usually the 24 hours' span is 00:00 ~ 23:59, which is 24 hours' format.

Users can copy the configuration to different date during the schedule programming.

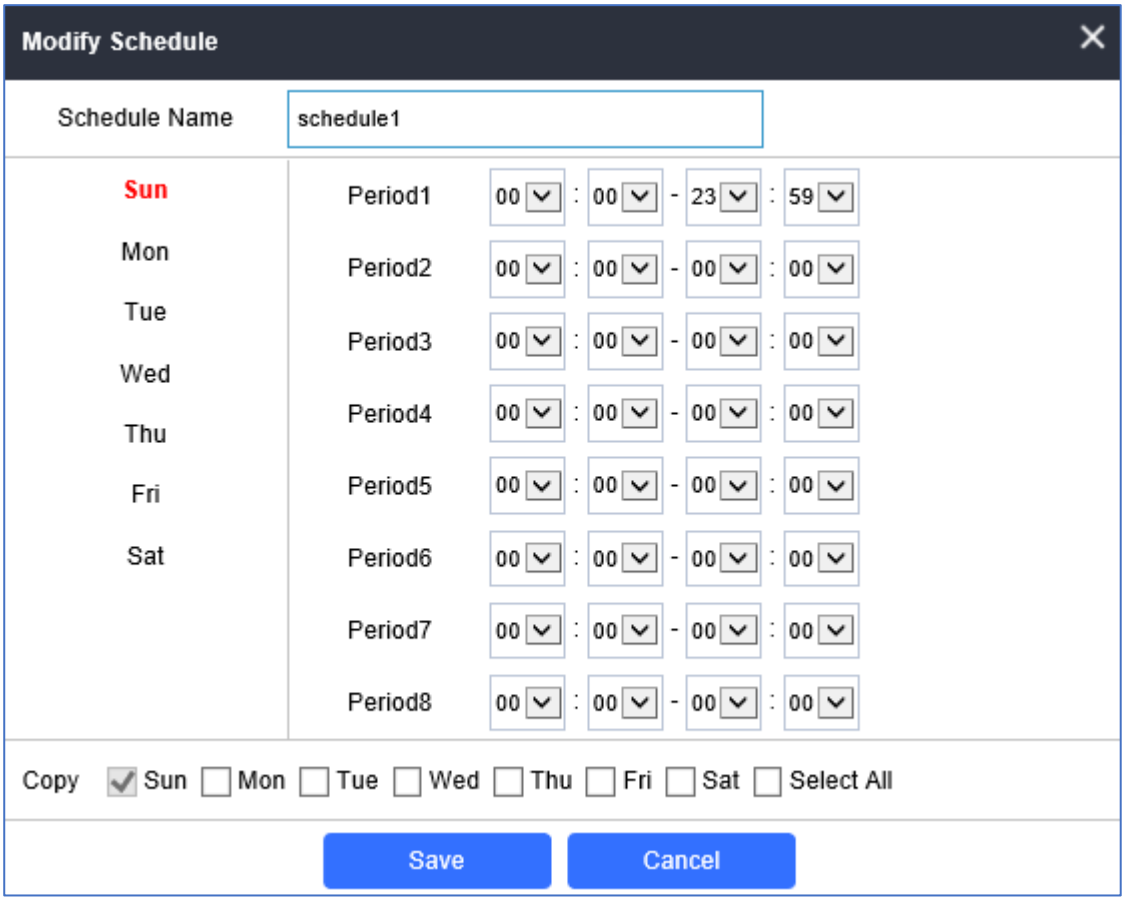


Figure 69: Edit Schedule

Alarm Action

This page specifies the configuration of Profile used by the Alarm Actions. A Profile is required before the Alarm Action can take effect.

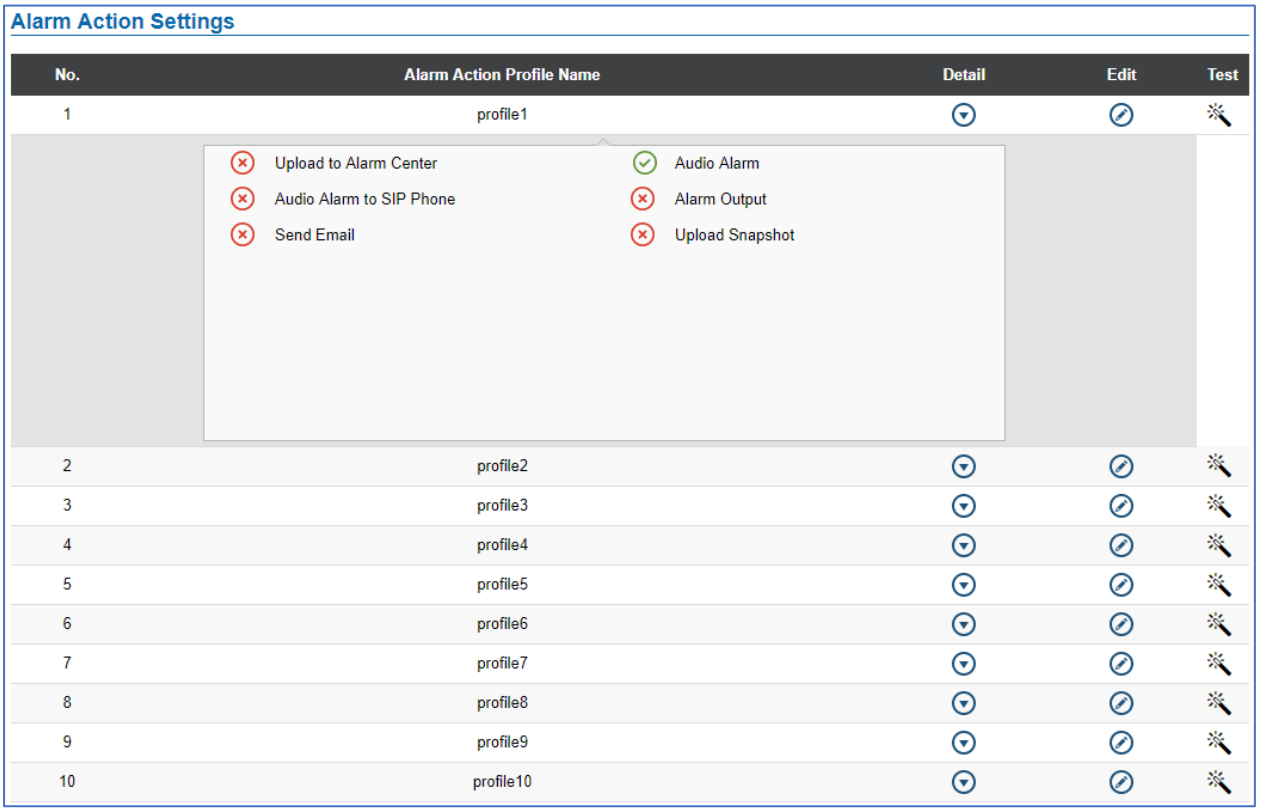


Figure 70: Alarm Action

User can edit the alarm action by clicking button, the following window will popup.

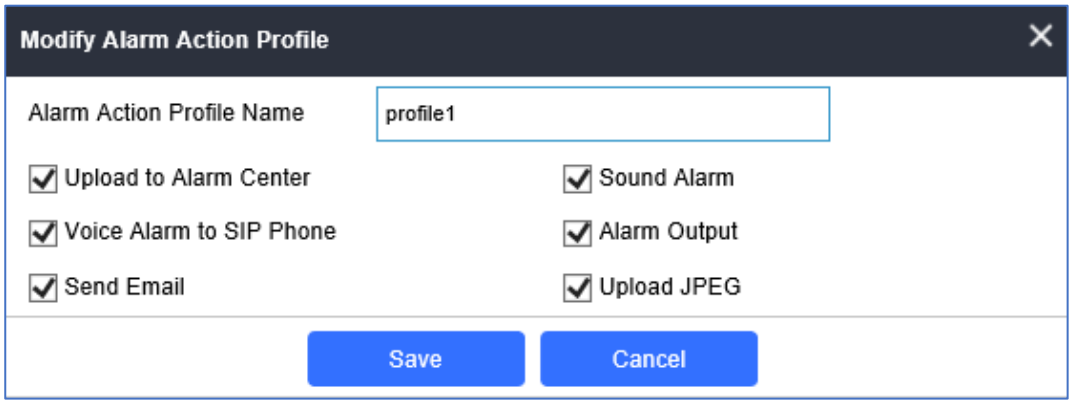


Figure 71: Edit Alarm Action

To test an alarm action profile, users can click on button and the GDS will initiate all actions specified on the select alarm profile.

Table 29: Alarm Actions

Upload to Alarm Center	If selected, the GDSManager will popup alarm window and sound alarm in the computer speaker.

Voice Alarm to SIP Phone	If selected, GDS3710 will call pre-configured (video or audio) phone and will play sound alarm.
Send Email	If selected, an email with snapshot will be sent to the pre-configured email destination.
Sound Alarm	If selected, GDS3710 will play alarm audio using built-in speaker.
Alarm Output	If selected, the alarm will be sent to the equipment (for example: Siren) connected to Alarm Output interface.
Upload JPEG	If selected, snapshots at the moment where the event is triggered will be sent to preconfigured destination (e.g.: FTP or email).

Alarm Phone List

This page allows users to configure the Alarm Phone List, which are phone numbers or extensions list that the GDS3710 will call out when event is trigged (e.g.: doorbell pressed).

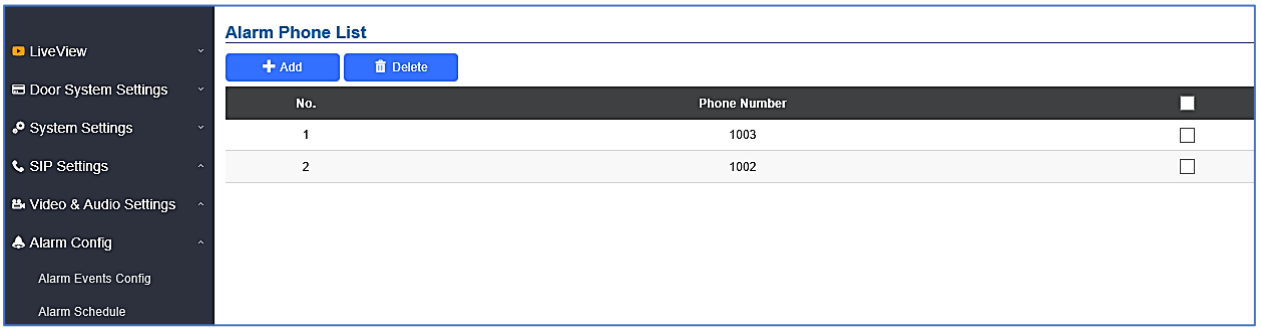


Figure 72: Alarm Phone List

Table 30: Alarm Phone List

Add	Adds new phone number to the alarm list.
Delete	Deletes a number from the phone alarm list.

Once the event is triggered (Motion Detection, Door Bell Pressed…), the GDS3710 will call the first number, once time out is reached and no answer is returned from the first number, the GDS3710 will try the next number on the list and so on. Once the remote phone answers the call, an alarm will be played to notify users that an event is triggered.

Email & FTP Settings

This page contains Email and FTP Settings.

Email Settings

This page allows users to configure email client to send out an email when the alarm is trigged.

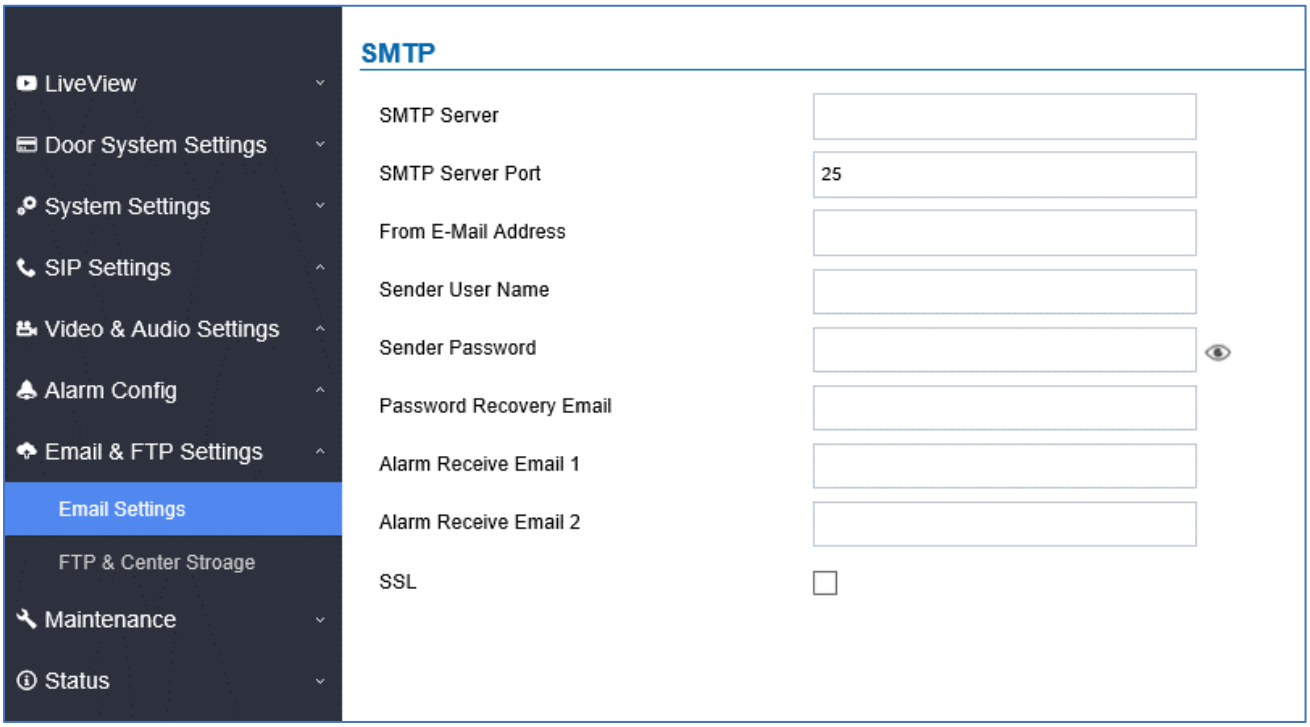


Figure 73: Email Settings - SMTP Page

Table 31: Email Settings - SMTP

SMTP Server	Configures the SMTP Email Server IP or Domain Name.
SMTP Server Port	Specifies the Port number used by server to send email.
From E-mail address	Specifies email address of alarm email sending from, usually client email ID.
Sender User Name	Specifies sender's User ID or account ID in the email system used.
Sender Password	Specifies sender's password of the email account.
Password Recovery Email	Specifies Email address used when password forgot and reset required.
Alarm Receive Email 1	Specifies the 1st email address to receive the alarm email.
Alarm Receive Email 2	Specifies the 2nd email address to receive the alarm email.
SSL	Check if the SMTP email server requires SSL.

Notes:

- Click “Save” to save the email configuration information.
- Click “Email Test” after configuration, if settings are correct, a test email will send out and “E-mail test successfully” message on the top page will appear E-Mail test successfully.

FTP & Center Storage

This page allows users to configure the FTP Settings in order to upload capture images.

Table 32: Picture Storage Settings

Storage Server Type	Selects whether to upload pictures to the GDS Manager or upload them to the FTP server.
FTP Server	Configures the IP address of the FTP server when selected to upload images to.
FTP Server Port	Specifies the FTP address port.
FTP User Name	Specifies the FTP server account name.
FTP Password	Specifies the FTP server password.
FTP Path	Specifies the storage path.
FTP Test	Click to test the connection with FTP server.

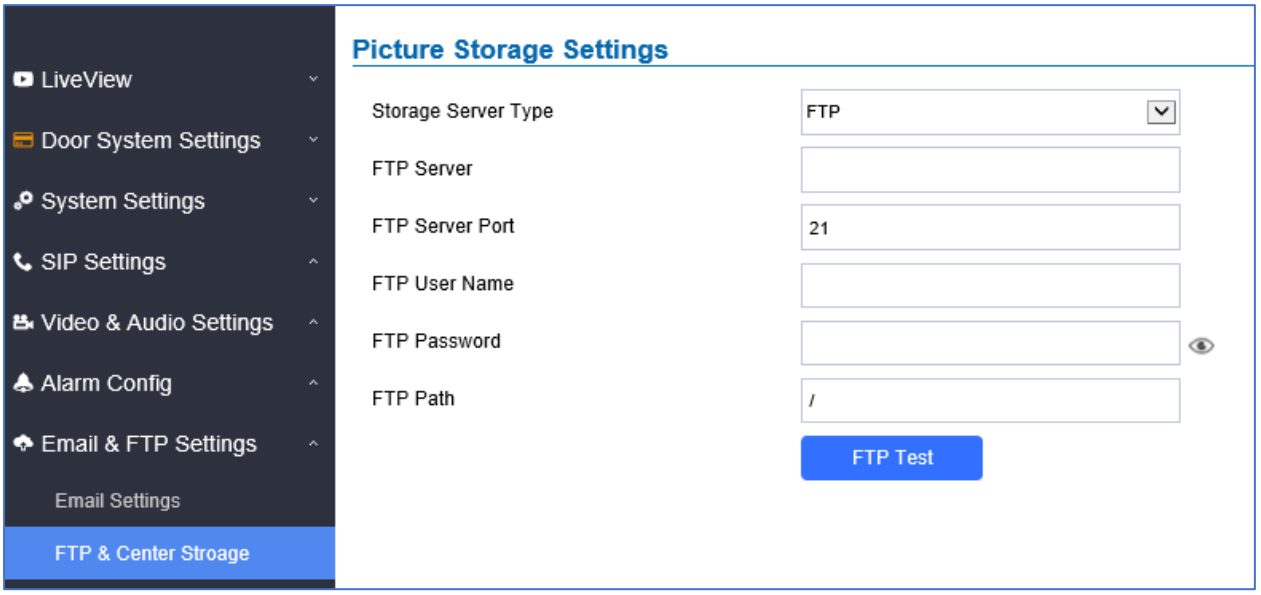


Figure 74: Picture Storage Settings

Notes:

- If the connection to the FTP server is successful, a ".txt" file containing a success message will be uploaded to the FTP server. And the following message will pop up on the webGUI 

.
- Central Storage will use GDS Manager built-in FTP server to store screenshots.

FTP Filenames

When setting up FTP server to store snapshots (when doorbell pressed or door Unlocked), the GDS will create folder with device MAC address (if multiple GDS3710s are sending snapshots to same FTP server).

In EACH folder based on MAC address or device, the file folder will be created by DATE, to organize and classify the snapshots received during different DATE for easy analysis.

In EACH folder classified with DATE, the snapshot file name is based on following naming schema:

Table 33: FTP Filenames

FTP Filename with	Description
CARD	Meaning that open door operation is using RFID card.
LPIN (Local PIN)	Meaning that open door operation is via Local PIN (Private PIN, or Unified PIN, or Guest PIN).
RPIN (Remote PIN)	Meaning that open door operation is via remote PIN or DTMF PIN. (by local or remote SIP extensions, or GS_Wave/Cellphone, or GDSManager if installed in operation).
RING	Meaning the snapshot taken when somebody pressed the Door Bell button.

The following figure illustrates the FTP filenames sent to the FTP server when the above operations have been taken:

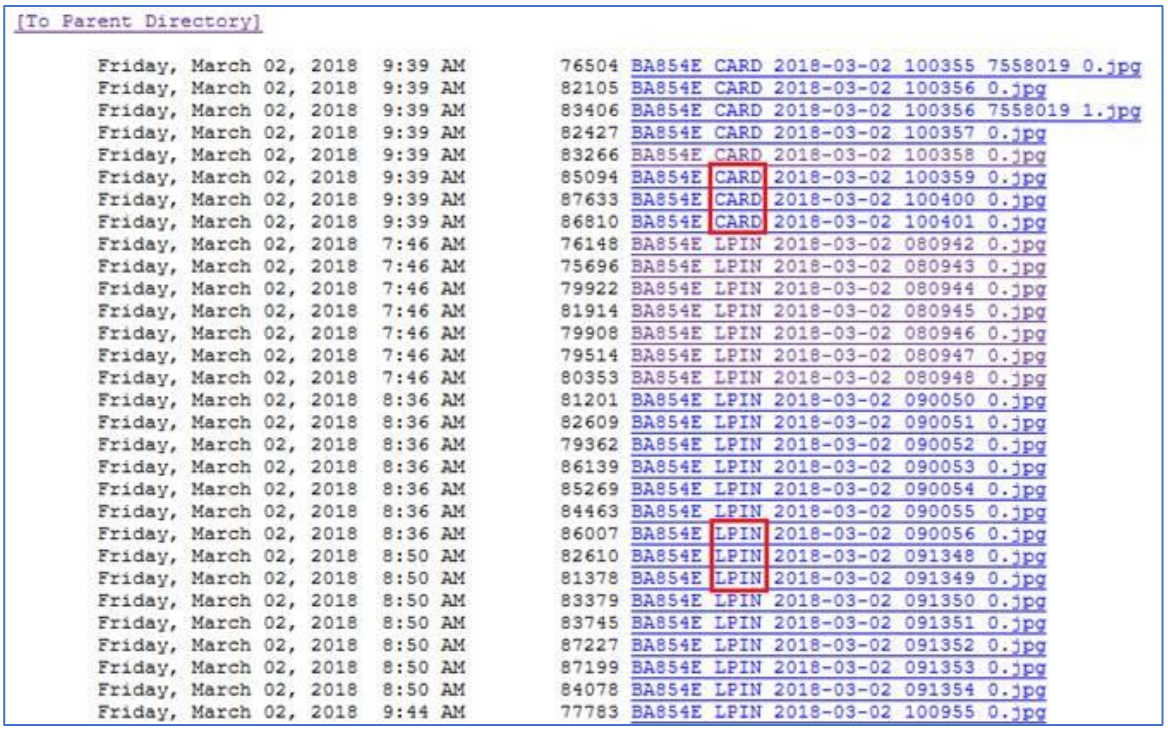


Figure 75 : FTP filenames

Maintenance Settings

This page shows the GDS3710 Maintenance parameters.

Upgrade

This page contains the upgrade and provisioning parameters of the GDS3710.

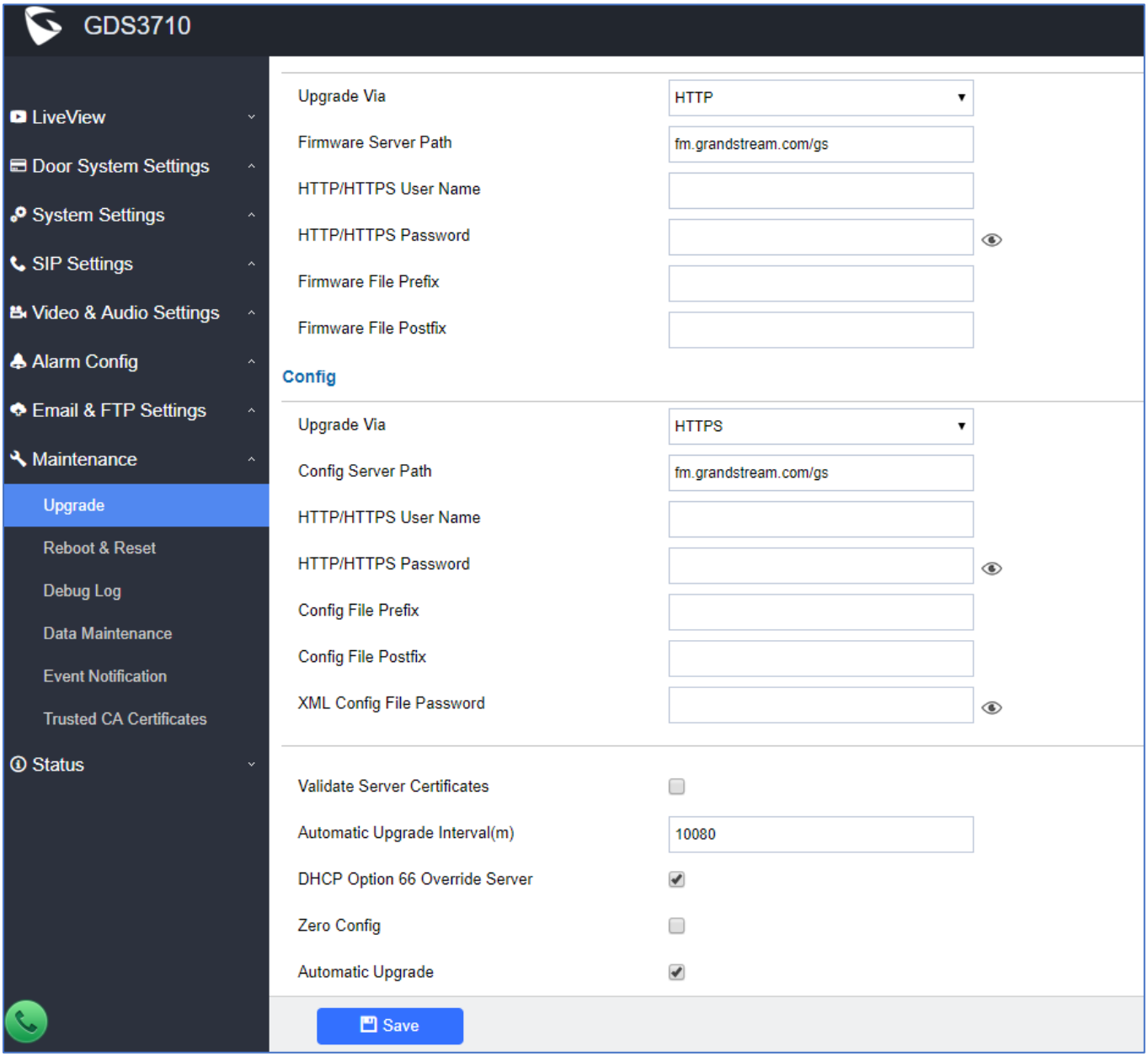


Figure 76: Upgrade Page

Table 34: Upgrade

Upgrade Via	Selects the upgrade method (TFTP, HTTP, HTTPS).
Firmware Server Path	Configures the IP address or the FQDN of the upgrade server.
Config Server Path	Configures the IP address or the FQDN of the configuration server.
XML Config File Password	Specifies the password for the configuration file.
Automatic Upgrade Interval	Specifies the upgrade interval in minutes.
Validate Server Certificate	Enable this option in order to validate certificate with trusted ones during TLS connection.

DHCP Option 66 Override Server	Activates DHCP option 66 to override upgrade/config servers.
Zero Config	Enables Zero Config feature for auto provisioning.
Automatic Upgrade	Enables automatic upgrade and provisioning.

LED Pattern:

During the upgrade process and starting from firmware 1.0.3.32, the GDS will give indication about the progress of the process using LED lighting as follow:

1) Doorbell button blue LED will flash when firmware files are downloading.
2) Digit 1,2,3 blue LED will flash during upgrading from 0 to 25%, then stays on.
3) Digit 4,5,6 blue LED will flash during upgrading from 25 to 50%, then stays on.
4) Digit 7,8,9 blue LED will flash during upgrading from 50 to 75%, then stays on.
5) Digit *,0,# blue LED will flash during upgrading from 75 to 100%, then stays on.
6) After all key's blue LEDs light on then flash twice then reboot itself to finish the upgrade process.

Reboot & Reset

This page allows user to reboot and reset the GDS3710.

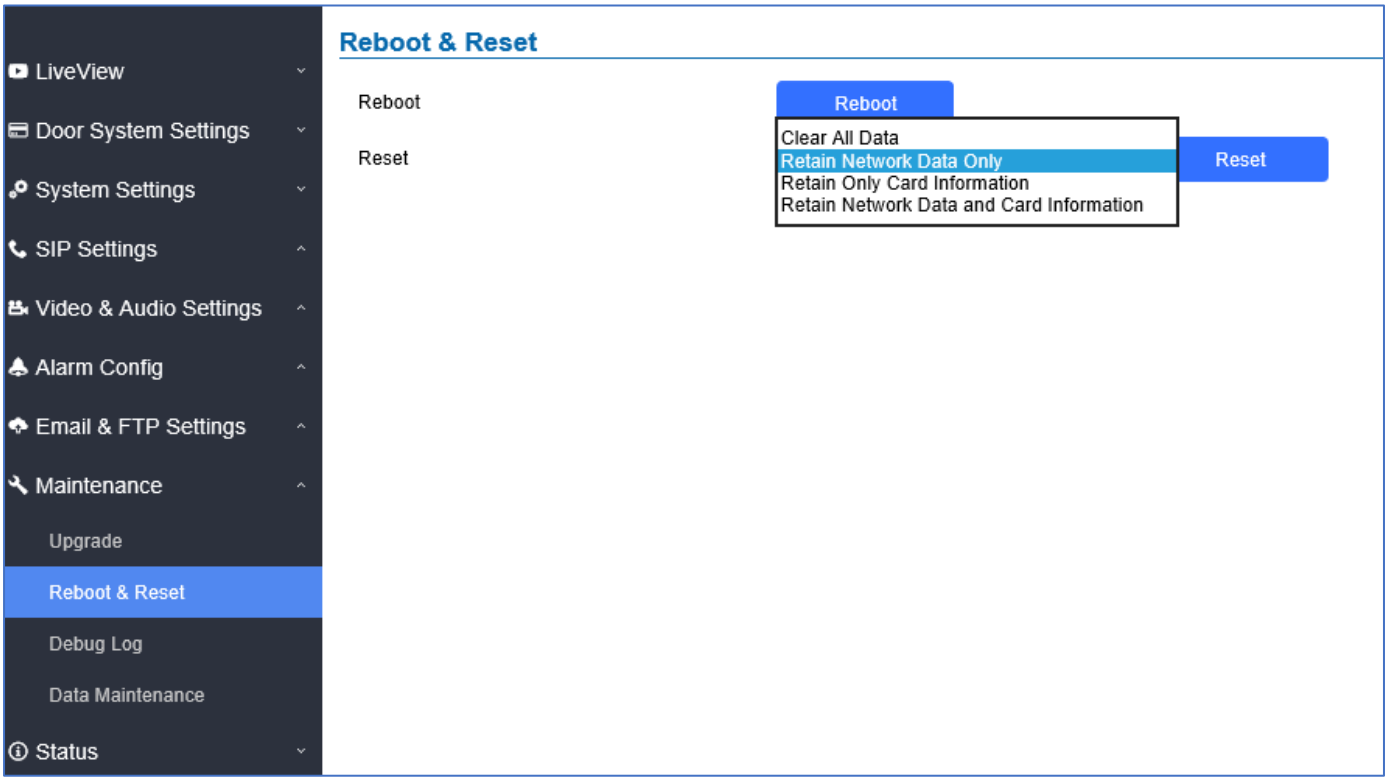


Figure 77: Reset & Reboot Page

Table 35: Reset & Reboot

Reboot	When clicked, the GDS3710 will restart (soft reboot).
Reset	There are two options for the reset function.
Clear All Data	All data will be reset, GDS3710 will be set to factory default.
Retain Network Data Only	All data will be erased except for Network data like IP address…
Retain Only Card Information	All data will be erased except for cards information.
Retain Network Data and Card Information	All data will be erased except for Network Data and Card Information.

Debug Log

This page allows user to configure SYSLOG to collect information to help troubleshooting issues with GDS3710.

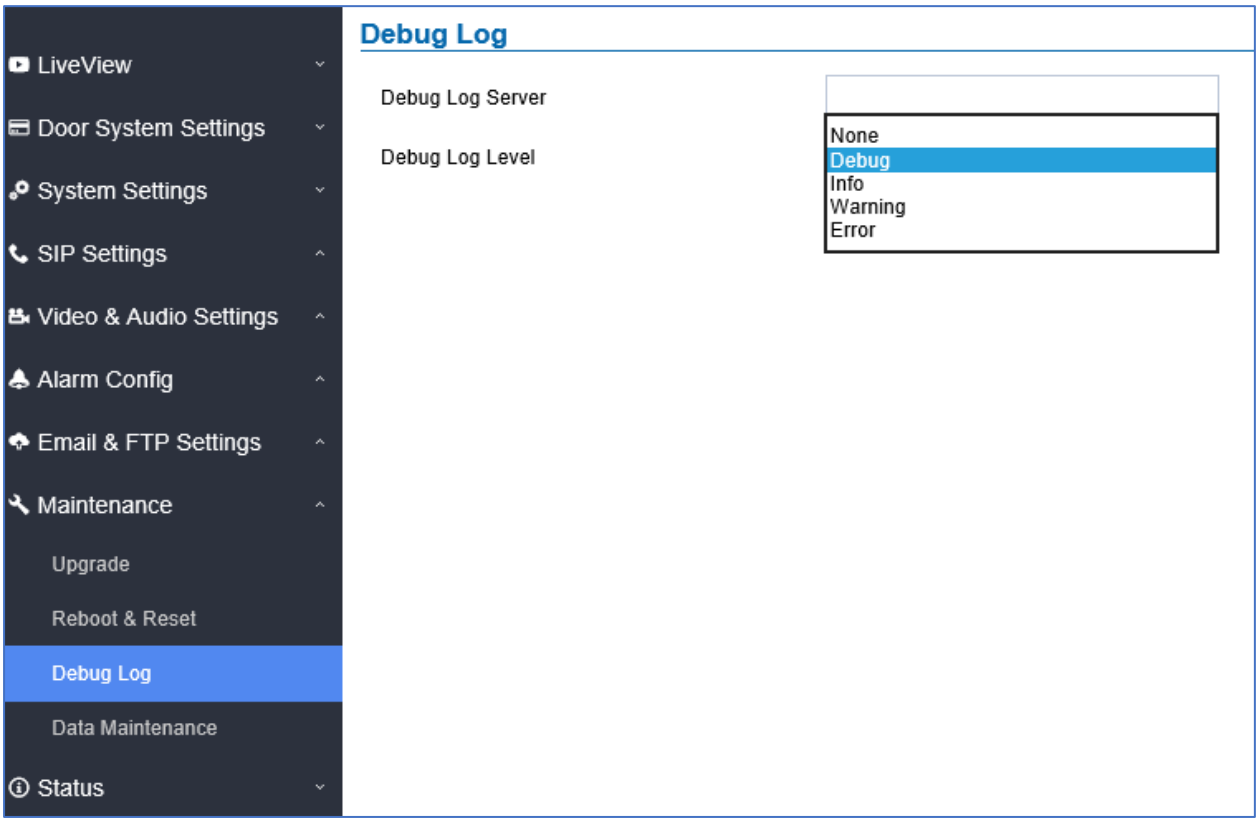


Figure 78: Debug Log Page

- Five levels of Debugging are available, None, Debug, Info, Warning, Error.
- Once the Syslog Server and the level entered, press “Save” and then Reboot the GDS3710 to apply the settings.

Data Maintenance

This page allows users to manage the GDS3710 configuration file by importing/exporting configuration files.

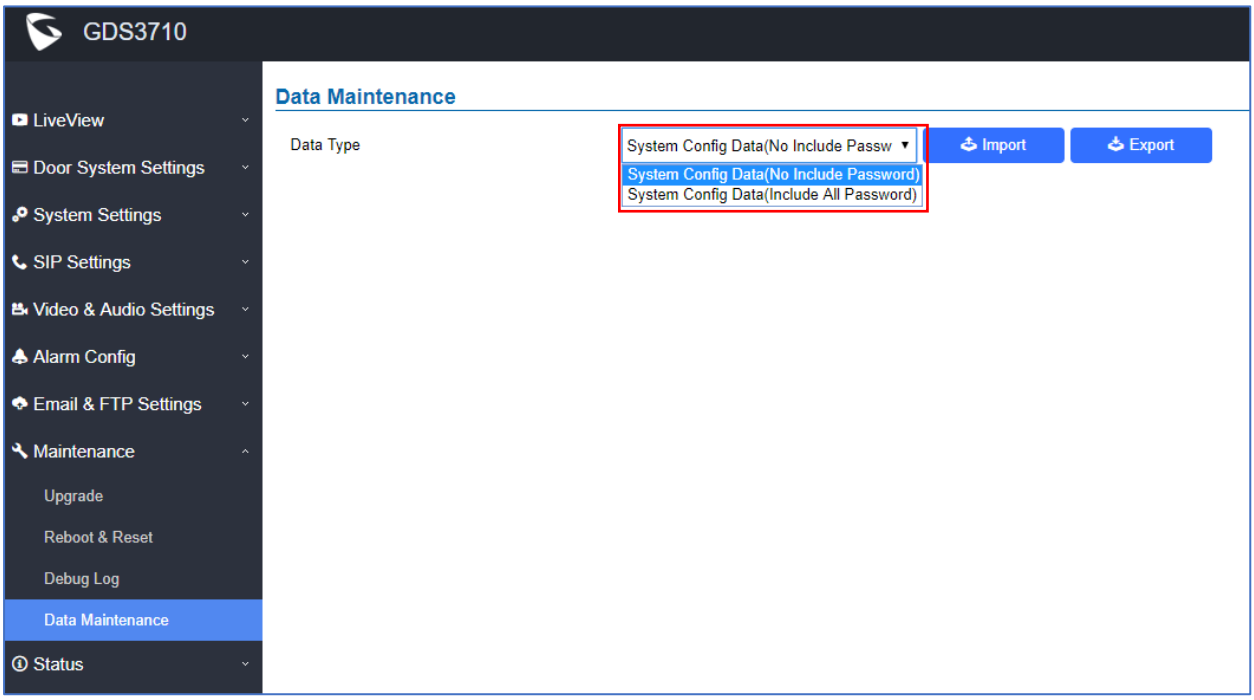


Figure 79: Data Maintenance Page

Click on Export to save the GDS3710 configuration in a predefined directory.

Note: Users can either select to include all the passwords (SIP, FTP, Remotes access…) on the configuration files exported or not including the passwords as displayed on the previous figure.

Event Notification

This page allows users to configure the event notification details that will be used by GDS3710 to communicate to an HTTP server to log the events. When the feature is enabled and configured, all the event logs will be uploaded to server: RFID open door, PIN open door, SIP Call, Alarm, etc..

Examples:

- After an RFID Card swiping, GDS3710 will send to the configured HTTP server the following HTTP POST containing "Use card open door" event:

```
POST / HTTP/1.1
Host: 192.168.6.107
Authorization: Basic Og==
Connection: keep-alive
Content-Length: 90

Date: 2017-11-09; Time: 14:07:27; Event describe: Use card open door. Card ID:
378690700.
```

- After making a Call, when doorbell pressed, GDS3710 will send to the configured HTTP server the following HTTP POST containing “Phone call” event:

```
POST/HTTP/1.1
Host:192.168.6.107
Authorization:BasicOg==
Connection:keep-alive
Content-Length:62

Date: 2017-11-09; Time: 14:13:12; Event describe: Phone call.
```

These HTTP POST messages can be used by a 3rd party software to integrate the GDS3710.

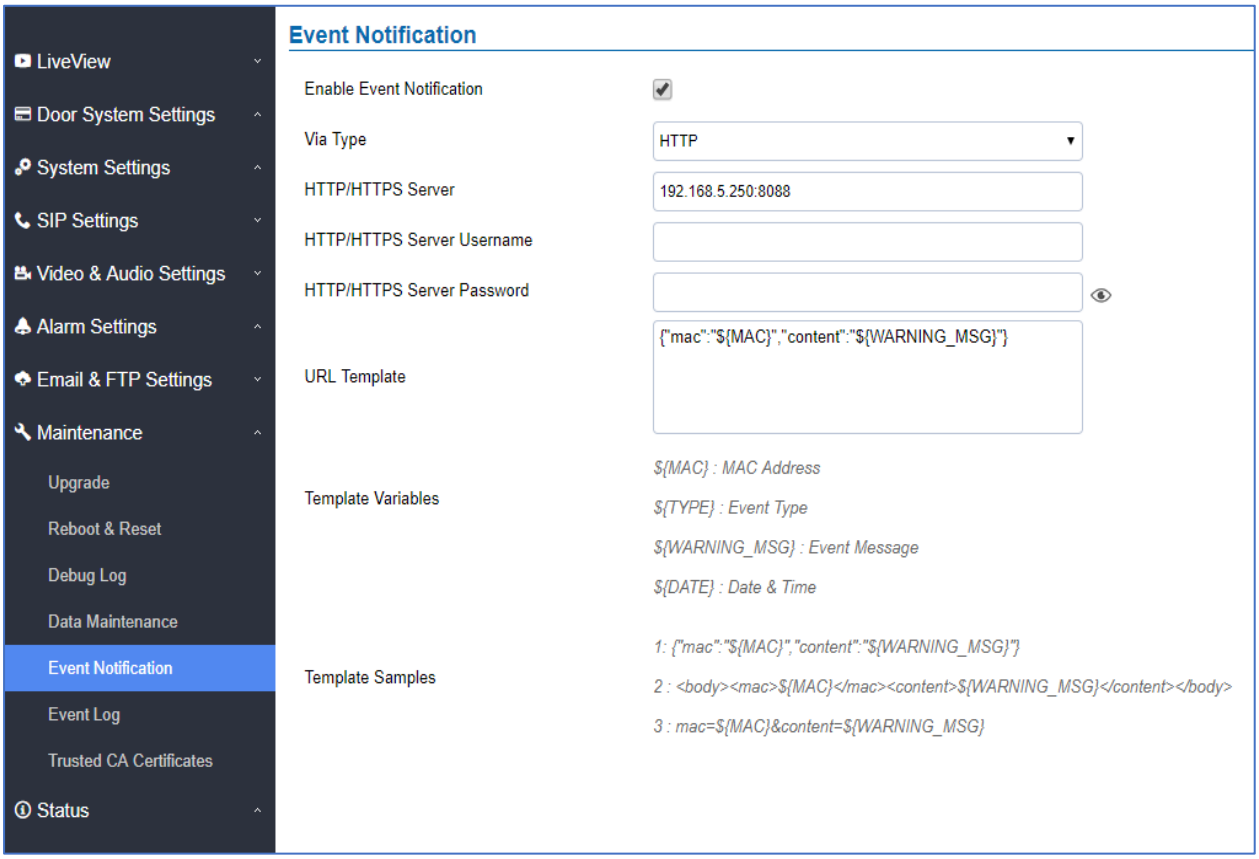


Figure 80: Log Manager Page

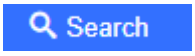
Table 36 : Log Manager settings

Enable Event Notification	Enables Event Notification feature
Via Type	Choose which protocol will be used to connect to the logs server (HTTP or HTTPs).
HTTP/HTTPs Server	Enter the IP address of domain name for the logs server.

HTTP Server Username	Configure the username of your HTTP(s) server
HTTP Server Password	Configure the password of your HTTP(s) server
URL Template	Specify the template for the event log messages that will be sent to the server, users can use the following variables to customize the message: • ${MAC} : MAC Address • ${TYPE} : Event Type • ${WARNING_MSG} : Event Message • ${DATE} : Date & Time

Event Log

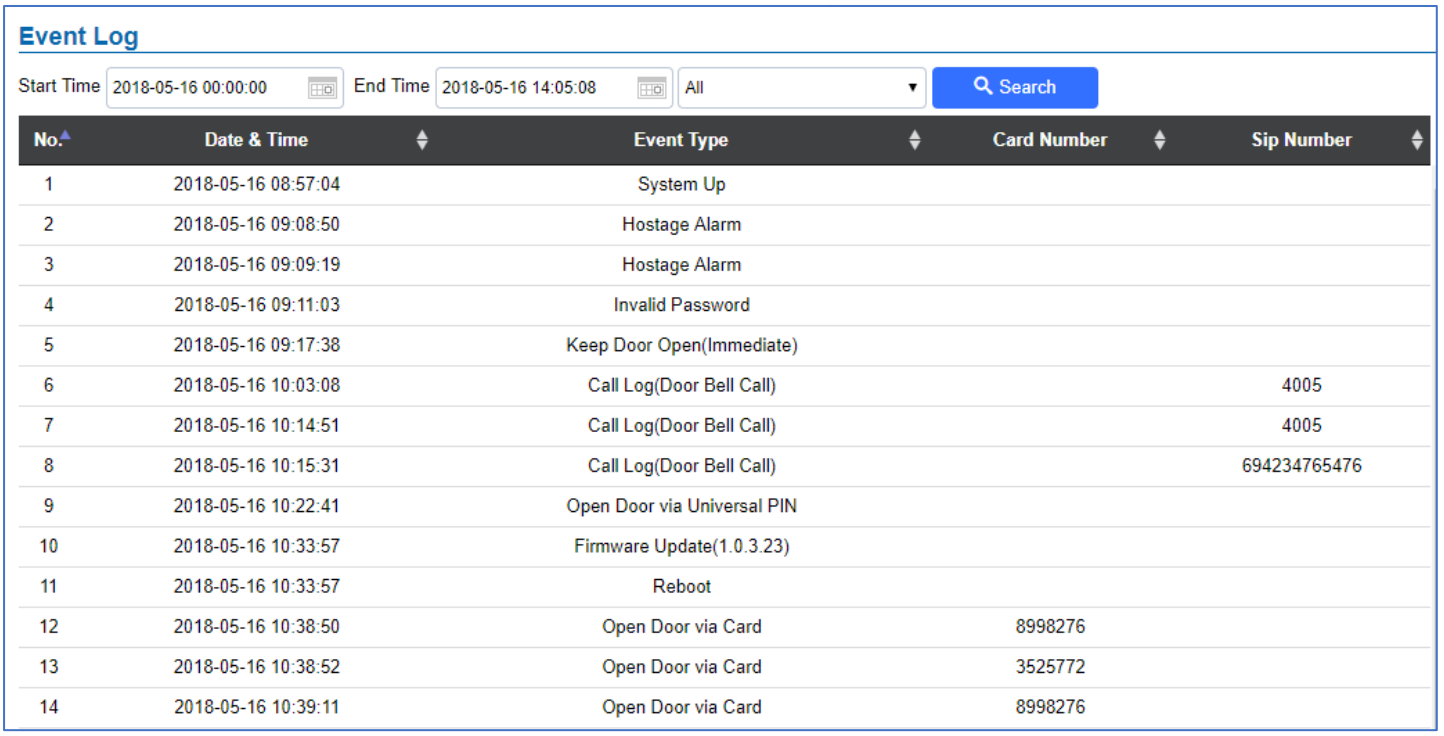
Users could check all device logs directly from the GDS web UI under the menu "**Maintenance → Event log**".

In order to get logs for a specific date interval, select the Start Time and End Time, then select which Event type you want to check using the drop-down list, and click on 

to display the records.

The following Event Types are included for filtering:

- Open Door via Card
- Visiting Log
- Open Door via PIN
- Open Door via DI
- Open door by SI
- Call Log
- Open Door via Card and PIN
- Open Door via Remote PIN
- Motion Detection
- DI Alarm
- Door & Lock Abnormal Alarm
- Dismantle by Force
- System Up
- Reboot
- Reset
- Config Update
- Firmware Update
- Non-scheduled Access
- Hostage Alarm
- Invalid Password
- Temperature Alarm



No.	Date & Time	Event Type	Card Number	Sip Number
1	2018-05-16 08:57:04	System Up		
2	2018-05-16 09:08:50	Hostage Alarm		
3	2018-05-16 09:09:19	Hostage Alarm		
4	2018-05-16 09:11:03	Invalid Password		
5	2018-05-16 09:17:38	Keep Door Open(Immediate)		
6	2018-05-16 10:03:08	Call Log(Door Bell Call)		4005
7	2018-05-16 10:14:51	Call Log(Door Bell Call)		4005
8	2018-05-16 10:15:31	Call Log(Door Bell Call)		694234765476
9	2018-05-16 10:22:41	Open Door via Universal PIN		
10	2018-05-16 10:33:57	Firmware Update(1.0.3.23)		
11	2018-05-16 10:33:57	Reboot		
12	2018-05-16 10:38:50	Open Door via Card	8998276	
13	2018-05-16 10:38:52	Open Door via Card	3525772	
14	2018-05-16 10:39:11	Open Door via Card	8998276	

Figure 81: Event Logs

For more information about event logs, please visit this guide.

Trusted CA Certificates

This page allows users to upload up to 6 CA certificate files which will be trusted by the GDS during SSL exchange.

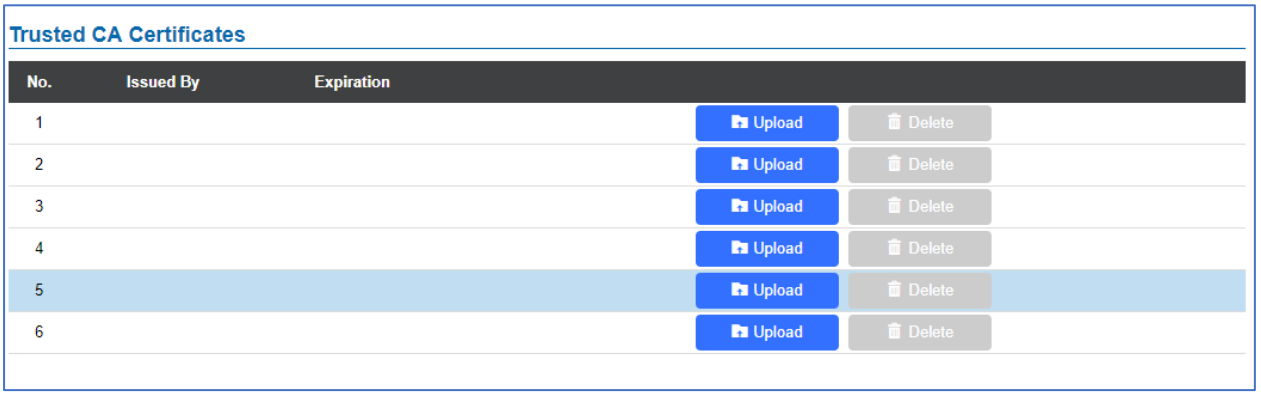
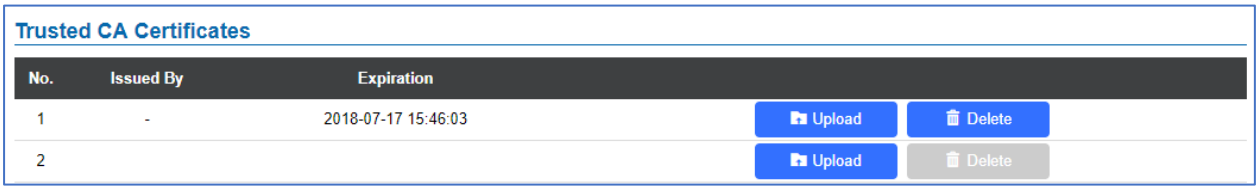


Figure 82: Upload Trusted CA files

Click on Upload button to upload a file and some related information to the uploaded file will be displayed, such as **"Issued by"** and **"Expiration date"**.



User could press Delete to delete one of the files.

Status

This page displays GDS3710 system and network information.

System Info

This page displays information such as the product model, the hardware version, firmware…

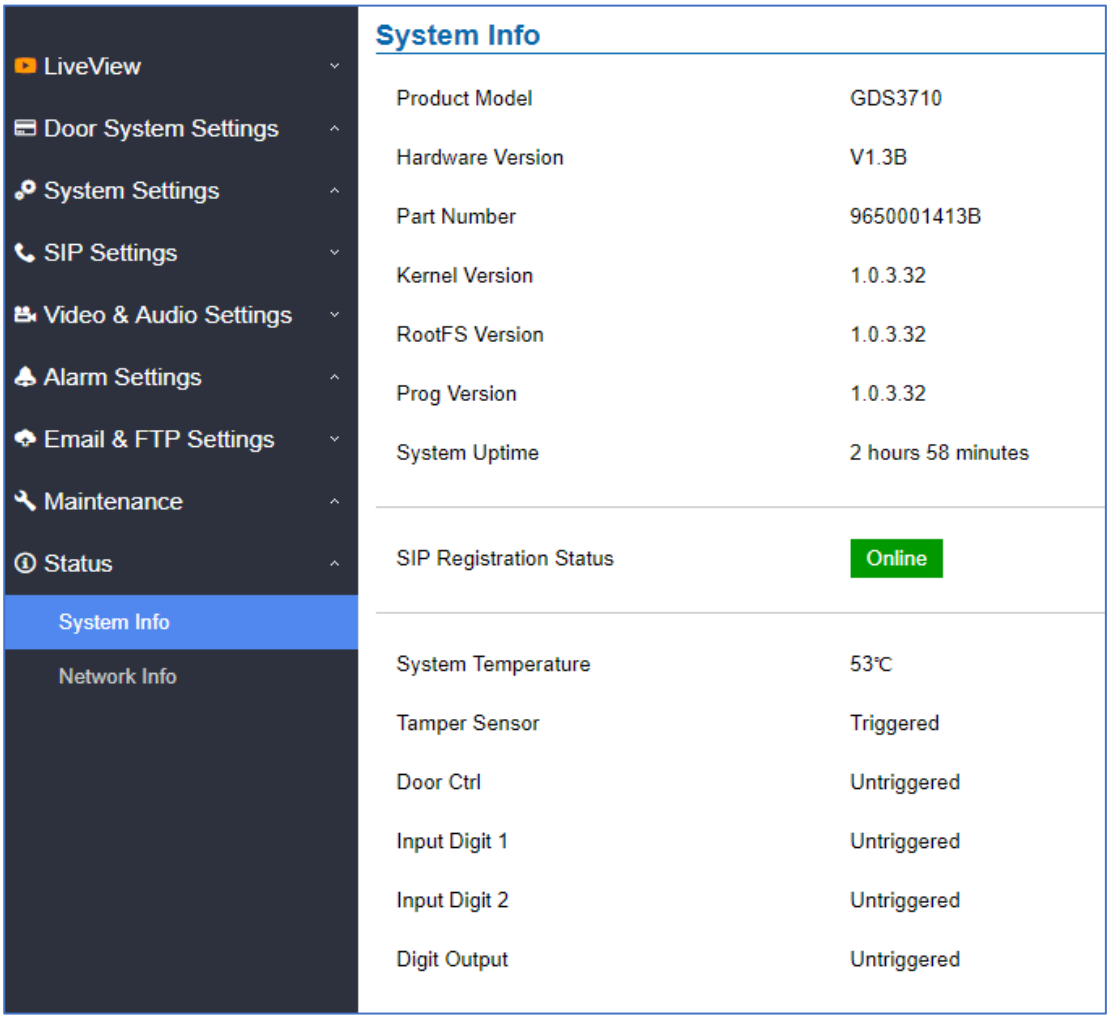


Figure 83: System Info Page

Table 37: System Info

Product Model	Displays the Product Model.
Hardware Version	Displays the Hardware Version.
Part Number	Displays the Part Number.
Kernel Version	Displays the Kernel Version.
RootFS Version	Displays the RootFS Version.
Prog Version	Displays the Prog Version.
System Up Time	Displays the time since the first boot of the GDS3710.
SIP Registration Status	Sows whether the SIP account is registered or not.
System Temperature	Shows the current system temperature.
Tamper Sensor	Shows if the Temper Sensor is triggered or not.
Door Control	Shows if the door control is triggered or not (in case door is opened for ex it will show triggered).
Input Digit 1	Shows if alarm IN 1 is triggered.
Input Digit 2	Shows if alarm IN 2 is triggered.
Digit Output	Shows if digital output is triggered.

Notes:

- When the SIP account is registered, the status display will be Online
- When SIP account is unregistered, the status display will be Offline

Network Info

This page displays the network system information of GDS3710.

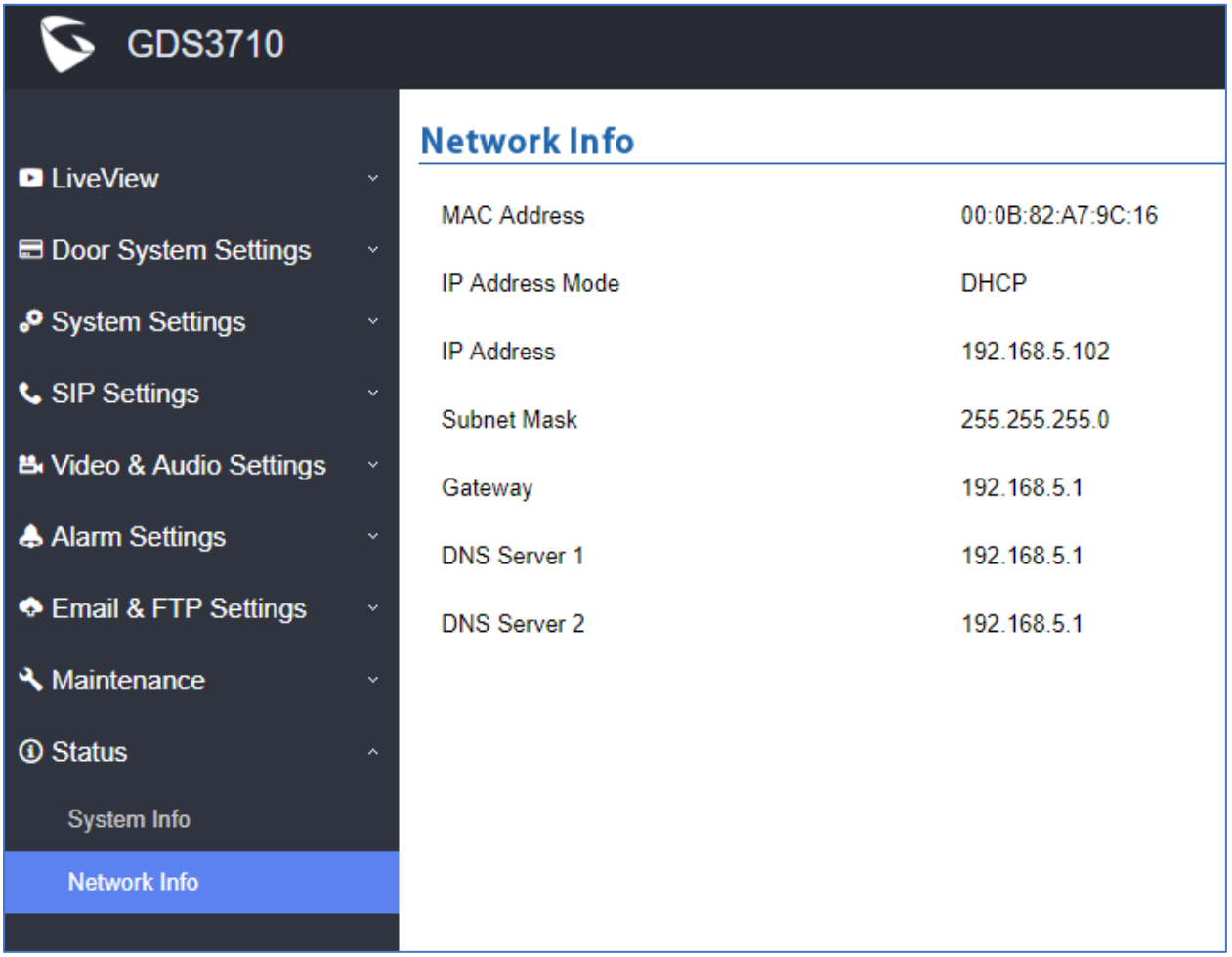


Figure 84: Network Info Page

Table 38: Network Info

MAC Address	Displays the GDS3710 MAC Address.
IP Address Mode	Displays the IP address mode used.
IP Address	Displays the IP address of the GDS3710.
Subnet Mask	Displays the Subnet Mask used.
Gateway	Displays the GDS3710 Gateway.
DNS Server 1	Displays the Preferred DNS Server.
DNS Server 2	Displays the secondary DNS Server.

CONNECTING GDS3710 WITH GXV32XX

The GDS3710 Door System offers a powerful integration with GXV32xx and allows users to open the door, initiates call to the GDS3710 and gets real time audio/video stream.

The GXV3275 can be connected with the GDS3710 in two different ways, either using peering mode (without a SIP server) or through a SIP server. For more details, please refer to following guide:

http://www.grandstream.com/sites/default/files/Resources/Connecting_the_GDS3710_with_GXV32XX_Configuration_Guide.pdf

CONNECTING GS WAVE WITH GDS3710 DOOR SYSTEM

The GDS3710 Door System can interact with the GS Wave softphone application to allow users to open door, initiate call to the GDS3710, offering more mobility during security monitoring and increasing connectivity to essential communications and real-time audio/video stream.

- **GS Wave Android**: For more details about needed steps for configuring the GDS3710 to connect with Grandstream Wave Android™ version, please refer to following guide:

http://www.grandstream.com/sites/default/files/Resources/Connecting_GDS3710_with_GS_Wave_Android_Guide.pdf

- **GS Wave IOS**: For more details about needed steps for configuring the GDS3710 to connect with Grandstream Wave iOS™ version, please refer to following guide:

http://www.grandstream.com/sites/default/files/Resources/Connecting_GDS3710_with_GS_Wave_iOS_Guide.pdf

GDS3710 HTTP API

Grandstream Door System supports HTTP API (Application Programming Interface).

For more details, please refer to following guide:
http://www.grandstream.com/sites/default/files/Resources/gds37xx_http_api.pdf

The document explains in detail the external HTTP-based application programming interface and parameters of functions via the supported method. The HTTP API is firmware dependent. Please refer to the related firmware Release Note for the supported functions.

Administrator Privilege is required, and administrator authentication verification has to be executed before any operation to the related parameter configuration.

FACTORY RESET

Restore to Factory Default via Web GUI

To perform factory reset to the GDS3710 via the Web GUI, please refer to following steps:

1. Access to GDS3710 Web GUI using the using the shipped default password.
2. Navigate to Maintenance →Reboot & Reset.
3. Select the reset type from Rest drop down menu and press reset button as displayed on the following screenshot.

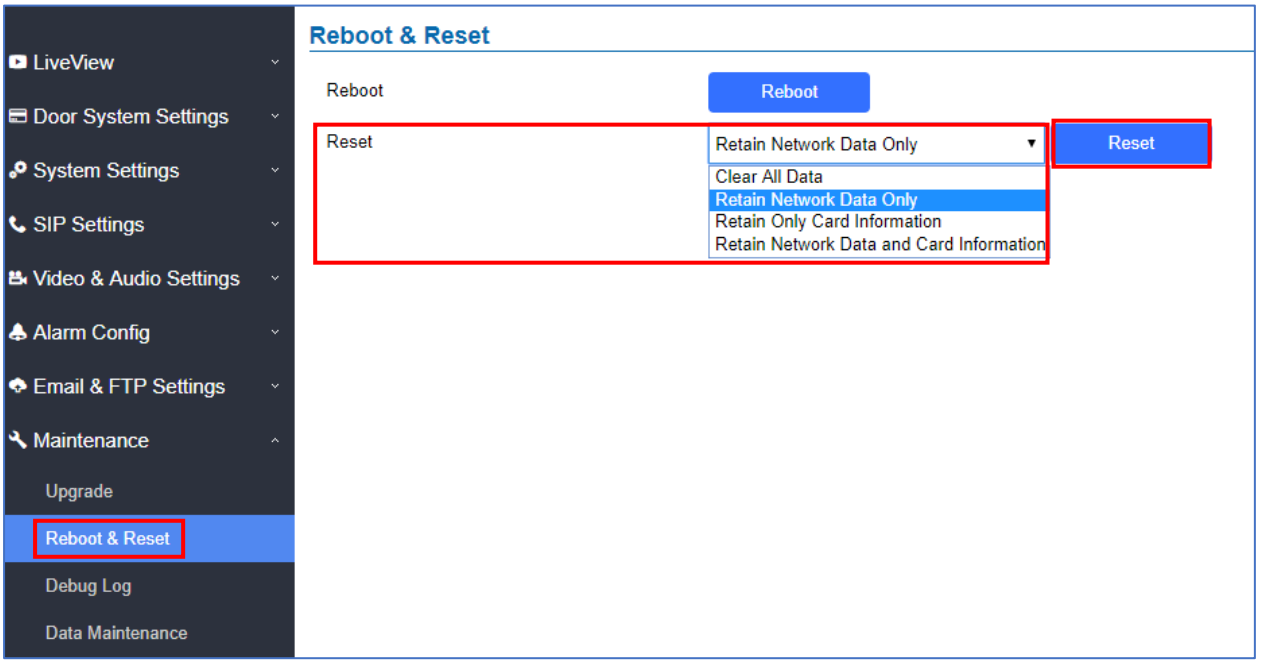


Figure 85: Reset via Web GUI

Hard Factory Reset

Some users did not keep the revised password safely and forgot the changed password. Due to GDS3710 did NOT have built-in reset button (Grandstream purposely designed this way to enhance security), this will make the GDS3710 inaccessible even for the true owner who lost the changed password.

Starting from firmware 1.0.2.21, Grandstream introduced a special way to do hard factory reset using the Wiegand Interface Cable shipped with GDS3710. Below is a photo of the normal connection of the provided Wiegand cable.

Important note: Power must **NOT** be lost while performing hard factory reset.

Figure 86: Wiegand Interface Cable

To perform hard factory reset to the GDS3710, please refer to following steps:

1. Power OFF the GDS3710.
2. Take the provided Wiegand cable, connect (or shorting) the related color wires as illustrated on the following picture. Please make sure the connection is correct and solid:
    - Connect **WHITE** and **BROWN** cable together.
    - Connect **GREEN** and **ORANGE** cable together.

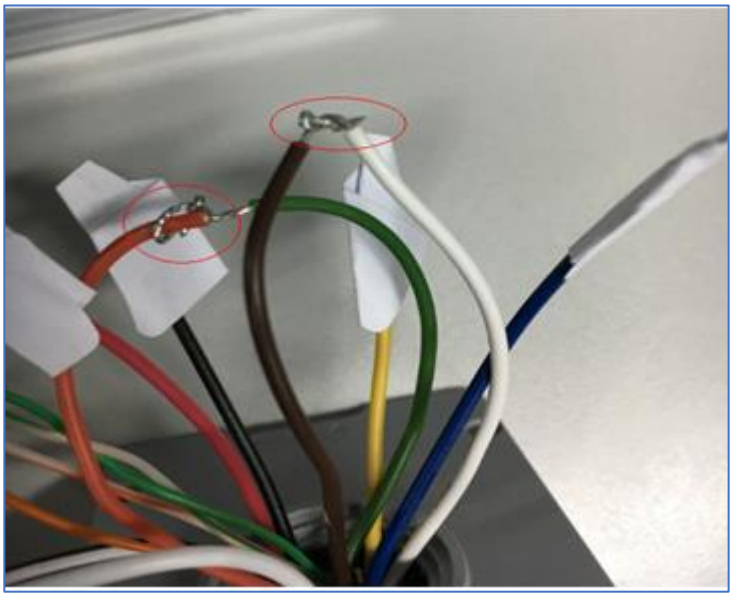


Figure 87: Wiegand Cable Connection

3. Power ON the GDS3710. In about 10 seconds, the key pad LED lighting will change from solid lighting to blinking, the blinking time window is about 30 seconds. The user needs to enter the following key combination ***0#** while the LED is blinking.

   Notes:

   - If the correct key combination inputted, the last key input will play with a long tone, illustrating the correct key combination entered, then the GDS3710 will get into factory reset mode.

   - During the blinking time window, if the user does not finish the key combination operation, or pressed the wrong key combination, the GDS3710 will play short beep quickly three times illustrating error. Nothing will happen and the GDS3710 will get into normal booting process. User who wants to do hard factory reset has to perform the operation from the beginning again.

4. After 3 ~ 5 minutes the GDS3710 will finish performing the reset process, then the user can log into the GDS3710 web GUI using the shipped default password.

5. User has to power OFF the GDS3710, unplug the Wiegand cable, power ON the GDS3710 again and make sure the GDS3710 is running correctly.

EXPERIENCING THE GDS3710

Please visit our website: http://www.grandstream.com to receive the most up-to-date updates on firmware releases, additional features, FAQs, documentation and news on new products.

We encourage you to browse our product related documentation, FAQs and User and Developer Forum for answers to your general questions. If you have purchased our products through a Grandstream Certified Partner or Reseller, please contact them directly for immediate support.

Our technical support staff is trained and ready to answer all your questions. Contact a technical support member or submit a trouble ticket online to receive in-depth support.

Thank you again for purchasing Grandstream Door Phone System, it will be sure to bring convenience and color to both your business and personal life.