

Grandstream Networks, Inc.

---

GDS3710

Hemispheric HD IP Video Door System

**User Manual**



## **COPYRIGHT**

©2020 Grandstream Networks, Inc. <http://www.grandstream.com>

All rights reserved. Information in this document is subject to change without notice. Reproduction or transmittal of the entire or any part, in any form or by any means, electronic or print, for any purpose without the express written permission of Grandstream Networks, Inc. is not permitted.

The latest electronic version of this user manual is available for download here:

<http://www.grandstream.com/support>

Grandstream is a registered trademark and Grandstream logo is trademark of Grandstream Networks, Inc. in the United States, Europe and other countries.

## **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



Manufacturer:

Grandstream Networks, Inc.

126 Brookline Ave, 3<sup>rd</sup> 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

<b>DOCUMENT PURPOSE .....</b>	<b>15</b>
<b>CHANGE LOG .....</b>	<b>16</b>
Firmware Version 1.0.7.19 .....	16
Firmware Version 1.0.7.14 .....	16
Firmware Version 1.0.7.11 .....	16
Firmware Version 1.0.7.10 .....	16
Firmware Version 1.0.7.8 .....	16
Firmware Version 1.0.7.7 .....	17
Firmware Version 1.0.7.4 .....	17
Firmware Version 1.0.5.6 .....	17
Firmware Version 1.0.5.2 .....	18
Firmware Version 1.0.4.9 .....	18
Firmware Version 1.0.3.35 .....	18
Firmware Version 1.0.3.34 .....	18
Firmware Version 1.0.3.32 .....	19
Firmware Version 1.0.3.31 .....	19
Firmware Version 1.0.3.23 .....	19
Firmware Version 1.0.3.13 .....	19
Firmware Version 1.0.2.25 .....	20
Firmware Version 1.0.2.22 .....	20
Firmware Version 1.0.2.21 .....	20
Firmware Version 1.0.2.13 .....	20
Firmware Version 1.0.2.9 .....	21
Firmware Version 1.0.2.5 .....	21
Firmware Version 1.0.1.19 .....	21
<b>WELCOME .....</b>	<b>22</b>
<b>PRODUCT OVERVIEW .....</b>	<b>23</b>



Feature Highlights.....	23
Technical Specifications.....	23
<b>GETTING STARTED.....</b>	<b>26</b>
Equipment Packaging.....	26
Description of the GDS3710 .....	27
Connecting and Setting up the GDS3710.....	27
GDS3710 Wiring Connection.....	28
GDS3710 Back Cover Connections .....	29
Connection Example.....	29
<i>Power the unit using PoE .....</i>	<i>30</i>
<i>Power the unit using PSU.....</i>	<i>30</i>
<b>GETTING TO KNOW GDS3710 .....</b>	<b>32</b>
Connecting GDS3710 to Network with DHCP Server .....	32
<i>Windows Platform .....</i>	<i>32</i>
UPnP.....	32
GS Search.....	34
GDS Manager Utility Tool.....	34
<i>Apple Platform .....</i>	<i>35</i>
Connect to the GDS3710 using Static IP.....	37
<b>GDS3710 APPLICATION SCENARIOS .....</b>	<b>39</b>
Peering Mode without SIP Server.....	39
Peering using SIP Server (UCM6XXX).....	39
Using a Network Video Recorder (NVR) .....	40
<b>GDS3710 PERIPHERAL CONNECTIONS .....</b>	<b>42</b>
Alarm IN/OUT .....	43
Protection Diode .....	43
Connection Examples.....	44
<i>Wiring Sample using 3<sup>rd</sup> Party Power Supply.....</i>	<i>45</i>
<i>Wiring Sample using Power Supply for both GDS3710 and Electric Strike .....</i>	<i>45</i>



<i>Wiring Sample using PoE to power GDS3710 and 3<sup>rd</sup> Party Power Supply for Electric Strike</i> ....	46
<i>Good Wiring Sample for Electric Strike and High-Power Device</i> .....	47
Wiegand Module Wiring Examples .....	48
<i>Input example with 3<sup>rd</sup> party power supply for Wiegand device</i> .....	48
<i>Input example with power supply for both GDS3710 and Wiegand device</i> .....	48
<i>Output example with 3<sup>rd</sup> party power supply for Wiegand device</i> .....	49
<i>Wiegand RFID Card Reader Example</i> .....	50
Siren alarming when door opened abnormally .....	50
<i>GDS3710 Connection: IN2 set as Normal Close and “Fail Safe” Electric Strike using 3<sup>rd</sup> Party Power Supply</i> .....	51
<i>GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3<sup>rd</sup> Party Power Supply</i> .....	51
<i>GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3<sup>rd</sup> Party Power Supply with Door sensor</i> .....	52
GSC3570 Secure Open Door via GDS37XX/GSC3570 Peering .....	53
<b>GDS3710 HOME WEB PAGE.....</b>	<b>56</b>
GDS3710 Configuration & Language Page .....	57
<b>GDS3710 SETTINGS.....</b>	<b>59</b>
Live View Page .....	59
<i>Live Snapshot</i> .....	59
<i>MJPEG Stream</i> .....	62
Door System Settings .....	65
<i>Basic Settings</i> .....	65
<i>Using Alarm Out (COM 1) to Control a Second Door</i> .....	74
<i>Keep Door Open</i> .....	78
<i>Emergency PIN</i> .....	80
<i>Card Management</i> .....	81
<i>Add Users Manually</i> .....	81
<i>Add Users Automatically</i> .....	83
<i>Users Operation</i> .....	83
<i>Group</i> .....	83





<i>Schedule</i> .....	84
<i>Holiday</i> .....	85
<b>System Settings</b> .....	86
<i>Date &amp; Time Settings</i> .....	86
<i>Network Settings</i> .....	87
<i>OpenVPN® Settings</i> .....	88
<i>Access Settings</i> .....	89
<i>User Management</i> .....	93
<b>Account</b> .....	93
<i>Account 1 - 4</i> .....	94
<b>Phone Settings</b> .....	97
<i>Phone Settings</i> .....	97
<i>Account [1-4] White List</i> .....	100
<i>Click-To-Dial</i> .....	100
<b>Video &amp; Audio Settings</b> .....	101
<i>Video Settings</i> .....	102
<i>OSD Settings</i> .....	104
<i>CMOS Settings</i> .....	104
<i>Audio Settings</i> .....	105
<i>Privacy Masks</i> .....	106
<b>Alarm Settings</b> .....	107
<i>Alarm Events Config</i> .....	107
<i>Motion Detection</i> .....	108
<i>Digital Input</i> .....	109
<i>Enable Silent Alarm Mode</i> .....	110
<i>Hostage Code</i> .....	110
<i>Tamper Alarm</i> .....	111
<i>Keypad Input Error Alarm</i> .....	111
<i>Non-Scheduled Access Alarm</i> .....	111
<i>Alarm Action When Illegal Card Swiped</i> .....	113
<i>Alarm Action Settings</i> .....	113
<i>Alarm Phone List</i> .....	114



Email & FTP Settings .....	115
<i>Email Settings</i> .....	115
<i>FTP &amp; Center Storage</i> .....	117
Maintenance Settings .....	119
<i>Upgrade</i> .....	119
<i>Reboot &amp; Reset</i> .....	122
<i>Debug Log</i> .....	122
<i>Data Maintenance</i> .....	123
<i>System Health Alert</i> .....	124
<i>Event Notification</i> .....	125
<i>Event Log</i> .....	127
<i>Certificates</i> .....	128
Status .....	129
<i>Account Status</i> .....	129
<i>System Info</i> .....	130
<i>Network Info</i> .....	131
<b>CONNECTING GDS3710 WITH GXV32XX .....</b>	<b>133</b>
<b>CONNECTING GS WAVE WITH GDS3710 DOOR SYSTEM.....</b>	<b>134</b>
<b>GDS3710 HTTP API .....</b>	<b>135</b>
<b>FACTORY RESET .....</b>	<b>136</b>
Restore to Factory Default via Web GUI .....	136
Hard Factory Reset.....	136
Restore to Factory Default Via SIP NOTIFY .....	138
Restore factory password via special key combination .....	139
<b>EXPERIENCING THE GDS3710 .....</b>	<b>141</b>



## Table of Tables

Table 1: GDS3710 Features in a Glance .....	23
Table 2: GDS3710 Technical Specifications .....	23
Table 3: Equipment Packaging .....	26
Table 4: GDS3710 Wiring Connection .....	28
Table 5: Home Page Description .....	56
Table 6: Door System Settings.....	67
Table 7: Immediate Open-Door Table .....	78
Table 8: Schedule Keep Door Open .....	79
Table 9: Card Info .....	82
Table 10: Add Group .....	84
Table 11: Date & Time .....	86
Table 12: Basic Settings.....	87
Table 13: Access Settings .....	90
Table 14: User Management.....	93
Table 15: SIP Account Basic & Advanced Settings.....	94
Table 16: Phone Settings .....	98
Table 17: White List.....	100
Table 18: Video Settings .....	102
Table 19: OSD Settings.....	104
Table 20: CMOS Settings.....	105
Table 21: Audio Settings.....	106
Table 22: Motion Detection.....	108
Table 23: Digital Input.....	109
Table 24: Silently Alarm Mode.....	110
Table 25: Hostage Code Alarm .....	110
Table 26: Tamper Alarm .....	111
Table 27: Keypad Input Error Alarm .....	111
Table 28 : Non-Scheduled Access Alarm .....	111
Table 29: Alarm action when illegal card swiped.....	113
Table 30: Alarm Actions.....	114
Table 31: Alarm Phone List .....	115
Table 32: Email Settings - SMTP .....	116
Table 33: Picture Storage Settings.....	117
Table 34: FTP Filenames .....	118
Table 35: Upgrade.....	120
Table 36: Reset & Reboot .....	122
Table 37 : Log Manager Settings .....	126
Table 38: System Info.....	131
Table 39: Network Info .....	132



## Table of Figures

Figure 1: GDS3710 Package .....	26
Figure 2: GDS3710 Front View .....	27
Figure 3: GDS3710 Back View .....	27
Figure 4: GDS3710 Back Cover Connections .....	29
Figure 5: GDS3710 Back Cover .....	30
Figure 6: Connection Example.....	30
Figure 7: Powering the GDS3710 .....	31
Figure 8: Detecting GDS3710 via UPnP .....	33
Figure 9: GDS3710 Login Page .....	33
Figure 10: GS Search Discovery .....	34
Figure 11: GDS3710 Detection .....	35
Figure 12: Apple Safari Settings Page .....	36
Figure 13: Bonjour Setting Page .....	36
Figure 14: Static IP on Windows .....	38
Figure 15: Peering GDS3710 with UCM6XXX.....	40
Figure 16: Peering GDS3710 with GVR3550 .....	41
Figure 17: Peripheral Connections for GDS3710 .....	42
Figure 18: Alarm_In/Out Circuit for GDS3710.....	43
Figure 19: Protection Diode - Example 1 .....	44
Figure 20: Protection Diode - Example 2 .....	44
Figure 21: 3 <sup>rd</sup> party Power Supply Wiring Sample .....	45
Figure 22: Power Supply used for both GDS3710 and Electric Strike .....	45
Figure 23: Wiring Sample using PoE to power GDS3710 and 3 <sup>rd</sup> party Power Supply for Electric Strike .....	46
Figure 24: Example to Avoid when Powering the Electric Strike .....	47
Figure 25: Electric Strike and High-Power Device Example.....	47
Figure 26: Wiegand Input Example with 3 <sup>rd</sup> party Power Supply.....	48
Figure 27: Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device .....	48
Figure 28: Wiegand Output Wiring Example.....	49
Figure 29: Wiegand RFID Card Reader Example .....	50
Figure 30: Digital Input set as Normal close .....	51
Figure 31: “Fail safe” Electric Strike using 3rd Party Power Supply .....	51
Figure 32: Digital Input set as Normal open.....	51
Figure 33: “Fail Secure” Electric Strike using 3rd Party Power Supply .....	52
Figure 34: “Fail Secure” Electric Strike using 3rd Party Power Supply with Door Sensor.....	52
Figure 35: GSC3570 secure open door via GDS3710 .....	53
Figure 36: GSC3570 secure open door via GDS3710-GDS3710 configuration.....	54
Figure 37: GSC3570 secure open door via GDS3710-GSC3570 Door System System configuration.....	54
Figure 38: GSC3570 secure open door via GDS3710-GSC3570 Digital Input configuration .....	54
Figure 39: Home Page: Internet Explorer 11 .....	56



Figure 40: Switch Language Page .....	58
Figure 41: Live View Page: Google Chrome.....	59
Figure 42: MJPEG Authentication Mode .....	60
Figure 43 : Snapshot admin credential .....	60
Figure 44 : Snapshot view using secured MJPEG authentication Mode .....	61
Figure 45: Snapshot view using Basic Authentication Mode .....	62
Figure 46: MJPEG Authentication Mode .....	62
Figure 47 : MJPEG view admin credential.....	63
Figure 48 : MJPEG live view using secured MJPEG Authentication Mode .....	64
Figure 49: MJPEG view using Basic MJPEG Authentication Mode.....	65
Figure 50: Door System Settings Page.....	66
Figure 51: Alarm_Out1 Feature .....	74
Figure 52: Universal Local PIN .....	75
Figure 53: Remote PIN to Open Door.....	76
Figure 54: Right of Card and Private PIN .....	77
Figure 55: Immediate Open Door .....	78
Figure 56: Schedule Open Door .....	79
Figure 57: Edit Schedule.....	80
Figure 58: Keep Door Open – Emergency PIN.....	80
Figure 59: Card Management .....	81
Figure 60: Card Info .....	82
Figure 61: Add Group.....	84
Figure 62: Groups List.....	84
Figure 63: Edit Schedule Time .....	85
Figure 64: Edit Holiday Time .....	85
Figure 65: Date & Time Page.....	86
Figure 66: Basic Settings Page.....	87
Figure 67: OpenVPN Settings page.....	88
Figure 68: Access Settings Page .....	90
Figure 69: User Management Page.....	93
Figure 70: Password Recovery Email.....	93
Figure 71: SIP Account Settings Page .....	94
Figure 72: Phone Settings Page .....	98
Figure 73: White List Page.....	100
Figure 74 : Click-To-Dial.....	101
Figure 75: Video Settings Page .....	102
Figure 76: OSD Settings Page.....	104
Figure 77: CMOS Settings Page.....	105
Figure 78: Audio Settings Page .....	105
Figure 79: Privacy Masks Configuration Page.....	106
Figure 80: Events Page.....	107
Figure 81: Region Config .....	108



Figure 82: Digital Input .....	109
Figure 83: Alarm Schedule .....	112
Figure 84: Edit Schedule .....	112
Figure 85: Alarm Action .....	113
Figure 86: Edit Alarm Action .....	114
Figure 87: Alarm Phone List .....	115
Figure 88: Email Settings - SMTP Page .....	116
Figure 89: Picture Storage Settings .....	117
Figure 90 : FTP filenames .....	119
Figure 91: Upgrade Page .....	120
Figure 92: Reset & Reboot Page .....	122
Figure 93: Debug Log Page .....	123
Figure 94: Data Maintenance Page .....	124
Figure 95: System Health Alert Page .....	124
Figure 96: Log Manager Page .....	126
Figure 97: Event Logs .....	128
Figure 98: Upload Certificate files .....	128
Figure 99: System Info Page .....	130
Figure 100: System Info Page .....	130
Figure 101: Network Info Page .....	132
Figure 102: Reset via Web GUI .....	136
Figure 103: Wiegand Interface Cable .....	137
Figure 104: Wiegand Cable Connection .....	137
Table 105: Encoding rule .....	139



## 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:

- [Product Overview](#)
- [Getting Started](#)
- [Getting to Know GDS3710](#)
- [GDS3710 Application Scenarios](#)
- [GDS3710 Peripheral Connections](#)
- [GDS3710 Home Web Page](#)
- [GDS3710 Settings](#)
- [Connecting GDS3710 with GXV32XX](#)
- [Connecting GS Wave with GDS3710 Door System](#)
- [GDS3710 HTTP API](#)
- [Factory Reset](#)
- [Experiencing the GDS3710](#)



## 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 1.0.7.19

- Added Alarm Action triggering when illegal card swiped. [Alarm Action When Illegal Card Swiped]
- Added Card Number limitation with maximum number to be 2147483647. [Card Number]
- Added Secure Open Door with GDS37xx/GSC3570 setup. [GSC3570 Secure Open Door via GDS37XX/GSC3570 Peering]
- Added Web Relay ON/OFF URL configuration field for some 3<sup>rd</sup> party Web Relay Door Controlling. [Door Relay Options]
- Set “RTSP password” and “GDSManager Configuration Password” initial value to be GDS37xx default random password. [RTSP Password][GDSManager Configuration Password]
- Added Newfoundland/Canada time zone. [Time Zone]

### Firmware Version 1.0.7.14

- Added OpenVPN® support [OpenVPN® Settings]
- Added displaying “Unauthorized door opening attempt” in the Event Log when illegal card used [Event Log]
- Added WebRelay Open Door Feature [Door Relay Options]
- Added reboot/resync via SIP Notify [Disable SIP NOTIFY Authentication]
- Added option to enable PIN/Password display [Enable PIN/Password Display (HTTPS)]
- Added support for “UserName” in HTTP Event Notification [Event Notification]

### Firmware Version 1.0.7.11

- Revised SIP Account Name to Display Name [SIP Basic Settings]
- Added support for Cisco QuoVadis/HydrantID CA [Certificates]

### Firmware Version 1.0.7.10

- Increased maximum unlock holding time to 1800 seconds (30 minutes). [Basic Settings]
- Added support for anonymous MJPEG stream viewing for each of the three streams. [Enable Anonymous LiveView]

### Firmware Version 1.0.7.8

- Enhanced the failover mechanism based on DNS SRV. [DNS Mode]





- Include Holidays on Keep Door Open Schedule for Door 2. [Holiday Mode]

### **Firmware Version 1.0.7.7**

- Added siren alarming function when door opened abnormally. [Connection Examples]
- Added option to only accept incoming SIP call from Proxy/Server. [Accept Incoming SIP from Proxy Only]
- Added support for including Holidays at Keep Door Open schedule. [Keep Door Open]  
Added reset/restore factory default password via special keypad combination operations. [FACTORY RESET]

### **Firmware Version 1.0.7.4**

- Added ability to separate webUI credentials from the GDSManager credentials. [GDSManager Configuration Password]
- Added G.729 audio codec support. [Technical Specifications] [Preferred Vocoder]
- Added ability to enable multiple audio codecs simultaneously and specify priority of codecs. [Preferred Vocoder]
- Added “Schedule” for firmware upgrade and provisioning. [Upgrade]
- Added support for randomize firmware upgrade and provisioning. [Upgrade]
- Added support for Voice Frame per TX in the audio settings. [Voice Frame Per TX]
- Added option to keep keypad blue light ON/OFF based on schedule. [Door System Settings]
- Added support for DHCP Option 120. [Enable DHCP Option 120 Override SIP Server]
- Added support for reregister before expiration option. [Re-register before Expiration (s)]
- Added support for anonymous RTSP Live View. [Enable Anonymous LiveView]
- Added support for DHCP Option 42. [Allow DHCP Option 42 to override NTP server]

### **Firmware Version 1.0.5.6**

- Added support for 4 SIP accounts. [Account]
- Added option to configure DTMF Payload value. [DTMF Payload Type]
- Added option to disable outbound proxy route header. [Outbound Proxy Mode]
- Added support for Packetization Mode 0. [SIP Packetization Compatibility Mode]
- Added support for “Normal Open” or “Normal Close” setting when Alarm Out1 is set to Open Door. [ALMOUT1 Status]
- Added support for System Health Alerts via Email. [System Health Alert]
- Added option to upload custom doorbell ringtone. [Enable Custom Doorbell Ringtone]
- Added option to set Schedule for “Local PIN to Open Door”. [Local PIN to Open Door Schedule]
- Added support for CSV format when Importing/Exporting Card user data. [Card Management]
- Added support for Anonymous Snapshot. [Enable Anonymous LiveView]
- Enhanced security by only allowing numbers existing under “White List” to open the door remotely when call is initiated from GDS3710. [Remote PIN to Open the Door]
- Added Boot version information into System status. [Boot Version]



## **Firmware Version 1.0.5.2**

- Added Alarm\_Out port (COM1 interface) be used as Open Door 2. [Using Alarm Out (COM 1) to Control a Second Door]
- Added option to Enable/Disable WebUI access. [Disable Web Access]
- Added option to define number of snapshots to be uploaded when opening door. [Number of Snapshots when Door Opened]
- Added option to specify digital input to be normal Open or normal Close. [Input Digit 1 Status]
- Added ability to set schedule for Alarm In door opening. [Select Alarm Schedule]
- Added support for using Digit Only as Private PIN. [Local PIN Type]
- Added option to configure “No Key Entry Timeout”. [No Key Input Timeout]
- Added ability to email snapshot when door opened. [Snapshot when Door Opened]
- Added option to allow anonymous viewing. [Enable Anonymous LiveView]
- Added option to configure payload type for H.264. [H.264 Payload Type]
- Extended VLAN tag range from 0 to 4094. [Layer 2 QoS 802.1Q/VLAN Tag]
- Added option to use Emergency PIN to overwrite “Keep Door Open” schedule and lockdown. [Emergency PIN]
- Added ability to configure device with custom certificate signed by custom CA certificate. [Certificates]
- Added support for special character “@” in the SIP User ID. [SIP User ID]
- Added SIP NOTIFY to factory reset the GDS3710. [Allow Reset Via SIP NOTIFY] [Restore to Factory Default Via SIP NOTIFY]
- Added event log showing the users (Username) opening door via private PIN. [Event Log]

## **Firmware Version 1.0.4.9**

- Added support for Parallel Hunting when doorbell pressed [Door Bell Call Mode]
- Enhanced HTTP Event Notification details: Added “CARDID” and “SIPNUM” [URL Template]
- Add support for TLSv1.2

## **Firmware Version 1.0.3.35**

- Added option to assign a schedule to the doorbell. [Press Doorbell Schedule]
- Added option to set the maximum number of digits dialed. [Maximum Number of Dialed Digits]

## **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 [Account [1-4] 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.
- [Added Self-defined Even Notification Message. [Event Notification]

### **Firmware Version 1.0.3.31**

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

### **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. [Enable two-way SIP Calling]
- 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 Door Opened]
- Issuing Mode automatically. [Card issuing State Expire Time(m)]
- Added ability for whitelist entries to open door using remote PIN. [Account [1-4] 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 3<sup>rd</sup> 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. [Enable Silent 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]
- Expanded the range of Ring timeout. [Ring Timeout]
- 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]

## **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. [Door System Settings]
- Added switch on the doorbell blue light by configured time period of the day. [Door System Settings]
- Implemented “Silent Alarm” mode. [Enable Silent 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.

## **Firmware Version 1.0.2.5**

- Added folder creation and file arrangement if multiple GDS3710s are uploading snapshots to FTP server.
- 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. [Enable 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 3<sup>rd</sup> 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**

	<ul style="list-style-type: none"> <li>• High-performance streaming server allowing multiple simultaneous streaming session accesses.</li> <li>• 2 Megapixel Progressive Scan CMOS, 1920H x 1080V.</li> <li>• Broad interoperability with most 3<sup>rd</sup> party SIP/VoIP devices and leading SIP/NGN/IMS platforms.</li> <li>• 2 Channels Input/Output alarm.</li> <li>• Wiegand (26 bits) Input and Output.</li> <li>• RFID card reader.</li> <li>• Weatherproof, vandal resistant.</li> </ul>
---	---

### 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**

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



<b>Snapshots</b>	Triggered upon events, sent via email and/or FTP.
<b>Multi-stream Resolution</b>	High-performance streaming server allowing multiple simultaneous accesses: <ul style="list-style-type: none"> <li>• <b>Primary video stream:</b> 1920 x 1080 resolution for continuous full HD recording.</li> <li>• <b>Secondary video stream:</b> 640 x 480 resolution for SIP/VoIP video calls.</li> <li>• <b>Third video stream:</b> 320 x 240 resolution for smartphone Apps.</li> </ul>
<b>Network Protocols</b>	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.
<b>SIP/VoIP Support</b>	Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
<b>Voice Codecs</b>	G.711μ/a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1P) and Layer 3 QoS (ToS, DiffServ, MPLS).
<b>Security</b>	User and administrator level access control (pending), MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
<b>Upgrade / Provisioning</b>	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 (Pending) or AES encrypted XML configuration file.
<b>Audio Input</b>	Built-in Digital Microphone, up to 1.5m with AEC.
<b>Audio Output</b>	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.
<b>Keypad / Buttons</b>	12-key touchpad plus a capacitive doorbell button, each with individual LED illumination.
<b>RFID</b>	125KHz: EM4100 (1 RFID card and 1 RFID key fob included).
<b>Alarm Input</b>	Yes, 2 channels, Vin < 15V, for door sensor or other devices.
<b>Alarm Output</b>	Yes, 2 channels, 125VAC/0.5A, 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch or other devices.
<b>Network Interface</b>	10M/100M auto-sensing.
<b>Expansion Interface</b>	Wiegand (26 bits) input and output.
<b>Dimensions and Weight</b>	173mm(H) x 80mm(W) x 36mm(D). 0.6 Kg.
<b>Power Supply</b>	PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).
<b>Interoperability</b>	ONVIF (Profile S).
<b>Ingress Protection</b>	Weatherproof, vandal resistant, with support for extra back reinforcing metal plate
<b>Temperature and</b>	Operation: -30°C to 60°C (-22°F to 140°F)





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

<ul style="list-style-type: none"> <li>• 1 x GDS3710</li> <li>• 1 x Installation Bracket</li> <li>• 1 x Drilling Template</li> <li>• 1 x Protecting Cap</li> <li>• 3 x Rubber Gaskets (for sealing the back cable)</li> <li>• 6 x Back Panel Screws</li> <li>• 6 x Bracket Screws and Anchors</li> <li>• 4 x Anti-tamper screws</li> <li>• 1 x Anti-Tamper Hex Key</li> </ul>	<ul style="list-style-type: none"> <li>• 1 x Wiegand Cable</li> <li>• 1 x Lens Cleaning Cloth</li> <li>• 1 x RFID Card (more can be purchased from Partner/reseller)</li> <li>• 1 x Key Fob (more can be purchased from Partner/reseller)</li> <li>• 1 x Frame Back Cover</li> <li>• 1 x Quick Installation Guide</li> <li>• 1 x GPL License</li> </ul>
---	---



**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:

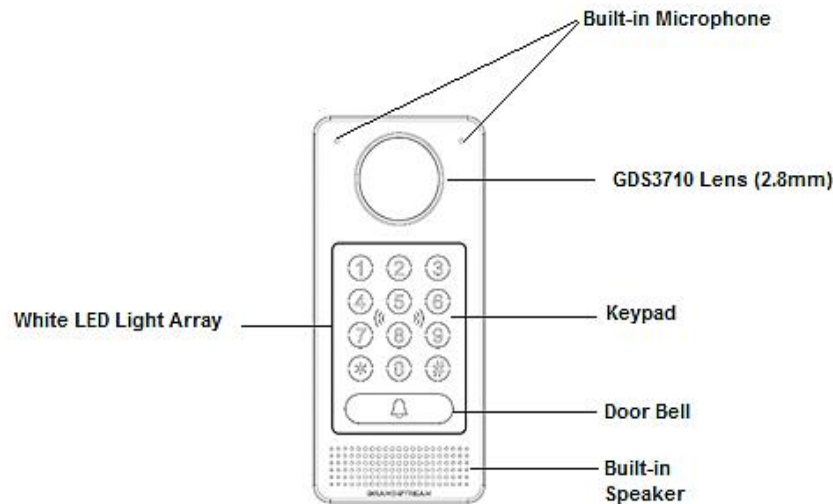


Figure 2: GDS3710 Front View

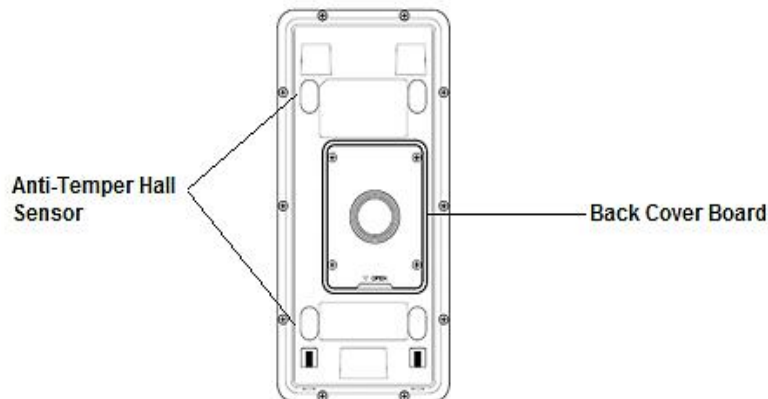


Figure 3: GDS3710 Back View

## 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	
	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 <b>COM2 &amp; NO2</b> . For "Fail Safe" (Open when No Power) Magnetic Lock, connect <b>COM2 &amp; NC2</b> . <b>Relay: 30VDC/2A; 125VAC/0.5A</b>	
	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

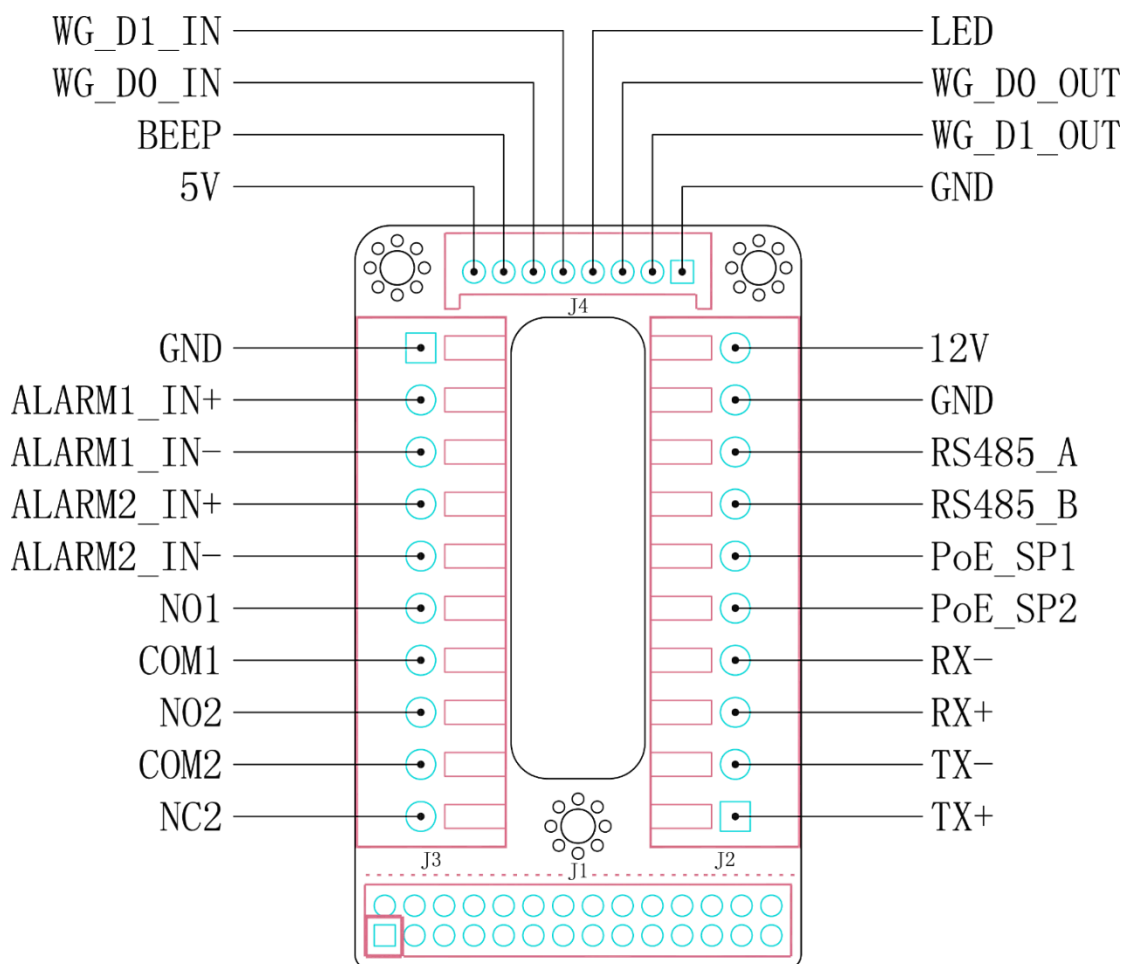
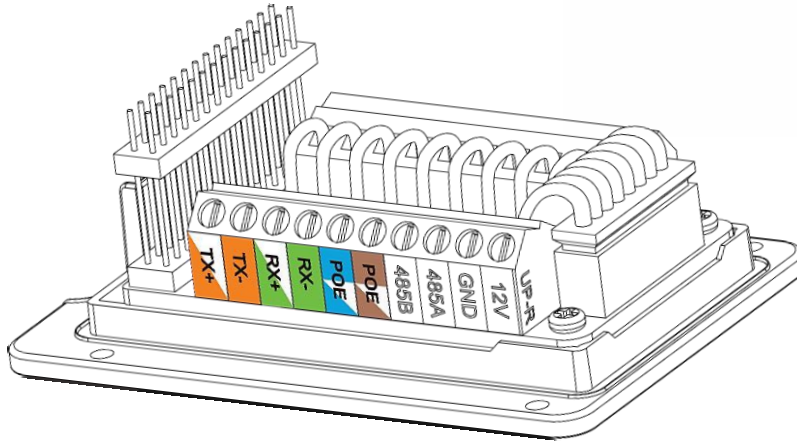


Figure 4: GDS3710 Back Cover Connections

## Connection Example

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

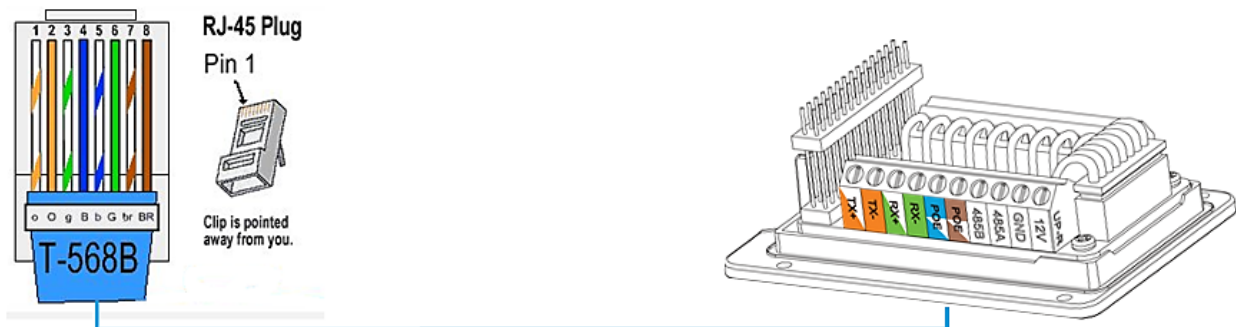
- Open the Back-Cover Board of the GDS3710 which should look like following figure.



**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.



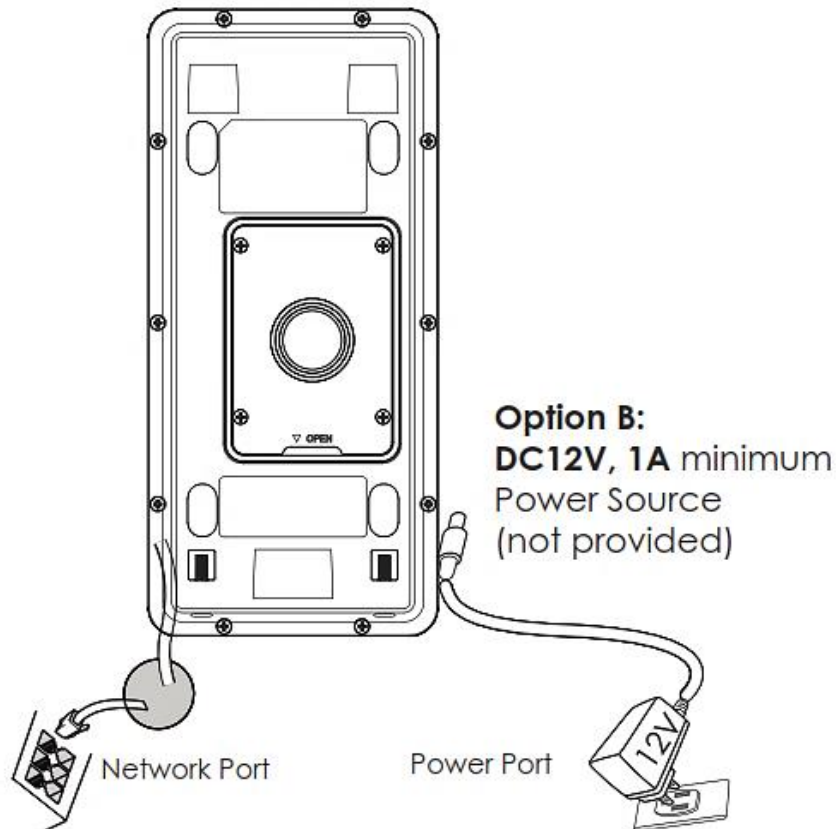
**Figure 6: Connection Example**

- 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

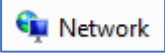
The GDS3710 by default has a DHCP client enabled, it will automatically get IP address from DHCP server.

### Windows Platform

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

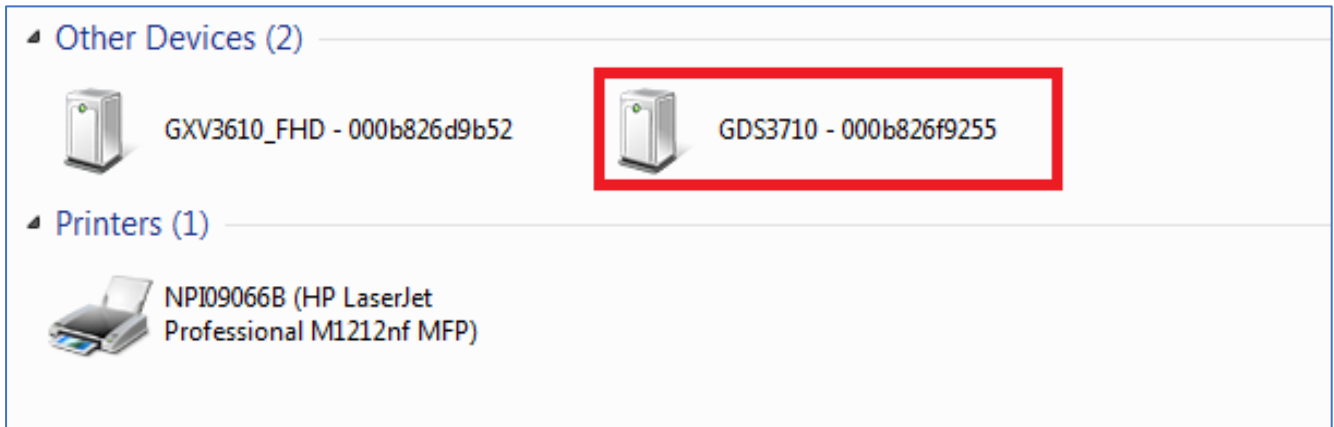
#### UPnP

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.

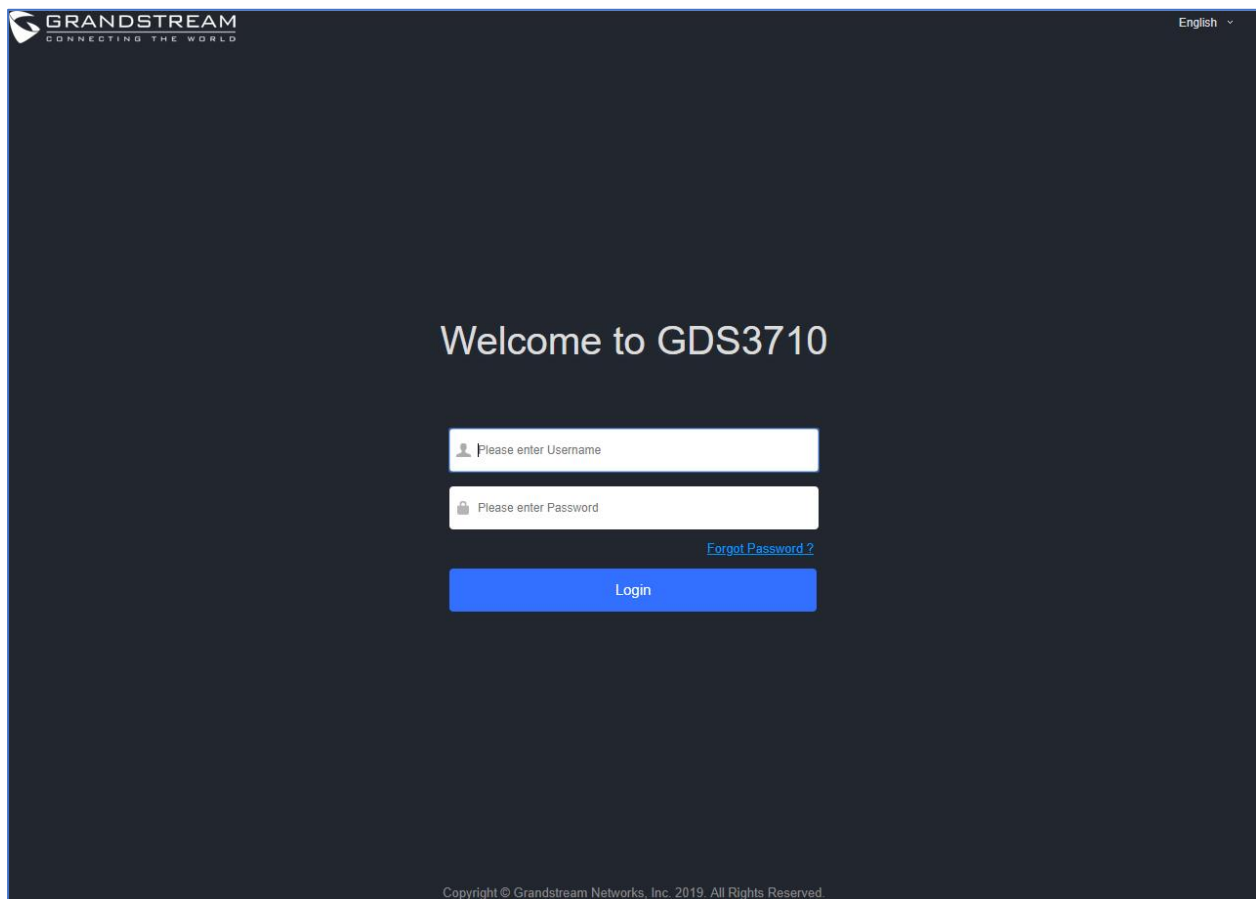






**Figure 8: Detecting GDS3710 via UPnP**

- 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.



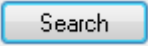
**Figure 9: GDS3710 Login Page**

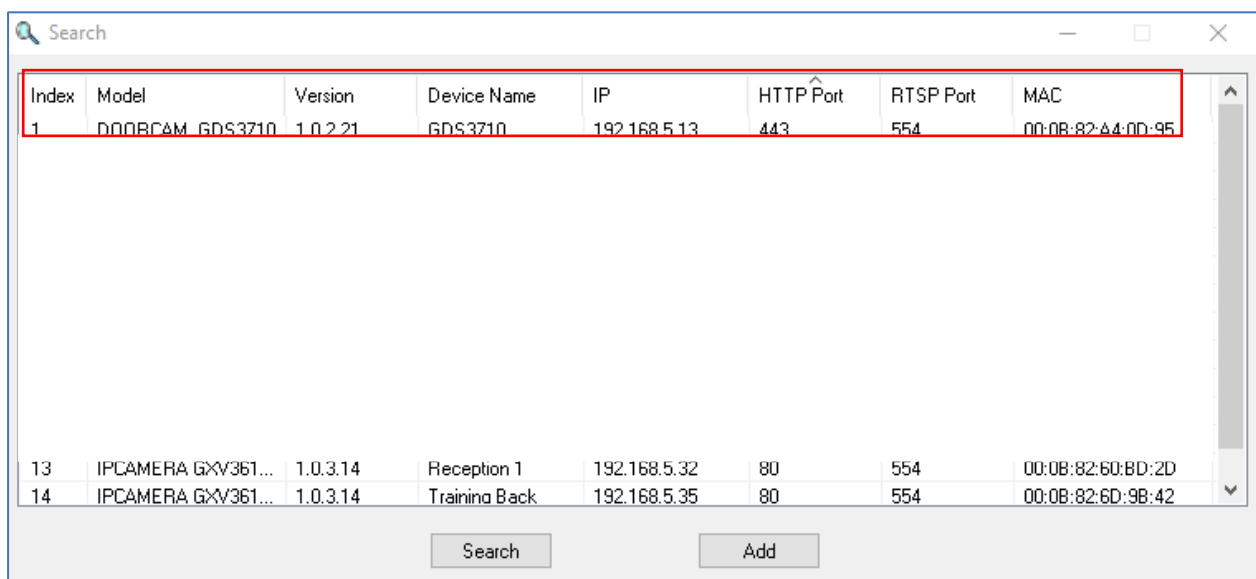
- Once logged in, the prompt message will display asking for plug-in installation.
- Disable security or antivirus software, download and install the plug-in, close and open the browser again, the embedded video will be displayed if clicking the “LiveView” and pressing the stream number.



## 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](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:



- On the GDS Manager access to Device → Search and Click on the  **Search** button to start device detection
- The detected devices will appear in the output field like below:

Function Navigation									
<div> <div> <div>Basic Information</div> <div>Administrator</div> <div>Group</div> <div>Member</div> <div>Schedule</div> <div>Holiday</div> <div>Device</div> <div>Search</div> <div>Configuration</div> <div>Card Info</div> </div> <div> <input checked="" type="checkbox"/> Search by server           <div>  Search           <div>+ Add</div> </div> </div> </div>									
<input type="checkbox"/> Index	Model	Version	Device Name	IP	HTTP Port	RTSP Port	Mac		
<input type="checkbox"/> 1	GDS3710	1.0.2.21	GDS3710	192.168.5.13	443	554	00:0B:82:A4:0D:95		
<input type="checkbox"/> 2	GDS3710	1.0.2.22	GDS3710	192.168.6.42	443	554	00:0B:82:A7:9C:16		

**Figure 11: GDS3710 Detection**

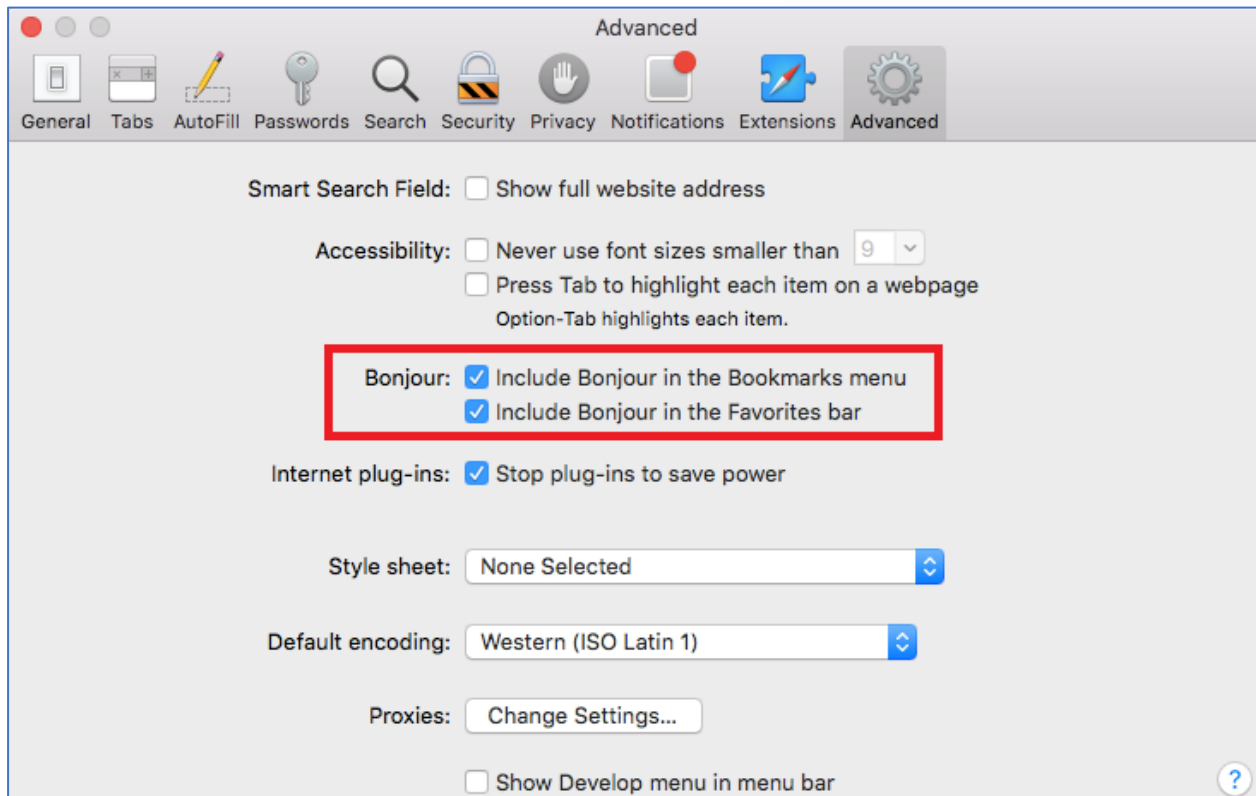
- Double click the column of the detected GDS3710, the browser will automatically open and show the device's web configuration page.
- The browser will ask for plug-in if not installed, please authorize the installation of the plug-in.
- Enter the administrator user name and password to access the Web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

- Open Safari, select "Advanced" to open the Advanced Setting.
- 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.



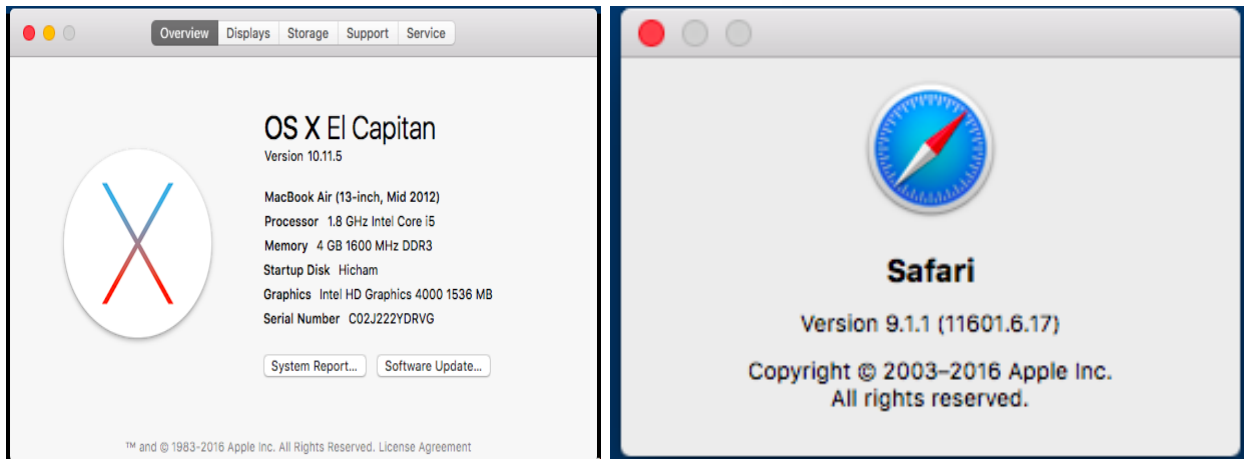
**Figure 13: Bonjour Setting Page**

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.





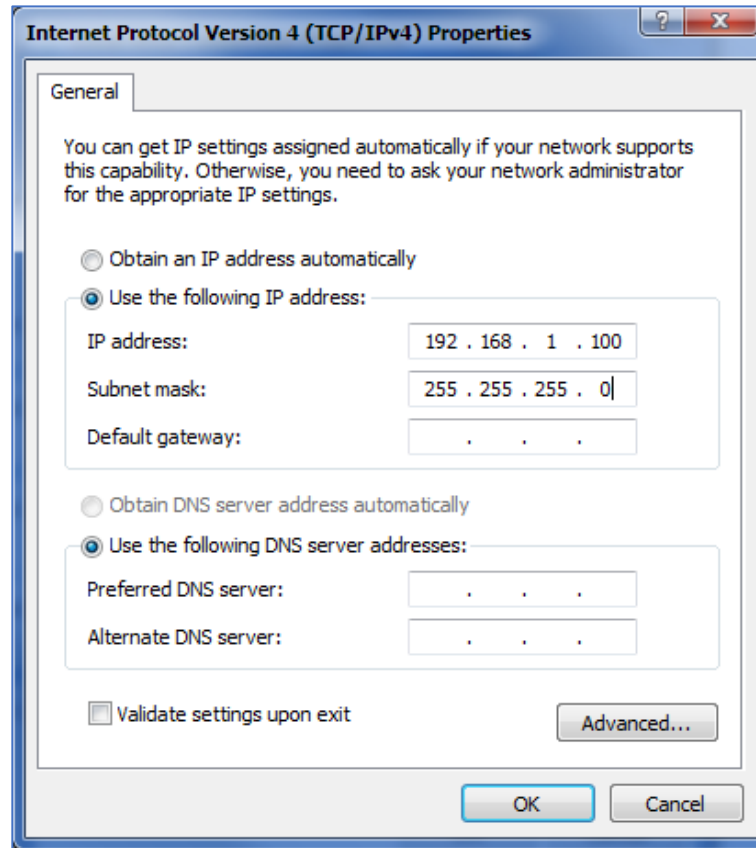
- iPhone/iPad (iOS) users are recommended to use Applications in Apple Store.
- Free or Paid applications from Apple Store like “IP Cam Viewer” is suggested and verified working with Grandstream GDS3710.
- Apple Store applications like “IP Cam Viewer” will support H.264 video codec.

## 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).



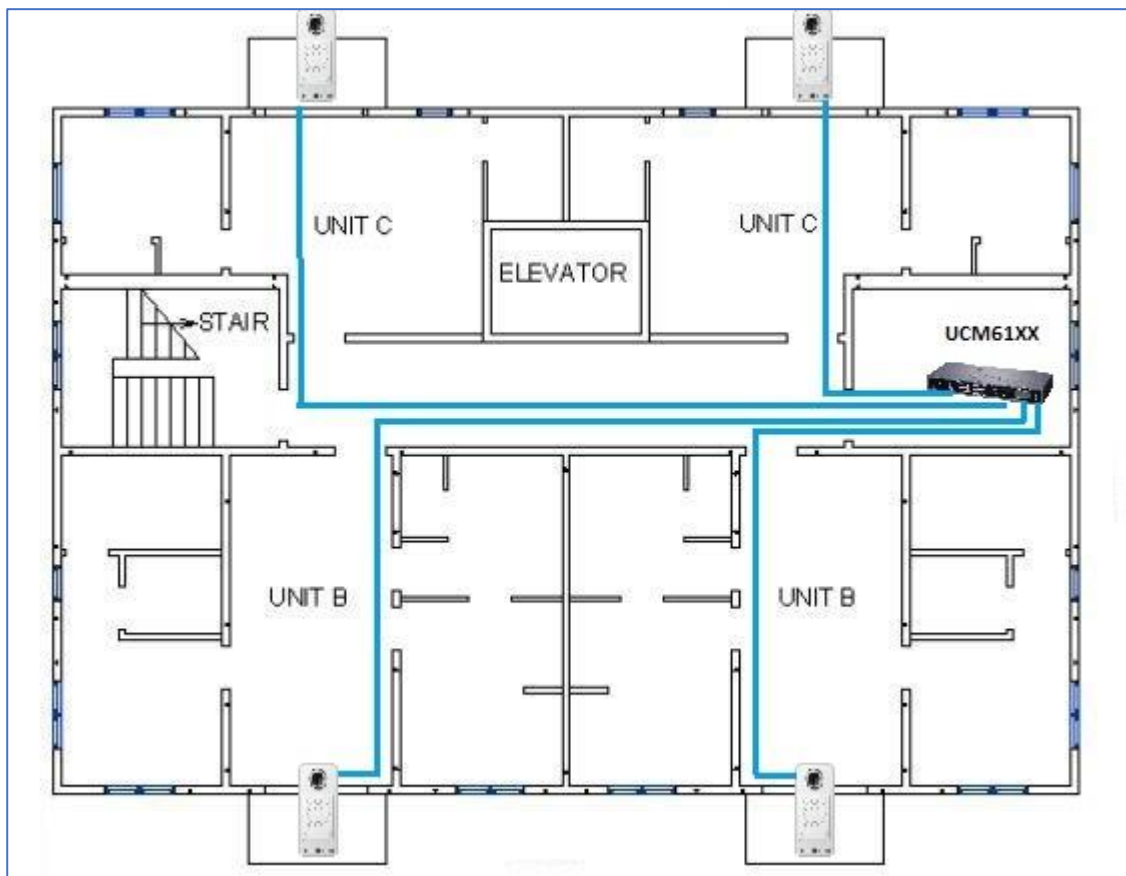


Figure 15: Peering GDS3710 with UCM6XXX

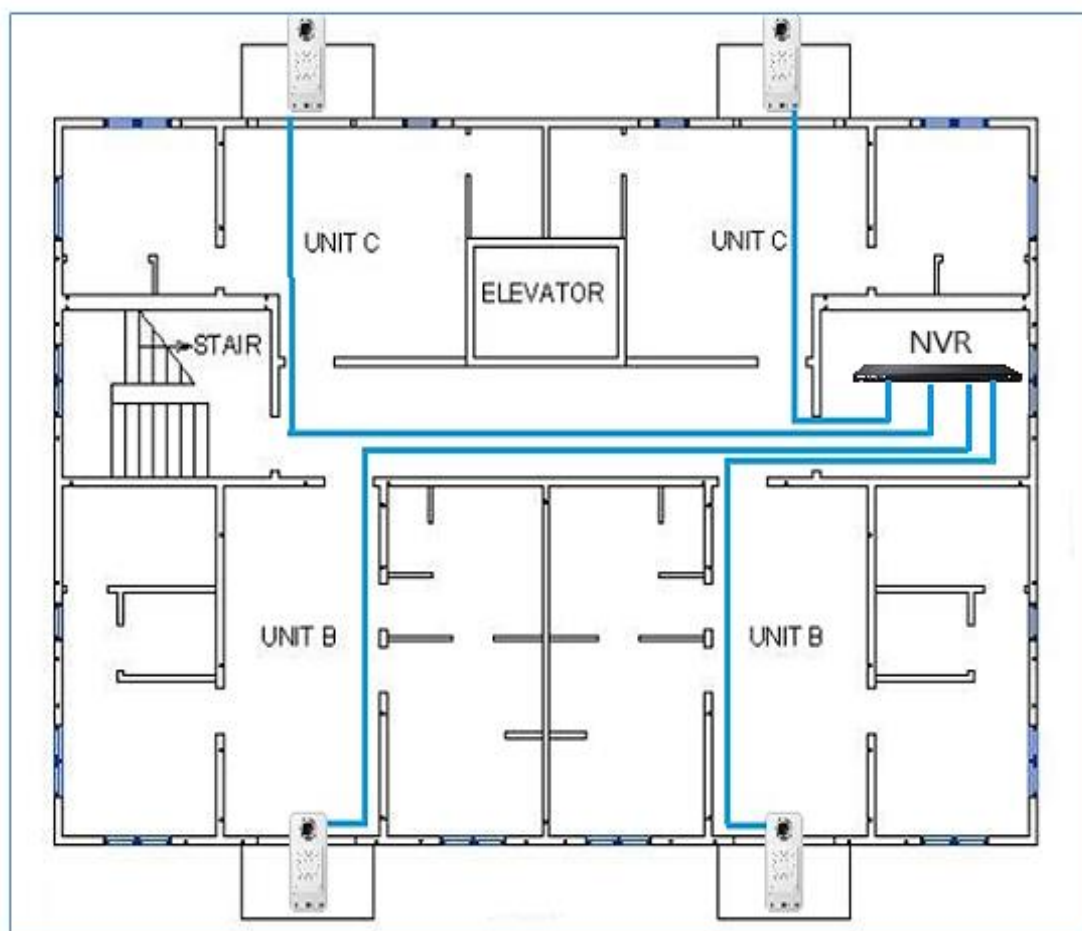
## Using a Network Video Recorder (NVR)

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

Equipment List:

- Several GDS3710
- NVR supporting Onvif Profile S.
- 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.

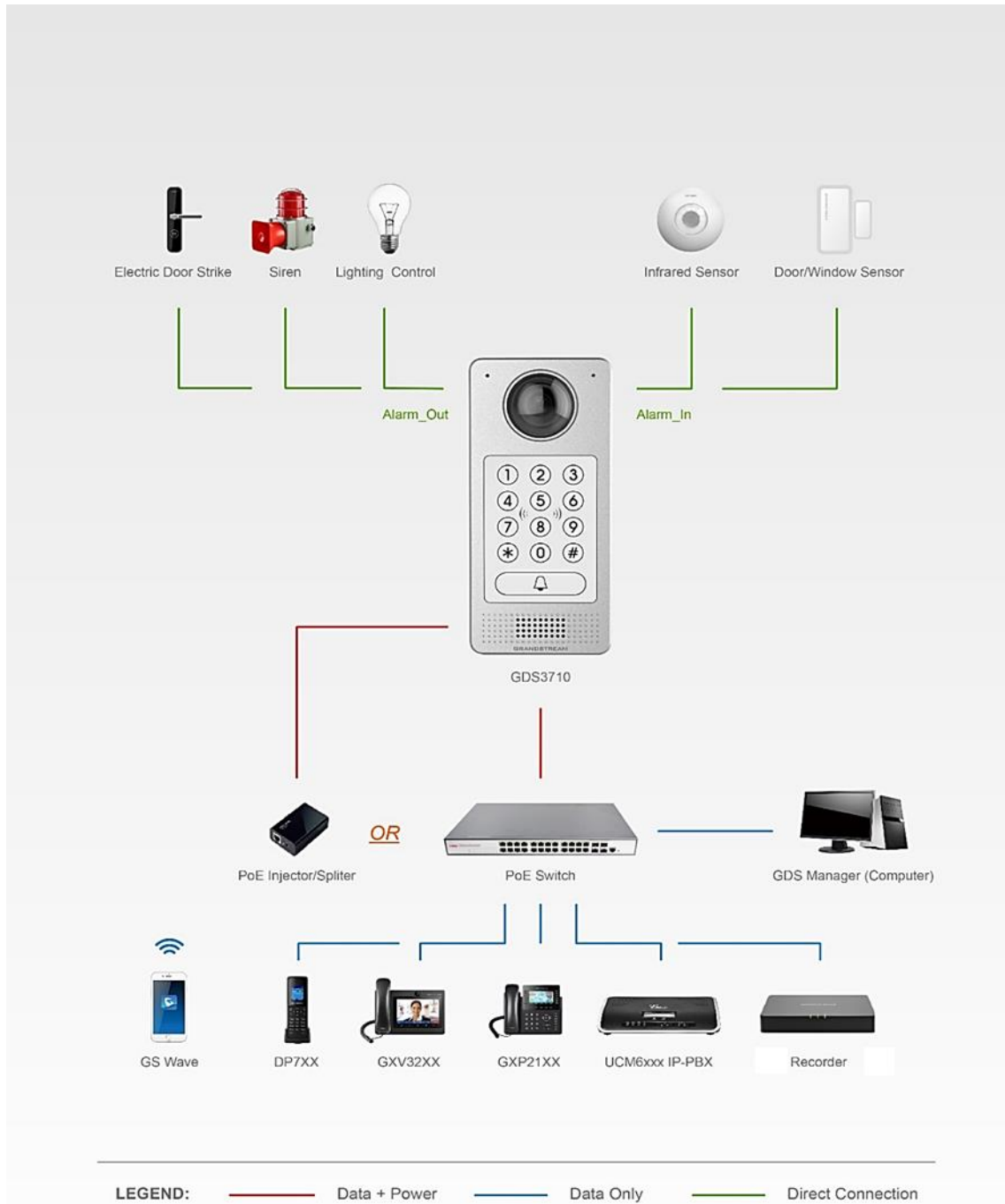


Figure 17: Peripheral Connections for GDS3710

## 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.

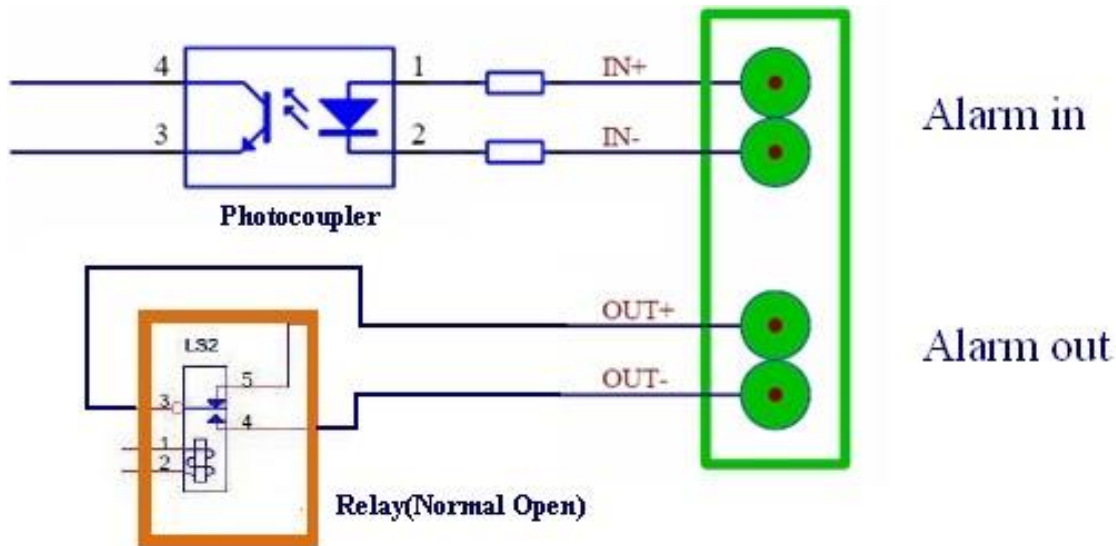


Figure 18: Alarm\_In/Out Circuit for GDS3710

### Notes:

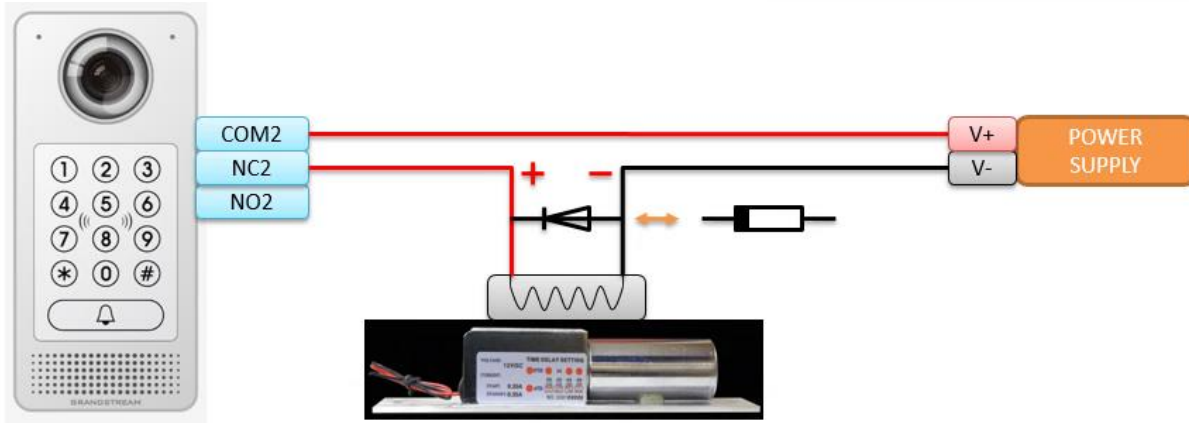
- The Alarm\_In and Alarm\_Out circuit for the GDS3710 should meet the following requirement:

<b>Alarm Input</b>	3V<V <sub>in</sub> <15V, PINs (1.02KΩ)
<b>Alarm Output</b>	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

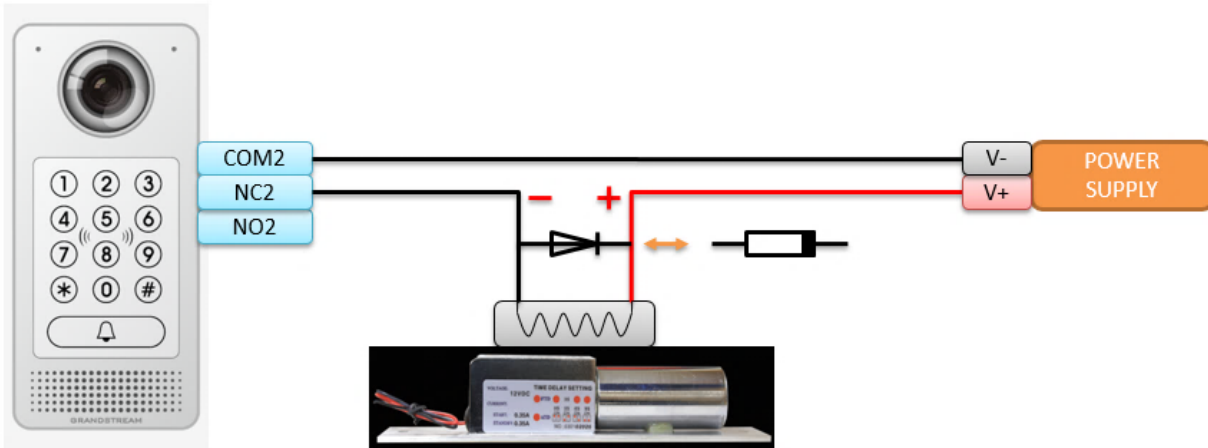
When connecting the GDS3710 to a door strike it is recommended to set an EMF protection diode in reverse polarity for a secure use, below examples of deployment for the protection diode.



**Electric lock**

**Figure 19: Protection Diode - Example 1**

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



**Electric lock**

**Figure 20: Protection Diode - Example 2**

**Note:** power polarity connection: Diode: SS24 or  $I_f \geq 2A$ ,  $V_r \geq 40V$ .

## 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 3<sup>rd</sup> Party Power Supply

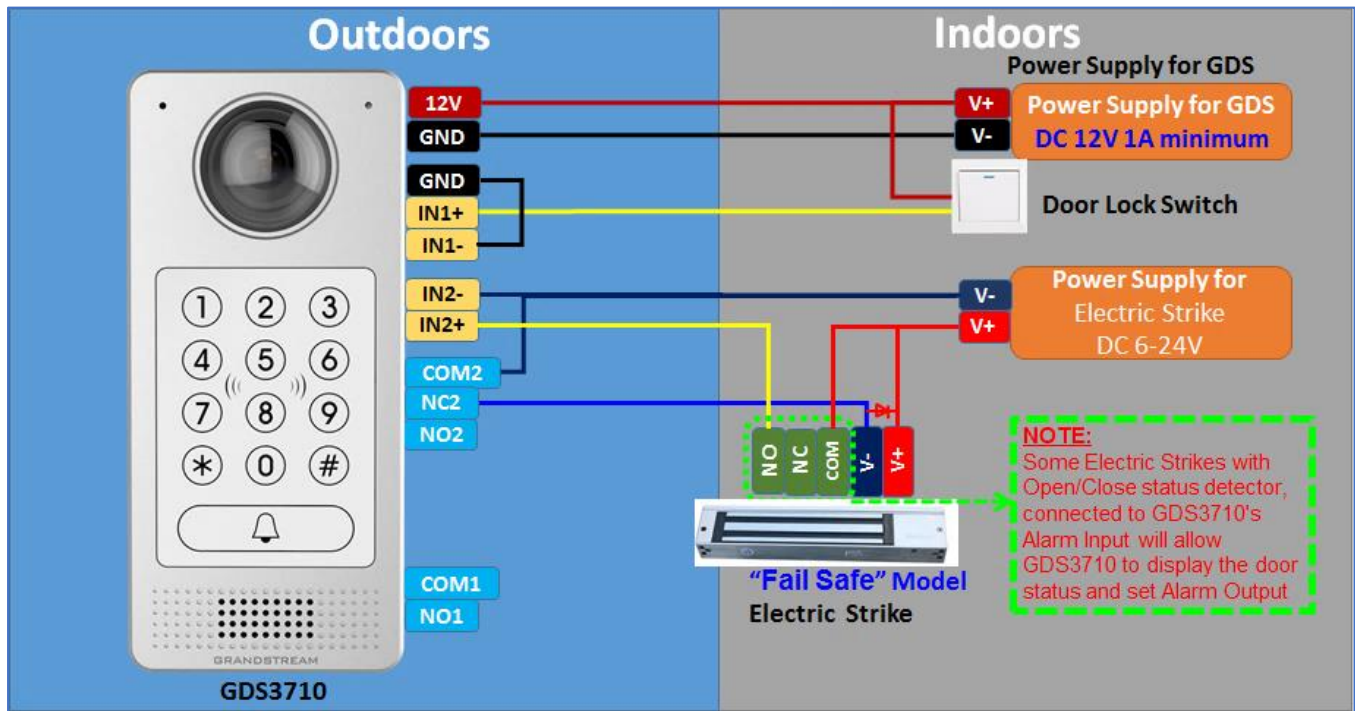


Figure 21: 3<sup>rd</sup> party Power Supply Wiring Sample

## Wiring Sample using Power Supply for both GDS3710 and Electric Strike

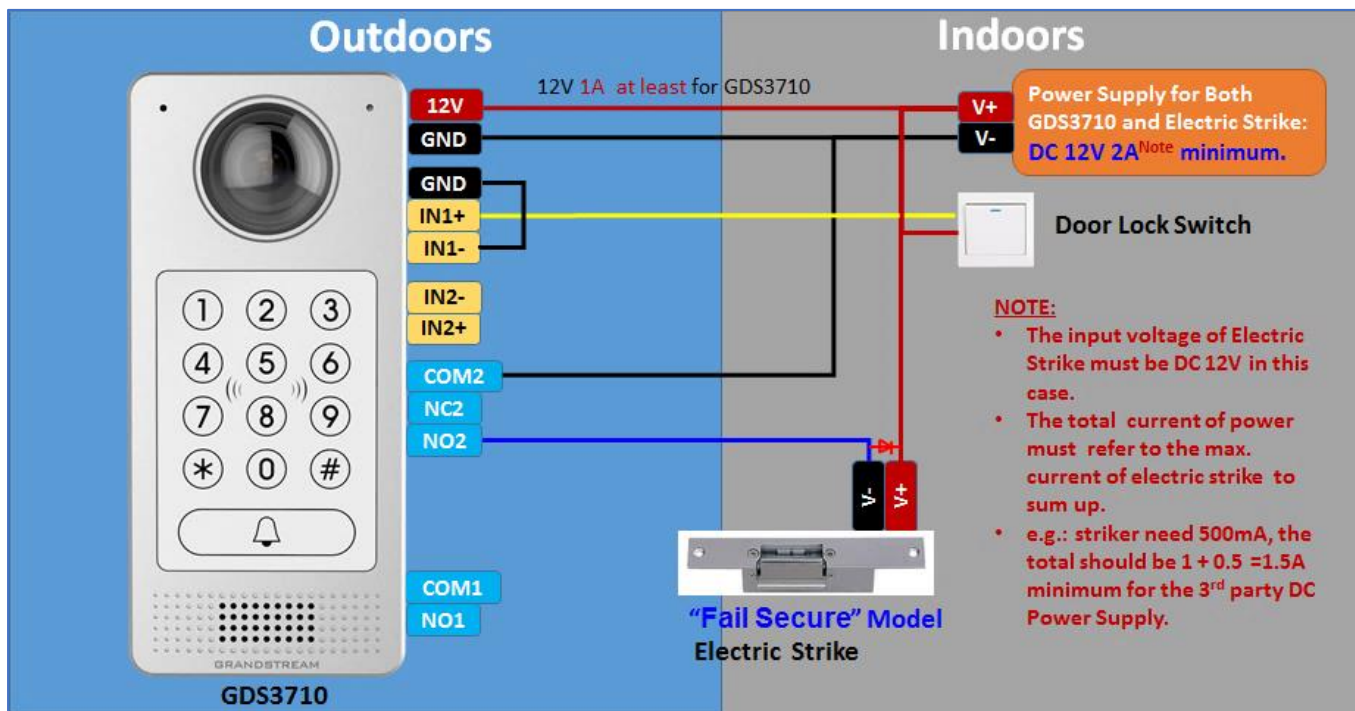


Figure 22: Power Supply used for both GDS3710 and Electric Strike

## Wiring Sample using PoE to power GDS3710 and 3<sup>rd</sup> Party Power Supply for Electric Strike

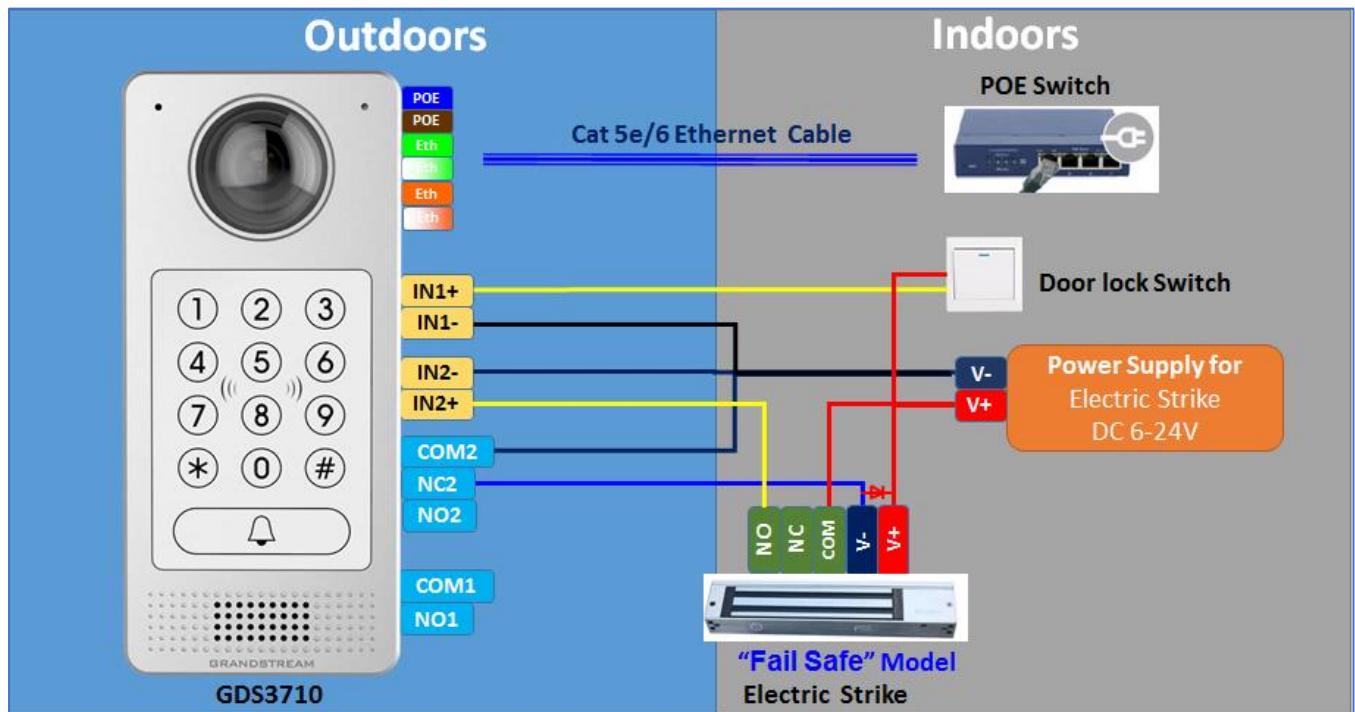


Figure 23: Wiring Sample using PoE to power GDS3710 and 3<sup>rd</sup> party Power Supply for Electric Strike

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



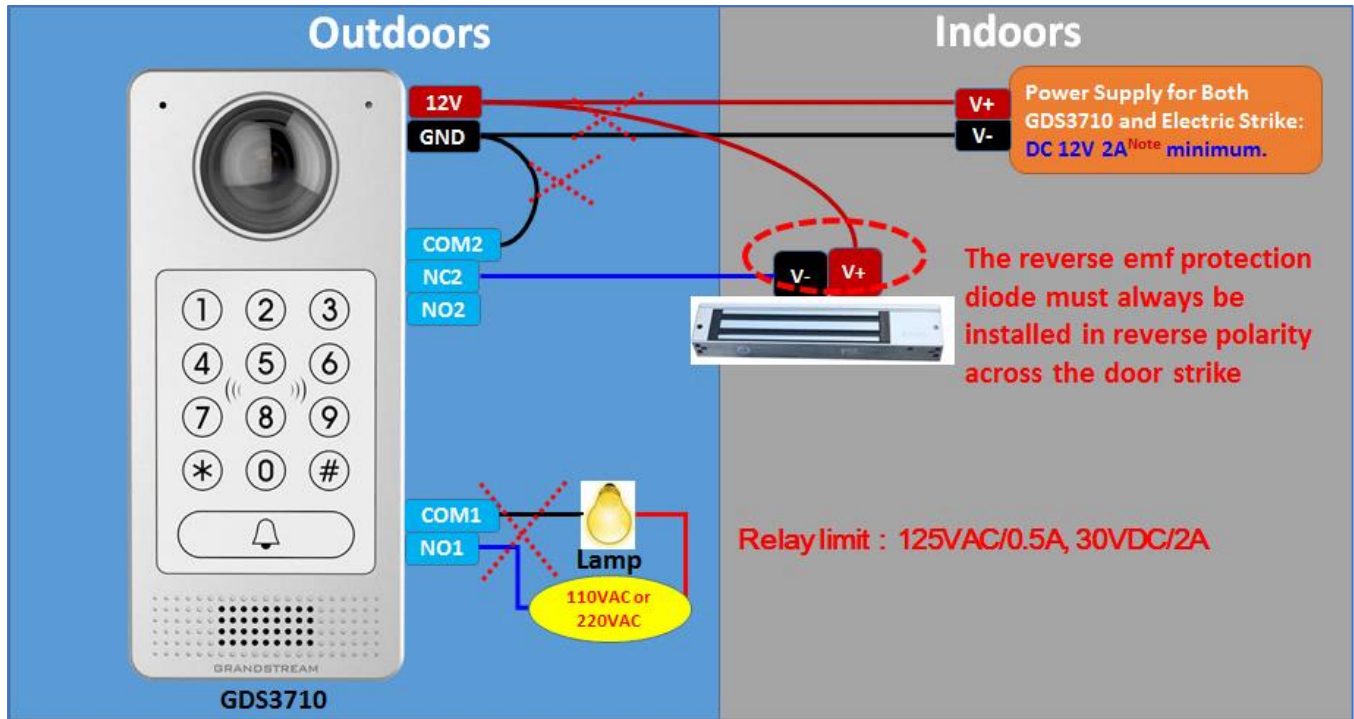


Figure 24: Example to Avoid when Powering the Electric Strike

### Good Wiring Sample for Electric Strike and High-Power Device

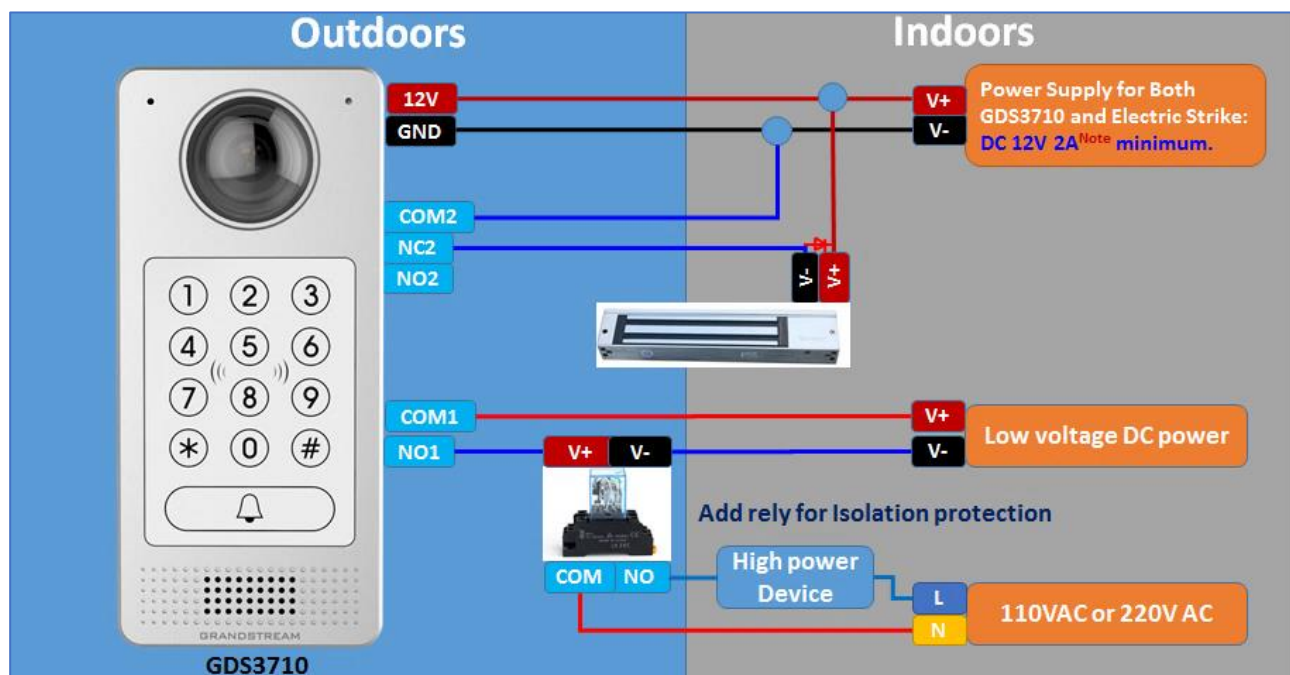


Figure 25: Electric Strike and High-Power Device Example

## 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 3<sup>rd</sup> party power supply for Wiegand device

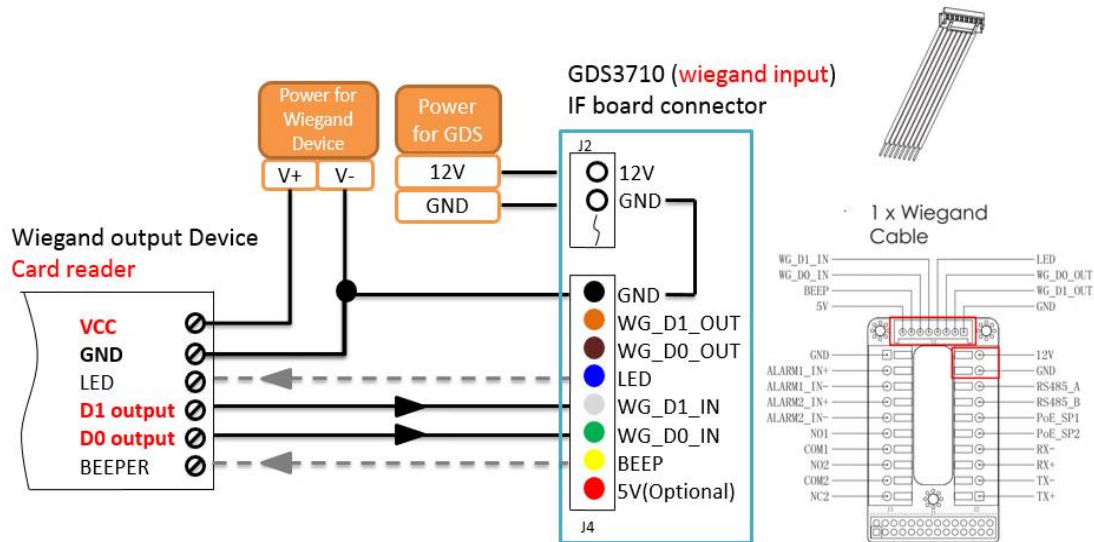


Figure 26: Wiegand Input Example with 3<sup>rd</sup> party Power Supply

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

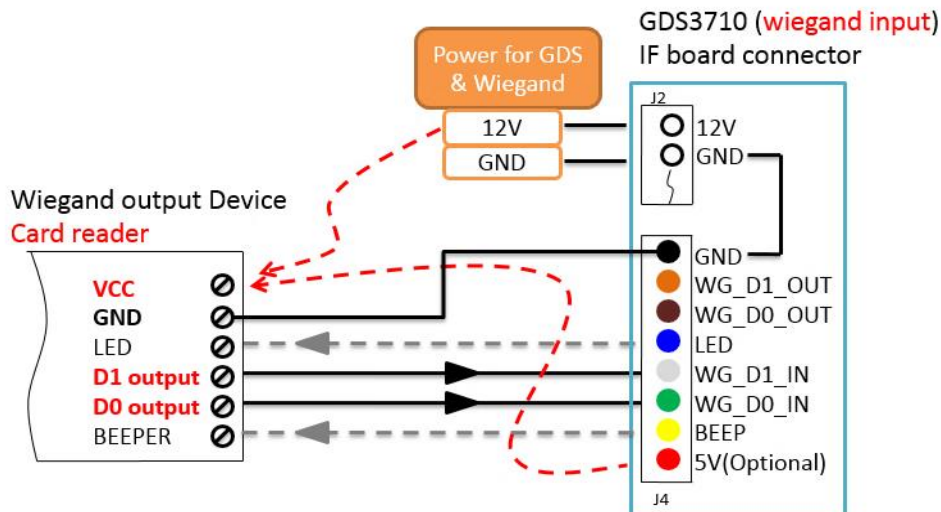


Figure 27: Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device



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 3<sup>rd</sup> party power supply for Wiegand device

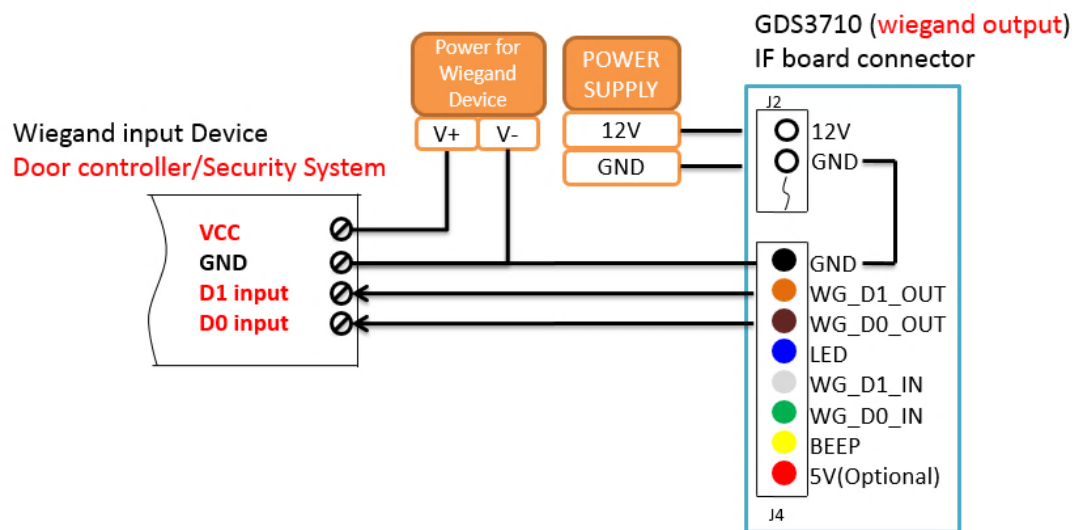


Figure 28: Wiegand Output Wiring Example

When the Wiegand output of the GDS3710 is connected, it acts as the signal receiver of the 3<sup>rd</sup> 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

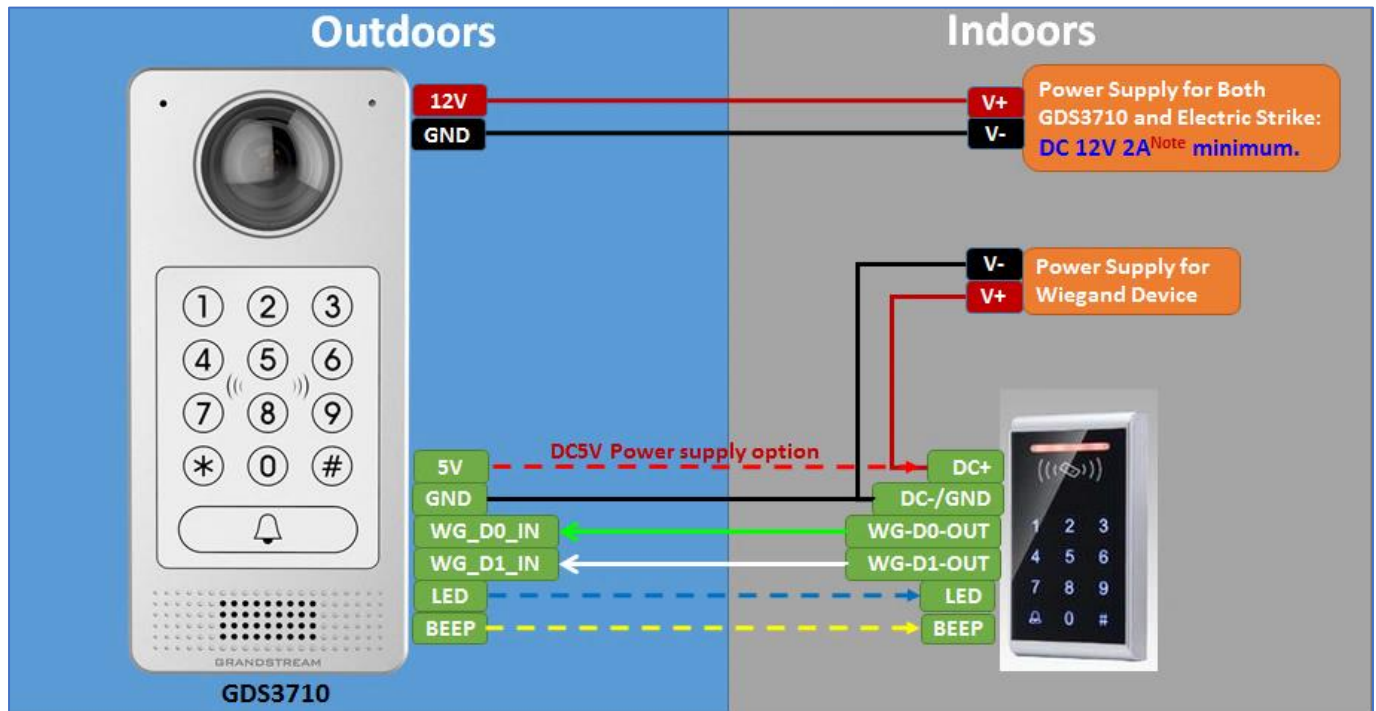


Figure 29: Wiegand RFID Card Reader Example

## Siren alarming when door opened abnormally

When this feature enabled (special wiring required, see below wiring diagram), abnormal open door will be detected by **DI** port (**Alarm\_In2** or **IN2** in below diagram showed) if wired correctly (connecting the **COMx** port to **Dlx** port) therefore trigger siren alarm. Once abnormal open door alarm triggered, the siren will sound non-stop, until manually override by related person.

There are several ways to stop and disable the alarm:

- 1) Power cycle the GDS37xx
- 2) Pick up the Alarm Phone Call (if configured)
- 3) Open Door using PIN (either public PIN or private PIN)

Once alarm triggered, the GDS3710 will take snapshots when the abnormal open door happened, email and upload the snapshots to FTP or Central Server (when configured); call the configured alarm SIP phone, send the alarm output (if connected). User will only be able to disable the siren using the 3 methods mentioned above.

Detailed action information please refer to GDS37xx User Manual, "Alarm Action Settings" configuration. Below are some diagrams showing the correct wiring to enable this new security enhancement feature:



## GDS3710 Connection: IN2 set as Normal Close and “Fail Safe” Electric Strike using 3<sup>rd</sup> Party Power Supply

Digit Input	
Digit Input 1	Abnormal Door Control ▼
Digit Input 1 Abnormal Door Control Options	<input checked="" type="radio"/> Door 1 <input type="radio"/> Door 2
Digit Input 1 Status	Normal Close ▼

Figure 30: Digital Input set as Normal close

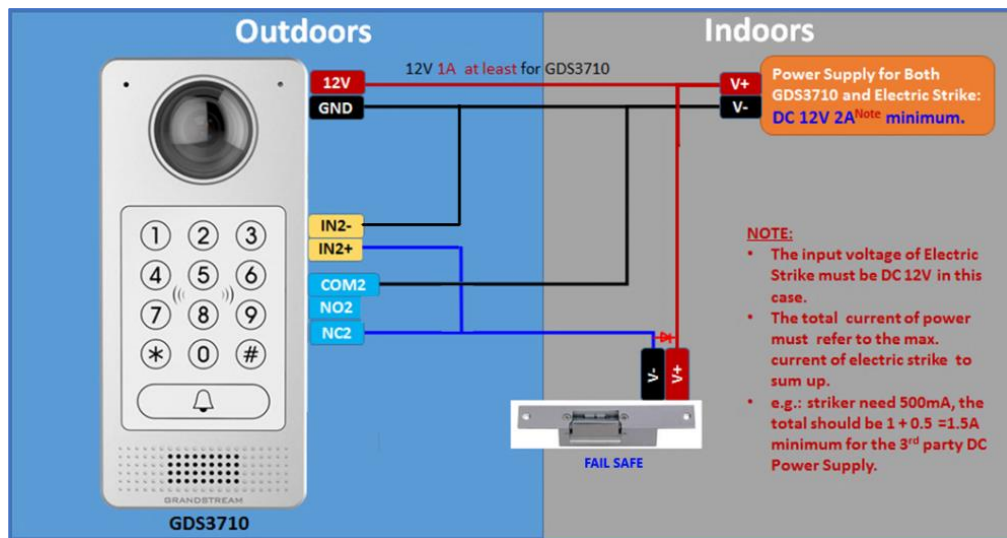


Figure 31: “Fail safe” Electric Strike using 3rd Party Power Supply

## GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3<sup>rd</sup> Party Power Supply

Digit Input	
Digit Input 1	Abnormal Door Control ▼
Digit Input 1 Abnormal Door Control Options	<input checked="" type="radio"/> Door 1 <input type="radio"/> Door 2
Digit Input 1 Status	Normal Open ▼

Figure 32: Digital Input set as Normal open

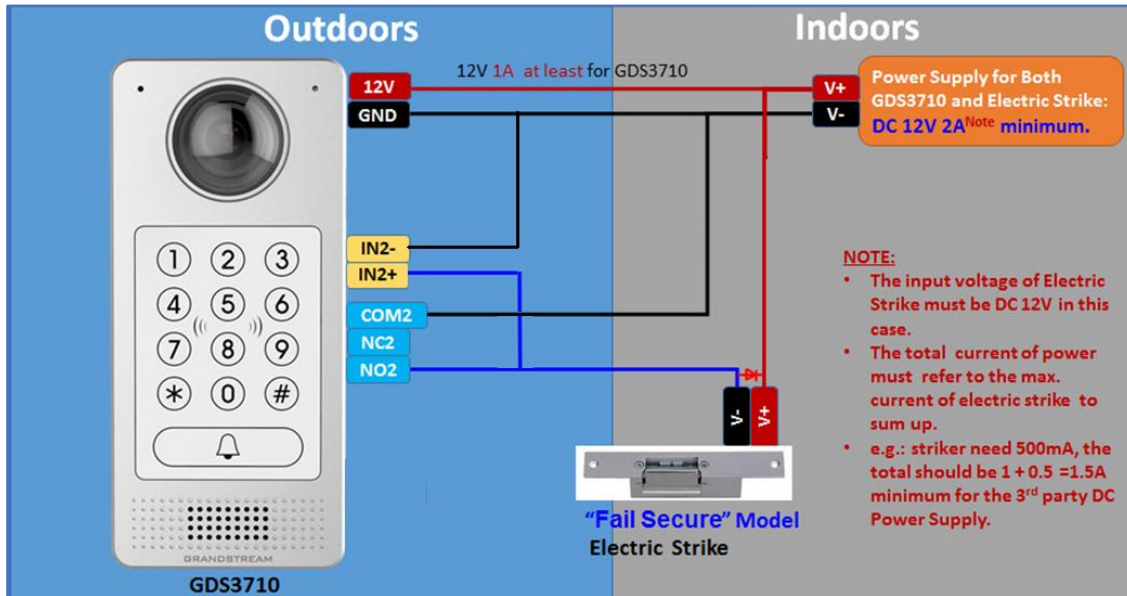


Figure 33: "Fail Secure" Electric Strike using 3rd Party Power Supply

### GDS3710 Connection: IN2 set as Normal Open and "Fail Secure" Electric Strike using 3<sup>rd</sup> Party Power Supply with Door sensor

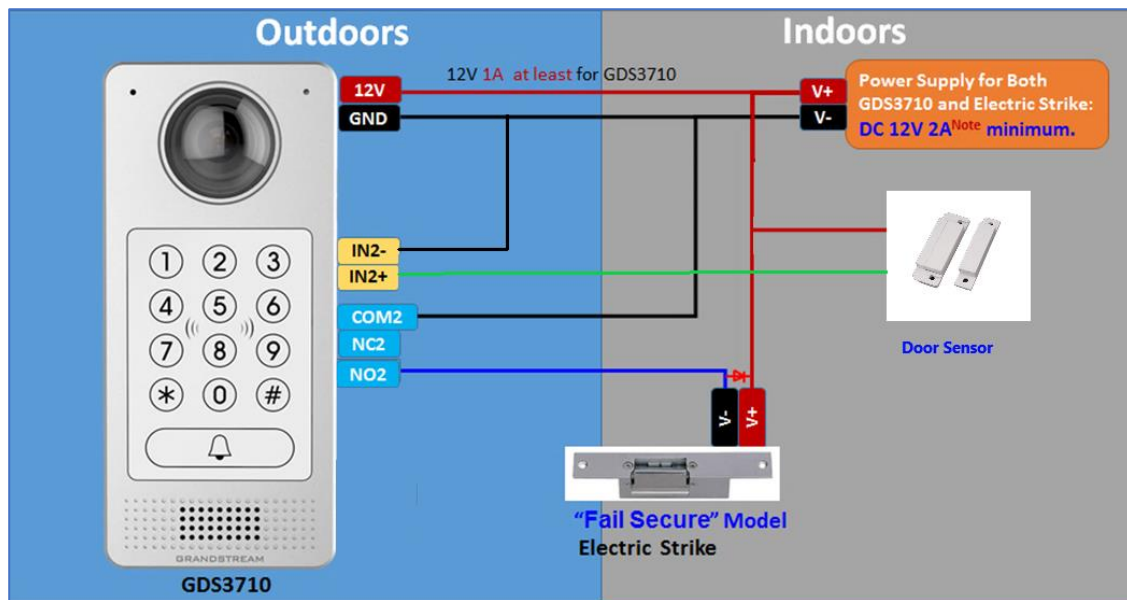


Figure 34: "Fail Secure" Electric Strike using 3rd Party Power Supply with Door Sensor

## GSC3570 Secure Open Door via GDS37XX/GSC3570 Peering

This secure open door new feature is a major enhancement to GDS37xx, but need to include GSC3570 to make it a whole solution. The GDS37xx/GSC3570 will be peering together in LAN/WAN via IP/SIP, the door lock/strike will be wired to GSC3570Alarm\_Out port and controlled by GSC3570. This way the strike control is inside the building with enhanced security. Below is a setup example:

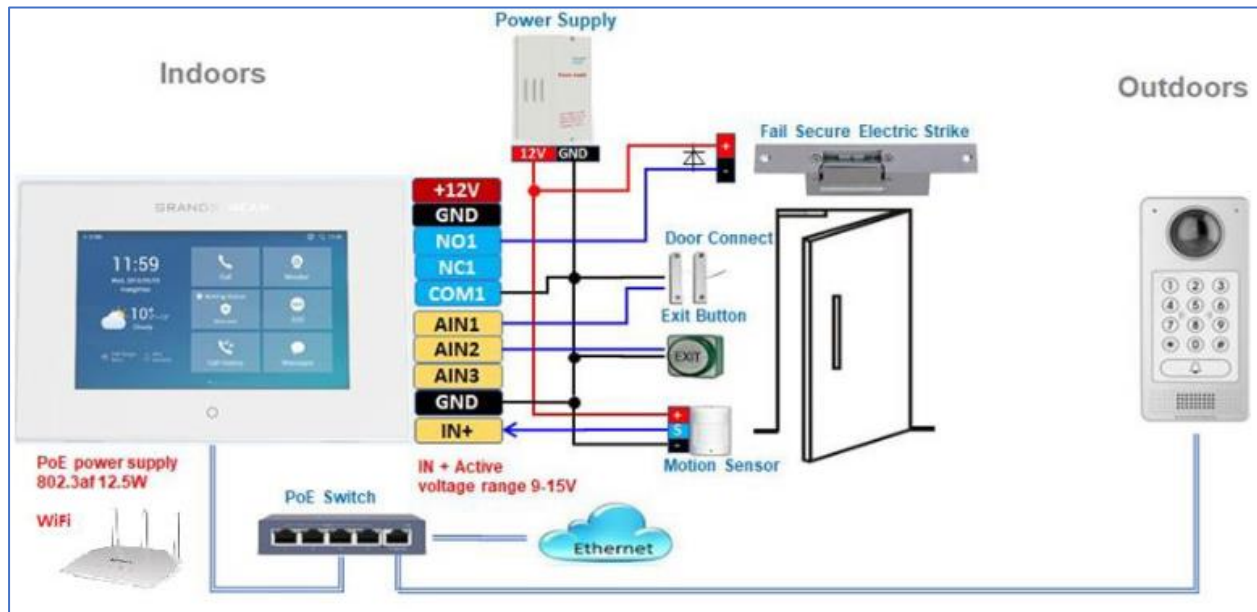


Figure 35: GSC3570 secure open door via GDS3710

### Note:

Minimum firmware required for this to work:

- Outdoor Device: GDS3710(FW1.0.7.19) and GDS3705(FW1.0.1.13)
- Indoor Device: GSC3570(FW1.0.5.2)

The GDS37xx can be powered via PoE; the GSC3570 can connect to same network via PoE or WiFi. For open door combination with GSC3570 and GDS37xx, if GSC3570 needs to control multiple GDS37xx, it has to use SIP and the related GDS37xx will control the strike/lock. The different GDS37xx doorbell call will have "One Button Open Door" displayed when in "Preview" (early media support) or when call established.

The GSC3570 user will press the virtual button on touch screen to remotely open the door controlled by the related GDS37xx. There is no door limitation for such usage but only ONE DOOR can be opened at one time. It is just a SIP call open door application, but strike/lock control circuit is located outdoor.

For "Secure Open Door", the GSC3570 is peering with GDS37xx. The GSC3570 controlling the relay/strike/lock from inside the building (Unlike GDS37xx installed outside), but only ONE door can be controlled because GSC3570 only has one Relay Control circuit build in.

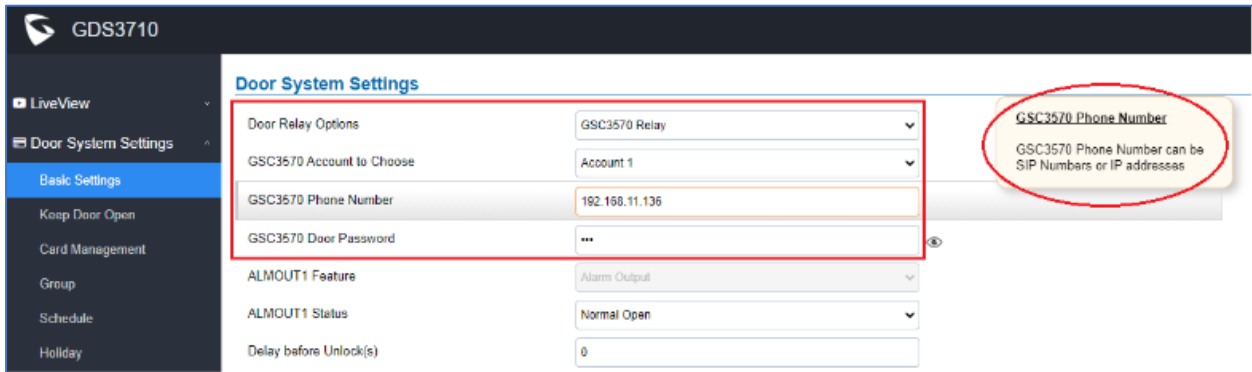
This peering can be via LAN/WAN but LAN is recommended and actually most of the application scene are in LAN environment because most likely the GSC3570 and GDS37xx are in the same building. Although SIP/UCM over Internet/WAN also works, it is recommended to use static IP if the GSC3570 (inside) and GDS37xx(outside) are at same location in the same LAN.

This setup is much simple and reliable in case there is network outage like Internet/UCM is down.

For the GSC3570 and GDS37xxpeering, it can be used via SIP only (Cloud or UCM); IP only (No SIP proxy or UCM but static IP address) and Mixed (SIP and fallback to IP if Proxy failed).

### GDS3710 Web Configuration

This setup can be found under device web UI→Door System Settings →Basic Settings:



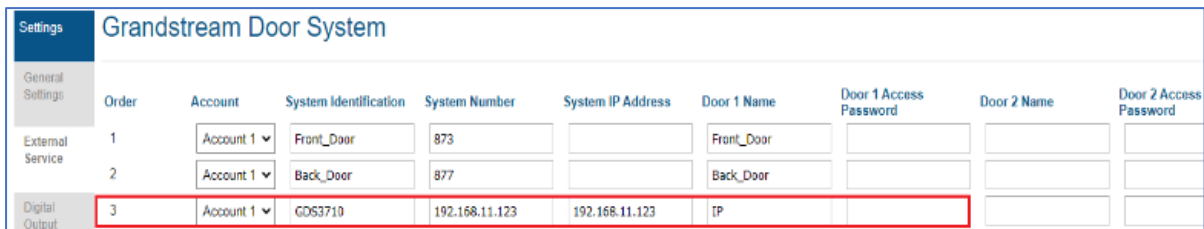
The screenshot shows the 'Door System Settings' page for GDS3710. The left sidebar has 'Door System Settings' expanded, with 'Basic Settings' selected. The main area contains several configuration fields. A red box highlights the 'GSC3570 Phone Number' field, which is set to '192.168.11.136'. A yellow callout box points to this field with the text: 'GSC3570 Phone Number can be SIP Numbers or IP addresses'.

Field	Value
Door Relay Options	GSC3570 Relay
GSC3570 Account to Choose	Account 1
GSC3570 Phone Number	192.168.11.136
GSC3570 Door Password	***
ALMOUT1 Feature	Alarm Output
ALMOUT1 Status	Normal Open
Delay before Unlock(s)	0

Figure 36: GSC3570 secure open door via GDS3710-GDS3710 configuration

### GSC3570 Web Configuration

The GSC3570 side also need to be configured according, like below:

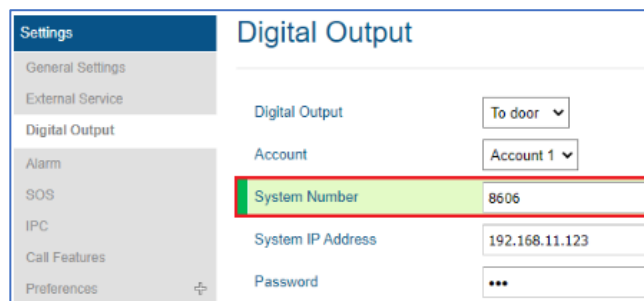


The screenshot shows the 'Grandstream Door System' configuration page on the GSC3570. It features a table with columns for Order, Account, System Identification, System Number, System IP Address, Door 1 Name, Door 1 Access Password, Door 2 Name, and Door 2 Access Password. A red box highlights the third row, which is for 'Digital Output'.

Settings	Order	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
External Service	1	Account 1	Front_Door	873		Front_Door			
	2	Account 1	Back_Door	877		Back_Door			
Digital Output	3	Account 1	GDS3710	192.168.11.123	192.168.11.123	TP			

Figure 37: GSC3570 secure open door via GDS3710-GSC3570 Door System System configuration

Then we will be configuring the Digital Input on the GSC3570 as the figure below:



The screenshot shows the 'Digital Output' configuration page on the GSC3570. The left sidebar has 'Digital Output' selected. The main area contains fields for Digital Output, Account, System Number, System IP Address, and Password. A red box highlights the 'System Number' field, which is set to '8606'.

Field	Value
Digital Output	To door
Account	Account 1
System Number	8606
System IP Address	192.168.11.123
Password	***

Figure 38: GSC3570 secure open door via GDS3710-GSC3570 Digital Input configuration

**Notes:**

- If the solution/integration is using static IP address without SIP Proxy, all the devices involved (GDS/GSC/IP Phone) should choose “NAT Traversal” to “No” and should NOT “Use Random Port”, otherwise will have problem of ghost call (SIP signaling working but NO media).
- The IP phone or GSC3570 can use any empty SIP account, meaning it can be mixed if Account 1 registered to UCM/Proxy and Account2 (blank) to use IP (but the account has to be configured as “Active”).





## GDS3710 HOME WEB PAGE

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

**Note:** the options displayed might differ from browser to another.

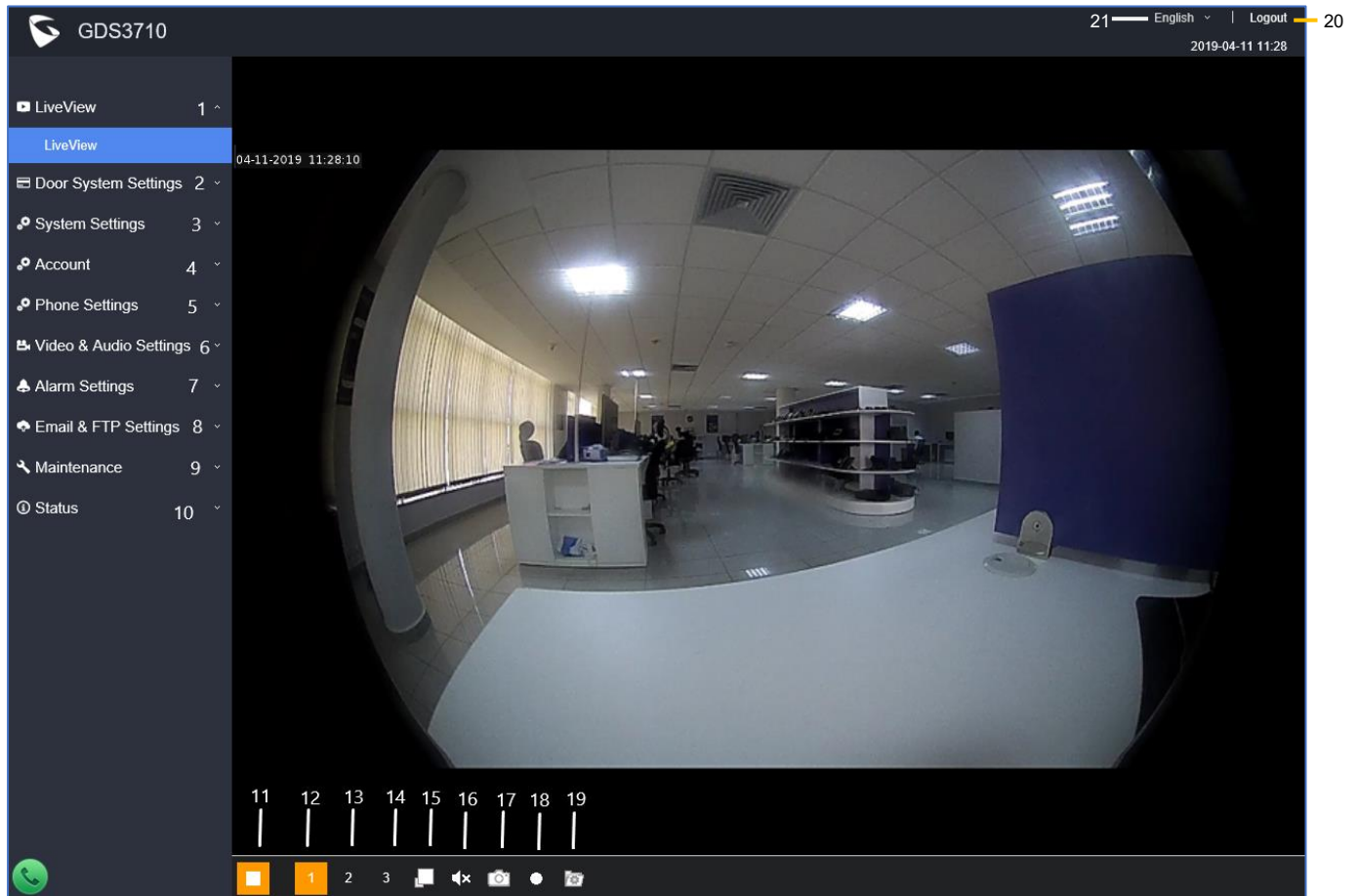


Figure 39: Home Page: Internet Explorer 11

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	Account	Access to “Account” configuration page.



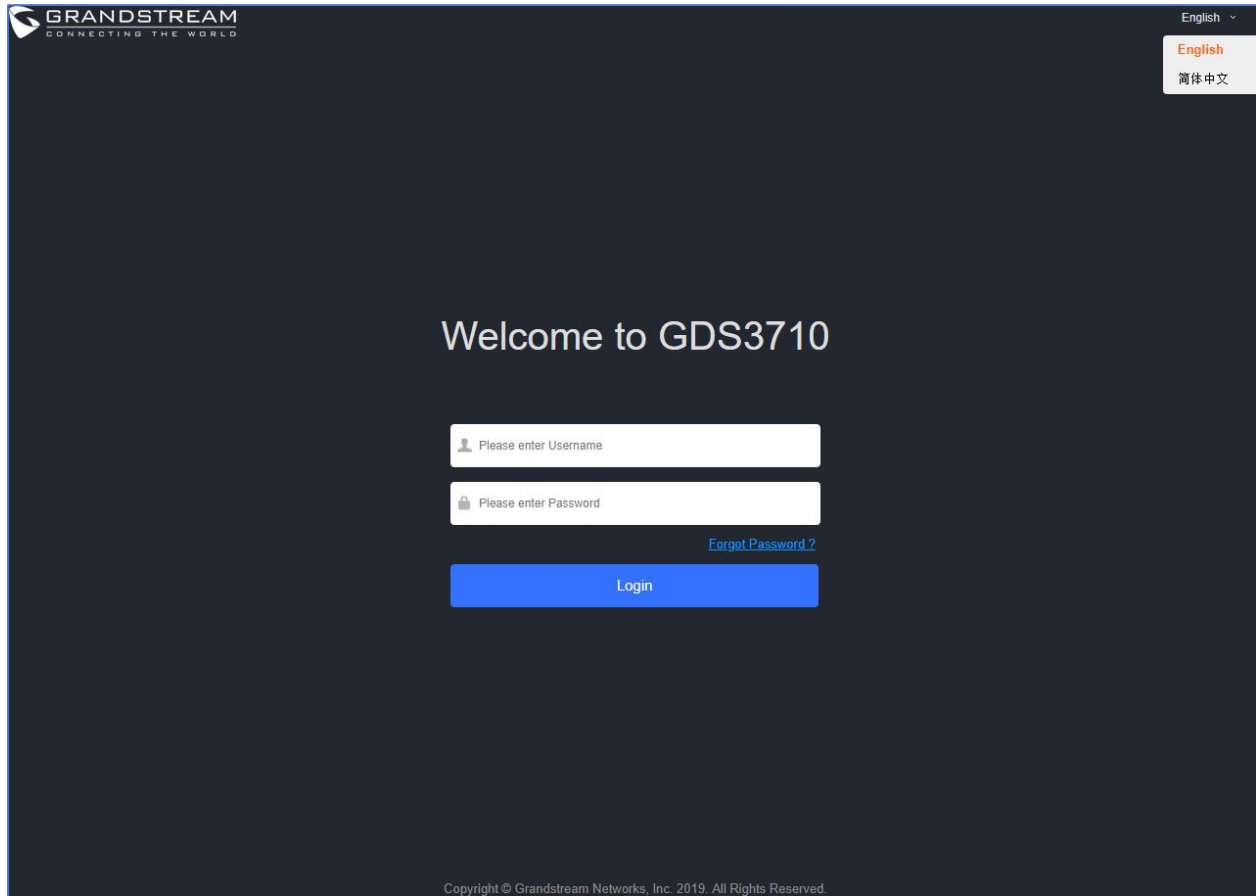


5	<b>Phone Settings</b>	Access to “Phone Settings” configuration page.
6	<b>Video &amp; Audio Settings</b>	Access to “Video & Audio settings” page.
7	<b>Alarm Settings</b>	Access to “Alarm settings” page.
8	<b>Email &amp; FTP Settings</b>	Access to “Email & FTP Settings” page.
9	<b>Maintenance</b>	Access to “Maintenance” page.
10	<b>Status</b>	Click to enter “Status” page.
11	<b>Play/Stop</b>	Start/Stop the video stream in the web page. (Internet Explorer 11)
12	<b>Stream 1</b>	Play the primary stream.
13	<b>Stream 2</b>	Play the secondary stream.
14	<b>Stream 3</b>	Play the third stream.
15	<b>Window size</b>	Resize the window. (Internet Explorer 11)
16	<b>Audio</b>	Click to mute / unmute the audio. (Internet Explorer 11)
17	<b>Snapshot</b>	Click to take a snapshot. (Internet Explorer 11)
18	<b>Recording</b>	Click to start recording. (Internet Explorer 11)
19	<b>File Path Saved</b>	Click to access Record and Capture paths. (Internet Explorer 11)
20	<b>Logout</b>	Logout from the web page.
21	<b>Language</b>	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 40: 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.

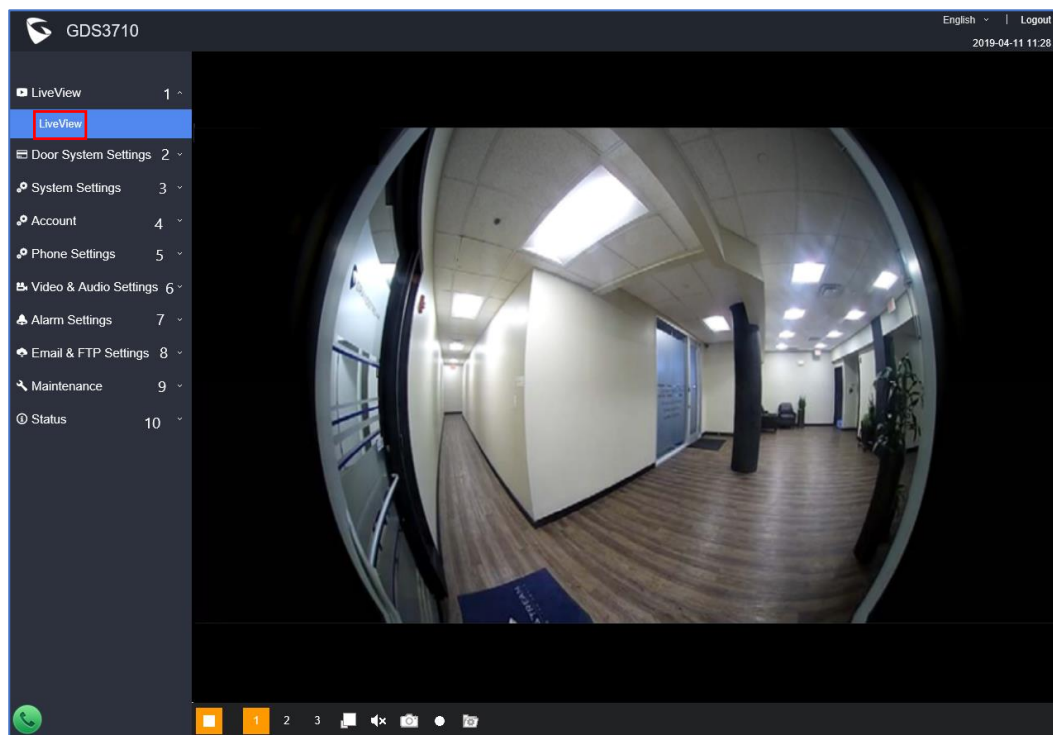


Figure 41: Live View Page: Google Chrome

Three streams are available:

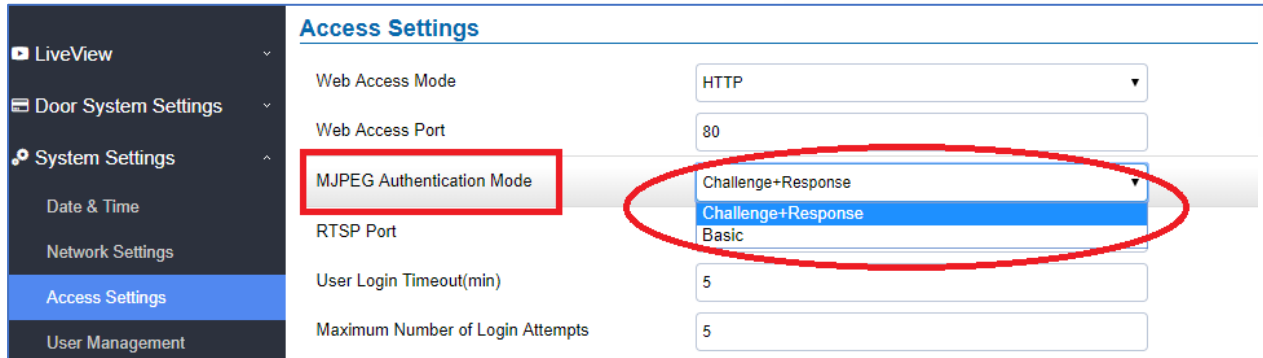
- **Primary video stream:** 1920\*1080 resolution, recommended for continuous full HD recording (If used with GXV355X NVR).
- **Secondary video stream:** 640\*480 resolution, recommended for SIP/VoIP video calls (if used with GXV3240/GXV3275).
- **Third video stream:** 320\*240 resolution, recommended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



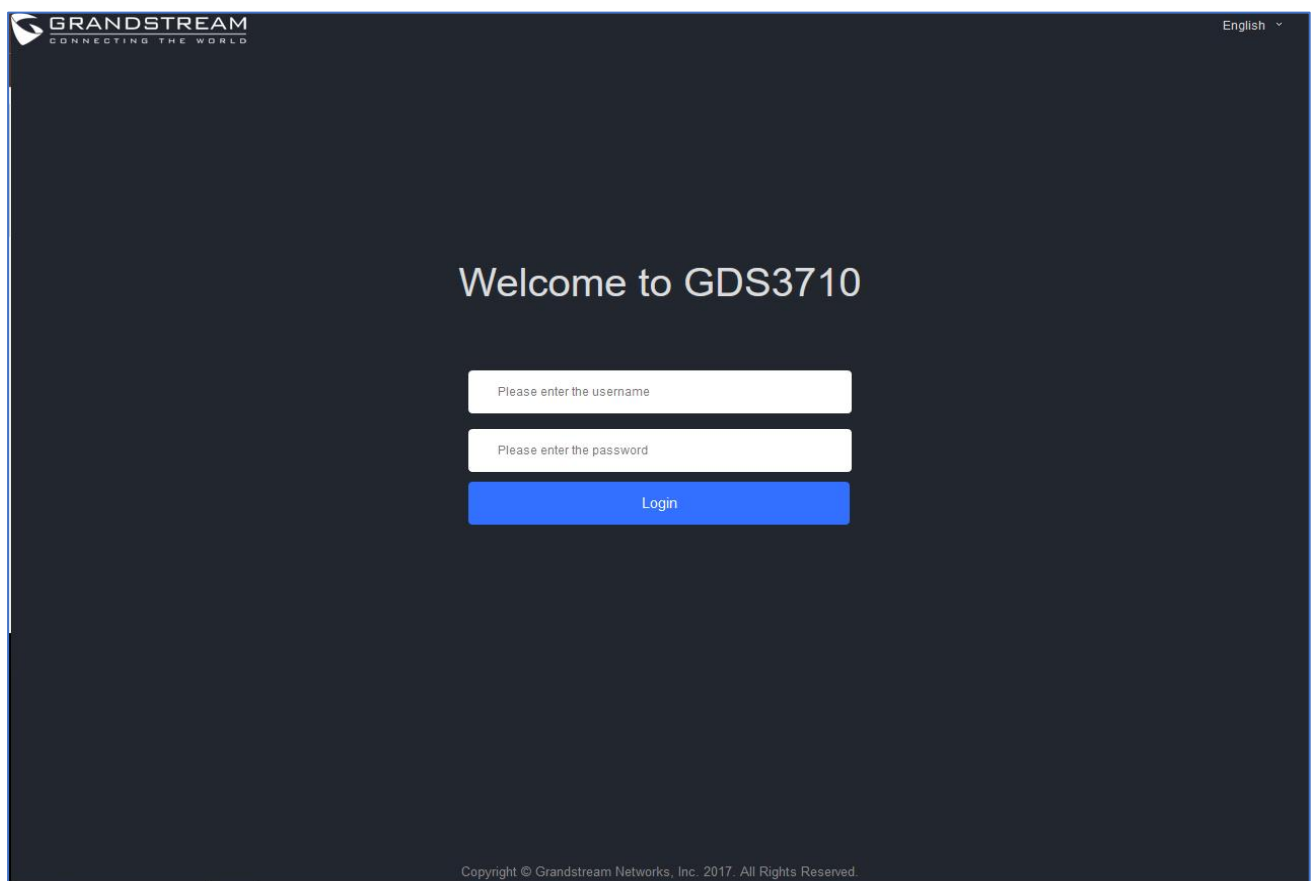


**Figure 42: MJPEG Authentication Mode**

### 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 43 : Snapshot admin credential**

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





**Figure 44 : 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.

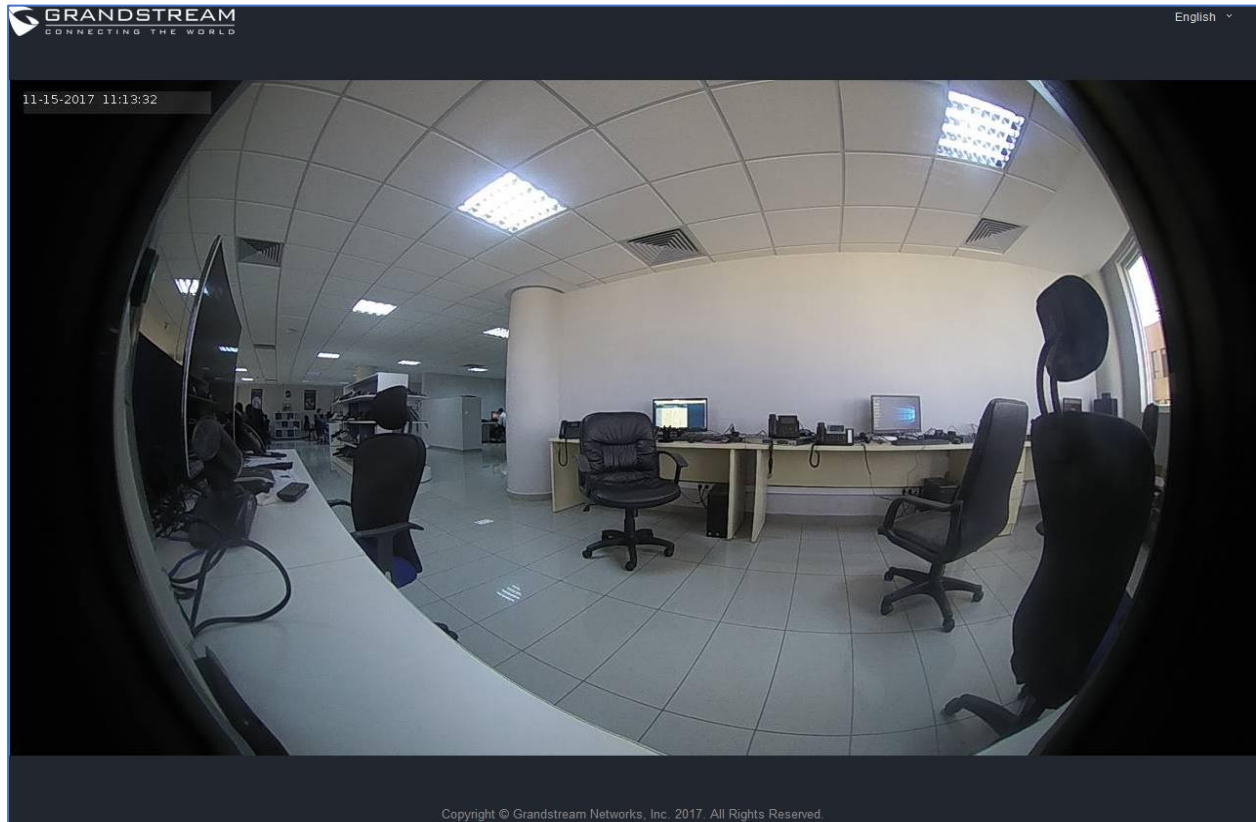


Figure 45: Snapshot view using Basic Authentication Mode

## 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**

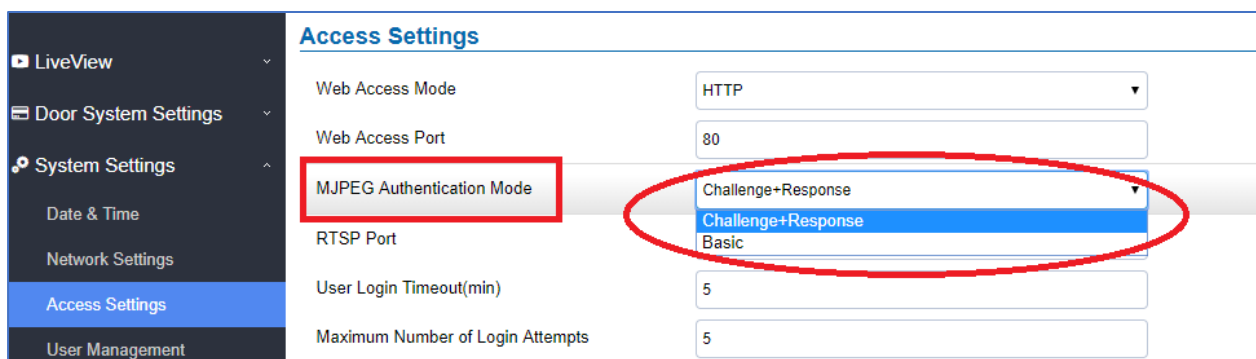


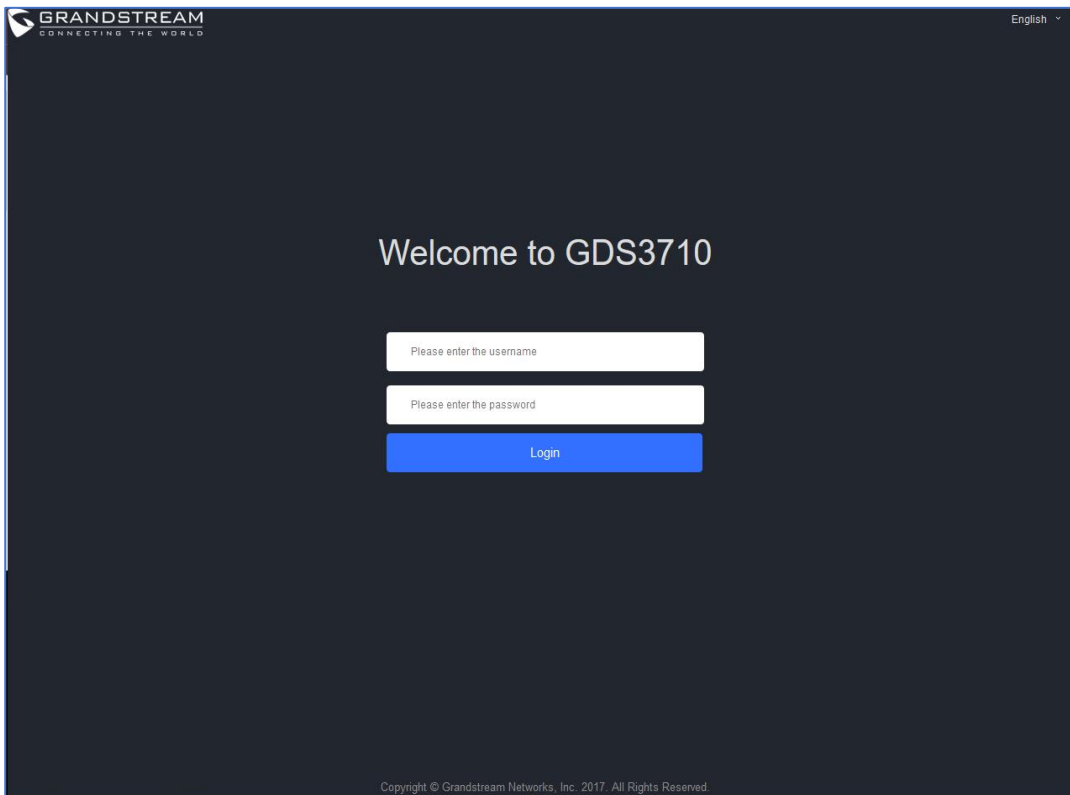
Figure 46: MJPEG Authentication Mode

### 1) Challenge+Response MJPEG Authentication Mode:



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

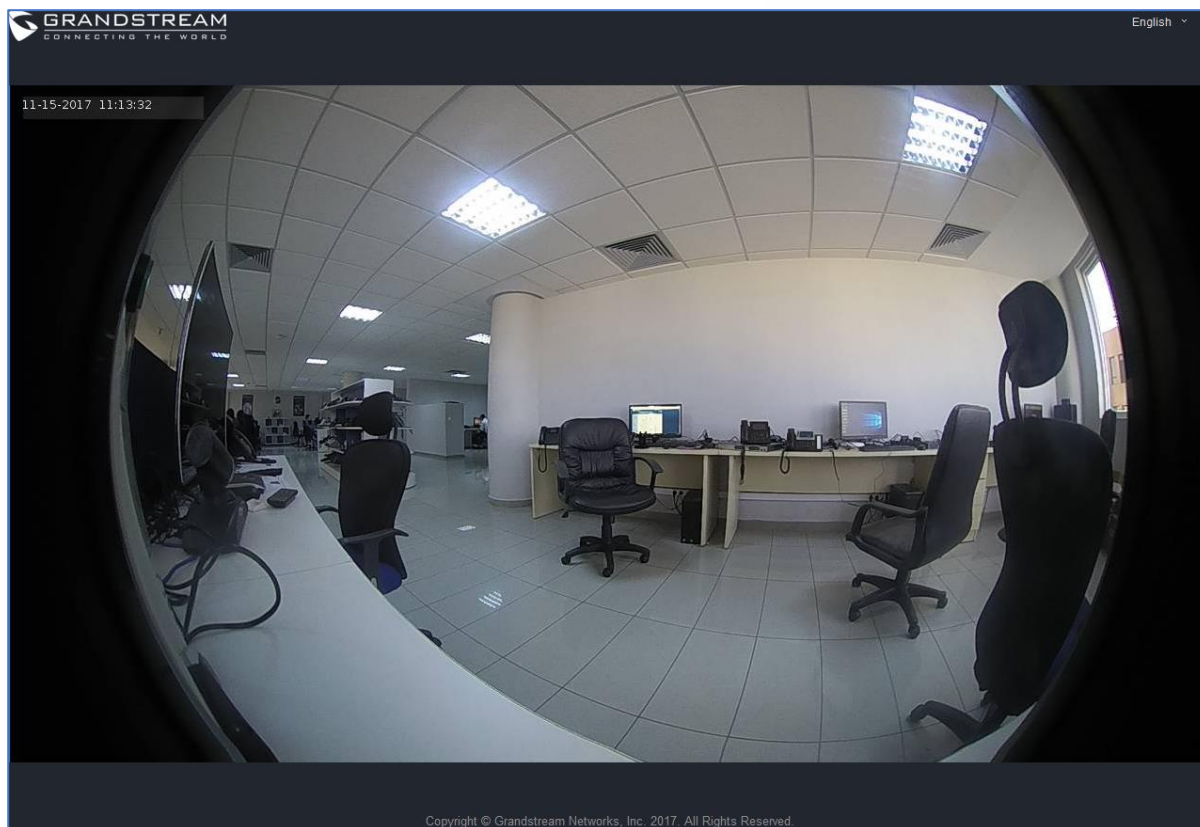
1. In browser type in: **http(s)://IP\_Address\_GDS:Port/jpeg/mjpeg.html**
2. The browser will pop up the window above asking for credentials, user needs to enter admin credential.



**Figure 47 : MJPEG view admin credential**



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



**Figure 48 : MJPEG live view using secured MJPEG Authentication Mode**

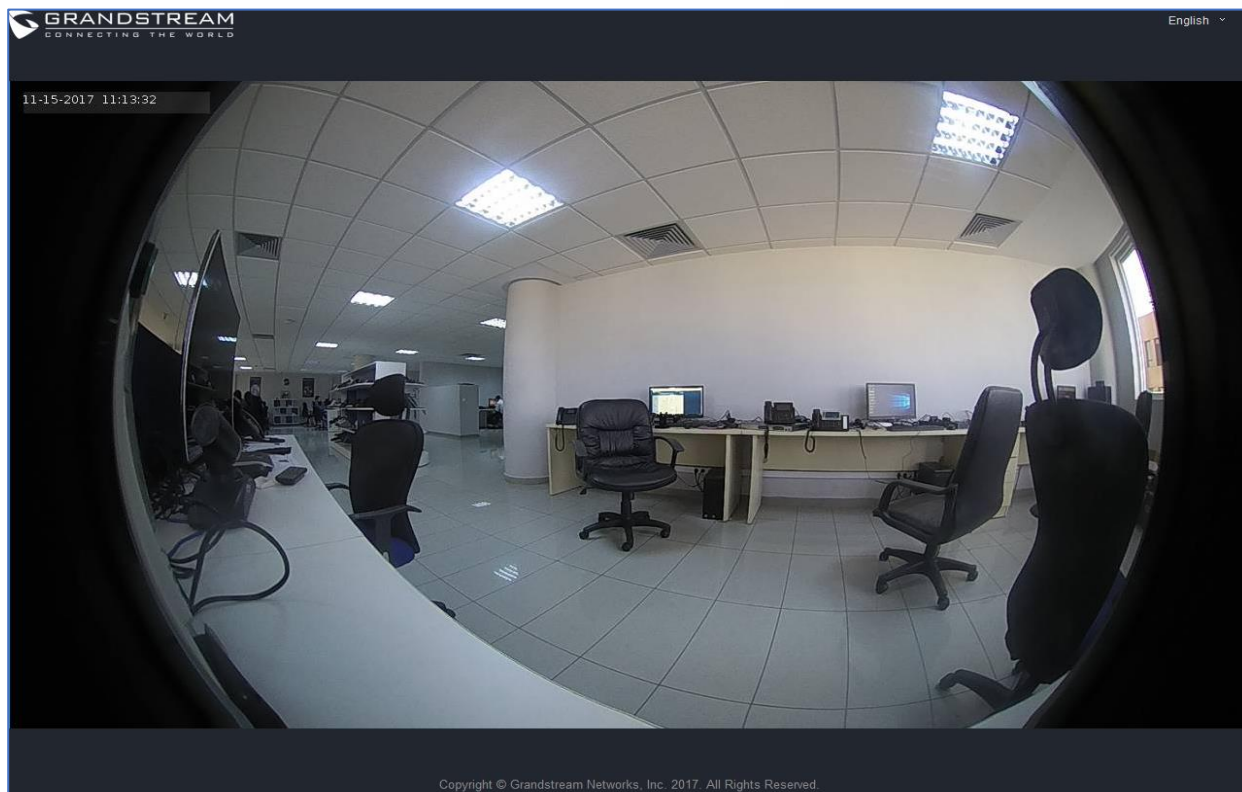
**Note:** This is supported on all browsers without installing any plugin and requires admin user authentication for more security.

## **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 49: 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 **1<sup>st</sup>, 2<sup>nd</sup> and 3<sup>rd</sup>** video stream (**2<sup>nd</sup>** recommended).

## Door System Settings

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

### Basic Settings


GDS3710

- [LiveView](#)
- [Door System Settings](#)
- Basic Settings
- [Keep Door Open](#)
- [Card Management](#)
- [Group](#)
- [Schedule](#)
- [Holiday](#)
- [System Settings](#)
- [Account](#)
- [Phone Settings](#)
- [Video & Audio Settings](#)
- [Alarm Settings](#)
- [Email & FTP Settings](#)
- [Maintenance](#)
- [Status](#)

### Door System Settings

Door Relay Options	Local Relay
Webrelay IP Address	<input type="text"/>
Webrelay Username	<input type="text"/>
Webrelay Password	<input type="password"/>
ALMOUT1 Feature	Alarm Output
ALMOUT1 Status	Normal Open
Delay before Unlock(s)	<input type="text" value="0"/>
Unlock Holding Time(s)	<input type="text" value="5"/>
Minimum Interval of Swiping Card(ms)	<input type="text" value="300"/>
Number of Snapshots when Door Opened	<input type="text" value="4"/>
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input type="checkbox"/> via FTP <input type="checkbox"/> via Email
Call Mode	Virtual Number
Doorbell Call Out Account	Auto
Doorbell Mode	Call Doorbell Number
Door Bell Call Mode	Serial Hunting

Save

Figure 50: Door System Settings Page

**Table 6: Door System Settings**

<b>Door Relay Options</b>	<p>This feature allows customers to integrate GDS37XX with 3rd party web relay to control door open over network, via script or other applications, to meet real application scene and enhance security. User need to input web relay IP address or domain name, as well as authentication information, to make this to work.</p> <p>There are two choices in the pull-down selection: Local Relay and Webrelay.</p> <ul style="list-style-type: none"> <li>• <b>Local Relay:</b> Local Relay is the GDS3710 controlling the relay. The strike is wired into the COM2 or COM1 port of the GDS3710 depending 1 door or 2 door need to be controlled.</li> <li>• <b>Webrelay:</b> When Webrelay is selected, customers need to continue configure the webrelay IP address or domain name, together with credentials like Username and Password. When legal open door event happened, the configured web relay will get the communication from GDS3710, and will operate the strike to open door for the authenticated open door request.</li> </ul> <p><b>Note:</b> In web relay mode, the strike is wired to the web relay controller device.</p> <p>For more details, please refer to the Webrelay documentation from this link: <a href="#">webrelay user manual</a></p>
<b>Webrelay URL ON</b>	<p>When Door relay Option set to Webrelay, then enter the correct URL used by the third party controller so that the GDS3710 send the command to activate the relay.</p> <p>This adds an extra layer of security so when legal open door event happened, the configured web relay will get the communication from GDS3710, and will operate the strike to open door for the authenticated open door request or use that command to operate other industry application.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Now there are two Webrelay URL fields available, with On or Off URL command allowed or other usage URL command allowed. Also allow Username and Password configured if the 3rdparty Webrelay requiring this security feature.</li> <li>• If some 3rdpartyWebrelay only support one URL command, then just leave another Off URL blank, or put whatever there as long as it is NOT a URL command.</li> </ul>



<b>Webrelay URL OFF</b>	When Door relay Option set to Webrelay, then enter the correct URL used by the third party controller so that the GDS3710 send the command to disable the relay.
<b>Webrelay Username</b>	Enter the web relay username.
<b>Webrelay Password</b>	Enter the web relay password.
<b>ALMOUT1 Feature</b>	<p>This option allows to choose to use Alarm_Out (COM1) interface for either as alarm out with 3<sup>rd</sup> party device, or to control a second door "Door 2" (the two functions are mutual exclusive).</p> <p>When option "<b>Open Door</b>" is selected, will enable GDS3710 to control the operation of two doors via RFID, local and remote PINs.</p>
<b>ALMOUT1 Status</b>	Select Normal Open or Normal Close depending on the lock used.
<b>Delay before Unlock (s)</b>	Device will open door after specified delay (in seconds) when user issuing the authorization.
<b>Unlock Holding Time (s)</b>	<p>Configures the lock holding time, in seconds (default value is 5 seconds).</p> <p>Device will hold the door unlocked for this specified duration.</p> <p>Range: 1-1800 seconds.</p>
<b>Minimum Interval of Swiping Card (ms)</b>	Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms.
<b>Number of Snapshots when Door Opened</b>	<p>Define number of snapshot to be sent by the GDS ( via FTP or Email)</p> <p>Maximum up to 4 screenshots.</p>
<b>Snapshot when Door Opened</b>	User can choose to email the snapshot when door is opened without sending the snapshots via FTP to the FTP server.
<b>Snapshot when Doorbell Pressed</b>	User can choose to email the snapshot when doorbell pressed without sending the snapshots via FTP to the FTP server.
<b>Call Mode</b>	Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3710 keypad.
<b>Doorbell Call Out Account</b>	This option sets the account to be used to make call upon the doorbell trigger. If set to Auto, the GDS will use the first available account.
<b>Doorbell Mode</b>	Configures the action to be taken when the doorbell is pressed, three options are available:



	<ul style="list-style-type: none"> <li>• <b>Call Doorbell Number:</b> when Doorbell is pressed, a call will be made to the “<b>Number Called When Door Bell Pressed</b>”</li> <li>• <b>Control Doorbell Output (Digital Output 1):</b> when Door Bell is pressed electronic lock for Output 1 is opened.</li> <li>• <b>Both of Above:</b> When selected, both Call Doorbell Number and Control Doorbell Output options are enabled.</li> </ul>
<b>Door Bell Call Mode</b>	<p>Select the ring strategy for the Numbers Called when pressing the Door Bell button to be either <b>Serial</b> or <b>Parallel</b>:</p> <ul style="list-style-type: none"> <li>• <b>Serial Hunting:</b> the configured extensions and/or IP addresses will ring one after one by order.</li> <li>• <b>Parallel Hunting:</b> The configured extensions and/or IP addresses will ring simultaneously (up to 4 simultaneous SIP calls).</li> </ul>
<b>Number Called When Door Bell Pressed</b>	<p>Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed:</p> <ul style="list-style-type: none"> <li>• <b>SIP Server mode:</b> <ul style="list-style-type: none"> <li>- 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 <b>Serial Hunting Mode</b> (GDS will ring each extension by default 15 seconds, this can be changed on the Ring Timeout) or ring them simultaneously in <b>Parallel Hunting Mode</b>.</li> <li>- 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.</li> <li>- If all phones are GXP21XX, the phone will stream the video frame by frame and users can open door either by pressing <b>Remote_PIN#</b> or by pressing Open Door button if already configured.</li> <li>- 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).</li> </ul> </li> <li>• <b>Peering mode:</b></li> </ul>



	<ul style="list-style-type: none"> <li>- 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 <b>Serial or Parallel Mode</b> according to Doorbell Call Mode strategy.</li> <li>- 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).</li> <li>- GXP21XX phones receive the GDS3710 video using JPEG streaming this means that it will receive video if early media is enabled or disabled.</li> </ul> <p><b>Note:</b> This field supports a Maximum of 256 characters.</p>
<b>Maximum Number of Dialed Digits</b>	Configure the maximum digits allowed to dial in the keypad. Once the configured condition satisfied, the device will send out the digit to call automatically without pressing #. Disabled if set to 0.
<b>No Key Input Timeout(s)</b>	Defines the timeout (in seconds) for no key entry. If no key is pressed after the timeout, the digits will be sent out without pressing #. The default value is 4 seconds. The valid range is from 1 to 15.
<b>Press Doorbell Schedule</b>	<p>Configure a schedule for the Doorbell button, once configured, the doorbell will turn ON/OFF based on configured schedule.</p> <p>Default setting is "All Day".</p>
<b>Remote PIN to Open the Door</b>	<p>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.</p> <p><b>Note:</b> For enhanced security, when the call is initiated from GDS then only the numbers existing in "White List" will be able to use DTMF PIN to open door remotely.</p>



<p><b>Local PIN Type</b></p>	<p>Three options are available: Private Card PIN, Unified PIN or Card and Private PIN.</p> <ul style="list-style-type: none"> <li>• <b>Private PIN:</b> 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 [<b>*Virtual Number*Private PIN#</b>].</li> </ul> <p><u>Notes:</u></p> <ol style="list-style-type: none"> <li>1. When Local PIN type is set to <b>private PIN</b>, users can also open the door by swiping their cards.</li> <li>2. If “Disable Keypad SIP Number Dialing” is checked, users will be able to open door using private PIN with following sequence [<b>Private PIN#</b>].</li> </ol> <p><b>Note:</b> Door can still be opened by <b>Card</b> and with the sequence [<b>*Virtual Number*Private PIN#</b>].</p> <p>For more details and conditions, refer to <i>[Disable Keypad SIP Number Dialing]</i>.</p> <ul style="list-style-type: none"> <li>• <b>Unified PIN:</b> 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 [<b>*Local PIN to Open the Door#</b>].</li> <li>• <b>Card &amp; Private PIN:</b> Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence [<b>Swipe the card + * Private PIN#</b>]</li> </ul>
<p><b>Local PIN to Open the Door</b></p>	<p>Configures PIN stored in GDS3710, input locally this PIN on the GDS3710 keypad will unlock the door.</p> <p>This feature needs <b>Private PIN</b>, means every member has a private PIN, the GDS will record who unlocked the door every time.</p> <p>Users need to enter the following sequence from the GDS3710 to open the door [<b>*Virtual Number*Private PIN#</b>].</p> <p><b>Note:</b> When local PIN type is set to private card PIN, users can also open the door by swiping their cards.</p>



<b>Local PIN to Open Door Schedule</b>	Configure a schedule for the Local PIN to open the door. Once configured, the door opening ability using local PIN with turn ON/OFF based on configured schedule. Default setting is “All Day”.
<b>Enable DTMF Open Door</b>	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.
<b>Enable Guest PIN</b>	Enables password entry for guests.
<b>Guest PIN</b>	Configures the password that will be used by guests.
<b>Guest PIN Start Time</b>	Selects the start time when the Guest PIN start to take effect.
<b>Guest PIN End Time</b>	Selects the end time when the Guest PIN will stop working.
<b>Disable Auto Answer</b>	If checked, GDS3710 will not answer incoming calls automatically, users can press any key to answer the call. Default setting in unchecked.
<b>Enable Doorbell Button to Hang up Call</b>	If checked, Users can hang up an active call when pressing the doorbell button. Enabled by default.
<b>Disable Keypad (except the Doorbell Button)</b>	When checked the Keypad will be disabled, only Door Bell button can be pressed.
<b>Enable On Hook After Remote Door Opened</b>	When checked calls will be disconnected automatically 5 seconds after the remote open door event.
<b>Enable HTTP API Remote Open Door</b>	<p>Enabling this option allows to use HTTP API command to open the door remotely.</p> <p><b>Important note:</b> 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.</p>
<b>Disable Keypad SIP Number Dialing</b>	<p>When Keypad SIP number Dialing disabled, device will interpret each digit entry as private-password open door request after pressing #.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• “Local PIN Type” should choose “Private PIN”.</li> <li>• Dial keypad to make SIP call will NOT work (except for doorbell button call).</li> <li>• Private PIN must be <b>UNIQUE</b> among users, otherwise the door will still open but log will NOT tell who opened the door due to duplicated PIN and whoever user last matched in the database with the Private PIN will be shown in the log.</li> </ul>





<b>Enable Card Issuing Mode</b>	Enables RFID card issuing/program into the GDS3710. When selected sweeping an RFID card into the GDS3710 will add card information into. [Card Management]
<b>Card issuing State Expire Time(m)</b>	Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes).
<b>Enable Key Blue Light</b>	When checked, the blue light will be activated when pressing the GDS3710 Keys.
<b>Enable Background Light</b>	When checked, the background light will turn on once clicking the GDS3710 Keys.
<b>Enable Doorbell Blue Light</b>	When enabled, Doorbell 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 Doorbell LED.
<b>Enable Keypad Blue Light</b>	When enabled, Keypad LED (except for Doorbell 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.
<b>Central Mode</b>	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.
<b>Key Tone Type</b>	Configures the key tones for the GDS3710. <ul style="list-style-type: none"> <li>• <b>Default:</b> Beeps will be played when pressing the GDS3710 keys.</li> <li>• <b>DTMF:</b> Tones will be played when pressing the GDS3710 keys.</li> <li>• <b>Mute:</b> No sound will be played when pressing keys.</li> </ul>
<b>Enable Wiegand Input</b>	This option needs to be enabled when GDS is connected to the wiegand. output device (RFID card reader for example)
<b>Wiegand Output</b>	This option is to be enabled when the GDS is the wiegand output device. (example: input device is a door controller)

**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 large number of users (limit is 2000), it's difficult for the GDS3710 to manage all these users, so a separate PC or Server should be involved for such kind of management and monitoring.

In environments with large number of users (limit is 2000), the GDS3710, another possibility would be to set one unified Local PIN for opening the door for all the users.

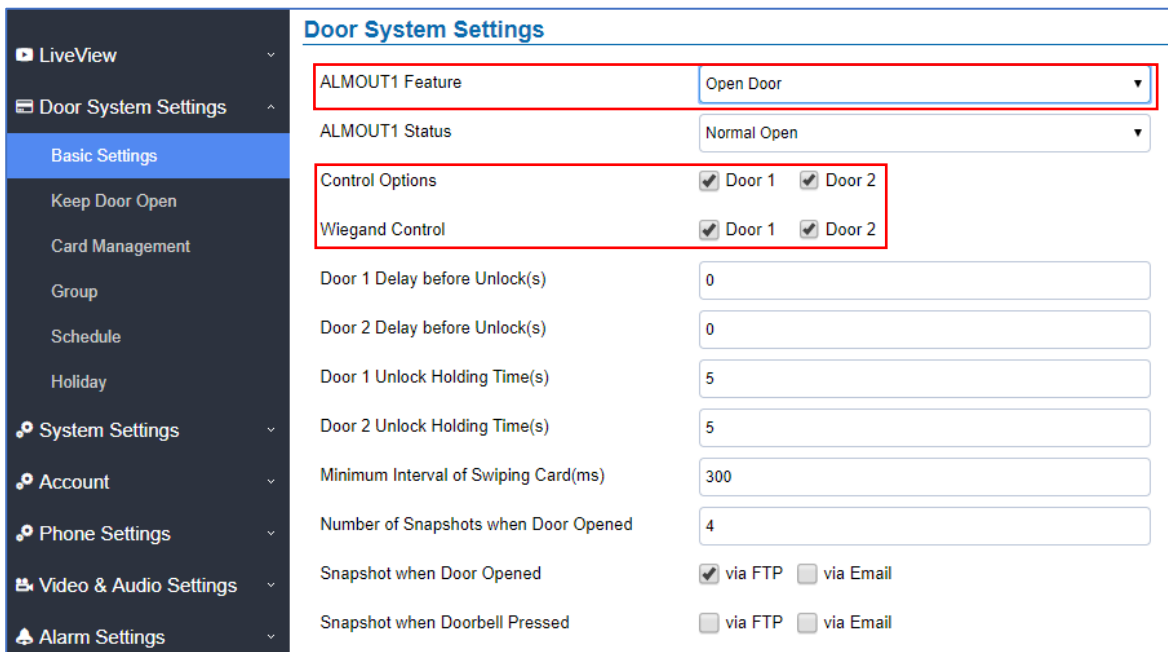


## Using Alarm Out (COM 1) to Control a Second Door

Starting from firmware 1.0.5.2, user can now set Alarm\_Out (COM1) interface to control a second Door, in addition to the existing Locker/COM2 interface (controlling Door1).

This feature allows GDS3710 to control the operation of two doors via RFID, local and remote PINs.

For example, a 3<sup>rd</sup> party Wiegand Input device or GDS3710 can be installed at Door2 with related cable wired into the control GDS3710 installed at Door1. The Door1 and Door2 can be configured to be open by programmed RFID cards, PINs either separately or both.



The screenshot shows the 'Door System Settings' page. On the left is a sidebar menu with options: LiveView, Door System Settings (expanded), Basic Settings, Keep Door Open, Card Management, Group, Schedule, Holiday, System Settings, Account, Phone Settings, Video & Audio Settings, and Alarm Settings. The main content area is titled 'Door System Settings' and contains several configuration fields. A red box highlights the 'ALMOUT1 Feature' dropdown menu, which is set to 'Open Door'. Another red box highlights the 'Control Options' and 'Wiegand Control' sections, both of which have checkboxes for 'Door 1' and 'Door 2', all of which are checked. Below these are input fields for delays and holding times for both doors, and checkboxes for snapshot notifications via FTP or Email.

Figure 51: Alarm\_Out1 Feature

- **Interface for Door Control (which Door can be OPEN):**

If Alarm\_Out (COM1) interface is set to control Door 2 opening, “ALMOUT1 Status” can be configured by choosing “Normal Open” or “Normal Close” based on the strike used.

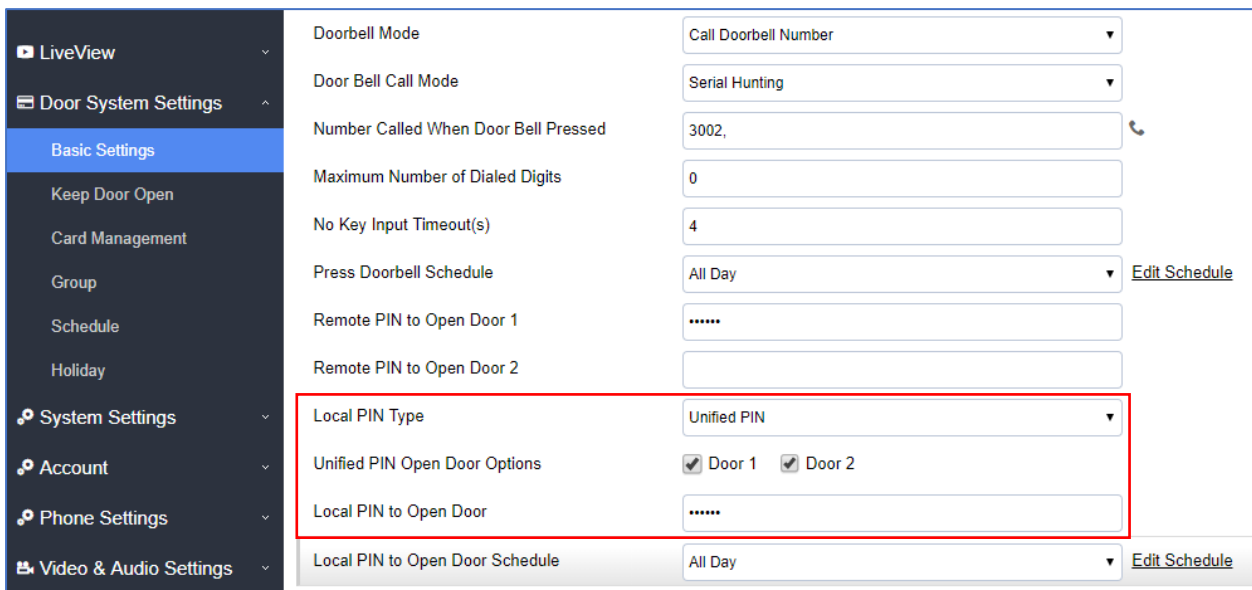
Unlike default COM2 which is designed for strike control and having three connecting sockets, the COM1 only has two connecting sockets. Therefore correct lock mode has to be configured to make the strike working as expected.

For above example, the GDS3710 is configured to control Door1 (wiring to COM2 interface); the 3<sup>rd</sup> party Wiegand Input is set to control Door2 (wiring to COM1 interface).

In case of a power loss then the DOOR STATUS when power is off will be depending on the following situations:



- COM2 has three wiring PINs, corresponding to NO or NC accordingly. Therefore when connecting NC2 and COM2 (Fail Safe) then strike will open when power is lost and when using a NO2 strike (connecting COM2 and NO2) then door is “locked” when power is lost (Fail Secure).
- COM1 (ALMOUT1) has only two PIN, and NO ONLY. If the connected strike/lock is a NO strike, this means ALMOUT1 Status should be set to “Normal Open” then door will be closed when power is lost, while if the strike connected is NC strike, and ALMOUT1 Status is set to “Normal Close” then door will be open when power is lost.
- **Universal PIN for Operation of Doors:**



LiveView	Doorbell Mode	Call Doorbell Number
Door System Settings	Door Bell Call Mode	Serial Hunting
Basic Settings	Number Called When Door Bell Pressed	3002,
Keep Door Open	Maximum Number of Dialed Digits	0
Card Management	No Key Input Timeout(s)	4
Group	Press Doorbell Schedule	All Day <a href="#">Edit Schedule</a>
Schedule	Remote PIN to Open Door 1	.....
Holiday	Remote PIN to Open Door 2	
System Settings	Local PIN Type	Unified PIN
Account	Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Phone Settings	Local PIN to Open Door	.....
Video & Audio Settings	Local PIN to Open Door Schedule	All Day <a href="#">Edit Schedule</a>

**Figure 52: Universal Local PIN**

If Unified PIN (Universal PIN) is configured to open door, then which door can be controlled by the PIN is configured in the UI once “Unified PIN” selected.

For example, like above screenshot, if this universal PIN is set to open both Door1 and Door2, but due to previous “Control Option” set to open Door1, and “Wiegand Control” set to open Door2, therefore the final result will be the INTERSECT result of both sets with condition qualified.

- **Remote PIN to Operation of Doors:**

For remote PIN to open door, the PIN can be configured in example down below.

The PIN can be different for Door1 and Door2 and has to be configured correctly in related IP Phone which will be used to operate “One Key Open Door”.

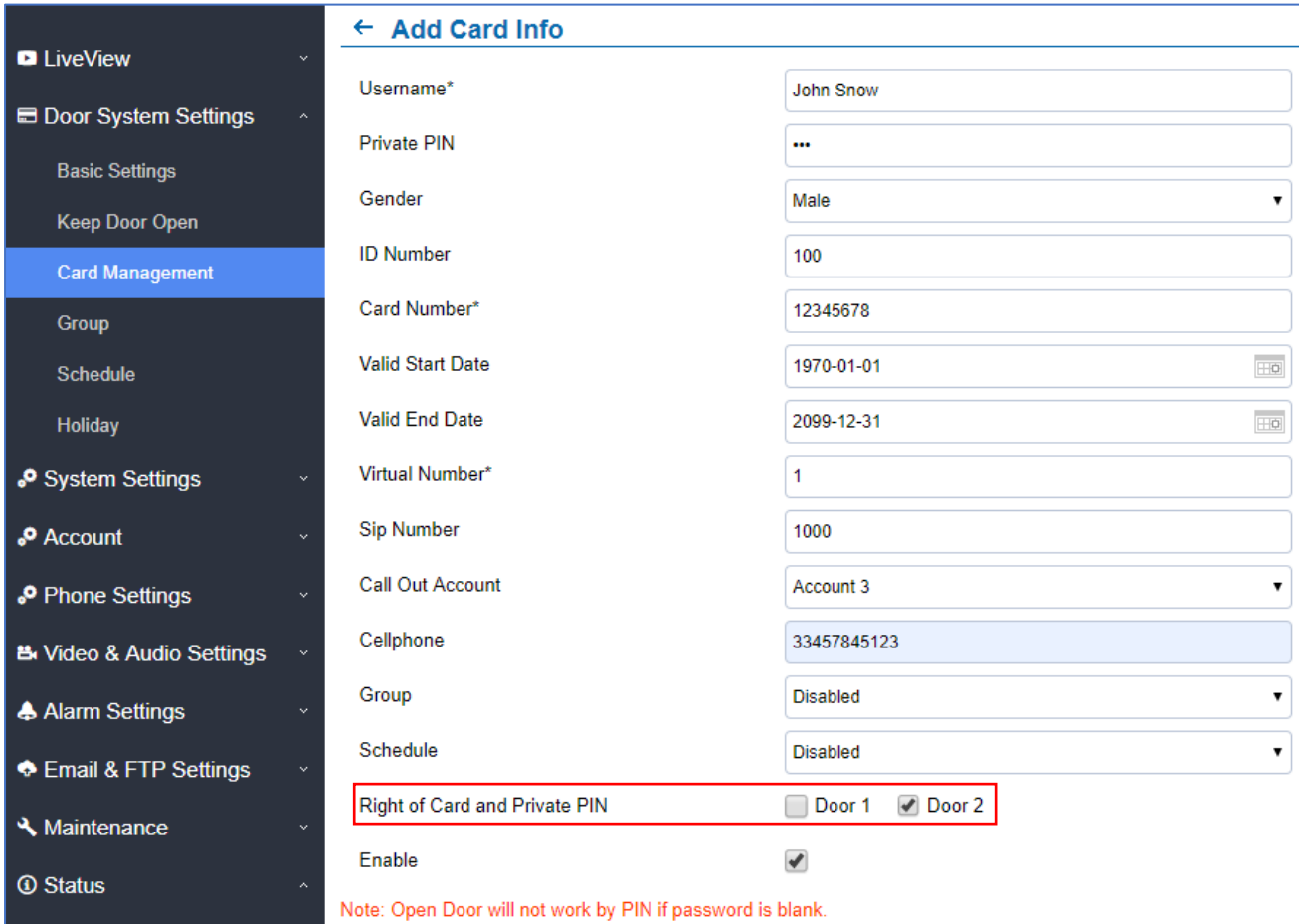
If BOTH doors need to be opened at the same time, then both Door1 and Door2 has to be configured with exactly SAME password or PIN as DTMF open door.

**Note:** For enhanced security, When call is initiated from GDS then only the numbers existing in “Number Called When Door Bell Pressed”, “Account White Lists” or “Card Management” will be able to use DTMF PIN to open door remotely.

<ul style="list-style-type: none"> <li>LiveView</li> <li>Door System Settings               <ul style="list-style-type: none"> <li>Basic Settings</li> <li>Keep Door Open</li> <li>Card Management</li> <li>Group</li> <li>Schedule</li> <li>Holiday</li> </ul> </li> <li>System Settings</li> <li>Account</li> <li>Phone Settings</li> <li>Video &amp; Audio Settings</li> <li>Alarm Settings</li> </ul>	Doorbell Mode	Call Doorbell Number
	Door Bell Call Mode	Serial Hunting
	Number Called When Door Bell Pressed	3002
	Maximum Number of Dialed Digits	0
	No Key Input Timeout(s)	4
	Press Doorbell Schedule	All Day <a href="#">Edit Schedule</a>
	Remote PIN to Open Door 1	*****
	Remote PIN to Open Door 2	
	Local PIN Type	Unified PIN
	Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
	Local PIN to Open Door	*****
	Local PIN to Open Door Schedule	All Day <a href="#">Edit Schedule</a>
	Enable DTMF Open Door	<input checked="" type="checkbox"/>

**Figure 53: Remote PIN to Open Door**

- **Private PIN or Card & Private PIN:**



**← Add Card Info**

Username*	John Snow
Private PIN	...
Gender	Male ▼
ID Number	100
Card Number*	12345678
Valid Start Date	1970-01-01
Valid End Date	2099-12-31
Virtual Number*	1
Sip Number	1000
Call Out Account	Account 3 ▼
Cellphone	33457845123
Group	Disabled ▼
Schedule	Disabled ▼
Right of Card and Private PIN	<input type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Enable	<input checked="" type="checkbox"/>

Note: Open Door will not work by PIN if password is blank.

**Figure 54: Right of Card and Private PIN**

If using RFID card or Private PIN to open door, then which door can be opened by the RFID card or Private PIN is configured via “Card Management”, see above screenshot.

### Notes:

For all the settings, the final result of which door can be opened is the **LOGIC INTERSECT OPERATOR** of ALL the sets of condition qualified.

Please refer to our Open Door Flow chart for better understanding on how to configure and control 2 Doors operation: [http://firmware.grandstream.com/GDS3710\\_opendoors\\_logic.pdf](http://firmware.grandstream.com/GDS3710_opendoors_logic.pdf)



## 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.

There are two modes under this section:

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

### Keep Door Open

Keep Door Open


Immediate Open Door ▼

Interval of Keep Door Open(min)

5

Figure 55: 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.

**Note:** When Alarm OUT 1 is set to Open Door then this option would be available separately for each door.

## 2- Schedule Open Door (Repeated Action)

### Keep Door Open

#### Door 1

Keep Door Open
Schedule Open Door

Schedule Start Time
2019-11-05 12:31:32

Schedule End Time
2019-11-27 00:00:00

Holiday Mode
holiday1
[Edit Holiday](#)

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 0

Sun																								
Mon																								
Tue																								
Wed																								
Thu																								
Fri																								
Sat																								
Holiday																								

#### Door 2

Keep Door Open
Disabled

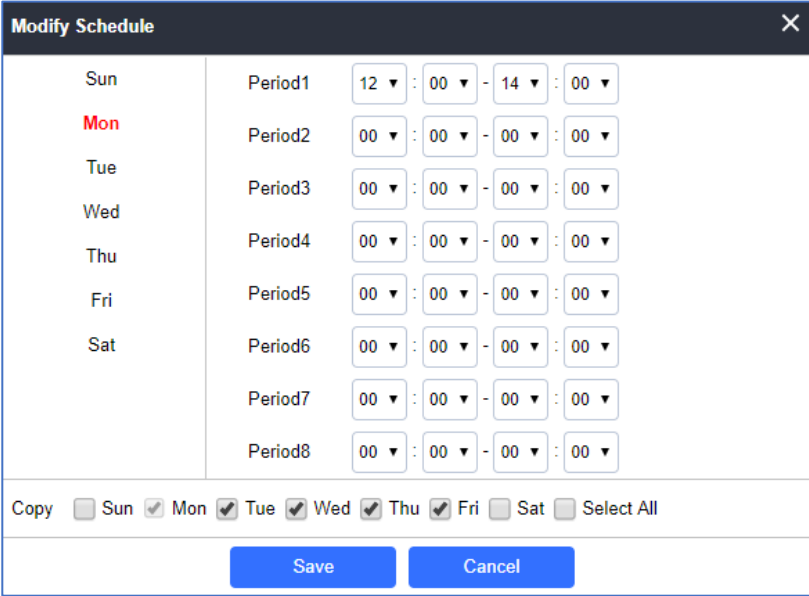
Emergency PIN to Disable Keep Door Open

Figure 56: Schedule Open Door

Table 8: Schedule Keep Door Open

<b>Keep Door Open</b>	Select the Keep Door Open mode (Schedule Open Door on this case).
<b>Valid Schedule Start Time</b>	Selects the start time when the door will be opened.
<b>Valid Schedule End Time</b>	Selects the end time when the door will be locked.
<b>Holiday Mode</b>	Selects the holiday schedule to be included into the Keep Door Open schedule (Supported for Door 1 and Door 2).

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



**Modify Schedule**

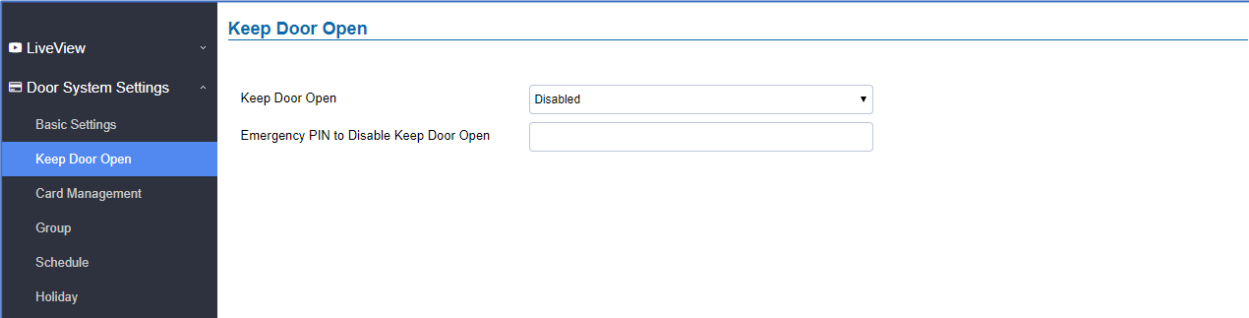
Day	Period1	Period2	Period3	Period4	Period5	Period6	Period7	Period8
Sun	12 : 00 - 14 : 00							
<b>Mon</b>		00 : 00 - 00 : 00						
Tue			00 : 00 - 00 : 00					
Wed				00 : 00 - 00 : 00				
Thu					00 : 00 - 00 : 00			
Fri						00 : 00 - 00 : 00		
Sat							00 : 00 - 00 : 00	

Copy ☐ Sun ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☐ Sat ☐ Select All

**Save** **Cancel**

**Figure 57: Edit Schedule**

## Emergency PIN



**Keep Door Open**

Keep Door Open Disabled

Emergency PIN to Disable Keep Door Open

**Figure 58: Keep Door Open – Emergency PIN**

When Keep Door Open option is set to “Disabled”, user is offered the possibility to force closing the door from the device keypad by dialing the Emergency PIN set to be used.

### Example:

1. Fill in the password in Emergency PIN to Disable Keep Door Open, in our example: 2018
2. Open the door using either Immediate/Scheduled Keep Door open
3. enter the following Emergency Password sequence: \*2018#
4. After entering the sequence \*Emergency PIN#, the GDS will close the door, and when entering the web GUI, the Keep Door Open section is switched automatically to "Disabled" Option.

**Note:** When ALMOUT1 Feature is set to Open Door then separated Keep Door Open features would be available on this page for each door.



## Card Management

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













Card Management													
 Add User		 Reload Data		 Delete Data		Username* <input type="text"/>				 Import Data		 Export Data	
No.	Username*	Card Number*	Virtual Number*	Sip Number	Account	Cellphone	ID Number	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	John	33656478	1	1000 	Auto	33457845123	412	Male	Disabled	Disabled	1970-01-01	2099-12-31	
2	Robert	124578	2	2000 	Account 1	212682522210	413	Male	Disabled	Disabled	1970-01-01	2099-12-31	

Figure 59: 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.
- Users can export and upload .CSV and .GS files:
- “.gs” format is encrypted database file, it can NOT be edited and the password or PIN inside also can NOT be viewed.
- “.csv” format is NOT encrypted therefore all the content are viewable and editable.
- System Administrator should be VERY careful when export database in such file format, as convenience is provided in the cost of security. It is STRONGLY suggested system administrator to set PASSWORD to Safe Guard the exported CSV format database file when edit or revise the file using Excel.

## Add Users Manually

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



LiveView

Door System Settings

Basic Settings

Keep Door Open

Card Management

Group

Schedule

Holiday

System Settings

Account

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status

← Modify Card Info

Previous Record

1

Next Record

Username\*

John

Private PIN

\*\*\*\*\*

Gender

Male

ID Number

412

Card Number\*

33656478

Valid Start Date

1970-01-01

Valid End Date

2099-12-31

Virtual Number\*

1

Sip Number

1000

Call Out Account

Auto

Cellphone

33457845123

Group

Disabled

Schedule

Disabled

Right of Card and Private PIN

☒ Door 1
 ☐ Door 2

Enable

☒

Note: Open Door will not work by PIN if password is blank.

**Figure 60: Card Info**

**Table 9: Card Info**

<b>Username</b>	Configures the username to identify the user.
<b>Private PIN</b>	Specifies a PIN to unlock the door for this particular user.
<b>Gender</b>	Selects a gender, either Male or Female.
<b>ID Number</b>	Enters an ID number (This number is set by the admin to identify each user uniquely).
<b>Card Number</b>	Enters the RFID Card number (this is the number written on the RFID card. When “card issuing mode” is enabled, this field will be added automatically. Maximum number that can be entered is 2147483647.
<b>Valid Start Date</b>	Configures the start date of validity of the RFID card.
<b>Valid End Date</b>	Configures the End date of validity of the RFID card.
<b>Virtual Number</b>	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.
<b>SIP Number</b>	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.

	<b>Note:</b> The SIP Number can be configured with an extension/phone number or IP address. Example: 192.168.5.124
<b>Call Out Account</b>	Select the Account from which the GDS3710 will call the User SIP Number when dialing from the keypad. Default is Auto.
<b>Cellphone</b>	Configures cellphone of the user.
<b>Group</b>	Specifies to which group the user will be added.
<b>Schedule</b>	Specifies the schedule that will be assigned to the user.
<b>Right of Card and Private PIN</b>	Select the doors that can be accessed by user.
<b>Enable</b>	When checked, the user's RFID and Private PIN will be active for door opening. If unchecked, the Private PIN nor RFID card swipe won't take effect.


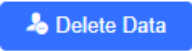





**Note:** - Group overrides Schedule.

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

### 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  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

 to create new groups or  to edit existing groups or  to delete the group.

**Note:** Users can create up to 50 groups.



Add Group

Group Name

Schedule

Disabled

Save

Cancel

Figure 61: Add Group

Table 10: Add Group

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



The following screenshots display the list of the created groups.

Group				
+ Add				
No.	Group Name	Schedule	Edit	Delete
1	Support	schedule1		
2	Sales	schedule2		
3	Documentation	schedule3		

Figure 62: 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.

Modify Schedule

✕

Schedule Name

Holiday Mode

Disabled

▼

Sun	Period1	08	:	00	--	17	:	00
Mon	Period2	00	:	00	--	00	:	00
Tue	Period3	00	:	00	--	00	:	00
Wed	Period4	00	:	00	--	00	:	00
Thu	Period5	00	:	00	--	00	:	00
Fri	Period6	00	:	00	--	00	:	00
Sat	Period7	00	:	00	--	00	:	00
Holiday	Period8	00	:	00	--	00	:	00

Copy

☒ Sun
 ☐ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu
 ☐ Fri
 ☐ Sat
 ☐ Holiday
 ☐ Select All

Save

Cancel

**Figure 63: 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.

Schedule Name

Duration1

- 

+

◀◀

◀

Sep

2017

▶

▶▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

Today

OK

Save

Cancel

**Figure 64: 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.

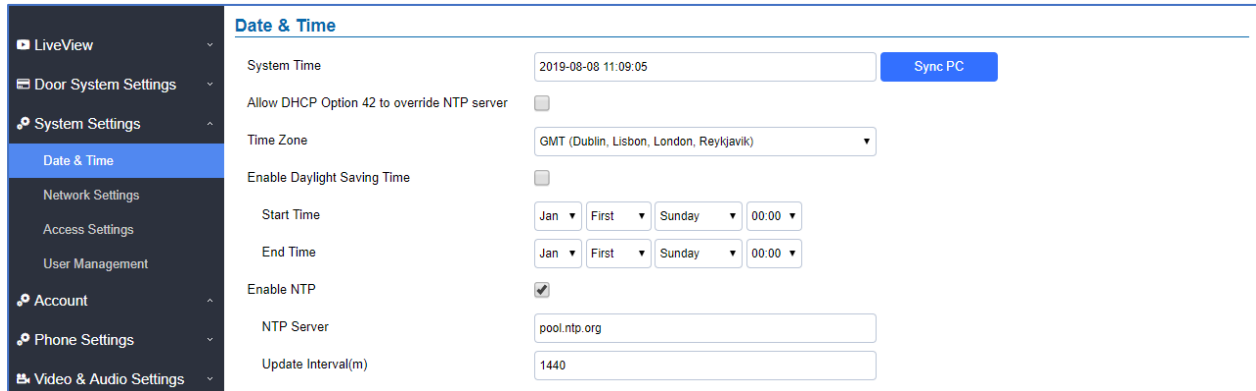


Figure 65: Date & Time Page

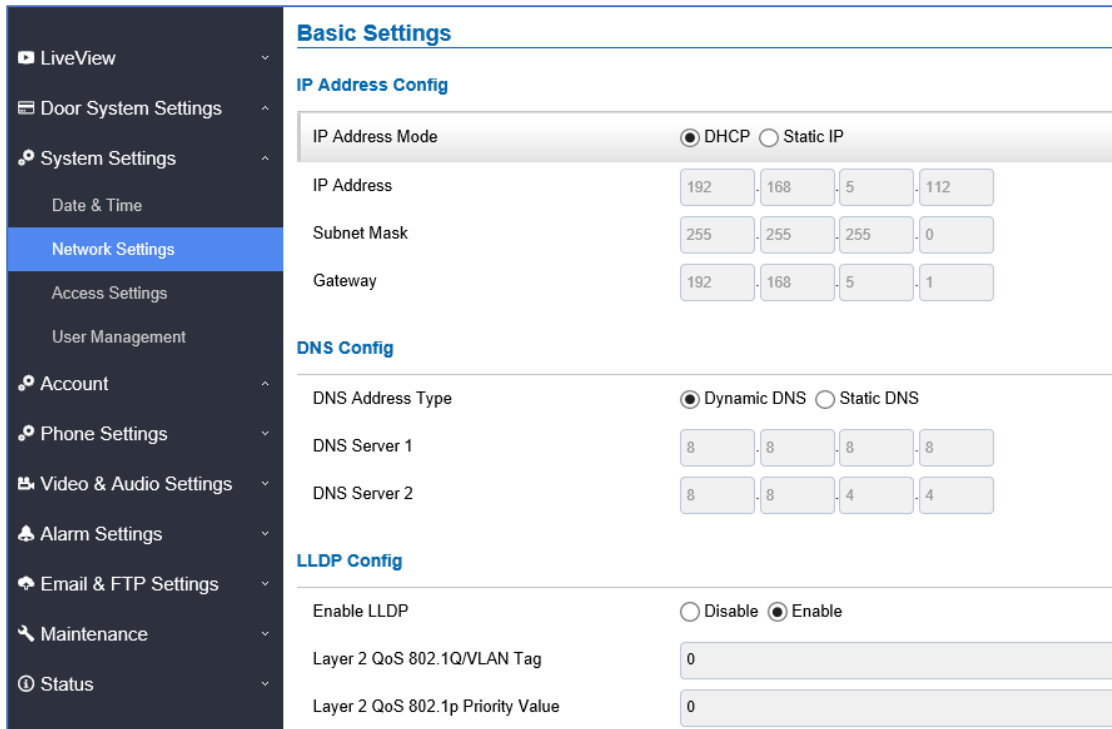
Table 11: Date & Time

<b>System Time</b>	Displays the current system time.
<b>Allow DHCP Option 42 to override NTP server</b>	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it's set up on the LAN. The default setting is "Yes".
<b>Sync PC</b>	Clicks to synchronize current time with the computer.
<b>Time Zone</b>	Selects from drop down menu the preferred time zone.
<b>Enable Daylight Saving Time</b>	Enables Daylight Saving Time.
<b>Start time</b>	Selects the Start time of DST.
<b>End Time</b>	Selects DST end time.
<b>Enable NTP</b>	Enables NTP to synchronize device time.
<b>NTP Server</b>	Configures the domain name of NTP server.
<b>Update Interval</b>	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 66: Basic Settings Page**

**Table 12: Basic Settings**

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

## OpenVPN® Settings

This page allows users to configure OpenVPN settings.

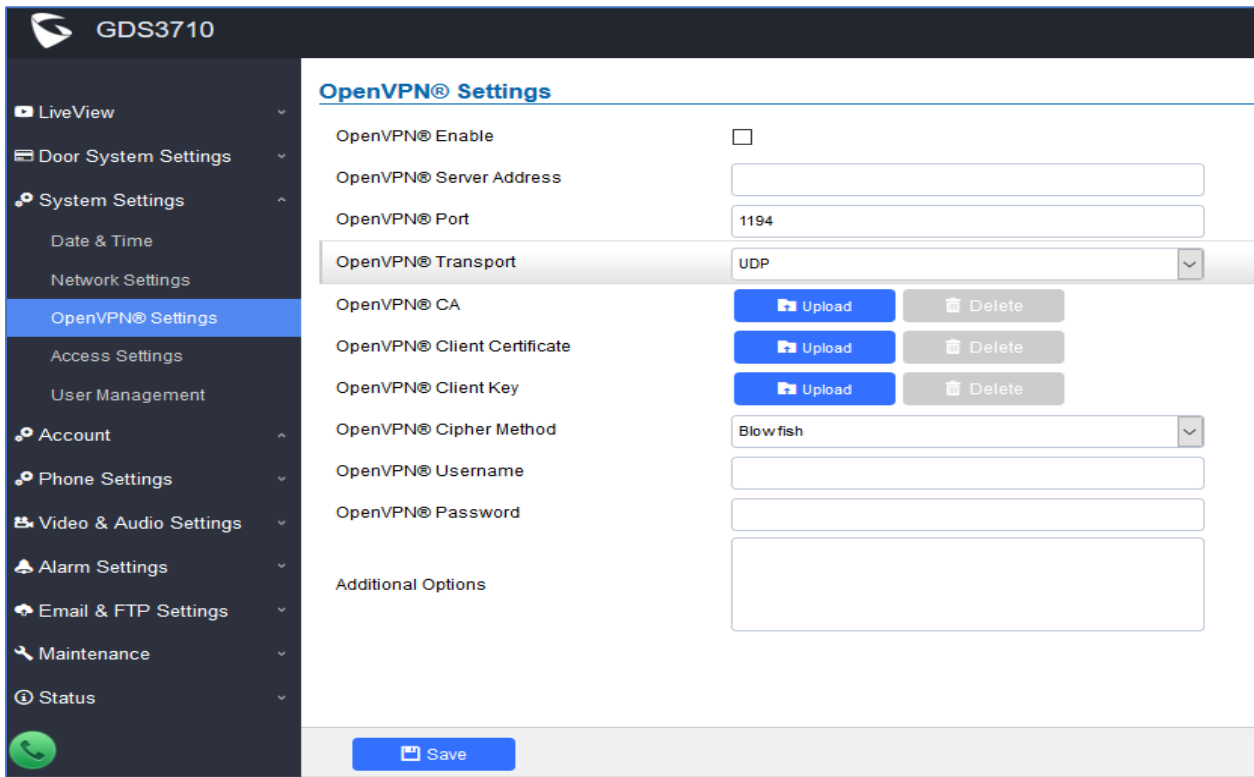


Figure 67: OpenVPN Settings page






<b>Enable OpenVPN®</b>	<p>Enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server.</p> <p><b>Note:</b> To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key. Additionally, the user must also set the SIP account to use "VPN" for the "NAT Traversal" (under Account → Network Settings).</p>
<b>OpenVPN® Server Address</b>	Defines the URL/IP address for the OpenVPN® server.
<b>OpenVPN® Port</b>	Defines the network port for the OpenVPN® server. The default setting is <b>1194</b> .
<b>OpenVPN® Transport</b>	<p>Determines network protocol used for OpenVPN® (UDP or TCP).</p> <p>The default setting is <b>TCP</b>.</p>
<b>OpenVPN® CA</b>	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Client Certificate</b>	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Client Key</b>	OpenVPN® Client key (*.key) required by OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Cipher Method</b>	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Supported methods are: Blowfish, AES-128, AES-256 and Triple-DES.
<b>OpenVPN® Username</b>	Configures the OpenVPN® authentication username (optional).
<b>OpenVPN® Password</b>	Configures the OpenVPN® authentication password (optional).
<b>Additional Options</b>	<p>Additional options to be appended to the OpenVPN® config file, separated by semicolons. For example, <i>comp-lzo no; auth SHA256</i></p> <p><b>Note:</b> Please use this option with caution. Make sure that the options are recognizable by OpenVPN® and do not unnecessarily override the other configurations above.</p>

## Access Settings

This page configures the GDS3710 access control parameters.




GDS3710

- LiveView ▼
- Door System Settings ▲
- System Settings ▲
  - Date & Time
  - Network Settings
  - OpenVPN® Settings
  - Access Settings
  - User Management
- Account ▼
- Phone Settings ▼
- Video & Audio Settings ▼
- Alarm Settings ▼
- Email & FTP Settings ▼
- Maintenance ▲
- Status ▼

### Access Settings

Web Access Mode	<input style="width: 90%;" type="text" value="HTTPS"/>
Web Access Port	<input style="width: 90%;" type="text" value="443"/>
MJPEG Authentication Mode	<input style="width: 90%;" type="text" value="Challenge+Response"/>
RTSP Port	<input style="width: 90%;" type="text" value="554"/>
User Login Timeout(min)	<input style="width: 90%;" type="text" value="5"/>
Maximum Number of Login Attempts	<input style="width: 90%;" type="text" value="5"/>
Locking Time of Login Error (m)	<input style="width: 90%;" type="text" value="5"/>
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>
SSH Port	<input style="width: 90%;" type="text" value="22"/>
GDSManager Configuration Password	<input style="width: 90%;" type="password" value="••••••"/> <span style="float: right; cursor: pointer;">👁</span>
RTSP Password	<input style="width: 90%;" type="password" value="•••••"/> <span style="float: right; cursor: pointer;">👁</span>

Save

**Figure 68: Access Settings Page**

**Table 13: Access Settings**

<b>Web Access Mode</b>	Selects the access mode to the webGUI either HTTP or HTTPS.
<b>Web Access Port</b>	Specifies the TCP port for Web Access, default 443.

<b>MJPEG Authentication Mode</b>	<p>Allows 3<sup>rd</sup> party system integrator or developers to implement related application for users. By default, this feature is disabled and use more secured “Challenge+Response” mode.</p> <p>If enabled, user can send HTTP API with correct credentials to retrieve MJPEG video stream or JPEG snapshot from GDS3710.</p> <p>Notes:</p> <p>1- The MJPEG stream can be retrieved via the following URL HTML based → <b><code>http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html</code></b> Stream → <b><code>http(s)://admin:password@ip:port/jpeg/stream</code></b></p> <p>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 [</p> <p>2- <b>Retrieving Video Streams</b>]</p>
<b>RTSP Port</b>	Specifies RTSP port for media stream, default TCP port 554.
<b>User Login Timeout(min)</b>	If no action is made within this time the GDS3710 will logout from the Web GUI, range is between 3 and 60.
<b>Maximum Number of Login Attempts</b>	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.
<b>Locking Time of Login Error (m)</b>	Specifies how long the GDS3710 is locked before a new login attempt is allowed.
<b>Disable Web Access</b>	<p>Allow or deny the web access to the GDS3710. (HTTP API do not take effect when this option is enabled).</p> <p><b>Note:</b> If both WebUI and SSH are disabled, GDS3710 will get blocked and not be able to be accessed. Only two ways to get it back:</p> <ol style="list-style-type: none"> <li>1. Re-provisioned by ITSP or Service Provider (by adjusting the related parameters)</li> <li>2. Hard Reset (GDS3710 has to be offline and uninstalled to perform this hard reset).</li> </ol>
<b>Enable UPnP Discovery</b>	UPnP (or mDNS) function for local discovery. Default setting is enabled.
<b>Enable Anonymous LiveView</b>	<ol style="list-style-type: none"> <li>1. When enabled, user can display the camera stream from GDS without admin credentials using the following URL scheme: <a href="http(s)://GDS3710_IP:port/videoview.html">http(s)://GDS3710_IP:port/videoview.html</a></li> <li>2. User can also retrieve a real-time snapshot without admin credentials using the following URL:</li> </ol>



	<p><a href="http(s)://IP:port/anonymous/snapshot/view.html">http(s)://IP:port/anonymous/snapshot/view.html</a></p> <p>Or with:</p> <p><a href="https://IP_GDS3710:Port/anonymous/snapshot/view.jpg">https://IP_GDS3710:Port/anonymous/snapshot/view.jpg</a></p> <p>3. To retrieve video stream via RTSP, users can use the following format: <a href="rtsp://IP_GDS3710:Port/X">rtsp://IP_GDS3710:Port/X</a> where X=0,4,8 for 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> streams respectively.</p> <p>4. To retrieve Anonymous MJPEG, user can use following URLs to retrieve the related MJPEG streams:</p> <p><a href="http(s)://IP:Port/anonymous/jpeg/stream=X">http(s)://IP:Port/anonymous/jpeg/stream=X</a> (X=0, 1, 2, or default 3)</p> <p>For example: <a href="https://192.168.1.128/anonymous/jpeg/stream=3">https://192.168.1.128/anonymous/jpeg/stream=3</a></p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• Except default value 3, the stream 0, 1, 2 mapped to the stream 1, 2, 3 in the “Video Setting” page.</li> <li>• Unless using default value 3, all other values require to choose “MJPEG” in the “Preferred Video Codec” in the “Preferred Video Codec”</li> </ul>
<b>Enable SSH</b>	Allows SSH access for remote secured configuration purposes (restart, upgrade, provision...)
<b>Enable PIN/Password Display (HTTPS)</b>	If Enabled, this option allows to view system PIN/Password. Default setting is Disabled.
<b>SSH Port</b>	Specifies the SSH port. Default setting is 22.
<b>GDSManager Configuration Password</b>	<p>User can set in this field a custom admin password instead of using GDS3710 webUI administrator's credentials, and this custom admin password will be the one used when adding the GDS3710 unit to GDSManager database.</p> <p>Default password is the Admin's default random password of the GDS3710.</p>
<b>RTSP Password</b>	<p>This feature enhancement is based on field feedback from customers. Customer request NOT using admin password to view the RTSP video stream via 3<sup>rd</sup> party applications like VLC Player or own development Scripts. Now customer can set the RTSP password and view the livestream via own scripts or 3<sup>rd</sup> party application like VLC Media Player.</p> <p>Default password is the Admin's default random password of the GDS3710.</p>



## 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.

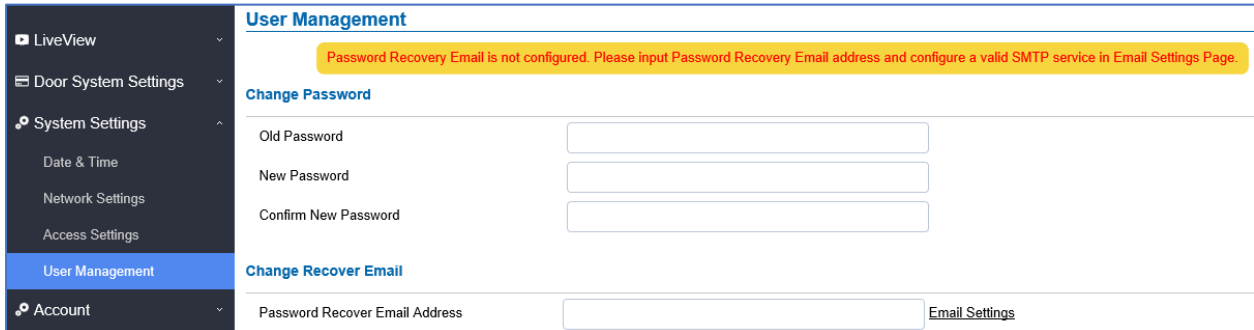


Figure 69: User Management Page

Table 14: User Management

<b>Old Password</b>	Old password must be entered to change new password.
<b>New Password</b>	Fill in the revised new password in this field.
<b>Confirm User Password</b>	Re-enter the new password for verification, must match.
<b>Password Recovery Email Address</b>	<p>This option is <b><u>highly recommended</u></b>, as if the password is lost, you can recover it on the configured Email address.</p> <p><b>Note:</b> Make sure to configure SMTP Email Settings under “<b>Email Settings</b>”</p>

### Note:

When trying to change the password, users need to set the “Password Recovery Email” which should be 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.

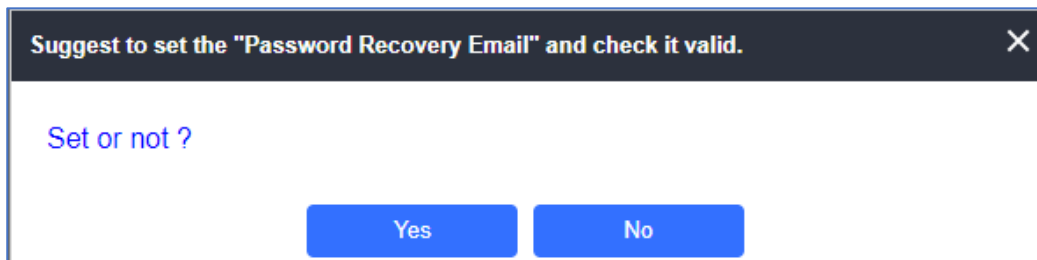


Figure 70: Password Recovery Email

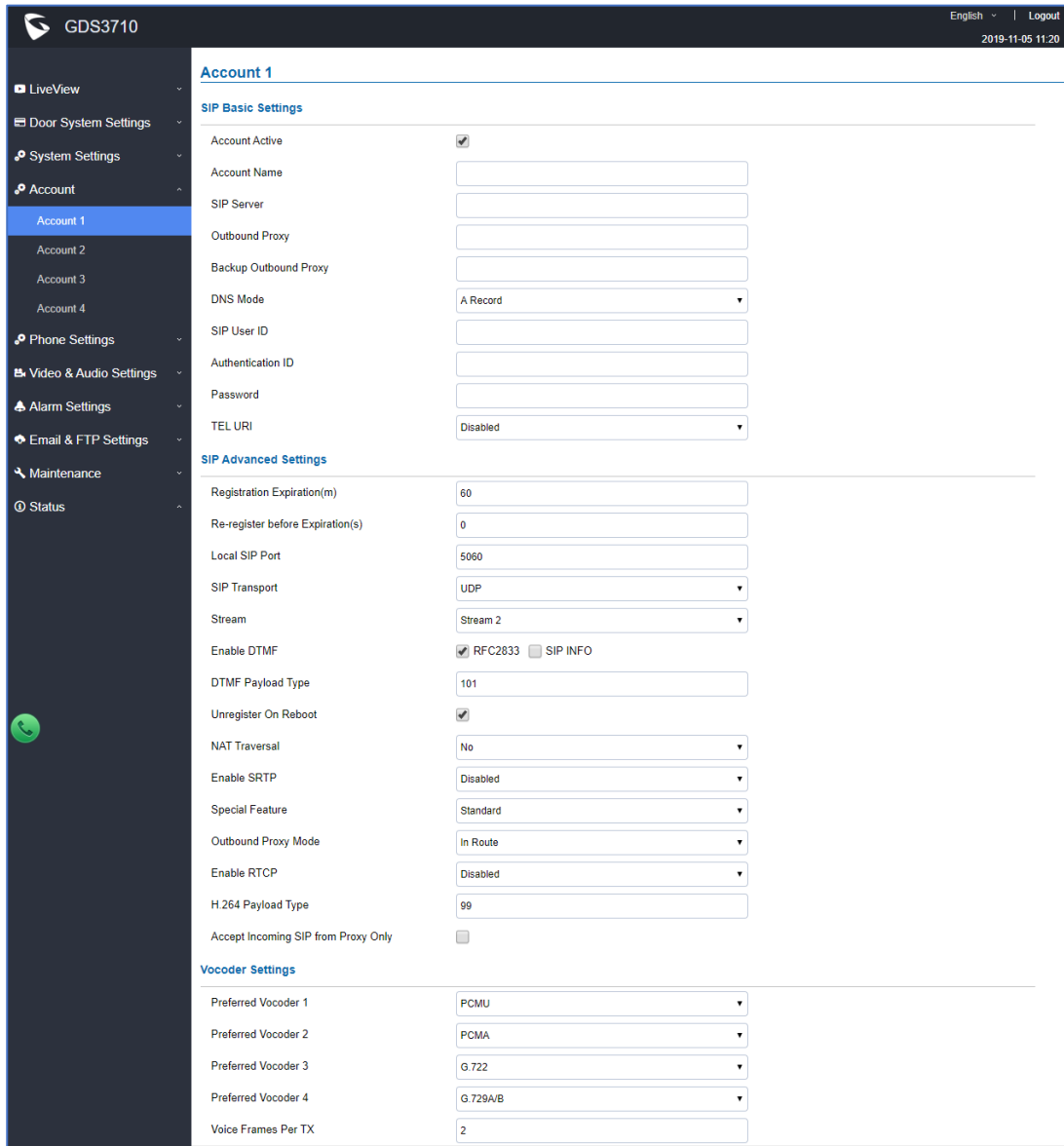
## Account

Starting from version 1.0.5.6, the GDS3710 supports for 4 SIP accounts and 4 lines, this section covers the configuration of basic and advanced sip settings for each account.



## Account 1 - 4

This page allows the administrator to configure the SIP account basic and advanced settings for each SIP account:



**Figure 71: SIP Account Settings Page**

**Table 15: SIP Account Basic & Advanced Settings**

SIP Basic Settings	
<b>Account Active</b>	This field indicates whether the account is active. Default setting is “Yes”.
<b>SIP Server</b>	Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.



<b>Outbound Proxy</b>	Configures the IP address or the domain name of the outbound proxy, media gateway, or session border controller. It's used by the GDS for firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and only an outbound proxy can provide a solution.
<b>Backup Outbound Proxy</b>	Configures the backup outbound proxy to be used when the "Outbound Proxy" registration fails. By default, this field is left empty.
<b>DNS Mode</b>	Configure which DNS mode will be used to translate the SIP Server FQDN (Default value is <b>A Record</b> ): <ul style="list-style-type: none"> <li>• <b>A Record.</b></li> <li>• <b>SRV.</b></li> <li>• <b>NAPTR/SRV.</b></li> </ul>
<b>SIP User ID</b>	Configures the SIP username or telephone number from ITSP. <b>Note:</b> Letters, digits and special characters including @ are supported.
<b>Authenticate ID</b>	Configures the Authenticate ID used by SIP proxy.
<b>Password</b>	Sets the Authenticate password used by SIP proxy. <b>Note:</b> For security reasons, the SIP password is invisible on the web UI.
<b>Display Name</b>	To allow user to input display name to be illustrated in far side SIP device(if having LCD display or similar hardware) so user will know what extension or device connected in SIP calling, to increase the usability.
<b>TEL URI</b>	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".
<b>SIP Advanced Settings</b>	
<b>Registration Expiration (m)</b>	Sets the registration expiration time. Default setting is 60 minutes. Valid range is from 1 to 64800 minutes.
<b>Re-register before Expiration (s)</b>	Specifies the time frequency (in seconds) that the GDS3710 sends re-registration request before the Register Expiration. The default value is 0. Range is from 0-64800 seconds.
<b>Local SIP Port</b>	Sets the local SIP port. Default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4.
<b>SIP Transport</b>	Chooses the SIP transport protocol. UDP, TCP or TCP/TLS. Default setting is UDP.



<b>Stream</b>	<p>Select the Video stream to be used by the GDS3710 when call is made from this SIP Account.</p> <p>Default is Stream 2.</p>
<b>Enable DTMF</b>	<p>Specifies the mechanism to transmit DTMF digits. There are 2 supported modes:</p> <ul style="list-style-type: none"> <li>• <b>RFC2833</b> sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.</li> <li>• <b>SIP INFO</b> uses SIP INFO to carry DTMF. Default setting is "RFC2833"</li> </ul>
<b>DTMF Payload Type</b>	<p>Configures the payload type for DTMF using RFC2833.</p> <p>Default value is 101.</p> <p>Range: 96~127.</p>
<b>Unregister On Reboot</b>	<p>Allows the SIP user's registration information to be cleared when the GDS reboots. The SIP REGISTER message will contain "Expires: 0" to unbind the connection.</p>
<b>NAT Traversal</b>	<p>This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, STUN, Keep-alive, UPnP, Auto. The default setting is "No".</p> <p>If set to "STUN" and STUN server is configured, the GDS will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the unit will try to use public IP addresses and port number in all the SIP&amp;SDP messages.</p> <p>The GDS will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be "Keep-alive". Configure this to be "No" if an outbound proxy is used. "STUN" cannot be used if the detected NAT is symmetric NAT. If the firewall and the SIP device behind the firewall are both able to use UPNP, it can be set to "UPNP". Both parties will negotiate to use which port to allow SIP through.</p>
<b>Enable SRTP</b>	<p>Enable SRTP mode based on your selection from the drop-down menu.</p> <p>The default setting is "Disabled", the two other modes are "Enabled but Not Forced" and "Enabled and Forced".</p>
<b>Special Feature</b>	<p>Configures GDS settings to meet different vendors' server requirements.</p> <p>Users can choose from Standard, Broadsoft or Telefonica Spain.</p> <p>The default setting is "Standard".</p>





<b>Outbound Proxy Mode</b>	<p><b>In route:</b> outbound proxy FQDN is placed in route header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall.</p> <p><b>Always sent to:</b> SIP messages will always be sent to Outbound proxy.</p> <p><b>Not in route:</b> remove the Route header from SIP requests.</p>
<b>Enable RTCP</b>	<p>This option allows 3rd party Service Provider or Cloud Solution to monitor the operation status of the GDS3710 by using related SIP Calls.</p> <p>By default, it's disabled. Users can choose either RTCP or RTCP-XR.</p>
<b>H.264 Payload Type</b>	<p>The H.264 payload type can now be configured to be compatible with 3rd party video phones, as well as other advanced SIP settings, to easy system integration process. Default is 99.</p>
<b>Accept Incoming SIP from Proxy Only</b>	<p>When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it doesn't match the SIP server address of the account, the call will be rejected. The default setting is disabled.</p>
<b>Vocoder Settings</b>	
<b>Preferred Vocoder</b>	<p>Select multiple audio codecs by priority order (lowest is the highest priority).</p> <p>Supported codecs are: PCMU, PCMA, G.722 and G.729A/B.</p>
<b>Voice Frame Per TX</b>	<p>Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality.</p> <p>The default setting is 2.</p> <p>Range is from 1-64.</p>

## Phone Settings

The phone settings allow users to configure the GDS3710 phone settings and the White list for all the SIP accounts.

### Phone Settings

This page allows users to configure the GDS3710 phone settings.



- LiveView
- Door System Settings
- System Settings
- Account
- Phone Settings
- Account 1 White List
- Account 2 White List
- Account 3 White List
- Account 4 White List
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

### Phone Settings

STUN Server	<input type="text"/>
Local RTP Port	<input type="text" value="5004"/>
Use Random Port	<input type="checkbox"/>
Auto On-Hook Timer(s)	<input type="text" value="300"/>
Ringing Timeout(s)	<input type="text" value="15"/>
SIP TLS Certificate	<div style="border: 1px solid #ccc; height: 40px;"></div>
SIP TLS Private Key	<div style="border: 1px solid #ccc; height: 40px;"></div>
SIP TLS Private Key Password	<input type="password" value="*****"/>
Enable Direct IP Call	<input checked="" type="checkbox"/>
Enable two-way SIP Calling	<input type="checkbox"/>
SIP Proxy Compatibility Mode	<input type="checkbox"/>
SIP Packetization Compatibility Mode	<input type="checkbox"/>
Enable Multi-channel Call Mode	<input type="checkbox"/>
Allow Reset Via SIP NOTIFY	<input type="checkbox"/>

**Figure 72: Phone Settings Page**

**Table 16: Phone Settings**

<b>STUN Server</b>	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.
<b>Local RTP Port</b>	Sets the local RTP port for media. Default setting is 5004. Range between 1024~65400.
<b>Use Random Port</b>	Forces the GDS to use random ports for both SIP and RTP messages. This is usually necessary when multiple units are behind the same full cone NAT. The default setting is “Disabled” <b>Note:</b> This parameter must be set to “Disabled” for Direct IP Calling to work.
<b>Auto On-Hook Timer</b>	Configures the auto on-hook timer (in seconds) for automatic disconnecting the SIP call. Default setting is 300. Range between 0~65535.
<b>Ring Timeout(s)</b>	Specifies the Ring timeout, when no reply is returned from the called party after exceeding this field, the GDS will hang up the call. The value is in the range of 0s – 90s. By default; it is “30” seconds.

<b>SIP TLS Certificate</b>	Input the TLS certificate here for encryption.
<b>SIP TLS Private Key</b>	Input private key here for TLS security protection.
<b>SIP TLS Private Key Password</b>	Specifies the password for SIP TLS private Key.
<b>Enable Direct IP Call</b>	Accepts peer-to-peer IP call (over UDP only) without SIP server. Default is "Enabled".
<b>Enable two-way SIP Calling</b>	Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.
<b>Enable two-way SIP Calling</b>	Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.
<b>SIP Proxy Compatibility Mode</b>	Enables more proxy compatibility with cost of bandwidth, the SIP call will send audio no matter what.
<b>SIP Packetization Compatibility Mode</b>	When enabled, the GDS will have in SDP "packetization-mode = 0". This is required when GDS is interacting with legacy video phones that only accepts this value to decode the RTP.
<b>Enable Multi-channel Call Mode</b>	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.
<b>Allow Reset Via SIP NOTIFY</b>	Allows to factory reset the devices directly through SIP Notify. If "Allow Reset Via SIP NOTIFY" is "check", then once the GDS3710 receives the SIP NOTIFY from the SIP server with Event: reset, the GDS3710 will perform a factory reset after authentication. This authentication can be either with: <ul style="list-style-type: none"> <li>• The admin password if no SIP account is configured on the GDS3710.</li> <li>• The SIP User ID and Password credentials of the SIP account if configured on the GDS3710.</li> </ul> Default is unchecked (disabled).



## Account [1-4] White List

This page allows users to configure the white list per account, 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, and all other inbound calls will be blocked), the user can configure up to 30 white phone numbers per SIP account.

Moreover, besides numbers associated to active cards, and numbers on the "Number Called When Door Bell Pressed" setting, all whitelisted numbers can open door remotely by using the respective PIN code.

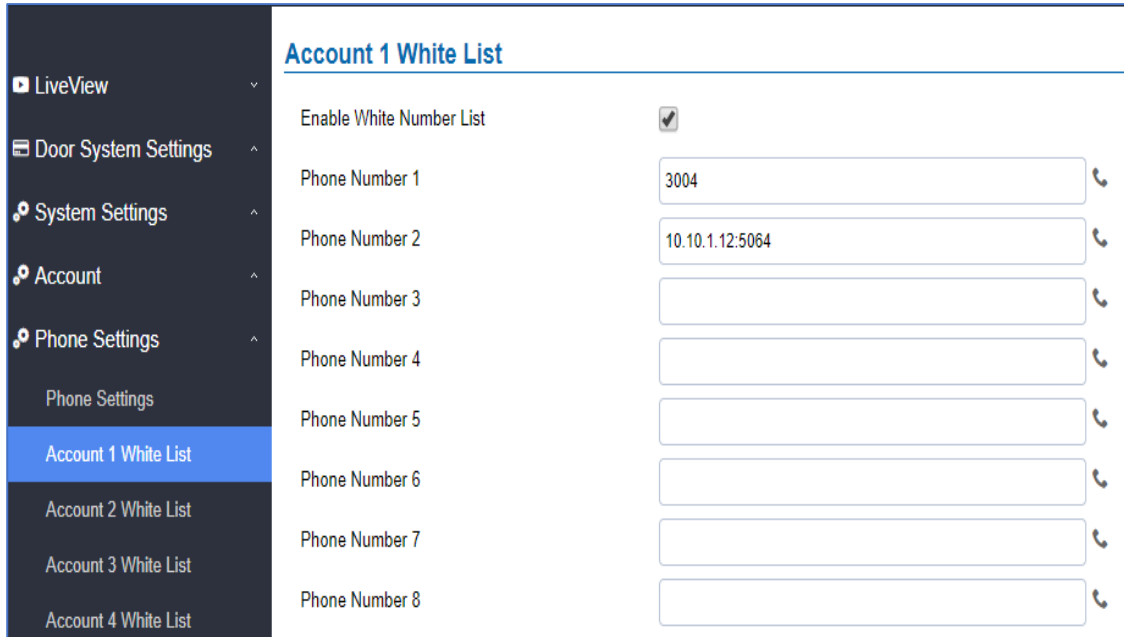


Figure 73: White List Page

The table below gives a brief overview of the options:

Table 17: White List

<b>Enable White Number List</b>	Enables the White List feature.
<b>Phone Number 1 -30</b>	Adds a new phone number to the white list.

## 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.



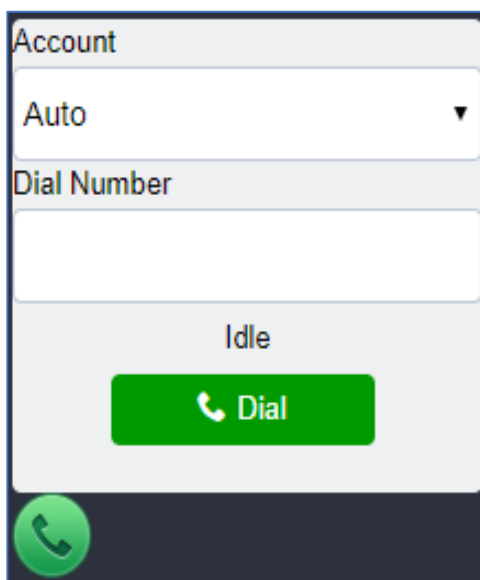


Figure 74 : Click-To-Dial

**Note:** Only the 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

LiveView

Door System Settings

System Settings

Account

Phone Settings

Video & Audio Settings

Video Settings

OSD Settings

CMOS Settings

Audio Settings

Privacy Masks

Alarm Settings

Email & FTP Settings

Maintenance

Status

### Video Settings

#### Stream 1

Preferred Video Codec

H264

Profile

Main Profile

Resolution

1920\*1080(16:9)

Bit Rate(kbps)

4096

Frame Rate(fps)

30

Bit Rate Control

CBR (Constant Bit Rate)

Image Quality

Normal

I-frame Interval

80

#### Stream 2

Preferred Video Codec

H264

Profile

Main Profile

Resolution

1280\*720(16:9)

Bit Rate(kbps)

512

Frame Rate(fps)

25

Bit Rate Control

CBR (Constant Bit Rate)

Image Quality

Normal

I-frame Interval

80

#### Stream 3

Preferred Video Codec

H264

Profile

Main Profile

Resolution

320\*240(4:3)

Save

Figure 75: Video Settings Page

Table 18: Video Settings

<b>Preferred Video Codec (Stream1)</b>	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
<b>Profile</b>	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is "Main Profile".
<b>Resolution</b>	Specifies the resolution in pixels used at video image, 1080p or 720p.
<b>Bit Rate(kbps)</b>	Selects the video bit rate or bandwidth used.
<b>Frame Rate(fps)</b>	Selects the maximum frame rate used (more data if big frame used).



<b>Bit Rate Control</b>	Selects the constantly bit rate, or variable bit rate.
<b>Image Quality</b>	Selects the image quality used when Variable Bit Rate used.
<b>I-frame Interval</b>	Configures the I-frame interval (suggested 2~3 times of frame rate).
<b>Preferred Video Codec(Stream2)</b>	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
<b>Profile</b>	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is "Main Profile".
<b>Resolution</b>	Specifies the resolution in pixels used at video image, 1080p or 720p.
<b>Bit Rate(kbps)</b>	Selects the video bit rate or bandwidth used.
<b>Frame Rate(fps)</b>	Selects the maximum frame rate used (more data if big frame used).
<b>Bit Rate Control</b>	Selects the constantly bit rate, or variable bit rate.
<b>Image Quality</b>	Selects the image quality used when Variable Bit Rate used.
<b>I-frame Interval</b>	Configures the I-frame interval (suggested 2~3 times of frame rate).
<b>Preferred Video Codec(Stream3)</b>	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
<b>Profile</b>	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is "Main Profile".
<b>Resolution</b>	Specifies the resolution in pixels used at video image, 1080p or 720p.
<b>Bit Rate(kbps)</b>	Selects the video bit rate or bandwidth used.
<b>Frame Rate(fps)</b>	Selects the maximum frame rate used (more data if big frame used).
<b>Bit Rate Control</b>	Selects the constantly bit rate, or variable bit rate.
<b>Image Quality</b>	Selects the image quality used when Variable Bit Rate used.
<b>I-frame Interval</b>	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 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> streams respectively
- To retrieve MJPEG video stream via http, users can use the following format:  
[http\(s\)://admin:password@IP:port/jpeg/stream=X](#) (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.

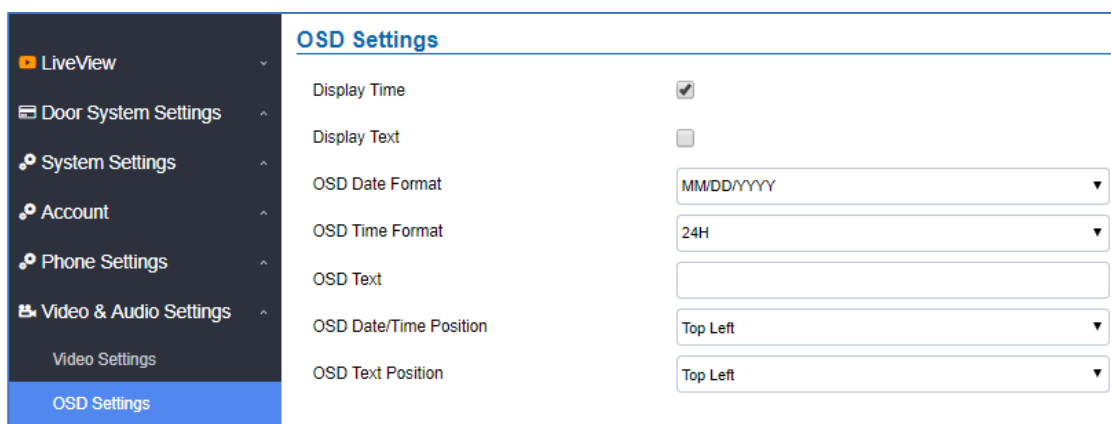


Figure 76: OSD Settings Page

Table 19: OSD Settings

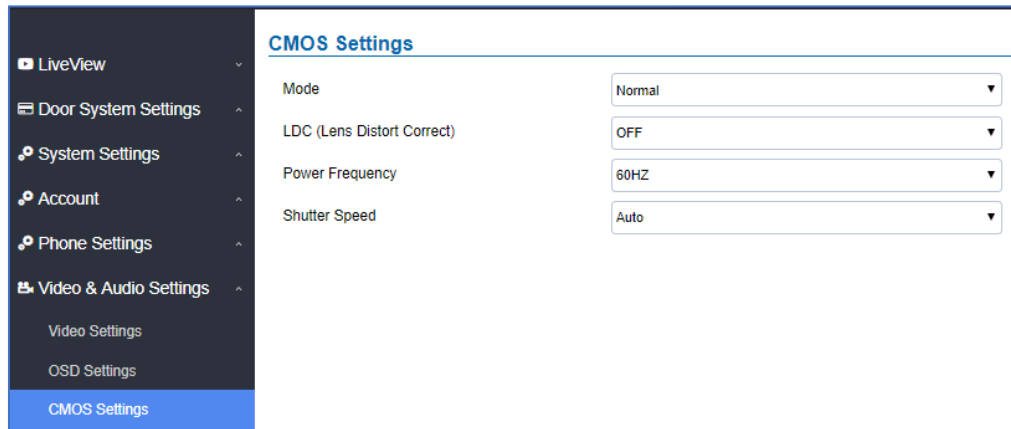
<b>Display Time</b>	When checked, time will be displayed inside the video image.
<b>Display Text</b>	When checked, inputted text on “OSD Test” will be displayed on the video image.
<b>OSD Date Format</b>	OSD Date format, choose based on user preference.
<b>OSD Time Format</b>	OSD Time format, choose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

## CMOS Settings

This page configures the CMOS parameters for different scenarios.







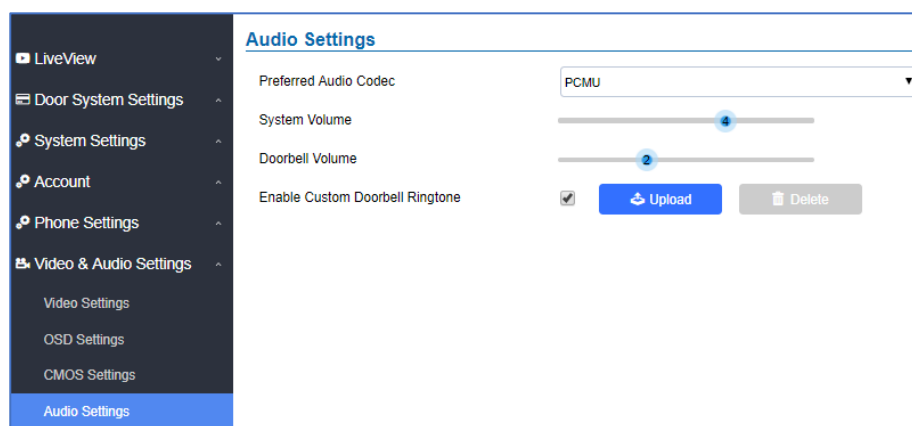
**Figure 77: CMOS Settings Page**

**Table 20: CMOS Settings**

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

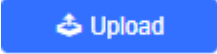
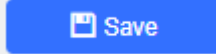



**Figure 78: Audio Settings Page**



**Table 21: Audio Settings**

<b>Preferred Audio Codec</b>	Configures the audio codec. Three codecs are available: PCMU, PCMA and G.722 are supported.
<b>System Volume</b>	Adjusts the speaker volume connected.
<b>Doorbell Volume</b>	Adjusts the doorbell volume.
<b>Enable Custom Doorbell Ringtone</b>	User can check this option in order to use the custom Doorbell Ringtone. Default Ringtone is used when this option is disabled.

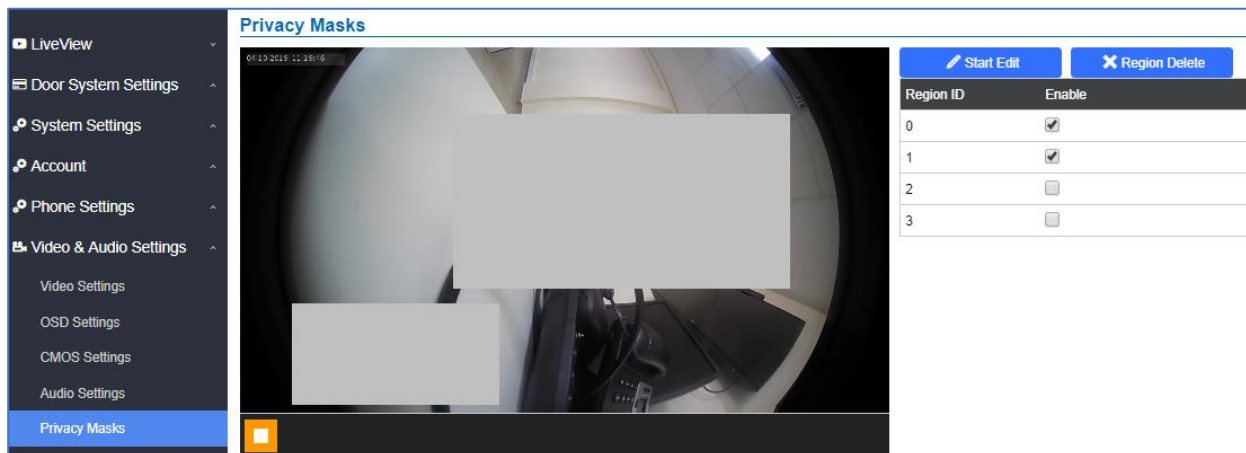
- Click on  to upload the ringtone file, then  press
- Click on  to delete the existent custom ringtone.
- Support upload WAV, PCM audio file(size <= 600K). Format limit to:  
**WAV:**
  1. Sample Rate: 8k or 16k.
  2. Channel: Mono-channel or Dual-channel.**PCM:**
  1. Sample Rate: 8K.
  2. Channel: Dual-channel.

**Note:** Empty audio file is not accepted.

## 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.



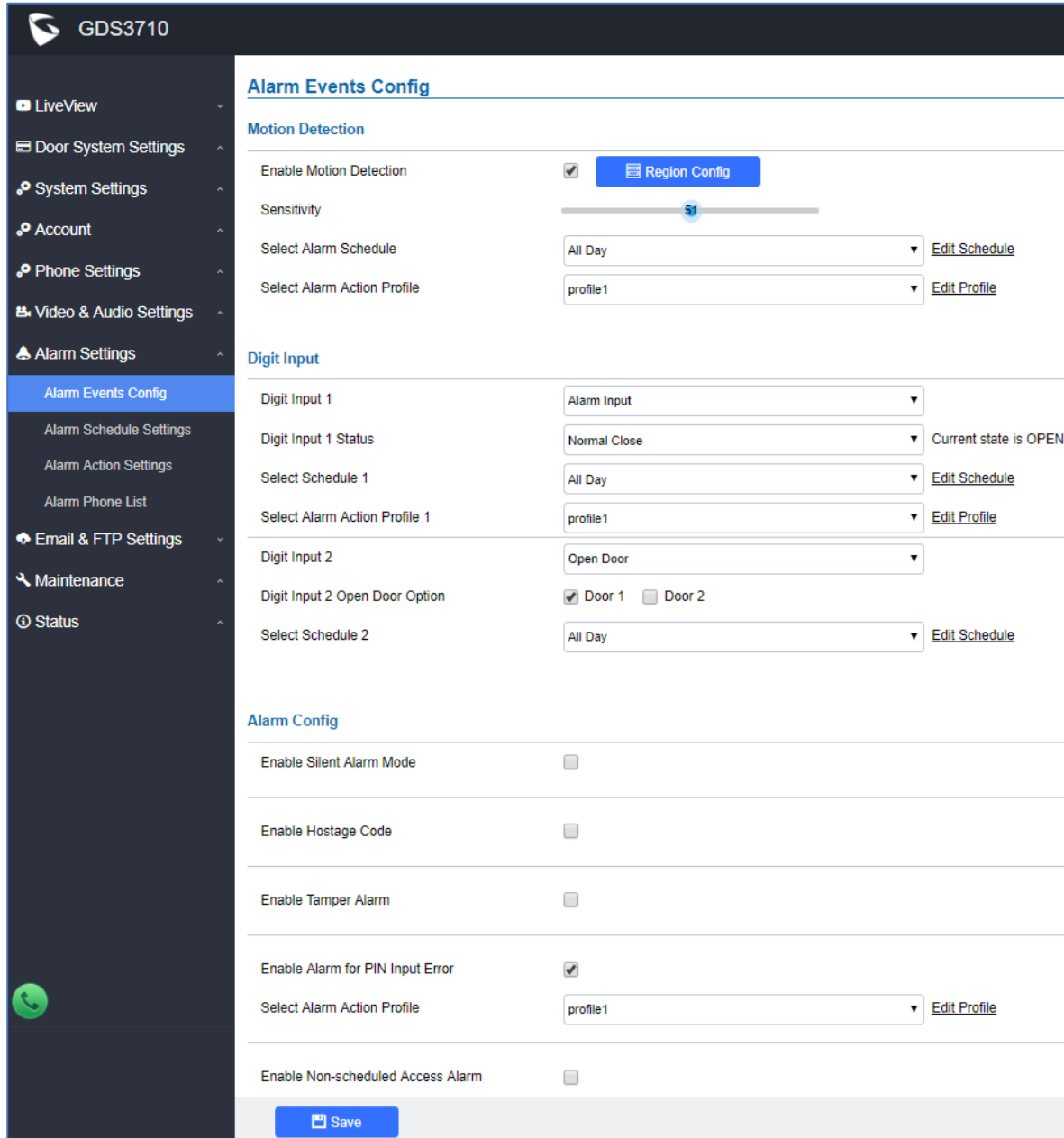
**Figure 79: Privacy Masks Configuration Page**

## Alarm Settings

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.



**GDS3710**

**Alarm Events Config**

**Motion Detection**

Enable Motion Detection ☒ [Region Config](#)

Sensitivity

Select Alarm Schedule All Day [Edit Schedule](#)

Select Alarm Action Profile profile1 [Edit Profile](#)

**Digit Input**

Digit Input 1 Alarm Input

Digit Input 1 Status Normal Close Current state is OPEN

Select Schedule 1 All Day [Edit Schedule](#)

Select Alarm Action Profile 1 profile1 [Edit Profile](#)

Digit Input 2 Open Door

Digit Input 2 Open Door Option ☒ Door 1 ☐ Door 2

Select Schedule 2 All Day [Edit Schedule](#)

**Alarm Config**

Enable Silent Alarm Mode ☐

Enable Hostage Code ☐

Enable Tamper Alarm ☐

Enable Alarm for PIN Input Error ☒

Select Alarm Action Profile profile1 [Edit Profile](#)

Enable Non-scheduled Access Alarm ☐

[Save](#)

Figure 80: 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.

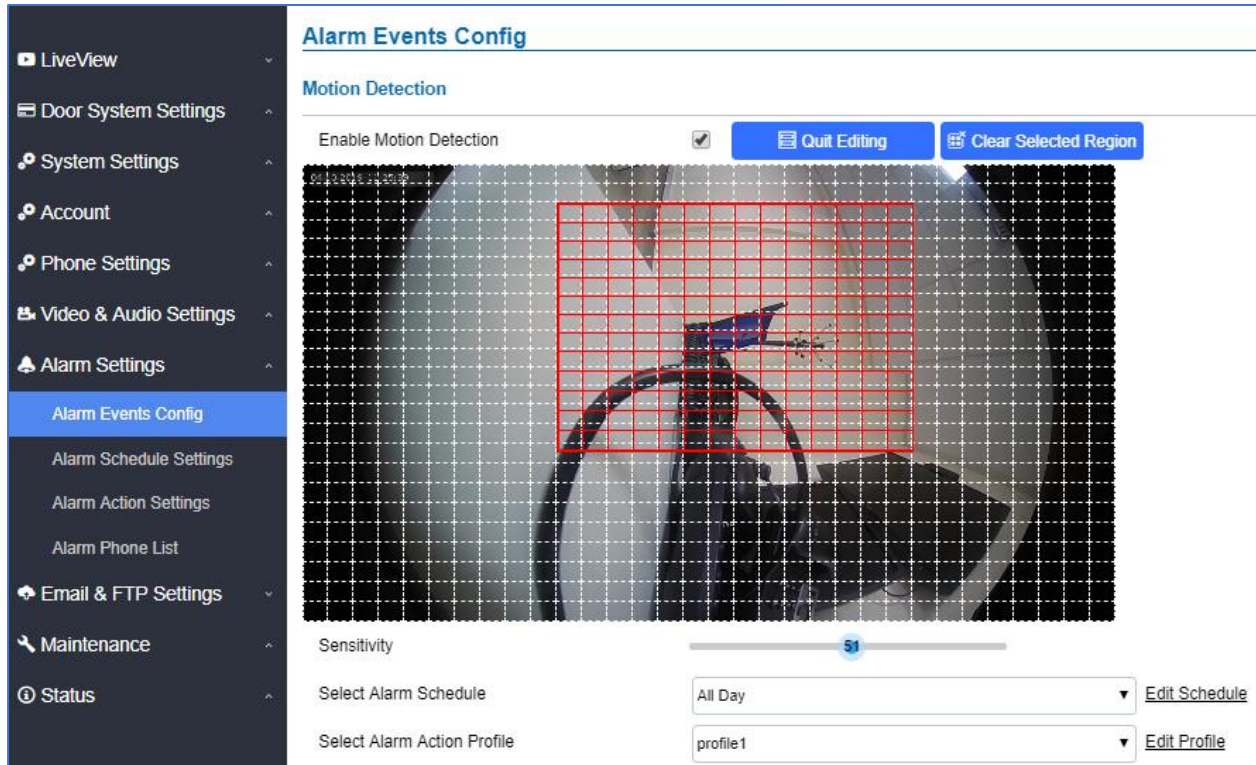


Figure 81: Region Config

Table 22: Motion Detection

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

## Digital Input

Digit Input	
Digit Input 1	Alarm Input ▼
Digit Input 1 Status	Normal Close ▼ <span>Current state is OPEN</span>
Select Schedule 1	All Day ▼ <a href="#">Edit Schedule</a>
Select Alarm Action Profile 1	profile1 ▼ <a href="#">Edit Profile</a>
Digit Input 2	Open Door ▼
Digit Input 2 Open Door Option	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Select Schedule 2	All Day ▼ <a href="#">Edit Schedule</a>

**Figure 82: Digital Input**

**Table 23: Digital Input**

<b>Digital Input 1</b>	<p>Selects the Input method (alarm Input or Door Open). Default disabled.</p> <p>Digital Input Port operates in 3 Modes:</p> <ol style="list-style-type: none"> <li><b>Alarm Input:</b> Connect sensor to trigger alarm.</li> <li><b>Open door:</b> Connect a switch to open door from inside.</li> <li><b>Abnormal Door Control:</b> This is a major security enhancement for GDS37xx when device be tampered to open the door abnormally. <i>Please check <b>Siren alarming when door opened abnormally</b> section.</i></li> </ol> <p>If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.</p>
<b>Digit Input 1 Open Door Option</b>	<ul style="list-style-type: none"> <li>When Digital Input is set to <b>Open door</b> then user can select the doors to be affected when Alarm IN 1 is triggered.</li> </ul>
<b>Input Digit 1 Status</b>	<ul style="list-style-type: none"> <li>If set to <b>Normal Open</b>: Configured alarm will be triggered when Digital Input Status switch from Close to Open.</li> <li>If set to <b>Normal Close</b>: Configured alarm will be triggered when Digital Input Status switch from Open to Close.</li> </ul> <p>By default, Input Digit 1 Status is “Disabled”.</p>
<b>Select Alarm Schedule 1</b>	Selects the predefined Alarm Schedule.
<b>Select Alarm Action Profile 1</b>	Selects the predefined Alarm Action for Profile 1.
<b>Digital Input 2</b>	<p>Selects the Input method (alarm Input or Door Open). Default disabled.</p> <p>Digital Input Port operates in 2 Modes:</p>



	<ol style="list-style-type: none"> <li>1. <b>Alarm Input:</b> Connect various of sensor to trigger alarm.</li> <li>2. <b>Open Door:</b> Connect a switch to open door from inside.</li> </ol> <p>If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.</p>
<b>Digit Input 2 Open Door Option</b>	When Digital Input is set to <b>Open door</b> then user can select the doors to be affected when Alarm IN 2 is triggered.
<b>Input Digit 2 Status</b>	<ul style="list-style-type: none"> <li>• If set to <b>Normal Open</b>: Configured alarm will be triggered when Digital Input Status switch from Close to Open.</li> <li>• If set to <b>Normal Close</b>: Configured alarm will be triggered when Digital Input Status switch from Open to Close.</li> </ul> <p>By default, Input Digit 2 Status is “Disabled”.</p>
<b>Select Alarm Schedule 2</b>	Selects the predefined Alarm Schedule.
<b>Select Alarm Action Profile 2</b>	Selects the predefined Alarm Action for Profile 2.
<b>Alarm Output Duration(s)</b>	<p>Select the duration of the alarm output: 5/10/15/20/25/30 seconds.</p> <p>This option is hidden when <b>ALMOUT1 Feature</b> is set to Open Door.</p>

### Enable Silent 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

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

### 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

<b>Enable Hostage Code</b>	Enable/Disable the Hostage password mode.
<b>Hostage Code</b>	Configures the password for the hostage mode.



<b>Select Alarm Action Profile</b>	Select the Alarm action to be taken when the hostage password is typed on the GDS3710 keypad.  <b>Note:</b> 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 it is removed.

**Table 26: Tamper Alarm**

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

### Keypad Input Error Alarm

**Table 27: Keypad Input Error Alarm**

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

### Non-Scheduled Access Alarm

**Table 28 : Non-Scheduled Access Alarm**

<b>Enable Non-Scheduled Access Alarm</b>	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
<b>Select Alarm Action Profile</b>	Select the type of alarms actions to be triggered.



LiveView

Door System Settings

System Settings

Account

Phone Settings

Video & Audio Settings

Alarm Settings

Alarm Events Config

Alarm Schedule Settings

Alarm Action Settings

Alarm Phone List

Email & FTP Settings


Maintenance

Status

Alarm Schedule Settings

No.	Schedule Name	Detail	Edit
1	schedule1	<div><div></div><div><div><div></div><div>0</div><div>1</div><div>2</div><div>3</div><div>4</div><div>5</div><div>6</div><div>7</div><div>8</div><div>9</div><div>10</div><div>11</div><div>12</div><div>13</div><div>14</div><div>15</div><div>16</div><div>17</div><div>18</div><div>19</div><div>20</div><div>21</div><div>22</div><div>23</div><div>0</div></div><div><div>Sun</div><div>Mon</div><div>Tue</div><div>Wed</div><div>Thu</div><div>Fri</div><div>Sat</div></div></div></div>	
2	schedule2	<div></div>	
3	schedule3	<div></div>	
4	schedule4	<div></div>	
5	schedule5	<div></div>	
6	schedule6	<div></div>	
7	schedule7	<div></div>	
8	schedule8	<div></div>	
9	schedule9	<div></div>	
10	schedule10	<div></div>	

**Figure 83: 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.

Modify Schedule

Schedule Name

Sun	Period1	00	:	00	-	23	:	59
Mon	Period2	00	:	00	-	00	:	00
Tue	Period3	00	:	00	-	00	:	00
Wed	Period4	00	:	00	-	00	:	00
Thu	Period5	00	:	00	-	00	:	00
Fri	Period6	00	:	00	-	00	:	00
Sat	Period7	00	:	00	-	00	:	00
	Period8	00	:	00	-	00	:	00

Copy
☒ Sun
☐ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Select All

Save

Cancel

**Figure 84: Edit Schedule**



## Alarm Action When Illegal Card Swiped

When this feature is enabled, any illegal card swiped trying to access the door will trigger alarm based on user's configuration.

**Table 29: Alarm action when illegal card swiped**

<b>Enable Non-authorized RFID Card Access Alarm</b>	Enable/Disable the option to activate the profile to be executed when unauthorized card swipes.
<b>Select Alarm Action Profile</b>	Select the type of alarms actions to be triggered after unauthorized card was swiped.

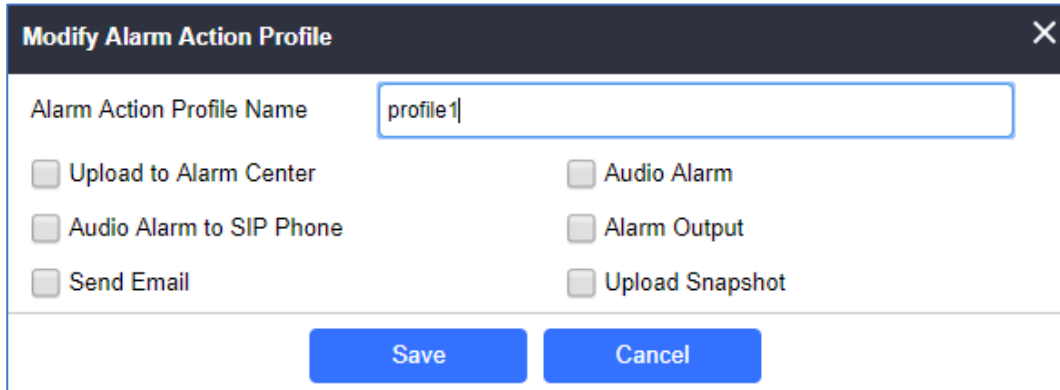
## Alarm Action Settings

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


Alarm Action Settings				
No.	Alarm Action Profile Name	Detail	Edit	Test
1	profile1			
<div> <div>  Upload to Alarm Center   Audio Alarm to SIP Phone   Send Email </div> <div>  Audio Alarm   Alarm Output   Upload Snapshot </div> </div>				
2	profile2			
3	profile3			
4	profile4			
5	profile5			
6	profile6			
7	profile7			
8	profile8			
9	profile9			
10	profile10			

**Figure 85: Alarm Action**

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



**Figure 86: 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.

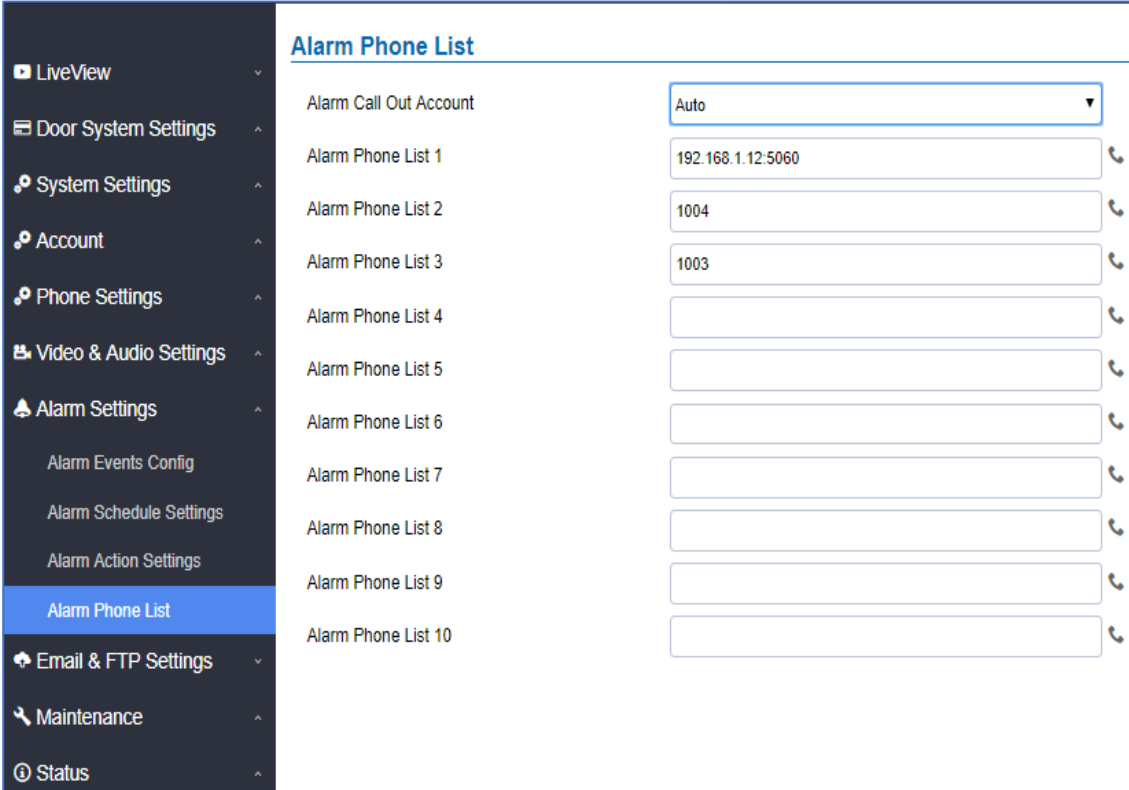
**Table 30: Alarm Actions**

<b>Upload to Alarm Center</b>	If selected, the GDSManager will popup alarm window and sound alarm in the computer speaker.
<b>Audio Alarm to SIP Phone</b>	If selected, GDS3710 will call pre-configured (video or audio) phone and will play sound alarm.
<b>Send Email</b>	If selected, an email with snapshot will be sent to the pre-configured email destination.
<b>Audio Alarm</b>	If selected, GDS3710 will play alarm audio using built-in speaker.
<b>Alarm Output</b>	If selected, the alarm will be sent to the equipment (for example: Siren) connected to Alarm Output interface.
<b>Upload Snapshot</b>	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 triggered (e.g.: doorbell pressed).





**Figure 87: Alarm Phone List**

**Table 31: Alarm Phone List**

<b>Alarm Call Out Account</b>	Select the SIP Account to be used by the GDS when alarm out is triggered.
<b>Alarm Phone List 1-10</b>	Add or delete number from the phone alarm list. (When IP address is used then the port needs to be appended, example: 192.168.1.12:5060).

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.

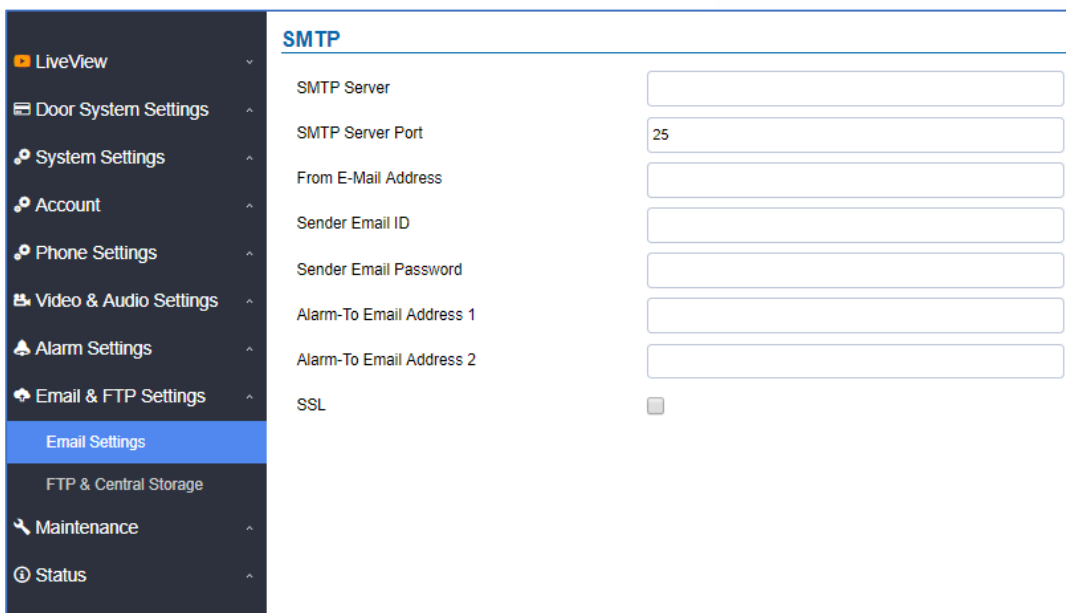
## Email & FTP Settings

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 triggered.



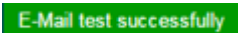


**Figure 88: Email Settings - SMTP Page**

**Table 32: Email Settings - SMTP**

<b>SMTP Server</b>	Configures the SMTP Email Server IP or Domain Name.
<b>SMTP Server Port</b>	Specifies the Port number used by server to send email.
<b>From E-mail address</b>	Specifies email address of alarm email sending from, usually client email ID.
<b>Sender Email ID</b>	Specifies sender's User ID or account ID in the email system used.
<b>Sender Email Password</b>	Specifies sender's password of the email account.
<b>Alarm-To Email Address 1</b>	Specifies the 1 <sup>st</sup> email address to receive the alarm email.
<b>Alarm-To Email Address 2</b>	Specifies the 2 <sup>nd</sup> email address to receive the alarm email.
<b>SSL</b>	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.



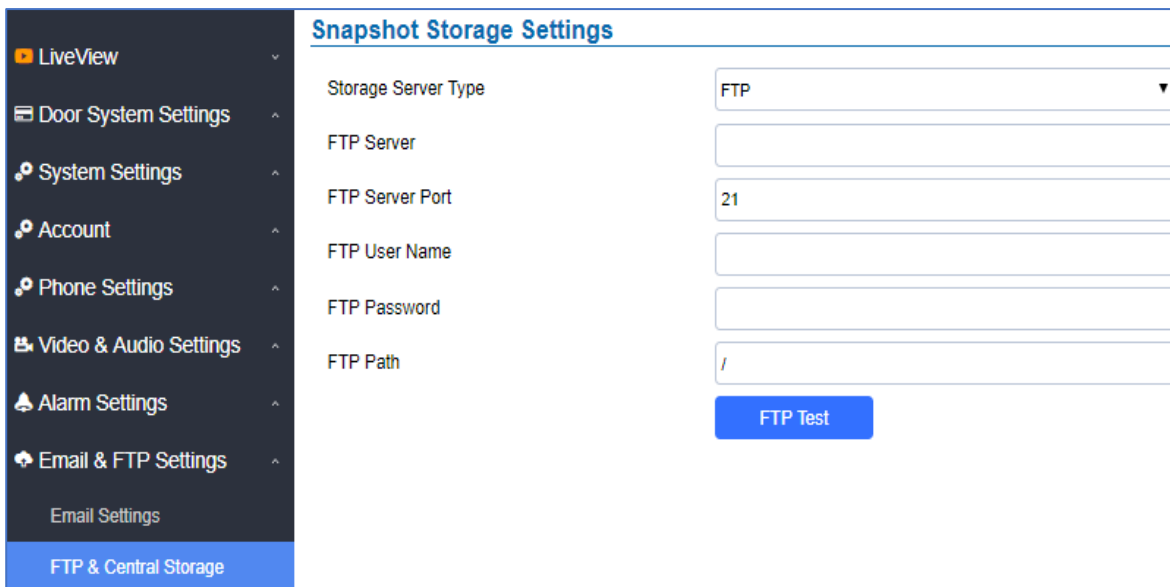
## FTP & Center Storage

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

**Table 33: Picture Storage Settings**

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

**Note:** Blank fields when using Storage Server Type as Central Storage might imply no configuration in GDSManager.



**Figure 89: 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:

FTP test successfully.



- 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 34: FTP Filenames**

FTP Filename with	Description
<b>CARD</b>	Meaning that open door operation is using RFID card.
<b>LPIN (Local PIN)</b>	Meaning that open door operation is via Local PIN (Private PIN, or Unified PIN, or Guest PIN).
<b>RPIN (Remote PIN)</b>	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).
<b>RING</b>	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:



[\[To Parent Directory\]](#)

Friday, March 02, 2018	9:39 AM	76504	<a href="#">BA854E CARD 2018-03-02 100355 7558019 0.jpg</a>
Friday, March 02, 2018	9:39 AM	82105	<a href="#">BA854E CARD 2018-03-02 100356 0.jpg</a>
Friday, March 02, 2018	9:39 AM	83406	<a href="#">BA854E CARD 2018-03-02 100356 7558019 1.jpg</a>
Friday, March 02, 2018	9:39 AM	82427	<a href="#">BA854E CARD 2018-03-02 100357 0.jpg</a>
Friday, March 02, 2018	9:39 AM	83266	<a href="#">BA854E CARD 2018-03-02 100358 0.jpg</a>
Friday, March 02, 2018	9:39 AM	85094	<a href="#">BA854E CARD 2018-03-02 100359 0.jpg</a>
Friday, March 02, 2018	9:39 AM	87633	<a href="#">BA854E CARD 2018-03-02 100400 0.jpg</a>
Friday, March 02, 2018	9:39 AM	86810	<a href="#">BA854E CARD 2018-03-02 100401 0.jpg</a>
Friday, March 02, 2018	7:46 AM	76148	<a href="#">BA854E LPIN 2018-03-02 080942 0.jpg</a>
Friday, March 02, 2018	7:46 AM	75696	<a href="#">BA854E LPIN 2018-03-02 080943 0.jpg</a>
Friday, March 02, 2018	7:46 AM	79922	<a href="#">BA854E LPIN 2018-03-02 080944 0.jpg</a>
Friday, March 02, 2018	7:46 AM	81914	<a href="#">BA854E LPIN 2018-03-02 080945 0.jpg</a>
Friday, March 02, 2018	7:46 AM	79908	<a href="#">BA854E LPIN 2018-03-02 080946 0.jpg</a>
Friday, March 02, 2018	7:46 AM	79514	<a href="#">BA854E LPIN 2018-03-02 080947 0.jpg</a>
Friday, March 02, 2018	7:46 AM	80353	<a href="#">BA854E LPIN 2018-03-02 080948 0.jpg</a>
Friday, March 02, 2018	8:36 AM	81201	<a href="#">BA854E LPIN 2018-03-02 090050 0.jpg</a>
Friday, March 02, 2018	8:36 AM	82609	<a href="#">BA854E LPIN 2018-03-02 090051 0.jpg</a>
Friday, March 02, 2018	8:36 AM	79362	<a href="#">BA854E LPIN 2018-03-02 090052 0.jpg</a>
Friday, March 02, 2018	8:36 AM	86139	<a href="#">BA854E LPIN 2018-03-02 090053 0.jpg</a>
Friday, March 02, 2018	8:36 AM	85269	<a href="#">BA854E LPIN 2018-03-02 090054 0.jpg</a>
Friday, March 02, 2018	8:36 AM	84463	<a href="#">BA854E LPIN 2018-03-02 090055 0.jpg</a>
Friday, March 02, 2018	8:36 AM	86007	<a href="#">BA854E LPIN 2018-03-02 090056 0.jpg</a>
Friday, March 02, 2018	8:50 AM	82610	<a href="#">BA854E LPIN 2018-03-02 091348 0.jpg</a>
Friday, March 02, 2018	8:50 AM	81378	<a href="#">BA854E LPIN 2018-03-02 091349 0.jpg</a>
Friday, March 02, 2018	8:50 AM	83379	<a href="#">BA854E LPIN 2018-03-02 091350 0.jpg</a>
Friday, March 02, 2018	8:50 AM	83745	<a href="#">BA854E LPIN 2018-03-02 091351 0.jpg</a>
Friday, March 02, 2018	8:50 AM	87227	<a href="#">BA854E LPIN 2018-03-02 091352 0.jpg</a>
Friday, March 02, 2018	8:50 AM	87199	<a href="#">BA854E LPIN 2018-03-02 091353 0.jpg</a>
Friday, March 02, 2018	8:50 AM	84078	<a href="#">BA854E LPIN 2018-03-02 091354 0.jpg</a>
Friday, March 02, 2018	9:44 AM	77783	<a href="#">BA854E LPIN 2018-03-02 100955 0.jpg</a>

Figure 90 : FTP filenames

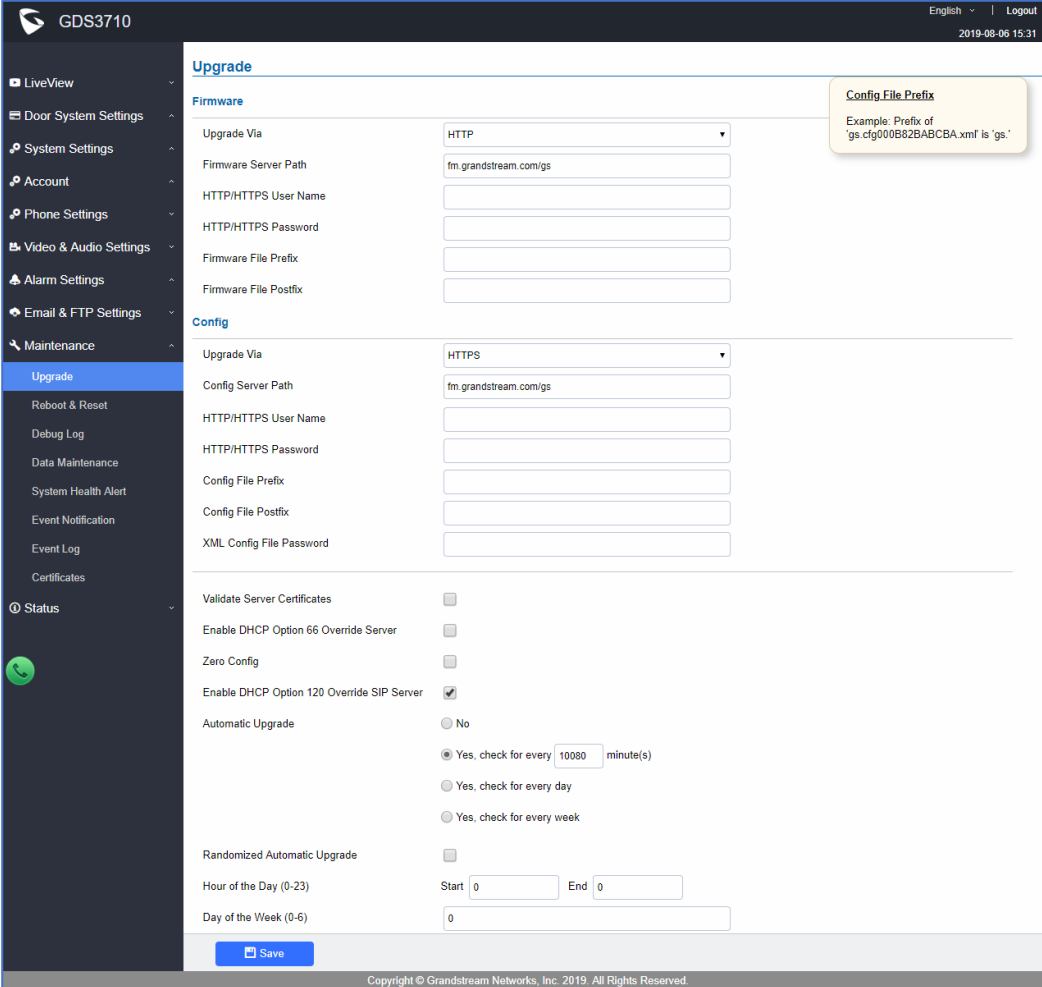
## Maintenance Settings

This page shows the GDS3710 Maintenance parameters.

## Upgrade

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





The screenshot shows the 'Upgrade' page of the GDS3710 web interface. The left sidebar contains a navigation menu with options like LiveView, Door System Settings, System Settings, Account, Phone Settings, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, Upgrade (selected), Reboot & Reset, Debug Log, Data Maintenance, System Health Alert, Event Notification, Event Log, Certificates, and Status. The main content area is divided into two sections: 'Firmware' and 'Config'. The 'Firmware' section includes fields for Upgrade Via (HTTP), Firmware Server Path (fm.grandstream.com/gs), HTTP/HTTPS User Name, HTTP/HTTPS Password, Firmware File Prefix, and Firmware File Postfix. The 'Config' section includes fields for Upgrade Via (HTTPS), Config Server Path (fm.grandstream.com/gs), HTTP/HTTPS User Name, HTTP/HTTPS Password, Config File Prefix, Config File Postfix, XML Config File Password, Validate Server Certificates, Enable DHCP Option 66 Override Server, Zero Config, Enable DHCP Option 120 Override SIP Server, Automatic Upgrade (radio buttons for No, Yes, check for every 10080 minute(s), Yes, check for every day, Yes, check for every week), Randomized Automatic Upgrade, Hour of the Day (0-23) with Start and End fields, and Day of the Week (0-6). A 'Save' button is at the bottom. A yellow callout box titled 'Config File Prefix' provides an example: 'Example: Prefix of 'gs.cfg000B82BABCBA.xml' is 'gs.''. The top right shows 'English' and 'Logout' with the date '2019-08-06 15:31'.

**Figure 91: Upgrade Page**

**Table 35: Upgrade**

<b>Upgrade Via</b>	Selects the upgrade method (TFTP, HTTP, and HTTPS).
<b>Firmware Server Path</b>	Configures the IP address or the FQDN of the upgrade server.
<b>HTTP/HTTPS User Name</b>	The user name for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	The password for the HTTP/HTTPS server.
<b>Firmware File Prefix</b>	Enables your ITSP to lock configuration updates. If configured, only the firmware file with the matching encrypted prefix will be downloaded and flashed into the phone.
<b>Firmware File Postfix</b>	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.
<b>Upgrade via</b>	Selects the upgrade method (TFTP, HTTP, and HTTPS).
<b>Config Server Path</b>	Configures the IP address or the FQDN of the configuration server.



<b>HTTP/HTTPS User Name</b>	The user name for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	The password for the HTTP/HTTPS server.
<b>Config File Prefix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
<b>Config File Postfix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
<b>XML Config File Password</b>	Specifies the password for the configuration file.
<b>Validate Server Certificate</b>	Enable this option in order to validate certificate with trusted ones during TLS connection.
<b>Automatic Upgrade Interval</b>	Specifies the upgrade interval in minutes.
<b>Enable DHCP Option 66 Override Server</b>	Activates DHCP option 66 to override upgrade/config servers.
<b>Zero Config</b>	Enables Zero Config feature for auto provisioning.
<b>Enable DHCP Option 120 Override SIP Server</b>	Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is enabled.
<b>Automatic Upgrade</b>	Enables automatic upgrade and provisioning. Set schedule for provisioning for either every X minutes, every day or every week. Default is No.
<b>Randomized Automatic Upgrade</b>	Enable and define the start/End hours of the day and days of the week where the GDS will randomly checking for update.
<b>Disable SIP NOTIFY Authentication</b>	If this option is checked, the Device will not challenge NOTIFY with 401. Default setting is Enabled.

#### 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.

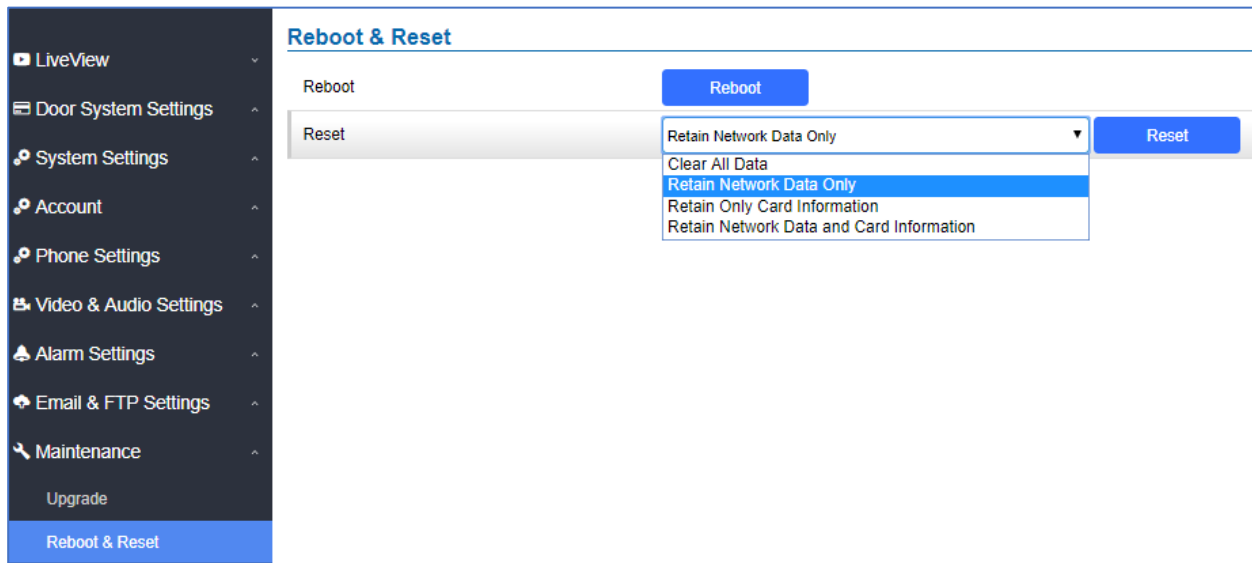


Figure 92: Reset & Reboot Page

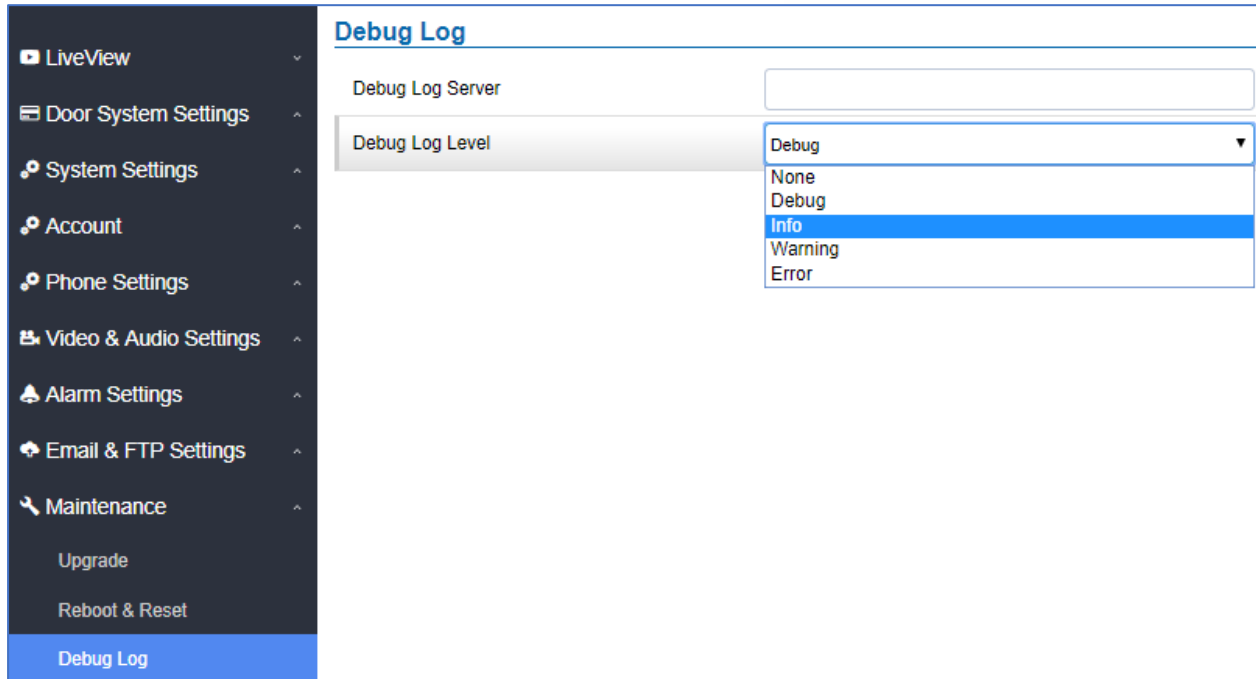
Table 36: Reset & Reboot

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



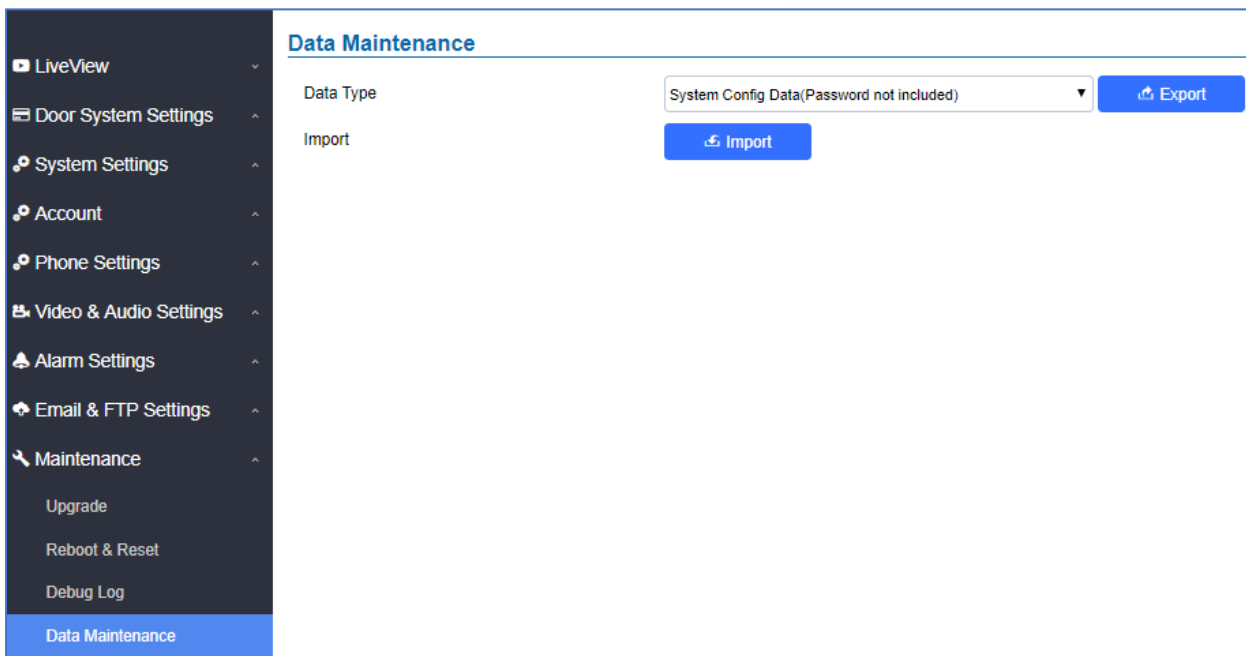


**Figure 93: Debug Log Page**


- 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.



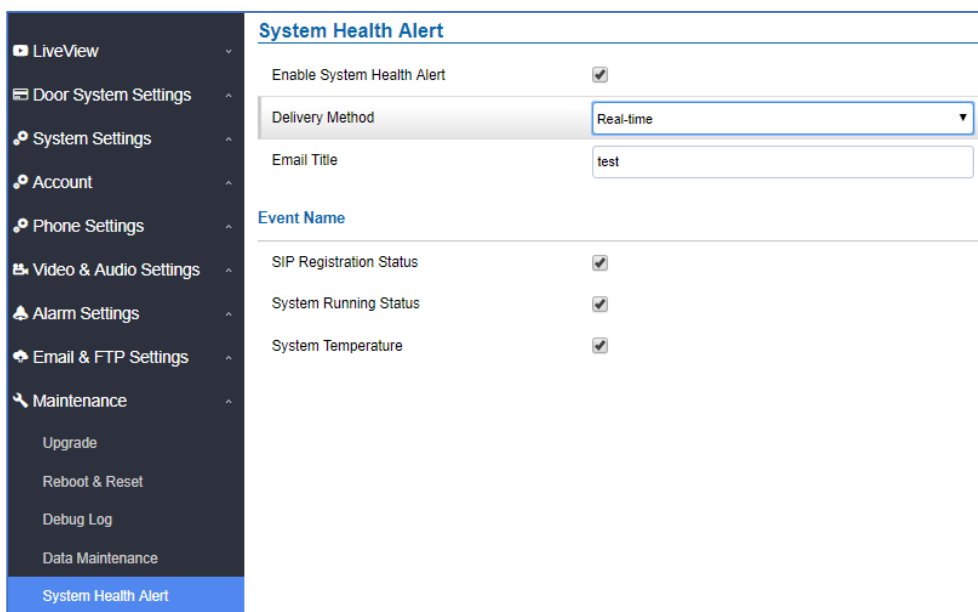
**Figure 94: Data Maintenance Page**

Click on  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.

## System Health Alert

This option allows users to receive alert emails regarding SIP Registration Status of accounts, System Running Status or System Temperature in real time or in a periodic manner.



**Figure 95: System Health Alert Page**



<b>Enable System Health Alert</b>	When this option is checked, then the GDS will send alert emails regarding the events selected under Event Name section using the already configured [Email Settings].
<b>Delivery Method</b>	When set to Realtime, the GDS will be sending successively alert emails every second.  When set to Periodic, user can define the time interval between alert emails.
<b>Email Title</b>	Customize the Email title. Maximum length is 256 character.
<b>SIP Registration Status</b>	When checked, Email will contain Offline/Online indication for all 4 accounts.
<b>System Running Status</b>	When checked, Email will contain the system uptime.
<b>System Temperature</b>	When checked, Email will contain Temperature value of the system in °C and °F, as well as whether the temperature is normal or not.

## 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.
```

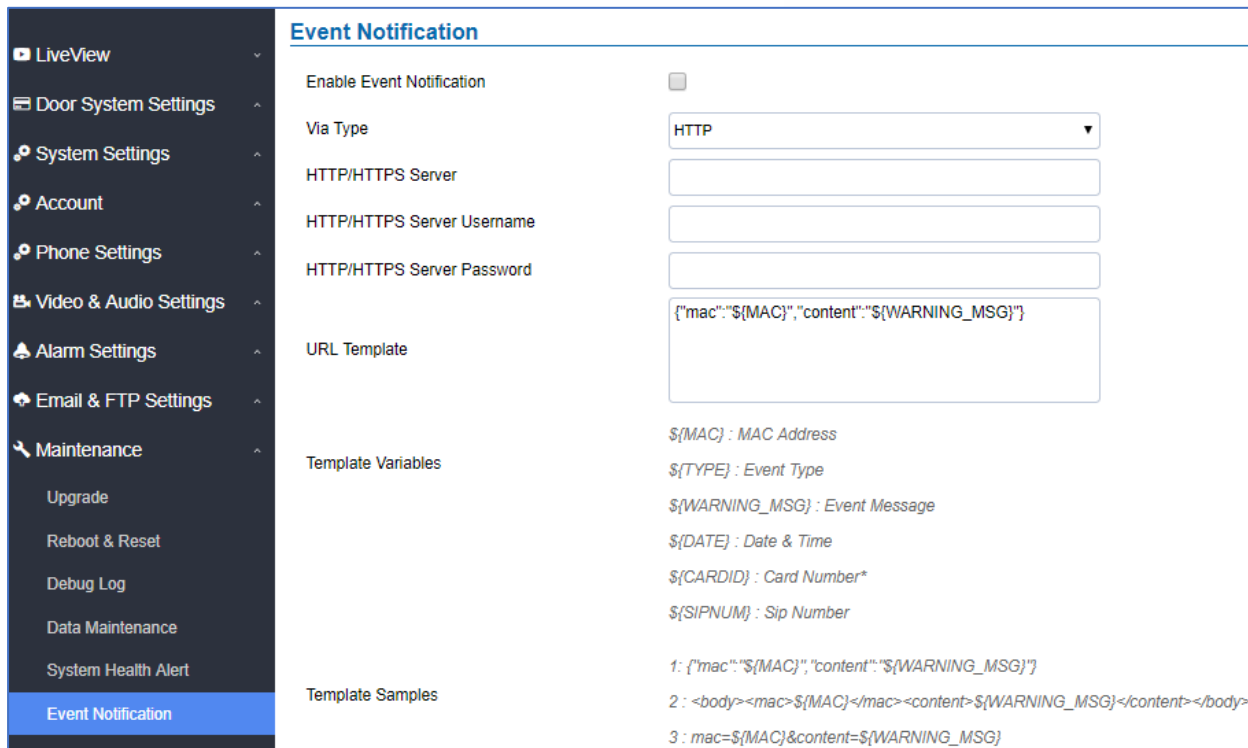
- After making a Call, when doorbell pressed, GDS3710 will send to the configured HTTP server the following HTTP POST containing "Phone call" event:

```
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 3<sup>rd</sup> party software to integrate the GDS3710.



**Event Notification**

Enable Event Notification ☐

Via Type HTTP

HTTP/HTTPS Server

HTTP/HTTPS Server Username

HTTP/HTTPS Server Password

URL Template 

```
{ "mac": "${MAC}", "content": "${WARNING_MSG}" }
```

Template Variables

- `${MAC}` : MAC Address
- `${TYPE}` : Event Type
- `${WARNING_MSG}` : Event Message
- `${DATE}` : Date & Time
- `${CARDID}` : Card Number\*
- `${SIPNUM}` : Sip Number

Template Samples

```
1: { "mac": "${MAC}", "content": "${WARNING_MSG}" }
2: <body><mac>${MAC}</mac><content>${WARNING_MSG}</content></body>
3: mac=${MAC}&content=${WARNING_MSG}
```

**Figure 96: Log Manager Page**

**Table 37 : Log Manager Settings**

<b>Enable Event Notification</b>	Enables Event Notification feature
<b>Via Type</b>	Choose which protocol will be used to connect to the logs server (HTTP or HTTPS).
<b>HTTP/HTTPS Server</b>	Enter the IP address of domain name for the logs server.
<b>HTTP Server Username</b>	Configure the username of your HTTP(s) server
<b>HTTP Server Password</b>	Configure the password of your HTTP(s) server

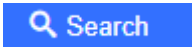
### URL Template

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
- \${CARDID} : Card Number
- \${SIPNUM} : SIP Number

## 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



<div>LiveView</div> <div>Door System Settings</div> <div>System Settings</div> <div>Account</div> <div>Phone Settings</div> <div>Video &amp; Audio Settings</div> <div>Alarm Settings</div> <div>Email &amp; FTP Settings</div> <div>Maintenance</div> <div>Upgrade</div> <div>Reboot &amp; Reset</div> <div>Debug Log</div> <div>Data Maintenance</div> <div>System Health Alert</div> <div>Event Notification</div> <div><b>Event Log</b></div> <div>Certificates</div> <div>Status</div>	<b>Event Log</b>				
	Start Time 2019-04-10 00:00:00 End Time 2019-04-10 14:34:09 All Search				
	No.	Date & Time	Event Type	Username	Card Number (Account) Sip Number
	1	2019-04-10 08:06:02	System Up		
	2	2019-04-10 08:14:55	Call Log(Door Bell Call)		(1)6400
	3	2019-04-10 08:15:13	Visiting Log(Door 1)		(1)6400
	4	2019-04-10 08:15:35	Call Log(Door Bell Call)		(1)4000
	5	2019-04-10 08:15:50	Visiting Log(Door 1)		(1)4000
	6	2019-04-10 08:16:44	Reboot		
	7	2019-04-10 08:17:09	System Up		
	8	2019-04-10 08:25:54	Call Log(Door Bell Call)		(1)4000
	9	2019-04-10 08:26:09	Visiting Log(Door 1)		(1)4000
	10	2019-04-10 08:31:52	System Up		
	11	2019-04-10 08:40:37	Call Log(Door Bell Call)		(1)6400
	12	2019-04-10 10:27:27	Call Log(Door Bell Call)		(1)3004
	13	2019-04-10 10:27:42	Call Log(Door Bell Call)		(1)3004
	14	2019-04-10 10:27:52	Call Log(Door Bell Call)		(2)3004
	15	2019-04-10 10:28:16	Call Log(Door Bell Call)		(1)3004
	16	2019-04-10 10:28:39	Call Out Log		(2)3004
	17	2019-04-10 11:12:21	Call Log(Door Bell Call)		(1)3004
	18	2019-04-10 11:12:35	Call Log(Door Bell Call)		(1)3004

**Figure 97: Event Logs**

For more information about event logs, please visit this [guide](#).

#### Notes:

- The maximum size of log storage space of GDS3710 is about 64M.
- The size of each event log is 48 bytes.
- If the log data exceeded the maximum storage space, then the oldest log will be automatically released which will be 128K of old data.

## Certificates

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

Also users are allowed to configure the device with custom certificate signed by custom CA certificate under the Custom Certificate section.

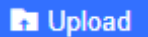
<b>Certificates</b>		
<b>Trusted CA Certificates</b>		
No.	Issued By	Expiration
1		Upload  Delete
2		Upload  Delete
3		Upload  Delete
4		Upload  Delete
5		Upload  Delete
6		Upload  Delete
<b>Custom Certificate</b>		
No.	Issued By	Expiration
1		Upload  Delete

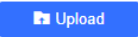

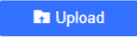

**Figure 98: Upload Certificate files**






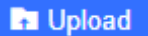
In order to upload your Trusted CA certificate:


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


Trusted CA Certificates			
No.	Issued By	Expiration	
1	-	2018-07-17 15:46:03	 
2			 

User could press  to delete one of the files.

In order to upload your Custom certificate:

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

Custom Certificate			
No.	Issued By	Expiration	
1			 

User could press  to delete one of the files.



## Status

This page displays GDS3710 system and network information.

### Account Status

This page displays of configured accounts’ SIP user ID, SIP server as well as the SIP Registration status, from Account 1 to Account 4.

#### Notes:

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



<div>LiveView</div> <div>Door System Settings</div> <div>System Settings</div> <div>Account</div> <div>Phone Settings</div> <div>Video &amp; Audio Settings</div> <div>Alarm Settings</div> <div>Email &amp; FTP Settings</div> <div>Maintenance</div> <div>Status</div> <div>Account Status</div> <div>System Info</div> <div>Network Info</div>	Account Status			
	Account	SIP User ID	SIP Server	SIP Registration Status
	Account 1	3000	192.168.5.100	Offline
	Account 2	3001	192.168.5.100	Online
	Account 3	3002	192.168.5.187	Offline
	Account 4	3003	192.168.5.187	Offline

Figure 99: System Info Page

## System Info


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

<div>LiveView</div> <div>Door System Settings</div> <div>System Settings</div> <div>Account</div> <div>Phone Settings</div> <div>Video &amp; Audio Settings</div> <div>Alarm Settings</div> <div>Email &amp; FTP Settings</div> <div>Maintenance</div> <div>Status</div> <div>Account Status</div> <div>System Info</div> <div>Network Info</div>	System Info	
	Product Model	GDS3710
	Hardware Version	V1.5A
	Part Number	9650001415A
	Boot Version	1.0.0.30
	Core Version	1.0.5.6
	Base Version	1.0.5.6
	Prog Version	1.0.5.6
	System Uptime	4 hours 6 minutes
	Firmware Status	<div>Press check button and reload page to check firmware availability</div> <div>Check</div>
	System Temperature	41°C (105.8°F)
	Tamper Sensor	Triggered
	Door 1 Ctrl	Untriggered
	Door 2 Ctrl	Untriggered
	Digit Input 1	Untriggered
	Digit Input 2	Untriggered

Figure 100: System Info Page



**Table 38: System Info**

<b>Product Model</b>	Displays the Product Model.
<b>Hardware Version</b>	Displays the Hardware Version.
<b>Part Number</b>	Displays the Part Number.
<b>Boot Version</b>	Displays the Boot Version.
<b>Core Version</b>	Displays the Core Version.
<b>Base Version</b>	Displays the Base Version.
<b>Prog Version</b>	Displays the Prog Version.
<b>System Up Time</b>	Displays the time since the first boot of the GDS3710.
<b>SIP Registration Status</b>	Shows whether the SIP account is registered or not.
<b>Firmware Status</b>	Click the  button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
<b>System Temperature</b>	Shows the current system temperature (in °C and °F).
<b>Tamper Sensor</b>	Shows if the Temper Sensor is triggered or not.
<b>Digit Output</b>	Shows if the Alarm Out is triggered or not. If <b>ALMOUT1 Feature</b> is set to Open Door, then two fields will show up indicating the state of both door 1 and door 2.
<b>Input Digit 1</b>	Shows if alarm IN 1 is triggered.
<b>Input Digit 2</b>	Shows if alarm IN 2 is triggered.

## Network Info

This page displays the network system information of GDS3710.



LiveView

Door System Settings

System Settings

Account

Phone Settings

Video & Audio Settings

Alarm Settings

Email & FTP Settings

Maintenance

Status
 

Account Status

System Info

Network Info

### Network Info

MAC Address	00:0B:82:AB:AE:8A
IP Address Mode	DHCP
IP Address	192.168.5.130
Subnet Mask	255.255.255.0
Gateway	192.168.5.1
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4

Figure 101: Network Info Page

Table 39: Network Info

<b>MAC Address</b>	Displays the GDS3710 MAC Address.
<b>IP Address Mode</b>	Displays the IP address mode used.
<b>IP Address</b>	Displays the IP address of the GDS3710.
<b>Subnet Mask</b>	Displays the Subnet Mask used.
<b>Gateway</b>	Displays the GDS3710 Gateway.
<b>DNS Server 1</b>	Displays the Preferred DNS Server.
<b>DNS Server 2</b>	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](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](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](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](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.

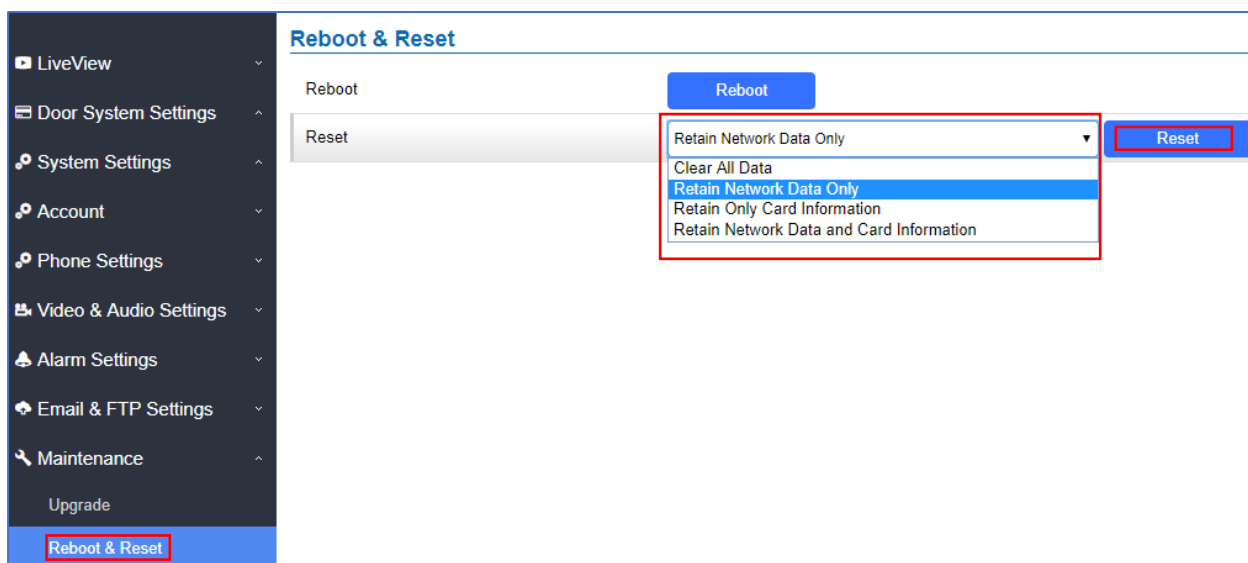


Figure 102: Reset via Web GUI

### 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 103: 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.

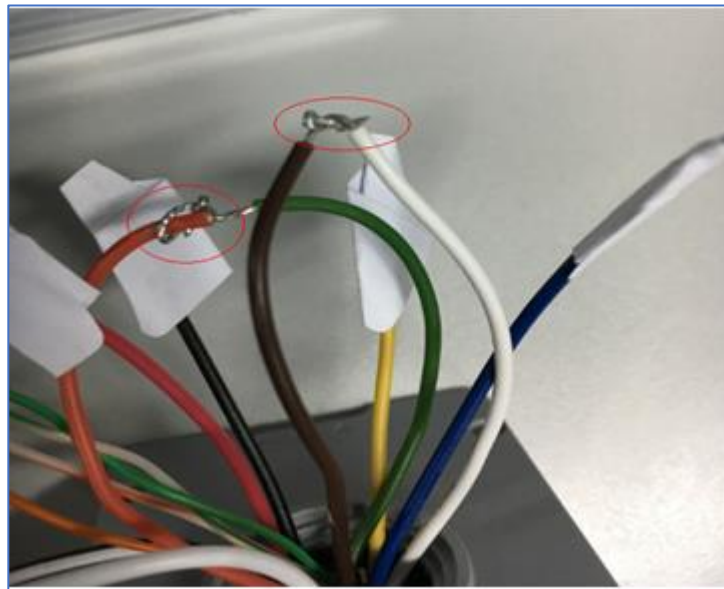


Figure 104: Wiegand Cable Connection

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.

## Restore to Factory Default Via SIP NOTIFY

1. Access your GDS3710 UI by entering its IP address in your favorite browser.
2. Go to Phone Settings # page.
3. Enable “Allow Reset Via SIP NOTIFY” by checking this option. (Default is disabled)
4. Once a **SIP NOTIFY** with “**event: reset**” is received, the GDS3710 will perform factory reset after authentication phase.

**Notes:**

- Received SIP NOTIFY will be first challenged for authentication purpose before taking factory reset action.
- The authentication can be done either using admin password (if no SIP account is configured) or via SIP account credentials (SIP User ID and Password).



## Restore factory password via special key combination

This feature allows customers to reset the device administrator password to factory default via keypad operation through some special key combination.

When performing this operation, ONLY password will be reset back to factory default. All other setting or parameters will NOT be changed and will remain the same. This feature is specially designed for field engineers or technicians when dispatched in field but for some reason the administrator password is not available therefore not able to access the GDS37xx device to do the related maintenance.

Here are the steps to do such password reset operation via keypad:

### Encoding Rules:

Alphabet A – Z mapping to digit 1 – 26 respectively, no difference in lower or up case.

**Table 105: Encoding rule**

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

### Note:

1. MAC address of the GDS37xx (check the sticker at back of the device)
2. Default password of the GDS37xx (check the sticker at the back of the device)
3. Correct decoding the last 6 MAC address into digits (refer to encoding rule)
4. Correct decoding the default password into digits (refer to encoding rule)
5. Finish keypad input within 1 minute

### Operation Steps:

- 1) When device is idle, input the special keypad combination with format: **\*\*\*last\_6\_MAC\*\*#**
- 2) Device will reach restore mode after correct digits in Step 1) entered. The backlight of keypad will flash quickly to tell operator the device is now in password reset/restore mode.
- 3) Operator will enter the correct decoded default password ending with # with format: **default\_password\_code#** via the keypad within 60 seconds.
- 4) If wrong code combination entered, the GDS37xx will beep with error sound (three short beeps) then exit the password reset mode, and the backlight will stop flashing.
- 5) If the correct default password decoded entered within 60 seconds, GDS37xx will play a long beep sound (advising correct operation), the device will reboot itself automatically.



6) If keypad entry time out (not finish the input within 60 seconds), the device will exit this password reset mode automatically and stop the backlight flashing. After successful password reset, operator will then be able to log into the GDS37xx webUI with default password, all the configuration inside the device will be the same and will NOT be changed.

**For example:**

Decoding the string into digits and write to paper before doing the operation:

- Device with last 6 MAC address: 33DDDD
- Decoding the last 6 MAC to digits would be: 334444
- Default password is: xwpxz6AA
- Decoding the default password to digits would be: 2423162426611

1) Enter **\*\*\*334444\*\*#** via keypad, get into the password reset mode, the keypad backlight will flash quickly. 2) Within 60 seconds, enter **2423162426611#**, the device will play one long beep then reboot itself.

2) Wait the device finishing boot up, log in the webUI using the default password, xwpxz6AA



## 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.

