COPYRIGHT

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);

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

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

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

Grandstream GNU GPL related source code can be downloaded from Grandstream website from:
# Table of Contents

## DOCUMENT PURPOSE

## CHANGE LOG

Firmware Version 1.0.7.8 ......................................................... 16
Firmware Version 1.0.7.7 ......................................................... 16
Firmware Version 1.0.7.4 ......................................................... 16
Firmware Version 1.0.5.6 ......................................................... 16
Firmware Version 1.0.5.2 ......................................................... 17
Firmware Version 1.0.4.9 ......................................................... 17
Firmware Version 1.0.3.35 ......................................................... 18
Firmware Version 1.0.3.34 ......................................................... 18
Firmware Version 1.0.3.32 ......................................................... 18
Firmware Version 1.0.3.31 ......................................................... 18
Firmware Version 1.0.3.23 ......................................................... 18
Firmware Version 1.0.3.13 ......................................................... 18
Firmware Version 1.0.2.25 ......................................................... 19
Firmware Version 1.0.2.22 ......................................................... 19
Firmware Version 1.0.2.21 ......................................................... 19
Firmware Version 1.0.2.13 ......................................................... 20
Firmware Version 1.0.2.9 ......................................................... 20
Firmware Version 1.0.2.5 ......................................................... 20
Firmware Version 1.0.1.19 ......................................................... 21

## WELCOME

## PRODUCT OVERVIEW

Feature Highlights ................................................................. 23
Technical Specifications ......................................................... 23

## GETTING STARTED

GDS3710 User Manual
Version 1.0.7.8
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
  Power the unit using PoE ................................................................. 30
  Power the unit using PSU ............................................................... 30

GETTING TO KNOW GDS3710 ............................................................ 32
  Connecting GDS3710 to Network with DHCP Server ................................ 32
    Windows Platform ................................................................. 32
    UPnP .............................................................................. 32
    GS Search .................................................................. 33
    GDS Manager Utility Tool ......................................................... 34
    Apple Platform .................................................................. 35
  Connect to the GDS3710 using Static IP ........................................... 37

GDS3710 APPLICATION SCENARIOS .............................................. 39
  Peering Mode without SIP Server ..................................................... 39
  Peering using SIP Server (UCM6XXX) ................................................ 39
  Using a Network Video Recorder (NVR) .............................................. 40

GDS3710 PERIPHERAL CONNECTIONS .......................................... 42
  Alarm IN/OUT ......................................................................... 43
  Protection Diode .................................................................. 43
  Connection Examples .................................................................. 44
    Wiring Sample using 3rd Party Power Supply .................................. 45
    Wiring Sample using Power Supply for both GDS3710 and Electric Strike ................................................................ 45
    Wiring Sample using PoE to power GDS3710 and 3rd Party Power Supply for Electric Strike .............................................. 46
    Good Wiring Sample for Electric Strike and High-Power Device .......................................................... 47
  Wiegand Module Wiring Examples .................................................... 47
Input example with 3rd party power supply for Wiegand device ............................................. 47
Input example with power supply for both GDS3710 and Wiegand device ................................. 48
Output example with 3rd party power supply for Wiegand device .......................................... 48
Wiegand RFID Card Reader Example ..................................................................................... 49
Siren alarming when door opened abnormally ........................................................................... 49
GDS3710 Connection: IN2 set as Normal Close and “Fail Safe” Electric Strike using 3rd Party Power Supply ........................................................................................................... 50
GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3rd Party Power Supply ................................................................................................................ 50
GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3rd Party Power Supply with Door sensor .......................................................................................... 51

**GDS3710 HOME WEB PAGE** ............................................................................................. 52

GDS3710 Configuration & Language Page .................................................................................. 53

**GDS3710 SETTINGS** ........................................................................................................... 55

Live View Page ....................................................................................................................... 55

Live Snapshot .......................................................................................................................... 55

MJPEG Stream ........................................................................................................................ 58

Door System Settings .............................................................................................................. 61

Basic Settings .......................................................................................................................... 61

Using Alarm Out (COM 1) to Control a Second Door .............................................................. 68

Keep Door Open ...................................................................................................................... 73

Emergency PIN ....................................................................................................................... 75

Card Management .................................................................................................................. 76

Add Users Manually ............................................................................................................... 76

Add Users Automatically ....................................................................................................... 78

Users Operation ..................................................................................................................... 78

Group .................................................................................................................................... 78

Schedule ................................................................................................................................. 79

Holiday .................................................................................................................................. 80

System Settings ..................................................................................................................... 81

Date & Time Settings .............................................................................................................. 81
**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 .................................................................................................... 52  
Table 6: Door System Settings ....................................................................................................... 63  
Table 7: Immediate Open-Door Table ............................................................................................ 73  
Table 8: Schedule Keep Door Open ................................................................................................ 74  
Table 9: Card Info ........................................................................................................................... 77  
Table 10: Add Group ....................................................................................................................... 79  
Table 11: Date & Time ..................................................................................................................... 81  
Table 12: Basic Settings ................................................................................................................ 82  
Table 13: Access Settings .............................................................................................................. 83  
Table 14: User Management .......................................................................................................... 85  
Table 15: SIP Account Basic & Advanced Settings ........................................................................ 87  
Table 16: Phone Settings .............................................................................................................. 91  
Table 17: White List ....................................................................................................................... 93  
Table 18: Video Settings ............................................................................................................... 95  
Table 19: OSD Settings ................................................................................................................ 96  
Table 20: CMOS Settings ............................................................................................................ 97  
Table 21: Audio Settings ............................................................................................................. 98  
Table 22: Motion Detection ........................................................................................................... 101  
Table 23: Digital Input .................................................................................................................. 102  
Table 24: Silently Alarm Mode ..................................................................................................... 103  
Table 25: Hostage Code Alarm .................................................................................................... 103  
Table 26: Tamper Alarm ............................................................................................................... 104  
Table 27: Keypad Input Error Alarm ............................................................................................ 104  
Table 28: Non-Scheduled Access Alarm ...................................................................................... 104  
Table 29: Alarm Actions .............................................................................................................. 107  
Table 30: Alarm Phone List ......................................................................................................... 107  
Table 31: Email Settings - SMTP ............................................................................................... 108  
Table 32: Picture Storage Settings ............................................................................................... 109  
Table 33: FTP Filenames ............................................................................................................. 110  
Table 34: Upgrade ....................................................................................................................... 112  
Table 35: Reset & Reboot ............................................................................................................ 114  
Table 36: Log Manager Settings ................................................................................................. 118  
Table 37: System Info ................................................................................................................ 123  
Table 38: Network Info ............................................................................................................... 124
## Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1:</td>
<td>GDS3710 Package</td>
<td>26</td>
</tr>
<tr>
<td>Figure 2:</td>
<td>GDS3710 Front View</td>
<td>27</td>
</tr>
<tr>
<td>Figure 3:</td>
<td>GDS3710 Back View</td>
<td>27</td>
</tr>
<tr>
<td>Figure 4:</td>
<td>GDS3710 Back Cover Connections</td>
<td>29</td>
</tr>
<tr>
<td>Figure 5:</td>
<td>GDS3710 Back Cover</td>
<td>30</td>
</tr>
<tr>
<td>Figure 6:</td>
<td>Connection Example</td>
<td>30</td>
</tr>
<tr>
<td>Figure 7:</td>
<td>Powering the GDS3710</td>
<td>31</td>
</tr>
<tr>
<td>Figure 8:</td>
<td>Detecting GDS3710 via UPnP</td>
<td>32</td>
</tr>
<tr>
<td>Figure 9:</td>
<td>GDS3710 Login Page</td>
<td>33</td>
</tr>
<tr>
<td>Figure 10:</td>
<td>GS Search Discovery</td>
<td>34</td>
</tr>
<tr>
<td>Figure 11:</td>
<td>GDS3710 Detection</td>
<td>35</td>
</tr>
<tr>
<td>Figure 12:</td>
<td>Apple Safari Settings Page</td>
<td>36</td>
</tr>
<tr>
<td>Figure 13:</td>
<td>Bonjour Setting Page</td>
<td>36</td>
</tr>
<tr>
<td>Figure 14:</td>
<td>Static IP on Windows</td>
<td>38</td>
</tr>
<tr>
<td>Figure 15:</td>
<td>Peering GDS3710 with UCM6XXX</td>
<td>40</td>
</tr>
<tr>
<td>Figure 16:</td>
<td>Peering GDS3710 with GVR3550</td>
<td>41</td>
</tr>
<tr>
<td>Figure 17:</td>
<td>Peripheral Connections for GDS3710</td>
<td>42</td>
</tr>
<tr>
<td>Figure 18:</td>
<td>Alarm_In/Out Circuit for GDS3710</td>
<td>43</td>
</tr>
<tr>
<td>Figure 19:</td>
<td>Protection Diode - Example 1</td>
<td>44</td>
</tr>
<tr>
<td>Figure 20:</td>
<td>Protection Diode - Example 2</td>
<td>44</td>
</tr>
<tr>
<td>Figure 21:</td>
<td>3rd party Power Supply Wiring Sample</td>
<td>45</td>
</tr>
<tr>
<td>Figure 22:</td>
<td>Power Supply used for both GDS3710 and Electric Strike</td>
<td>45</td>
</tr>
<tr>
<td>Figure 23:</td>
<td>Wiring Sample using PoE to power GDS3710 and 3rd party Power Supply for Electric Strike</td>
<td>46</td>
</tr>
<tr>
<td>Figure 24:</td>
<td>Example to Avoid when Powering the Electric Strike</td>
<td>46</td>
</tr>
<tr>
<td>Figure 25:</td>
<td>Electric Strike and High-Power Device Example</td>
<td>47</td>
</tr>
<tr>
<td>Figure 26:</td>
<td>Wiegand Input Example with 3rd party Power Supply</td>
<td>47</td>
</tr>
<tr>
<td>Figure 27:</td>
<td>Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device</td>
<td>48</td>
</tr>
<tr>
<td>Figure 28:</td>
<td>Wiegand Output Wiring Example</td>
<td>48</td>
</tr>
<tr>
<td>Figure 29:</td>
<td>Wiegand RFID Card Reader Example</td>
<td>49</td>
</tr>
<tr>
<td>Figure 30:</td>
<td>Digital Input set as Normal close</td>
<td>50</td>
</tr>
<tr>
<td>Figure 31:</td>
<td>“Fail safe” Electric Strike using 3rd Party Power Supply</td>
<td>50</td>
</tr>
<tr>
<td>Figure 32:</td>
<td>Digital Input set as Normal open</td>
<td>50</td>
</tr>
<tr>
<td>Figure 33:</td>
<td>“Fail Secure” Electric Strike using 3rd Party Power Supply</td>
<td>51</td>
</tr>
<tr>
<td>Figure 34:</td>
<td>“Fail Secure” Electric Strike using 3rd Party Power Supply with Door Sensor</td>
<td>51</td>
</tr>
<tr>
<td>Figure 35:</td>
<td>Home Page: Internet Explorer 11</td>
<td>52</td>
</tr>
<tr>
<td>Figure 36:</td>
<td>Switch Language Page</td>
<td>54</td>
</tr>
<tr>
<td>Figure 37:</td>
<td>Live View Page: Google Chrome</td>
<td>55</td>
</tr>
<tr>
<td>Figure 38:</td>
<td>MJPEG Authentication Mode</td>
<td>56</td>
</tr>
<tr>
<td>Figure 39:</td>
<td>Snapshot admin credential</td>
<td>56</td>
</tr>
</tbody>
</table>
Figure 40: Snapshot view using secured MJPEG authentication Mode ........................................... 57
Figure 41: Snapshot view using Basic Authentication Mode ......................................................... 58
Figure 42: MJPEG Authentication Mode ....................................................................................... 58
Figure 43: MJPEG view admin credential .................................................................................... 59
Figure 44: MJPEG live view using secured MJPEG Authentication Mode .................................... 60
Figure 45: MJPEG view using Basic MJPEG Authentication Mode ............................................. 61
Figure 46: Door System Settings Page ......................................................................................... 62
Figure 47: Alarm_Out1 Feature ..................................................................................................... 69
Figure 48: Universal Local PIN ...................................................................................................... 70
Figure 49: Remote PIN to Open Door ........................................................................................... 71
Figure 50: Right of Card and Private PIN .................................................................................... 72
Figure 51: Immediate Open Door ................................................................................................. 73
Figure 52: Schedule Open Door ................................................................................................... 74
Figure 53: Edit Schedule ................................................................................................................ 75
Figure 54: Keep Door Open – Emergency PIN ............................................................................ 75
Figure 55: Card Management ....................................................................................................... 76
Figure 56: Card Info ..................................................................................................................... 77
Figure 57: Add Group .................................................................................................................... 79
Figure 58: Groups List .................................................................................................................. 79
Figure 59: Edit Schedule Time ..................................................................................................... 80
Figure 60: Edit Holiday Time ........................................................................................................ 80
Figure 61: Date & Time Page ........................................................................................................ 81
Figure 62: Basic Settings Page ...................................................................................................... 82
Figure 63: Access Settings Page .................................................................................................... 83
Figure 64: User Management Page .............................................................................................. 85
Figure 65: Password Recovery Email .......................................................................................... 86
Figure 66: SIP Account Settings Page ......................................................................................... 87
Figure 67: Phone Settings Page ................................................................................................... 91
Figure 68: White List Page ............................................................................................................ 93
Figure 69: Click-To-Dial ............................................................................................................... 93
Figure 70: Video Settings Page .................................................................................................... 94
Figure 71: OSD Settings Page ....................................................................................................... 96
Figure 72: CMOS Settings Page .................................................................................................... 97
Figure 73: Audio Settings Page ..................................................................................................... 98
Figure 74: Privacy Masks Configuration Page ............................................................................. 99
Figure 75: Events Page ................................................................................................................ 100
Figure 76: Region Config ............................................................................................................. 101
Figure 77: Digital Input ................................................................................................................ 102
Figure 78: Alarm Schedule .......................................................................................................... 105
Figure 79: Edit Schedule .............................................................................................................. 105
Figure 80: Alarm Action .............................................................................................................. 106
Figure 81: Edit Alarm Action....................................................................................................... 106
Figure 82: Alarm Phone List

Figure 83: Email Settings - SMTP Page

Figure 84: Picture Storage Settings

Figure 85: FTP filenames

Figure 86: Upgrade Page

Figure 87: Reset & Reboot Page

Figure 88: Debug Log Page

Figure 89: Data Maintenance Page

Figure 90: System Health Alert Page

Figure 91: Log Manager Page

Figure 92: Event Logs

Figure 93: Upload Certificate files

Figure 94: System Info Page

Figure 95: System Info Page

Figure 96: Network Info Page

Figure 97: Reset via Web GUI

Figure 98: Wiegand Interface Cable

Figure 99: Wiegand Cable Connection

Table 100: Encoding rule
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 1.0.7.8

- 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 3rd party Software Integration. [Event Notification]

**Firmware Version 1.0.2.22**

- No major changes.

**Firmware Version 1.0.2.21**

- Allow config and call IP address format on SIP field when dialing the Virtual Number. [SIP Number]
- Added “Silent Alarm” Mode. [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]
- Expended 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]

- Added enforcement that when admin password is changed via WebGUI, user has to fill in a Valid Email Account to retrieve the email before the new admin password taking effect. [User Management]

**Firmware Version 1.0.2.13**

- Added support of ONVIF Profile S.
- Added “Privacy Mask” support in Motion Detection Setting. [Privacy Masks]
- Updated OCX plugin engine to Version 3.1.0.74
- Added DTMF Open Door control option in WebGUI [Enable DTMF Open Door]
- Added HTTP API support [GDS3710 HTTP API].
- Optimized HTTP API for Card Management.
- Added “Enable Blue Doorbell Light” option in the webGUI. [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 3rd party applications and other surveillance systems.

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

Feature Highlights

The following table contains the major features of the GDS3710.

Table 1: GDS3710 Features in a Glance

<table>
<thead>
<tr>
<th>Feature Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>• High-performance streaming server allowing multiple simultaneous streaming session accesses.</td>
</tr>
<tr>
<td>• 2 Megapixel Progressive Scan CMOS, 1920H x 1080V.</td>
</tr>
<tr>
<td>• Broad interoperability with most 3rd party SIP/VOIP devices and leading SIP/NGN/IMS platforms.</td>
</tr>
<tr>
<td>• 2 Channels Input/Output alarm.</td>
</tr>
<tr>
<td>• Wiegand (26 bits) Input and Output.</td>
</tr>
<tr>
<td>• RFID card reader.</td>
</tr>
<tr>
<td>• Weather proof, vandal resistant.</td>
</tr>
</tbody>
</table>

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

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

Triggered upon events, sent via email and/or FTP.

### Multi-stream Resolution

High-performance streaming server allowing multiple simultaneous accesses:

- **Primary video stream**: 1920 x 1080 resolution for continuous full HD recording.
- **Secondary video stream**: 640 x 480 resolution for SIP/VoIP video calls.
- **Third video stream**: 320 x 240 resolution for smartphone Apps.

### Network Protocols

TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS local upload and mass provisioning using TR-069 (pending), ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP.

### SIP/VoIP Support

Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.

### Voice Codecs

G.711μ/a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.

### QoS

Layer 2 QoS (802.1Q, 802.1P) and Layer 3 QoS (ToS, DiffServ, MPLS).

### Security

User and administrator level access control (pending), MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.

### Upgrade / Provisioning

Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 (Pending) or AES encrypted XML configuration file.

### Audio Input

Built-in Digital Microphone, up to 1.5m with AEC.

### Audio Output

Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3m.

### Keypad / Buttons

12-key touchpad plus a capacitive doorbell button, each with individual LED illumination.

### RFID

125KHz: EM4100 (1 RFID card and 1 RFID key fob included).

### Alarm Input

Yes, 2 channels, Vin < 15V, for door sensor or other devices.

### Alarm Output

Yes, 2 channels, 125VAC/0.5A, 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch or other devices.

### Network Interface

10M/100M auto-sensing.

### Expansion Interface

Wiegand (26 bits) input and output.

### Dimensions and Weight

173mm(H) x 80mm(W) x 36mm(D).

0.6 Kg.

### Power Supply

PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).

### Interoperability

ONVIF (Profile S).

### Ingress Protection

Weather proof, vandal resistant, with support for extra back reinforcing metal plate.

### Temperature and Humidity

Operation: -30°C to 60°C (-22°F to 140°F)

Storage: -35°C to 60°C (-31°F to 140°F)
<table>
<thead>
<tr>
<th>Protection Class</th>
<th>Humidity: 10% to 90% Non-condensing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>FCC: Part 15 subpart B Class B; Part 15 C; MPE</td>
</tr>
<tr>
<td></td>
<td>CE: EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311</td>
</tr>
<tr>
<td></td>
<td><strong>RCM</strong>: AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1</td>
</tr>
<tr>
<td></td>
<td><strong>IC</strong>: ICES-003; RSS310</td>
</tr>
</tbody>
</table>
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

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

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>
<thead>
<tr>
<th>Jack</th>
<th>Signal</th>
<th>Function</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>J2 (Basic)</strong></td>
<td><strong>3.81mm</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TX+</td>
<td>3.81mm</td>
<td>Ethernet</td>
<td>Orange / White</td>
</tr>
<tr>
<td>TX-</td>
<td>3.81mm</td>
<td>PoE</td>
<td>Orange</td>
</tr>
<tr>
<td>RX+</td>
<td>3.81mm</td>
<td>Ethernet</td>
<td>Green / White</td>
</tr>
<tr>
<td>RX-</td>
<td>3.81mm</td>
<td>PoE</td>
<td>Green</td>
</tr>
<tr>
<td>PoE_SP2</td>
<td>3.81mm</td>
<td>PoE</td>
<td>Blue + Blue/White</td>
</tr>
<tr>
<td>PoE_SP1</td>
<td>3.81mm</td>
<td>PoE</td>
<td>Brown + Brown/White</td>
</tr>
<tr>
<td>GND</td>
<td>3.81mm</td>
<td>Power</td>
<td>DC 12V, 1A Minimum</td>
</tr>
<tr>
<td>12V</td>
<td>3.81mm</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>J3 (Advanced)</strong></td>
<td><strong>3.81mm</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GND</td>
<td>3.81mm</td>
<td>Alarm</td>
<td>Alarm GND</td>
</tr>
<tr>
<td>ALARM1_IN+</td>
<td>3.81mm</td>
<td>Alarm</td>
<td>Vin&lt;15V</td>
</tr>
<tr>
<td>ALARM1_IN-</td>
<td>3.81mm</td>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td>ALARM2_IN+</td>
<td>3.81mm</td>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td>ALARM2_IN-</td>
<td>3.81mm</td>
<td>Alarm</td>
<td></td>
</tr>
<tr>
<td>NO1</td>
<td>3.81mm</td>
<td>Alarm</td>
<td>Relay: 30VDC/2A; 125VAC/0.5A</td>
</tr>
<tr>
<td>COM1</td>
<td>3.81mm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO2</td>
<td>3.81mm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COM2</td>
<td>3.81mm</td>
<td>Electric</td>
<td>For &quot;Fail Secure&quot; (Locked when Power Lost) Strike, connect COM2 &amp;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lock</td>
<td>NO2.</td>
</tr>
<tr>
<td>NC2</td>
<td>3.81mm</td>
<td></td>
<td>For &quot;Fail Safe&quot; (Open when No Power) Magnetic Lock, connect COM2 &amp;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NC2. Relay: 30VDC/2A; 125VAC/0.5A</td>
</tr>
<tr>
<td><strong>J4 (Special)</strong></td>
<td><strong>2.0mm</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GND</td>
<td>2.0mm</td>
<td>Wiegand</td>
<td>Black Both Input and Output MUST be connected</td>
</tr>
<tr>
<td>WG_D1_OUT</td>
<td>2.0mm</td>
<td>Output</td>
<td>GDS3710 function as Output of Card Reader, Connect Pin 1, 2, 3</td>
</tr>
<tr>
<td>WG_D0_OUT</td>
<td>2.0mm</td>
<td>Signal</td>
<td></td>
</tr>
<tr>
<td>LED</td>
<td>2.0mm</td>
<td>Wiegand</td>
<td>Blue For External Card Reader; Or GDS3710 as Receiver Only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output</td>
<td></td>
</tr>
<tr>
<td>WG_D1_IN</td>
<td>2.0mm</td>
<td>Input</td>
<td>White For External Card Reader Connect Pin 1,4,5,6,7,8</td>
</tr>
<tr>
<td>WG_D0_IN</td>
<td>2.0mm</td>
<td>Signal</td>
<td></td>
</tr>
<tr>
<td>BEEP</td>
<td>2.0mm</td>
<td>Wiegand</td>
<td>Yellow For External Reader Only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Output</td>
<td></td>
</tr>
<tr>
<td>5V</td>
<td>2.0mm</td>
<td>Wiegand</td>
<td>Red For External Card Reader Only, 12VDC powered External Card Reader must use own power source, can NOT use this Pin.</td>
</tr>
</tbody>
</table>
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.
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.

![Diagram of Ethernet cable pin outs]

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.

**Option B:**
**DC12V, 1A minimum**
Power Source (not provided)

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]

GDS3710 User Manual
Version 1.0.7.8
3. Click on the displayed icon of related GDS3710, the default browser (e.g.: Internet Explorer, Firefox or Chrome) will open and connect directly to the login webpage.

![GDS3710 Login Page]

**Figure 9: GDS3710 Login Page**

4. Once logged in, the prompt message will display asking for plug-in installation.

5. Disable security or antivirus software, download and install the plug-in, close and open the browser again, the embedded video will be displayed if clicking the “LiveView” and pressing the stream number.

**GS Search**

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

1. Download the GS Search utility tool from Grandstream website using the following link: [http://www.grandstream.com/sites/default/files/Resources/GS_Search.zip](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 the button to start the discovery for Grandstream devices.

4. The detected devices will appear in the output field like below.
5. Double click on a device to access its webGUI.

**GDS Manager Utility Tool**

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

1. Download the GDS Manager utility tool from Grandstream website using the following link:
   
   http://www.grandstream.com/sites/default/files/Resources/gdsmanager.zip

2. Install and run the Grandstream GDS Manager, a client/server architecture application, the server should be running first, then GDSManager (client) later:

3. On the GDS Manager access to Device → Search and Click on the button to start device detection

4. The detected devices will appear in the output field like below:
5. Double click the column of the detected GDS3710, the browser will automatically open and show the device’s web configuration page.

6. The browser will ask for plug-in if not installed, please authorize the installation of the plug-in.

7. Enter the administrator user name and password to access the Web Configuration Interface, the default admin username is “admin” and the default random password can be found at the sticker on the GDS3710.

8. The plug-in can be downloaded from the GDS3710 Web GUI.

**Apple Platform**

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

1. Open Safari, select “Advanced” to open the Advanced Setting.

2. Click “Include Bonjour in the Bookmarks menu” and “Include Bonjour in the Favorites bar” then close the setting page and back to Safari.
3. Bonjour will now display embedded at Safari. Select “Bonjour” pull-down menu and select “Webpages”, the related device like GDS3710 will be there.

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:
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).
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.

![Alarm_In/Out Circuit for GDS3710](image)

**Figure 18: Alarm_In/Out Circuit for GDS3710**

**Notes:**

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

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

- The Alarm_In circuit, if there is any voltage change between 3V and 15V, as specified in the table above, the GDS3710 Alarm_In port will detect it and trigger the action and event.

- Higher voltage and wrong polarity connection are prohibited because this will damage the devices.

**Protection Diode**

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

**Note:** power polarity connection: Diode: SS24 or If>=2A, Vr>=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 3rd Party Power Supply

Figure 21: 3rd party Power Supply Wiring Sample

Wiring Sample using Power Supply for both GDS3710 and Electric Strike

Figure 22: Power Supply used for both GDS3710 and Electric Strike
Wiring Sample using PoE to power GDS3710 and 3\textsuperscript{rd} Party Power Supply for Electric Strike

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

\textbf{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

Wiegand Module Wiring Examples

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

Input example with 3rd party power supply for Wiegand device
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

![Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device](image)

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

Output example with 3rd party power supply for Wiegand device

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

**Wiegand RFID Card Reader Example**

![Wiegand RFID Card Reader Example](image)

**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 DIx 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.

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 3rd Party Power Supply**

![Figure 30: Digital Input set as Normal close](image)

**GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3rd Party Power Supply**

![Figure 32: Digital Input set as Normal open](image)
Figure 33: “Fail Secure” Electric Strike using 3rd Party Power Supply

GDS3710 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3rd Party Power Supply with Door sensor

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

![Home Page](image)

**Figure 35: Home Page: Internet Explorer 11**

<table>
<thead>
<tr>
<th>Number</th>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LiveView</td>
<td>Access to live view stream page.</td>
</tr>
<tr>
<td>2</td>
<td>Door System Settings</td>
<td>Access to “Door System Settings” page.</td>
</tr>
<tr>
<td>3</td>
<td>System Settings</td>
<td>Access to “System Settings” page.</td>
</tr>
<tr>
<td>4</td>
<td>Account</td>
<td>Access to “Account” configuration page.</td>
</tr>
<tr>
<td>5</td>
<td>Phone Settings</td>
<td>Access to “Phone Settings” configuration page.</td>
</tr>
<tr>
<td></td>
<td><strong>Video &amp; Audio Settings</strong></td>
<td>Access to “Video &amp; Audio settings” page.</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>7</td>
<td><strong>Alarm Settings</strong></td>
<td>Access to “Alarm settings” page.</td>
</tr>
<tr>
<td>8</td>
<td><strong>Email &amp; FTP Settings</strong></td>
<td>Access to “Email &amp; FTP Settings” page.</td>
</tr>
<tr>
<td>9</td>
<td><strong>Maintenance</strong></td>
<td>Access to “Maintenance” page.</td>
</tr>
<tr>
<td>10</td>
<td><strong>Status</strong></td>
<td>Click to enter “Status” page.</td>
</tr>
<tr>
<td>11</td>
<td><strong>Play/Stop</strong></td>
<td>Start/Stop the video stream in the web page. (Internet Explorer 11)</td>
</tr>
<tr>
<td>12</td>
<td><strong>Stream 1</strong></td>
<td>Play the primary stream.</td>
</tr>
<tr>
<td>13</td>
<td><strong>Stream 2</strong></td>
<td>Play the secondary stream.</td>
</tr>
<tr>
<td>14</td>
<td><strong>Stream 3</strong></td>
<td>Play the third stream.</td>
</tr>
<tr>
<td>15</td>
<td><strong>Window size</strong></td>
<td>Resize the window. (Internet Explorer 11)</td>
</tr>
<tr>
<td>16</td>
<td><strong>Audio</strong></td>
<td>Click to mute / unmute the audio. (Internet Explorer 11)</td>
</tr>
<tr>
<td>17</td>
<td><strong>Snapshot</strong></td>
<td>Click to take a snapshot. (Internet Explorer 11)</td>
</tr>
<tr>
<td>18</td>
<td><strong>Recording</strong></td>
<td>Click to start recording. (Internet Explorer 11)</td>
</tr>
<tr>
<td>19</td>
<td><strong>File Path Saved</strong></td>
<td>Click to access Record and Capture paths. (Internet Explorer 11)</td>
</tr>
<tr>
<td>20</td>
<td><strong>Logout</strong></td>
<td>Logout from the web page.</td>
</tr>
<tr>
<td>21</td>
<td><strong>Language</strong></td>
<td>Select the webpage language.</td>
</tr>
</tbody>
</table>

**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 36: 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.

![Live View Page: Google Chrome](image)

Figure 37: 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**
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.

3. The browser will show one frame of the video (720p) as a snapshot.
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 41: 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**

<table>
<thead>
<tr>
<th>Access Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MJPEG Authentication Mode</strong></td>
</tr>
<tr>
<td>Challenge+Response</td>
</tr>
<tr>
<td>Challenge+Response</td>
</tr>
<tr>
<td>Basic</td>
</tr>
</tbody>
</table>

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 43: MJPEG view admin credential](image)
3. The browser will show MJPEG stream (720p).

![Figure 44: MJPEG live view using secured MJPEG Authentication Mode](image)

**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 45: MJPEG view using Basic MJPEG Authentication Mode

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

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

**Door System Settings**

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

**Basic Settings**
Figure 46: Door System Settings Page
### Table 6: Door System Settings

<table>
<thead>
<tr>
<th>ALMOUT1 Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALMOUT1 Feature</td>
<td>This option allows to choose to use Alarm_Out (COM1) interface for either as alarm out with 3rd party device, or to control a second door “Door 2” (the two functions are mutual exclusive). When option “Open Door” is selected, will enable GDS3710 to control the operation of two doors via RFID, local and remote PINs.</td>
</tr>
<tr>
<td>ALMOUT1 Status</td>
<td>Select Normal Open or Normal Close depending on the lock used.</td>
</tr>
<tr>
<td>Delay before Unlock (s)</td>
<td>Device will open door after specified delay (in seconds) when user issuing the authorization.</td>
</tr>
<tr>
<td>Unlock Holding Time (s)</td>
<td>Configures the lock holding time, in seconds (default value is 5 seconds). Device will hold the door unlocked for this specified duration. Range: 1-20 seconds.</td>
</tr>
<tr>
<td>Minimum Interval of Swiping Card (ms)</td>
<td>Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms.</td>
</tr>
<tr>
<td>Number of Snapshots when Door Opened</td>
<td>Define number of snapshot to be sent by the GDS (via FTP or Email) Maximum up to 4 screenshots.</td>
</tr>
<tr>
<td>Snapshot when Door Opened</td>
<td>User can choose to email the snapshot when door is opened without sending the snapshots via FTP to the FTP server.</td>
</tr>
<tr>
<td>Snapshot when Doorbell Pressed</td>
<td>User can choose to email the snapshot when doorbell pressed without sending the snapshots via FTP to the FTP server.</td>
</tr>
<tr>
<td>Call Mode</td>
<td>Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3710 keypad.</td>
</tr>
<tr>
<td>Doorbell Call Out Account</td>
<td>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.</td>
</tr>
<tr>
<td>Doorbell Mode</td>
<td>Configures the action to be taken when the doorbell is pressed, three options are available:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Call Doorbell Number</strong>: when Doorbell is pressed, a call will be made to the “Number Called When Door Bell Pressed”</td>
</tr>
<tr>
<td></td>
<td>• <strong>Control Doorbell Output (Digital Output 1)</strong>: when Door Bell is pressed electronic lock for Output 1 is opened.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Both of Above</strong>: When selected, both Call Doorbell Number and Control Doorbell Output options are enabled.</td>
</tr>
</tbody>
</table>
### Door Bell Call Mode

Select the ring strategy for the Numbers Called when pressing the Door Bell button to be either **Serial** or **Parallel**:

- **Serial Hunting**: the configured extensions and/or IP addresses will ring one after one by order.
- **Parallel Hunting**: The configured extensions and/or IP addresses will ring simultaneously (up to 4 simultaneous SIP calls).

### Number Called When Door Bell Pressed

Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed:

- **SIP Server mode**:
  - The field can be configured to store multiple one or multiple SIP extensions, if configured with multiple extensions (ex: 1001, 1002, 1003), separated with "," the GDS3710 will ring one extension after the other in a **Serial Hunting Mode** (GDS will ring each extension by default 15 seconds, this can be changed on the Ring Timeout) or ring them simultaneously in **Parallel Hunting Mode**.
  - When using UCM, users can also configure there a Ring Group extension (6400 for example) that will ring multiple extensions simultaneously, or one by one depending on the Ring Group ring strategy.
  - If all phones are GXP21XX, the phone will stream the video frame by frame and users can open door either by pressing `Remote_PIN#` or by pressing Open Door button if already configured.
  - If early medial is enabled on phone side, user can send the PIN code using the Open-Door button before answering the call (Of course users can open the door also after answering the call).

- **Peering mode**:
  - User should configure multiple IP addresses of phones instead of SIP extensions, when Door Bell pressed the GDS3710 will ring the configured IP Addresses in **Serial or Parallel Mode** according to Doorbell Call Mode strategy.
  - If early media is enabled, the GXV32XX will receive the video stream while it is ringing, and user can open door by pressing the Open-Door button if already configured (Of course users can open the door also after answering the call).
- GXP21XX phones receive the GDS3710 video using JPEG streaming this means that it will receive video if early media is enabled or disabled.

**Note:** This field supports a Maximum of 256 characters.

<table>
<thead>
<tr>
<th>Maximum Number of Dialed Digits</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Key Input Timeout(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Press Doorbell Schedule</td>
<td>Configure a schedule for the Doorbell button, once configured, the doorbell with turn ON/OFF based on configured schedule. Default setting is “All Day”.</td>
</tr>
</tbody>
</table>
| Remote PIN to Open the Door     | Configures PIN code stored in the GDS3710, remote SIP phone needs to input and match this PIN (the PIN is sent via DTMF while in call) so that the GDS3710 can open the door.

**Note:** 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. |

<table>
<thead>
<tr>
<th>Local PIN Type</th>
<th>Three options are available: Private Card PIN, Unified PIN or Card and Private PIN.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Private PIN:</strong> 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 [<em>Virtual Number</em>Private PIN#].</td>
</tr>
<tr>
<td></td>
<td><strong>Notes:</strong> 1. When Local PIN type is set to <strong>private PIN</strong>, users can also open the door by swiping their cards. 2. If “Disable Keypad SIP Number Dialing” is checked, users will be able to open door using private PIN with following sequence [Private PIN#].</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Door can still be opened by <strong>Card</strong> and with the sequence [<em>Virtual Number</em>Private PIN#].</td>
</tr>
</tbody>
</table>
For more details and conditions, refer to [Disable Keypad SIP Number Dialing].

- **Unified PIN**: Means all members share a same PIN to unlock the door. Users need to enter the following sequence from the GDS3710 keypad to open the door [*Local PIN to Open the Door#*].

- **Card & Private PIN**: Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence [Swipe the card + * Private PIN#].

| Local PIN to Open the Door | Configures PIN stored in GDS3710, input locally this PIN on the GDS3710 keypad will unlock the door. This feature needs **Private PIN**, means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3710 to open the door [*Virtual Number*Private PIN#].

**Note**: When local PIN type is set to private card PIN, users can also open the door by swiping their cards.

| Local PIN to Open Door Schedule | 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”.

| Enable DTMF Open Door | When enabled, remote SIP phones can open the door while in call by entering the remote PIN code configured (the PIN code is sent via DTMF). Default settings is disabled.

| Enable Guest PIN | Enables password entry for guests.

| Guest PIN | Configures the password that will be used by guests.

| Guest PIN Start Time | Selects the start time when the Guest PIN start to take effect.

| Guest PIN End Time | Selects the end time when the Guest PIN will stop working.

| Disable Auto Answer | If checked, GDS3710 will not answer incoming calls automatically, users can press any key to answer the call. Default setting in unchecked.

| Enable Doorbell Button to Hang up Call | If checked, Users can hang up an active call when pressing the doorbell button. Enabled by default.

| Disable Keypad (except the Doorbell Button) | When checked the Keypad will be disabled, only Door Bell button can be pressed.
| **Enable On Hook After Remote Door Opened** | When checked calls will be disconnected automatically 5 seconds after the remote open door event. |
| **Enable HTTP API Remote Open Door** | Enabling this option allows to use HTTP API command to open the door remotely. **Important note:** We will not be responsible for any security problems resulting from opening the HTTP API remote function, this option is disabled by default and the user should enable it while knowing how to mitigate the risk. |
| **Disable Keypad SIP Number Dialing** | When Keypad SIP number Dialing disabled, device will interpret each digit entry as private-password open door request after pressing #. **Notes:**  
  - “Local PIN Type” should choose “Private PIN”.  
  - Dial keypad to make SIP call will NOT work (except for doorbell button call).  
  - Private PIN must be **UNIQUE** 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. |
| **Enable Card Issuing Mode** | Enables RFID card issuing/program into the GDS3710. When selected sweeping an RFID card into the GDS3710 will add card information into. [Card Management] |
| **Card issuing State Expire Time(m)** | Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes). |
| **Enable Key Blue Light** | When checked, the blue light will be activated when pressing the GDS3710 Keys. |
| **Enable Background Light** | When checked, the background light will turn on once clicking the GDS3710 Keys. |
| **Enable Doorbell Blue Light** | 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. |
| **Enable Keypad Blue Light** | 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. |
| **Central Mode** | If enabled, Group/Schedule/Holiday can only be synchronized from the Central (GDS Manager), local configuration will not be allowed. |
If disabled, only local configuration from GDS3710 is allowed.

**Key Tone Type**

- **Default**: Beeps will be played when pressing the GDS3710 keys.
- **DTMF**: Tones will be played when pressing the GDS3710 keys.
- **Mute**: No sound will be played when pressing keys.

**Enable Wiegand Input**

This option needs to be enabled when GDS is connected to the wiegand output device (RFID card reader for example)

**Wiegand Output**

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 3rd 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.
• **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 3rd 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:**

![Figure 48: Universal Local PIN](image)

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.
Figure 49: Remote PIN to Open Door
• **Private PIN or Card & Private PIN:**

![Add Card Info](image)

**Figure 50: 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 OPERATON** 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)

<table>
<thead>
<tr>
<th>Keep Door Open</th>
<th>Immediate Open Door</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval of Keep Door Open (min)</td>
<td>5</td>
</tr>
</tbody>
</table>

Figure 51: Immediate Open Door

Table 7: Immediate Open-Door Table

<table>
<thead>
<tr>
<th>Keep Door Open</th>
<th>Select the Keep Door Open mode.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval of Keep Door Open (min)</td>
<td>Set the amount of time in minutes where the door will keep opened. Click to open door immediately.</td>
</tr>
</tbody>
</table>

**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)

Table 8: Schedule Keep Door Open

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

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

**Figure 55: 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.
### Figure 56: Card Info

<table>
<thead>
<tr>
<th>Username</th>
<th>Configures the username to identify the user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private PIN</td>
<td>Specifies a specific password to unlock the door.</td>
</tr>
<tr>
<td>Gender</td>
<td>Selects a gender, either Male or Female.</td>
</tr>
<tr>
<td>ID Number</td>
<td>Enters an ID number (This number is set by the admin to identify each user uniquely).</td>
</tr>
<tr>
<td>Card Number</td>
<td>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.</td>
</tr>
<tr>
<td>Valid Start Date</td>
<td>Configures the start date of validity of the RFID card.</td>
</tr>
<tr>
<td>Valid End Date</td>
<td>Configures the End date of validity of the RFID card.</td>
</tr>
<tr>
<td>Virtual Number</td>
<td>When dialing directly from the keypad, the GDS3710 accepts only Virtual number to identify a user, once the Virtual number is typed followed by # key, the SIP Number will be dialed.</td>
</tr>
</tbody>
</table>
| SIP Number  | Configures the SIP Number which is mapped with virtual number. Once the virtual number is dialed the GDS3710 will send an INVITE to the SIP Number.  
**Note:** The SIP Number can be configured with an extension/phone number or IP address. Example: 192.168.5.124 |
<table>
<thead>
<tr>
<th>Call Out Account</th>
<th>Select the Account from which the GDS3710 will call the User SIP Number when dialing from the keypad. Default is Auto.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cellphone</td>
<td>Configures cellphone of the user.</td>
</tr>
<tr>
<td>Group</td>
<td>Specifies to which group the user will be added.</td>
</tr>
<tr>
<td>Schedule</td>
<td>Specifies the schedule that will be assigned to the user.</td>
</tr>
<tr>
<td>Right of Card and Private PIN</td>
<td>Select the doors that can be accessed by user.</td>
</tr>
<tr>
<td>Enable</td>
<td>Enable/Disable the RFID card.</td>
</tr>
</tbody>
</table>

**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 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.
Figure 57: Add Group

Table 10: Add Group

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

The following screenshots display the list of the created groups.

Figure 58: 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.
**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.
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.

![Date & Time Page](image)

**Figure 61: Date & Time Page**

**Table 11: Date & Time**

<table>
<thead>
<tr>
<th><strong>System Time</strong></th>
<th>Displays the current system time.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow DHCP Option 42 to override NTP server</td>
<td>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”.</td>
</tr>
<tr>
<td>Sync PC</td>
<td>Clicks to synchronize current time with the computer.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Selects from drop down menu the preferred time zone.</td>
</tr>
<tr>
<td>Enable Daylight Saving Time</td>
<td>Enables Daylight Saving Time.</td>
</tr>
<tr>
<td>Start time</td>
<td>Selects the Start time of DST.</td>
</tr>
<tr>
<td>End Time</td>
<td>Selects DST end time.</td>
</tr>
<tr>
<td>Enable NTP</td>
<td>Enables NTP to synchronize device time.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Configures the domain name of NTP server.</td>
</tr>
<tr>
<td>Update Interval</td>
<td>Configures the Interval (in minutes) to retrieve updates from the NTP server.</td>
</tr>
</tbody>
</table>
Network Settings

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address Mode</td>
<td>Selects DHCP or Static IP. Default DHCP. (Static recommended)</td>
</tr>
<tr>
<td>IP Address</td>
<td>Configures the Static IP of the GDS3710.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Configures the Associated Subnet Mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Configures the Gateway IP address.</td>
</tr>
<tr>
<td>DNS Address Type</td>
<td>Specifies the DNS type used: Dynamic DNS or Static DNS.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Configures DNS Server 1 IP address.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Configures DNS Server 2 IP address.</td>
</tr>
<tr>
<td>Enable LLDP</td>
<td>Controls the LLDP (Link Layer Discovery Protocol) service. Default setting is “Enabled”.</td>
</tr>
<tr>
<td>Layer 2 QoS 802.1Q/VLAN Tag</td>
<td>Assigns the VLAN Tag of the Layer 2 QoS packets.</td>
</tr>
<tr>
<td>Layer 2 QoS 802.1p Priority Value</td>
<td>Assigns the priority value of the Layer2 QoS packets.</td>
</tr>
</tbody>
</table>

Notes:
• If the GDS3710 is behind SOHO (Small Office Home Office) router with port forwarding configured for remote access, static IP should be used to avoid IP address changes after router reboot.

• TCP port above 5000 is suggested to Port forward HTTP for remote access, due to some ISP would block port 80 for inbound traffic. For example, change the default HTTP port from 80 to 8088, to make sure the TCP port will not be blocked.

• In addition to HTTP port, RTSP port is also required to configure via port forwarding, so that the remote party can view the video stream.

• If the default TCP port 80 is changed to port “A”, then RTSP port should be “2000+A” (changed from default TCP 554). Both TCP port “A” and “2000+A” should be configured for port forwarding in the router. For example, of the HTTP port is changed to 8088, the RTSP port should be 10088, both TCP ports 8088 and 10088 should be configured for port forwarding to have remote GDS3710 access: 8088 for web portal, and 10088 for video streaming.

Access Settings

This page configures the GDS3710 access control parameters.

![Access Settings Page]

Figure 63: Access Settings Page

<table>
<thead>
<tr>
<th>Table 13: Access Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web Access Mode</strong></td>
</tr>
<tr>
<td><strong>Web Access Port</strong></td>
</tr>
<tr>
<td><strong>MJPEG Authentication Mode</strong></td>
</tr>
<tr>
<td><strong>RTSP Port</strong></td>
</tr>
<tr>
<td><strong>User Login Timeout(min)</strong></td>
</tr>
<tr>
<td><strong>Maximum Number of Login Attempts</strong></td>
</tr>
<tr>
<td><strong>Locking Time of Login Error (m)</strong></td>
</tr>
<tr>
<td><strong>Disable Web Access</strong></td>
</tr>
<tr>
<td><strong>Enable UPnP Discovery</strong></td>
</tr>
<tr>
<td><strong>Enable Anonymous LiveView</strong></td>
</tr>
</tbody>
</table>
3. To retrieve video stream via RTSP, users can use the following format: `rtsp://IP_GDS3710:Port/X` where X=0,4,8 for 1st, 2nd, 3rd streams respectively.

### Enable SSH

Allows SSH access for remote secured configuration purposes (restart, upgrade, provision...)

### SSH Port

Specifies the SSH port. Default setting is 22.

### GDSManager Configuration Password

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.

**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.

![User Management Page](https://IP_GDS3710:Port/anonymous/snapshot/view.jpg)

**Table 14: User Management**

<table>
<thead>
<tr>
<th>Old Password</th>
<th>Old password must be entered to change new password.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Password</strong></td>
<td>Fill in the revised new password in this field.</td>
</tr>
<tr>
<td><strong>Confirm User Password</strong></td>
<td>Re-enter the new password for verification, must match.</td>
</tr>
<tr>
<td><strong>Password Recovery Email Address</strong></td>
<td>This option is <strong>highly recommended</strong>, as if the password is lost, you can recover it on the configured Email address.</td>
</tr>
</tbody>
</table>

**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.
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 66: SIP Account Settings Page](image)

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

<table>
<thead>
<tr>
<th>SIP Basic Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Active</td>
<td>This field indicates whether the account is active. Default setting is “Yes”.</td>
</tr>
<tr>
<td>Account Name</td>
<td>Configures the SIP account name used for identification.</td>
</tr>
<tr>
<td>SIP Server</td>
<td>Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.</td>
</tr>
<tr>
<td><strong>Outbound Proxy</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Backup Outbound Proxy</strong></td>
<td>Configures the backup outbound proxy to be used when the “Outbound Proxy” registration fails. By default, this field is left empty.</td>
</tr>
</tbody>
</table>
| **DNS Mode** | Configure which DNS mode will be used to translate the SIP Server FQDN (Default value is **A Record**):  
- **A Record**.  
- **SRV**.  
- **NAPTR/SRV**. |
| **SIP User ID** | Configures the SIP username or telephone number from ITSP.  
**Note:** Letters, digits and special characters including @ are supported. |
| **Authenticate ID** | Configures the Authenticate ID used by SIP proxy. |
| **Password** | Sets the Authenticate password used by SIP proxy.  
**Note:** For security reasons, the SIP password is invisible on the web UI. |
| **TEL URI** | Select “User=Phone” or “Enabled” from the dropdown list.  
If the SIP account has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable". |
| **SIP Advanced Settings** |  
| **Registration Expiration (m)** | Sets the registration expiration time.  
Default setting is 60 minutes. Valid range is from 1 to 64800 minutes. |
| **Re-register before Expiration (s)** | 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. |
| **Local SIP Port** | Sets the local SIP port. Default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4. |
| **SIP Transport** | Chooses the SIP transport protocol. UDP, TCP or TCP/TLS.  
Default setting is UDP. |
| **Stream** | Select the Video stream to be used by the GDS3710 when call is made from this SIP Account.  
Default is Stream 2. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable DTMF</strong></td>
<td>Specifies the mechanism to transmit DTMF digits. There are 2 supported modes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>RFC2833</strong> sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SIP INFO</strong> uses SIP INFO to carry DTMF. Default setting is &quot;RFC2833&quot;</td>
</tr>
<tr>
<td><strong>DTMF Payload Type</strong></td>
<td>Configures the payload type for DTMF using RFC2833. Default value is 101. Range: 96~127.</td>
</tr>
<tr>
<td><strong>Unregister On Reboot</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>NAT Traversal</strong></td>
<td>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”.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable SRTP</strong></td>
<td>Enable SRTP mode based on your selection from the drop-down menu. The default setting is “Disabled”, the two other modes are “Enabled but Not Forced” and “Enabled and Forced”.</td>
</tr>
<tr>
<td><strong>Special Feature</strong></td>
<td>Configures GDS settings to meet different vendors’ server requirements. Users can choose from Standard, Broadsoft or Telefonica Spain. The default setting is “Standard”.</td>
</tr>
<tr>
<td><strong>Outbound Proxy Mode</strong></td>
<td>In route: 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.</td>
</tr>
<tr>
<td></td>
<td>Always sent to: SIP messages will always be sent to Outbound proxy.</td>
</tr>
<tr>
<td></td>
<td>Not in route: remove the Route header from SIP requests.</td>
</tr>
<tr>
<td><strong>Enable RTCP</strong></td>
<td>This option allows 3rd party Service Provider or Cloud Solution to monitor the operation status of the GDS3710 by using related SIP Calls. By default, it's disabled. Users can choose either RTCP or RTCP-XR.</td>
</tr>
<tr>
<td><strong>H.264 Payload Type</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Accept Incoming SIP from Proxy Only</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Vocoder Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Preferred Vocoder</strong></td>
<td>Select multiple audio codecs by priority order (lowest is the highest priority). Supported codecs are: PCMU, PCMA, G.722 and G.729A/B.</td>
</tr>
<tr>
<td><strong>Voice Frame Per TX</strong></td>
<td>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. The default setting is 2. Range is from 1-64.</td>
</tr>
</tbody>
</table>

**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.
Figure 67: Phone Settings Page

Table 16: Phone Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STUN Server</td>
<td>Configures the STUN server FQDN or IP. If the device is behind a non-symmetric router, STUN server can help to penetrate &amp; resolve NAT issues.</td>
</tr>
<tr>
<td>Local RTP Port</td>
<td>Sets the local RTP port for media. Default setting is 5004. Range between 1024~65400.</td>
</tr>
<tr>
<td>Use Random Port</td>
<td>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”</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This parameter must be set to “Disabled” for Direct IP Calling to work.</td>
</tr>
<tr>
<td>Auto On-Hook Timer</td>
<td>Configures the auto on-hook timer (in seconds) for automatic disconnecting the SIP call. Default setting is 300. Range between 0~65535.</td>
</tr>
<tr>
<td>Ring Timeout(s)</td>
<td>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.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>SIP TLS Certificate</strong></td>
<td>Input the TLS certificate here for encryption.</td>
</tr>
<tr>
<td><strong>SIP TLS Private Key</strong></td>
<td>Input private key here for TLS security protection.</td>
</tr>
<tr>
<td><strong>SIP TLS Private Key Password</strong></td>
<td>Specifies the password for SIP TLS private Key.</td>
</tr>
<tr>
<td><strong>Enable Direct IP Call</strong></td>
<td>Accepts peer-to-peer IP call (over UDP only) without SIP server. Default is “Enabled”.</td>
</tr>
<tr>
<td><strong>Enable two-way SIP Calling</strong></td>
<td>Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.</td>
</tr>
<tr>
<td><strong>Enable two-way SIP Calling</strong></td>
<td>Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.</td>
</tr>
<tr>
<td><strong>SIP Proxy Compatibility Mode</strong></td>
<td>Enables more proxy compatibility with cost of bandwidth, the SIP call will send audio no matter what.</td>
</tr>
<tr>
<td><strong>SIP Packetization Compatibility Mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Enable Multi-channel Call Mode</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Allow Reset Via SIP NOTIFY</strong></td>
<td>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: - The admin password if no SIP account is configured on the GDS3710. - The SIP User ID and Password credentials of the SIP account if configured on the GDS3710. Default is unchecked (disabled).</td>
</tr>
</tbody>
</table>

**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 68: White List Page](image)

The table below gives a brief overview of the options:

<table>
<thead>
<tr>
<th>Table 17: White List</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable White Number List</strong></td>
</tr>
<tr>
<td><strong>Phone Number 1 -30</strong></td>
</tr>
</tbody>
</table>

**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 69: Click-To-Dial](image)

**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

![Video Settings Page]

Figure 70: Video Settings Page
Table 18: Video Settings

<table>
<thead>
<tr>
<th>Preferred Video Codec (Stream1)</th>
<th>Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is “Main Profile”.</td>
</tr>
<tr>
<td>Resolution</td>
<td>Specifies the resolution in pixels used at video image, 1080p or 720p.</td>
</tr>
<tr>
<td>Bit Rate(kbps)</td>
<td>Selects the video bit rate or bandwidth used.</td>
</tr>
<tr>
<td>Frame Rate(fps)</td>
<td>Selects the maximum frame rate used (more data if big frame used).</td>
</tr>
<tr>
<td>Bit Rate Control</td>
<td>Selects the constantly bit rate, or variable bit rate.</td>
</tr>
<tr>
<td>Image Quality</td>
<td>Selects the image quality used when Variable Bit Rate used.</td>
</tr>
<tr>
<td>I-frame Interval</td>
<td>Configures the I-frame interval (suggested 2~3 times of frame rate).</td>
</tr>
</tbody>
</table>

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

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

Notes:
- H.264 suggested if the GDS3710 needs to be viewed via Internet.
- For definition of Baseline, Main Profile and High profile of H.264 please refer to: H.264 Profiles.
• If MJPEG is selected, reduce the frame rate to the minimal value to save bandwidth and get better image.

• Grandstream GDS3710 provides three video streams, users can use them with flexibility. For example, the high-resolution stream for local recording, another low or high resolution for SIP video phone call or remote smartphone monitoring application, or vice versa depending application scenarios.

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

**Retrieving Video Streams**

• To retrieve video stream via RTSP, users can use the following format:
  rtsp://admin:password@IP_GDS3710:Port/X where X=0,4,8 for 1\textsuperscript{st}, 2\textsuperscript{nd}, 3\textsuperscript{rd} 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.

\[Figure 71: OSD Settings Page\]

<table>
<thead>
<tr>
<th><strong>Table 19: OSD Settings</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display Time</strong></td>
</tr>
<tr>
<td><strong>Display Text</strong></td>
</tr>
<tr>
<td><strong>OSD Date Format</strong></td>
</tr>
</tbody>
</table>
OSD Time Format | OSD Time format, choose based on user preference.
---|---
OSD Text | Input a text (to identify the GDS3710) it will be shown on the screen.
OSD Date/Time Position | Show the Date/Time position on the screen.
OSD Text Position | Show the text position on the screen.

**CMOS Settings**

This page configures the CMOS parameters for different scenarios.

![CMOS Settings Page](image)

**Figure 72: CMOS Settings Page**

**Table 20: CMOS Settings**

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

**Audio Settings**

This page allows users to configure the audio settings.
Table 21: Audio Settings

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

- Click on [Upload] to upload the ringtone file, then press [Save] to save it.
- Click on [Delete] 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.
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.
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.
Table 22: Motion Detection

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Motion Detection</td>
<td>Enables the motion detection feature.</td>
</tr>
<tr>
<td>Region Config</td>
<td>Configures the motion detection region.</td>
</tr>
<tr>
<td>Quit Config</td>
<td>Exits the motion detection region config menu.</td>
</tr>
<tr>
<td>Clear Selected Region</td>
<td>Selects a zone on the screen then click on &quot;Clear&quot; to delete the region.</td>
</tr>
<tr>
<td>Sensitivity</td>
<td>Specifies the region sensitivity (value between 0-100%).</td>
</tr>
<tr>
<td>Select Alarm Schedule</td>
<td>Selects the alarm schedule.</td>
</tr>
<tr>
<td>Select Alarm Action Profile</td>
<td>Selects the programmed Alarm Action profile.</td>
</tr>
</tbody>
</table>
Digital Input

<table>
<thead>
<tr>
<th>Digital Input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digit Input 1</td>
<td>Selects the Input method (alarm Input or Door Open). Default disabled. Digital Input Port operates in 3 Modes: 1. <strong>Alarm Input</strong>: Connect sensor to trigger alarm. 2. <strong>Open door</strong>: Connect a switch to open door from inside. 3. <strong>Abnormal Door Control</strong>: This is a major security enhancement for GDS37xx when device be tampered to open the door abnormally. <em>Please check Siren alarming when door opened abnormally section.</em> If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.</td>
</tr>
<tr>
<td>Digit Input 1 Open Door Option</td>
<td>- When Digital Input is set to <strong>Open door</strong> then user can select the doors to be affected when Alarm IN 1 is triggered.</td>
</tr>
<tr>
<td>Input Digit 1 Status</td>
<td>- If set to <strong>Normal Open</strong>: Configured alarm will be triggered when Digital Input Status switch from Close to Open. - If set to <strong>Normal Close</strong>: Configured alarm will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 1 Status is “Disabled”.</td>
</tr>
<tr>
<td>Select Alarm Schedule 1</td>
<td>Selects the predefined Alarm Schedule.</td>
</tr>
<tr>
<td>Select Alarm Action Profile 1</td>
<td>Selects the predefined Alarm Action for Profile 1.</td>
</tr>
<tr>
<td>Digital Input 2</td>
<td>Selects the Input method (alarm Input or Door Open). Default disabled. Digital Input Port operates in 2 Modes: 1. <strong>Alarm Input</strong>: Connect various of sensor to trigger alarm.</td>
</tr>
</tbody>
</table>

Figure 77: Digital Input

Table 23: Digital Input

<table>
<thead>
<tr>
<th>Digit Input 1</th>
<th>Alarm Input</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digit Input 1 Status</td>
<td>Normal Close</td>
</tr>
<tr>
<td>Select Schedule 1</td>
<td>All Day</td>
</tr>
<tr>
<td>Select Alarm Action Profile 1</td>
<td>profile1</td>
</tr>
<tr>
<td>Digit Input 2</td>
<td>Open Door</td>
</tr>
<tr>
<td>Digit Input 2 Open Door Option</td>
<td></td>
</tr>
<tr>
<td>Select Schedule 2</td>
<td>All Day</td>
</tr>
</tbody>
</table>
2. **Open door**: Connect a switch to open door from inside. If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.

<table>
<thead>
<tr>
<th>Digit Input 2 Open Door Option</th>
<th>When Digital Input is set to <strong>Open door</strong> then user can select the doors to be affected when Alarm IN 2 is triggered.</th>
</tr>
</thead>
</table>
| Input Digit 2 Status          | • If set to **Normal Open**: Configured alarm will be triggered when Digital Input Status switch from Close to Open.  
                                • If set to **Normal Close**: Configured alarm will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 2 Status is “Disabled”. |
| Select Alarm Schedule 2       | Selects the predefined Alarm Schedule. |
| Select Alarm Action Profile 2 | Selects the predefined Alarm Action for Profile 2. |
| Alarm Output Duration(s)      | Select the duration of the alarm output: 5/10/15/20/25/30 seconds. This option is hidden when **ALMOUT1 Feature** is set to Open Door. |

**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>
<thead>
<tr>
<th><strong>Table 24: Silently Alarm Mode</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Silent Alarm Mode</strong></td>
</tr>
<tr>
<td><strong>Silently Alarm Options</strong></td>
</tr>
</tbody>
</table>

**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>
<thead>
<tr>
<th><strong>Table 25: Hostage Code Alarm</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Hostage Code</strong></td>
</tr>
<tr>
<td><strong>Hostage Code</strong></td>
</tr>
<tr>
<td><strong>Select Alarm Action Profile</strong></td>
</tr>
<tr>
<td><strong>Note</strong>: No sound alarm will be triggered in this mode.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>Table 26: Tamper Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Tamper Alarm</strong></td>
</tr>
<tr>
<td><strong>Select Alarm Action Profile</strong></td>
</tr>
</tbody>
</table>

Keypad Input Error Alarm

<table>
<thead>
<tr>
<th>Table 27: Keypad Input Error Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Keypad Input Error Alarm</strong></td>
</tr>
<tr>
<td><strong>Select Alarm Action Profile</strong></td>
</tr>
</tbody>
</table>

Non-Scheduled Access Alarm

<table>
<thead>
<tr>
<th>Table 28 : Non-Scheduled Access Alarm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable Non-Scheduled Access Alarm</strong></td>
</tr>
<tr>
<td><strong>Select Alarm Action Profile</strong></td>
</tr>
</tbody>
</table>

Alarm Schedule Settings

This page specifies the configuration of Alarm Schedule.

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

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

![Modify Alarm Action Profile]

To test an alarm action profile, users can click on the button and the GDS will initiate all actions specified on the select alarm profile.
Table 29: Alarm Actions

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Upload to Alarm Center</strong></td>
<td>If selected, the GDSManager will popup alarm window and sound alarm in the computer speaker.</td>
</tr>
<tr>
<td><strong>Audio Alarm to SIP Phone</strong></td>
<td>If selected, GDS3710 will call pre-configured (video or audio) phone and will play sound alarm.</td>
</tr>
<tr>
<td><strong>Send Email</strong></td>
<td>If selected, an email with snapshot will be sent to the pre-configured email destination.</td>
</tr>
<tr>
<td><strong>Audio Alarm</strong></td>
<td>If selected, GDS3710 will play alarm audio using built-in speaker.</td>
</tr>
<tr>
<td><strong>Alarm Output</strong></td>
<td>If selected, the alarm will be sent to the equipment (for example: Siren) connected to Alarm Output interface.</td>
</tr>
<tr>
<td><strong>Upload Snapshot</strong></td>
<td>If selected, snapshots at the moment where the event is triggered will be sent to preconfigured destination (e.g.: FTP or email).</td>
</tr>
</tbody>
</table>

**Alarm Phone List**

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

![Alarm Phone List](image)

Figure 82: Alarm Phone List

Table 30: Alarm Phone List

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Alarm Call Out Account</strong></td>
<td>Select the SIP Account to be used by the GDS when alarm out is triggered.</td>
</tr>
<tr>
<td><strong>Alarm Phone List 1-10</strong></td>
<td>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).</td>
</tr>
</tbody>
</table>
Once the event is triggered (Motion Detection, Door Bell Pressed…), the GDS3710 will call the first number, once time out is reached and no answer is returned from the first number, the GDS3710 will try the next number on the list and so on. Once the remote phone answers the call, an alarm will be played to notify users that an event is triggered.

**Email & FTP Settings**

This page contains Email and FTP Settings.

**Email Settings**

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

**Figure 83: Email Settings - SMTP Page**

<table>
<thead>
<tr>
<th>Table 31: Email Settings - SMTP</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SMTP Server</strong></td>
</tr>
<tr>
<td><strong>SMTP Server Port</strong></td>
</tr>
<tr>
<td><strong>From E-mail address</strong></td>
</tr>
<tr>
<td><strong>Sender Email ID</strong></td>
</tr>
<tr>
<td><strong>Sender Email Password</strong></td>
</tr>
<tr>
<td><strong>Alarm-To Email Address 1</strong></td>
</tr>
</tbody>
</table>
**Alarm-To Email Address 2**

Specifies the 2nd email address to receive the alarm email.

**SSL**

Check if the SMTP email server requires SSL.

**Notes:**

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

**FTP & Center Storage**

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

**Table 32: Picture Storage Settings**

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

**Note:** Blank fields when using Storage Server Type as Central Storage might imply no configuration in GDSManager.
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>
<thead>
<tr>
<th>FTP Filename with</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CARD</td>
<td>Meaning that open door operation is using RFID card.</td>
</tr>
<tr>
<td>LPIN (Local PIN)</td>
<td>Meaning that open door operation is via Local PIN (Private PIN, or Unified PIN, or Guest PIN).</td>
</tr>
<tr>
<td>RPIN (Remote PIN)</td>
<td>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).</td>
</tr>
</tbody>
</table>
RING

Meaning the snapshot taken when somebody pressed the Door Bell button.

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

![Figure 85: FTP filenames](image)

**Maintenance Settings**

This page shows the GDS3710 Maintenance parameters.

**Upgrade**

This page contains the upgrade and provisioning parameters of the GDS3710.
### Table 34: Upgrade

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Via</td>
<td>Selects the upgrade method (TFTP, HTTP, and HTTPS).</td>
</tr>
<tr>
<td>Firmware Server Path</td>
<td>Configures the IP address or the FQDN of the upgrade server.</td>
</tr>
<tr>
<td>HTTP/HTTPS User Name</td>
<td>The user name for the HTTP/HTTPS server.</td>
</tr>
<tr>
<td>HTTP/HTTPS Password</td>
<td>The password for the HTTP/HTTPS server.</td>
</tr>
<tr>
<td>Firmware File Prefix</td>
<td>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.</td>
</tr>
<tr>
<td>Firmware File Postfix</td>
<td>Enables your ITSP to lock firmware updates. If configured, only the firmware file with the matching encrypted postfix will be downloaded and flashed into the phone.</td>
</tr>
<tr>
<td>Upgrade via</td>
<td>Selects the upgrade method (TFTP, HTTP, and HTTPS).</td>
</tr>
<tr>
<td>Config Server Path</td>
<td>Configures the IP address or the FQDN of the configuration server.</td>
</tr>
<tr>
<td><strong>HTTP/HTTPS User Name</strong></td>
<td>The user name for the HTTP/HTTPS server.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td><strong>HTTP/HTTPS Password</strong></td>
<td>The password for the HTTP/HTTPS server.</td>
</tr>
<tr>
<td><strong>Config File Prefix</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Config File Postfix</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>XML Config File Password</strong></td>
<td>Specifies the password for the configuration file.</td>
</tr>
<tr>
<td><strong>Validate Server Certificate</strong></td>
<td>Enable this option in order to validate certificate with trusted ones during TLS connection.</td>
</tr>
<tr>
<td><strong>Automatic Upgrade Interval</strong></td>
<td>Specifies the upgrade interval in minutes.</td>
</tr>
<tr>
<td><strong>Enable DHCP Option 66 Override Server</strong></td>
<td>Activates DHCP option 66 to override upgrade/config servers.</td>
</tr>
<tr>
<td><strong>Zero Config</strong></td>
<td>Enables Zero Config feature for auto provisioning.</td>
</tr>
<tr>
<td><strong>Enable DHCP Option 120 Override SIP Server</strong></td>
<td>Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is enabled.</td>
</tr>
<tr>
<td><strong>Automatic Upgrade</strong></td>
<td>Enables automatic upgrade and provisioning. Set schedule for provisioning for either every X minutes, every day or every week. Default is No.</td>
</tr>
<tr>
<td><strong>Randomized Automatic Upgrade</strong></td>
<td>Enable and define the start/End hours of the day and days of the week where the GDS will randomly checking for update.</td>
</tr>
</tbody>
</table>

**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 87: Reset & Reboot Page

Table 35: Reset & Reboot

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

Debug Log

This page allows user to configure SYSLOG to collect information to help troubleshooting issues with GDS3710.
• 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.
Click on **Export** to save the GDS3710 configuration in a predefined directory.

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

**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.
**Enable System Health Alert**

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].

**Delivery Method**

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.

**Email Title**

Customize the Email title. Maximum length is 256 character.

**SIP Registration Status**

When checked, Email will contain Offline/Online indication for all 4 accounts.

**System Running Status**

When checked, Email will contain the system uptime.

**System Temperature**

When checked, Email will contain Temperature value of the system in °C and °F, as well as whether the temperature is normal on 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 3rd party software to integrate the GDS3710.

![Event Notification](image)

**Figure 91: Log Manager Page**

**Table 36: Log Manager Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Event Notification</td>
<td>Enables Event Notification feature</td>
</tr>
<tr>
<td>Via Type</td>
<td>Choose which protocol will be used to connect to the logs server (HTTP or HTTPs).</td>
</tr>
<tr>
<td>HTTP/HTTPS Server</td>
<td>Enter the IP address of domain name for the logs server.</td>
</tr>
<tr>
<td>HTTP Server Username</td>
<td>Configure the username of your HTTP(s) server.</td>
</tr>
<tr>
<td>HTTP Server Password</td>
<td>Configure the password of your HTTP(s) server.</td>
</tr>
<tr>
<td>URL Template</td>
<td>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:</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
|              | • ${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 **Search** 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
For more information about event logs, please visit this [guide](#).

**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.

In order to upload your Trusted CA certificate:

Click on the [Upload](#) button to upload a file and some related information to the uploaded file will be displayed, such as “**Issued by**” and “**Expiration date**”.
User could press **Delete** to delete one of the files.

In order to upload your Custom certificate:

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

User could press **Delete** to delete one of the files.

**Status**

This page displays GDS3710 system and network information.

**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 **Online**
- When SIP account is unregistered, the SIP Registration status display will be **Offline**
System Info

This page displays information such as the product model, the hardware version, firmware…
Table 37: System Info

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

**Network Info**

This page displays the network system information of GDS3710.
**Network Info**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>00:0B:82:AB:AE:8A</td>
</tr>
<tr>
<td>IP Address Mode</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP Address</td>
<td>192.168.5.130</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway</td>
<td>192.168.5.1</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>8.8.4.4</td>
</tr>
</tbody>
</table>

**Figure 96: Network Info Page**

**Table 38: Network Info**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the GDS3710 MAC Address.</td>
</tr>
<tr>
<td>IP Address Mode</td>
<td>Displays the IP address mode used.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the GDS3710.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the Subnet Mask used.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Displays the GDS3710 Gateway.</td>
</tr>
<tr>
<td>DNS Server 1</td>
<td>Displays the Preferred DNS Server.</td>
</tr>
<tr>
<td>DNS Server 2</td>
<td>Displays the secondary DNS Server.</td>
</tr>
</tbody>
</table>
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:

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:
  

- **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:
  
GDS3710 HTTP API

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

For more details, please refer to following guide:

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.
3. Select the reset type from Rest drop down menu and press reset button as displayed on the following screenshot.

![Reboot & Reset](image)

Figure 97: 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.
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.
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.

| 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.
3) 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](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.