

Grandstream Networks, Inc.

**GDS371x - User Manual**



# WELCOME

Thank you for purchasing Grandstream GDS3710/GDS3712.


The GDS3710 is an IP Video Door System that also serves as a high-definition IP surveillance camera and IP intercom to offer facility access control and security monitoring for buildings of all sizes. This powerful IP Video Door System offers a 180-degree video viewing angle for wall-to-wall coverage, has a built-in RFID chip reader for secure keyless entry, includes a built-in microphone and speaker to support intercom functionality, and offers alarm-in and alarm-out support for integration with existing security devices. The GDS3710 integrates with Grandstream's free management utility software, GDS Manager, allowing RFID card information, video feeds as well as the device itself to be fully managed by this software. By being ONVIF Profile S compliant, the GDS3710 can be integrated with any third-party ONVIF-compliant surveillance or recording solution. Powered by an advanced Image Sensor Processor (ISP) and state-of-the-art image algorithms, the GDS3710 delivers 1080p FHD video resolutions and offers exceptional performance in all lighting conditions. It features SIP/VoIP technology with 2-way audio and video streaming feeds loaded directly to smartphones, SIP endpoints, and the GDS management software. The GDS3710 is equipped with integrated PoE for seamless installation, bright LEDs for illumination, a motion detector for security protection, a lighting control switch, and more. The combination of the GDS3710, Grandstream's GXP21xx IP phones, GXV video phones, and Grandstream Wave mobile app provide a complete solution for access control, video intercom, and security needs.

The GDS3712 is a hemispheric IP Video Intercom System that also serves as a high-definition IP surveillance camera to offer facility access control and security monitoring for buildings of all sizes. Powered by an advanced Image Sensor Processor (ISP) and state-of-the-art image algorithms, it delivers exceptional performance without blind spots. The GDS3712 IP video intercom system features industry-leading SIP/VoIP for 2-way audio and video streaming to smartphones and SIP phones and the GDS management software. This system is equipped with integrated PoE for seamless installation, motion detection for security protection, a lighting control switch, Alarm Input/Output, and more. The GDS3712 can also 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. The combination of the GDS3712, Grandstream's IP phones, video phones, and Wave mobile app provides a complete end-to-end solution for access control, video intercom, and security recording needs.

## PRODUCT OVERVIEW

### Feature Highlights

The following table contains the major features of the GDS3710 and GDS3712.

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

## Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, telephony features, and upgrade/provisioning settings for GDS371x.

### o GDS3710

<b>Video Compression</b>	H.264 High Profile / Main Profile / Base Profile, Motion JPEG.
<b>Image Sensor Resolution</b>	1/2.7", 2 Megapixel, 1920H x 1080V.
<b>Lens Type</b>	1/2", F2.5, FOV: 180°(W) x 150°(H).
<b>Day &amp; Night Mode</b>	White LEDs with smart brightness control.
<b>Max Video Resolution</b>	1920×1080.
<b>Max Frame Rate</b>	30 frames per second.
<b>Minimum Illumination</b>	0.5Lux.
<b>Wide Dynamic Range</b>	Yes, up to 120dB.
<b>Embedded Analytics</b>	Motion detection.
<b>Snapshots</b>	Triggered upon events, sent via email and/or FTP.
<b>Multi-stream Resolution</b>	High-performance streaming server allowing multiple simultaneous accesses: <ul style="list-style-type: none"> <li>• <b>Primary video stream:</b> 1920 x 1080 resolution for continuous full HD recording.</li> <li>• <b>Secondary video stream:</b> 640 x 480 resolution for SIP/VoIP video calls.</li> <li>• <b>Third video stream:</b> 320 x 240 resolution for smartphone Apps.</li> </ul>
<b>Network Protocols</b>	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS local upload and mass provisioning using TR-069, ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP.
<b>SIP/VoIP Support</b>	Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
<b>Voice Codecs</b>	G.711μ/a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1P) and Layer 3 QoS (ToS, DiffServ, MPLS).
<b>Security</b>	Administrator level access control, MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
<b>Upgrade / Provisioning</b>	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file.
<b>Audio Input</b>	Built-in Digital Microphone, up to 1.5m with AEC.
<b>Audio Output</b>	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.

<b>Keypad / Buttons</b>	12-key touchpad plus a capacitive doorbell button, each with individual LED illumination.
<b>RFID</b>	125KHz: EM4100 (1 RFID card and 1 RFID key fob included).
<b>Alarm Input</b>	Yes, 2 channels, Vin < 15V, for door sensor or other devices.
<b>Alarm Output</b>	Yes, 2 channels, 125VAC/0.5A, 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch or other devices.
<b>Network Interface</b>	10M/100M auto-sensing.
<b>Expansion Interface</b>	Wiegand (26 bits) input and output.
<b>Dimensions and Weight</b>	173mm(H) x 80mm(W) x 36mm(D). 0.6 Kg.
<b>Power Supply</b>	PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).
<b>Interoperability</b>	ONVIF (Profile S).
<b>Ingress Protection</b>	Weatherproof, vandal resistant, with support for extra back reinforcing metal plate
<b>Temperature and Humidity</b>	Operation: -30°C to 60°C (-22°F to 140°F) Storage: -35°C to 60°C (-31°F to 140°F) Humidity: 10% to 90% Non-condensing
<b>Protection Class</b>	IP66 (EN60529), IK09 (IEC62262).
<b>Compliance</b>	<b>FCC:</b> Part 15 subpart B Class B; Part 15 C; MPE <b>CE:</b> EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311 <b>RCM:</b> AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1 <b>IC:</b> ICES-003; RSS310

*GDS3710 Technical Specifications*

o **GDS3712**

<b>Video Compression</b>	H.264 High Profile / Main Profile / Baseline Profile, Motion JPEG.
<b>Image Sensor Resolution</b>	1/2.7", 2 Megapixel, 1920H x 1080V.
<b>Lens Type</b>	1/2", F2.5, FOV:180°(W) x 150°(H).
<b>Max Video Resolution</b>	1920×1080.
<b>Max Frame Rate</b>	30 frames per second.
<b>Minimum Illumination</b>	0.5Lux.
<b>Wide Dynamic Range</b>	Yes, up to 120dB.
<b>Video Bit Rates</b>	128 Kbps to 4 Mbps, multi-rate for preview & recording.



<b>PoE</b>	IEEE 802.3af Class 3.
<b>Embedded Analytics</b>	Motion detection (up to 4 privacy masks).
<b>Snapshots</b>	Triggered upon events, sent via email and/or FTP.
<b>Multi-stream Resolution</b>	High-performance streaming server allowing multiple simultaneous accesses: <ul style="list-style-type: none"> <li>● <b>Primary video stream:</b> 1920 x 1080 resolution for continuous full HD recording.</li> <li>● <b>Secondary video stream:</b> 1280 x 720 resolution for SIP/VoIP video calls.</li> <li>● <b>Third video stream:</b> 320 x 240 resolution for smartphone Apps.</li> </ul>
<b>Network Protocols</b>	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS local upload and mass provisioning using TR-069, ARP/RARP, ICMP, LLDP-MED, DNS, DHCP, SSH, SMTP, TFTP, NTP, STUN, TLS, SRTP.
<b>SIP/VoIP Support</b>	Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
<b>Voice Codecs</b>	G.711µ/a-law, G.722, G.729A/B, DTMF (RFC2833, SIP INFO), AEC.
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1P) and Layer 3 QoS (ToS, DiffServ, MPLS).
<b>Security</b>	Administrator level access control, MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
<b>Upgrade / Provisioning</b>	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file.
<b>Audio Input</b>	Built-in microphone, up to 1.5m with AEC
<b>Audio Output</b>	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.
<b>Button</b>	1 call button with Blue LED backlight
<b>Alarm Input</b>	2 Optocoupler Input, Vin < 15V, for door sensor or another low voltage device.
<b>Alarm Output</b>	2 Relay, 125VAC/0.5A or 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch, or other device.
<b>Network Interface</b>	10M/100M auto-sensing.
<b>Dimensions and Weight</b>	On-Wall: 173mm(H) x 80mm(W) x 36mm(D); In-Wall: 217mm(H) x 120mm(W) x 11.6mm(D) Weight: 0.625 kg
<b>Power Supply</b>	PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).
<b>Ingress Protection</b>	Weatherproof, vandal resistant, with support for extra back reinforcing metal plate.
<b>Temperature and Humidity</b>	Operation: -30°C to 60°C (-22°F to 140°F) Storage: -35°C to 60°C (-31°F to 140°F) Humidity: 10% to 90% Non-condensing
<b>Protection Class</b>	IP66 (EN60529), IK09 (IEC62262).

<b>Compliance</b>	<p><b>FCC:</b> Part 15 subpart B Class B; Part 15 C; MPE</p> <p><b>CE:</b> EN 55032 Class B; EN 61000-3-2; EN 61000-3-3; EN 50130; EN 60950-1; EN 300330; EN 301489; EN 62311</p> <p><b>RCM:</b> AS/NZS CISPR 22; AS/NZS 4268; AS/NZS 60950.1</p> <p><b>IC:</b> ICES-003; RSS310</p> <p><b>UKCA</b></p>
-------------------	---

*GDS3712 Technical Specifications*

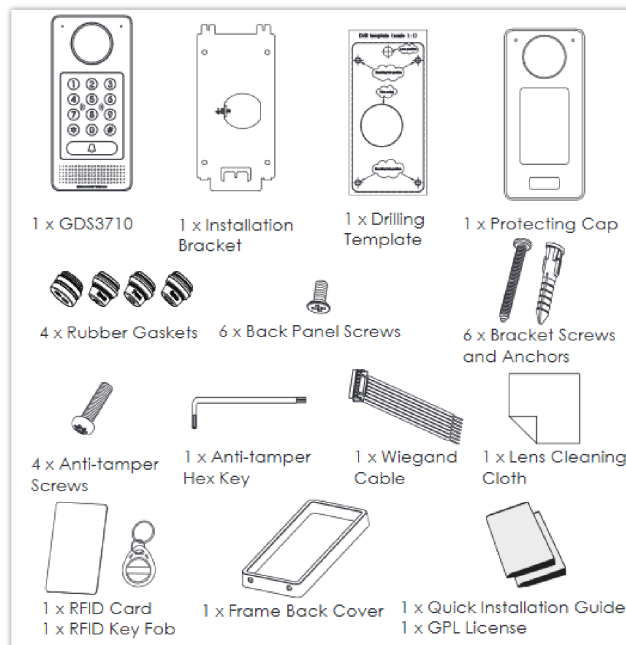
## GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and information for obtaining the best performance using the GDS371x Video Door System.

### Equipment Packaging

#### GDS3710

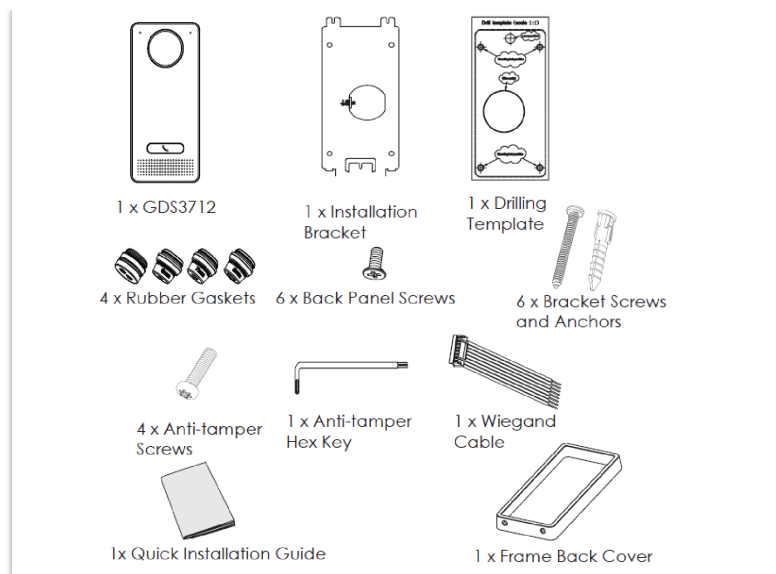
<ul style="list-style-type: none"> <li>● 1 x GDS3710.</li> <li>● 1 x Installation Bracket.</li> <li>● 1 x Drilling Template.</li> <li>● 1 x Protecting Cap.</li> <li>● 4 x Rubber Gaskets (for sealing the back cable).</li> <li>● 6 x Back Panel Screws.</li> <li>● 6 x Bracket Screws and Anchors.</li> <li>●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



*GDS3710 Package Content*

#### GDS3712

<ul style="list-style-type: none"> <li>● 1 x GDS3712.</li> <li>● 1 x Installation Bracket.</li> <li>● 1 x Drilling Template.</li> <li>● 4 x Rubber Gaskets (for sealing the back cable).</li> <li>● 6 x Back Panel Screws.</li> </ul>	<ul style="list-style-type: none"> <li>● 6 x Bracket Screws and Anchors.</li> <li>● 1 x Anti-Tamper Hex Key.</li> <li>● 4 x Anti-tamper screws.</li> <li>● 1 x Frame Back Cover.</li> <li>● 1 x Quick Installation Guide.</li> </ul>
---	--



*GDS3712 Package Content*

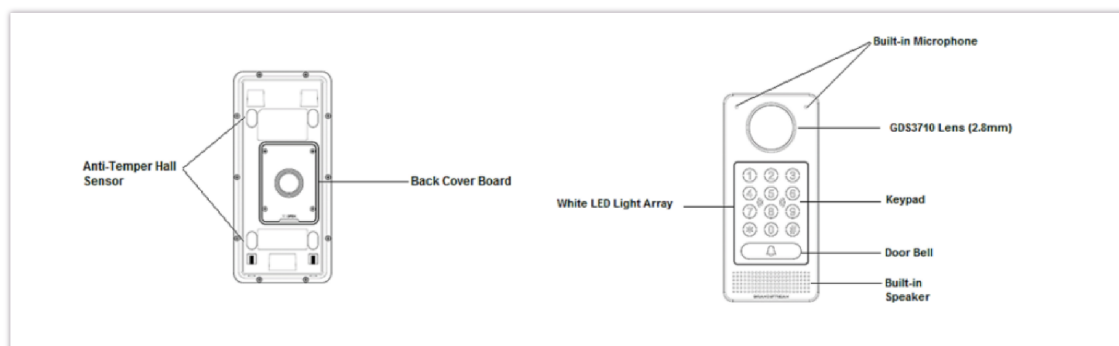
**Note**

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

**Description of the GDS371x**

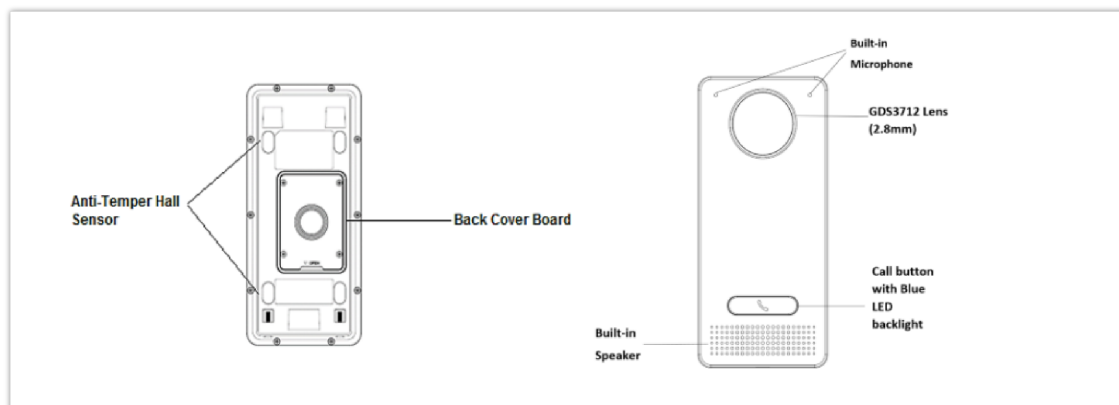
Below figures show the component of the back and front view of GDS371x IP Video Door System:

**GDS3710**



*GDS3710 Front and Back View*

**GDS3712**



*GDS3712 Front and Back View*

**Connecting and Setting up the GDS371x**

The GDS371x 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 GDS371x.

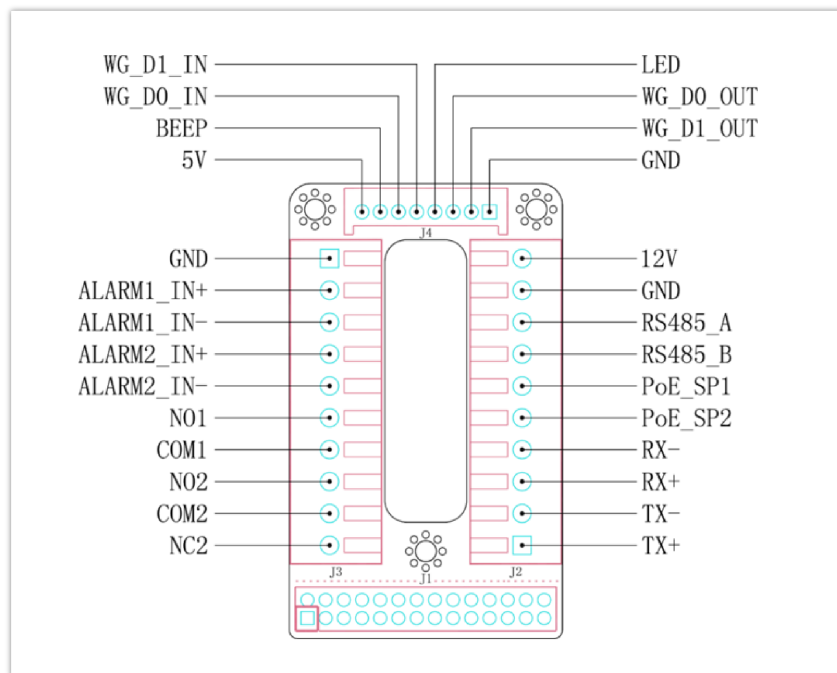
## GDS371x Wiring Connection

Jack	Signal	Function	Note	
J2 (Basic) 3.81mm	TX+	Ethernet PoE 802.3af Class 3, 12.95W	Orange / White	Data
	TX-		Orange	
	RX+		Green / White	
	RX-		Green	
	PoE_SP2		Blue + Blue/White	Please twist these two wires together and connect to SP1, SP2 respectively even the PoE NOT used.
	PoE_SP1		Brown + Brown/White	
	GND	Power Supply	DC 12V, 1A Minimum	
	12V			
J3 (Advanced) 3.81mm	GND	Alarm GND		
	ALARM1_IN+	Alarm In	Vin<15V	
	ALARM1_IN-			
	ALARM2_IN+			
	ALARM2_IN-			
	NO1	Alarm Out	Relay: 30VDC/2A; 125VAC/0.5A	
	COM1			
	NO2	Electric Lock	For " <b>Fail Secure</b> " (Locked when Power Lost) Strike, connect <b>COM2 &amp; NO2</b> . For " <b>Fail Safe</b> " (Open when No Power) Magnetic Lock, connect <b>COM2 &amp; NC2</b> . <b>Relay:</b> 30VDC/2A; 125VAC/0.5A	
	COM2			
NC2				
J4 (Special) 2.0mm	GND	Wiegand Power GND	Black	Both Input and Output MUST be connected

WG_D1_OUT	Wiegand Output Signal	Orange	GDS3710 function as Output of Card Reader, Connect Pin 1, 2, 3
WG_D0_OUT		Brown	
LED	Wiegand Output LED Signal	Blue	For External Card Reader; Or GDS3710 as Receiver Only
WG_D1_IN	Wiegand Input Signal	White	For External Card Reader Connect Pin 1,4,5,6,7,8
WG_D0_IN		Green	
BEEP	Wiegand Output BEEP Signal	Yellow	For External Reader Only
5V	Wiegand Power Output	Red	For External Card Reader Only. 12VDC powered External Card Reader must use own power source, can NOT use this Pin.

GDS371x Wiring Connection

### GDS371x Back Cover Connections

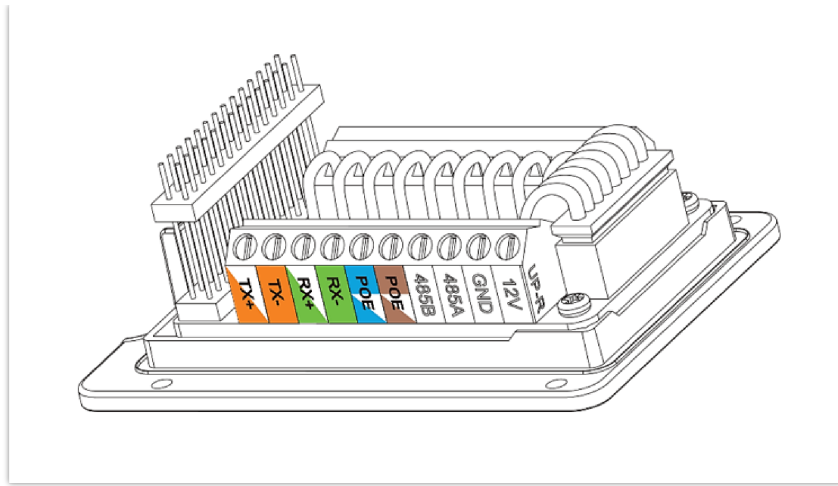


GDS371x Back Cover Connections

### Connection Example

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

- Open the Back-Cover Board of the GDS371x which should look like following figure.

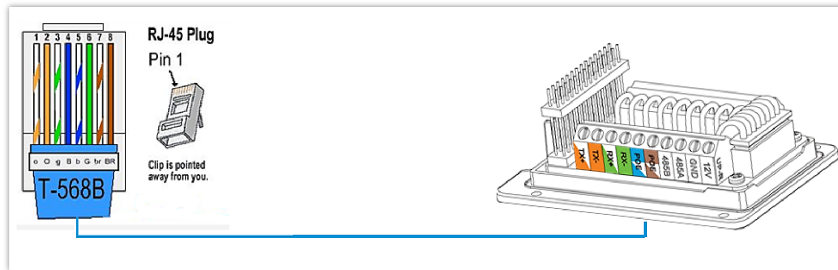


GDS371x Back Cover

## Power the unit using PoE

- Cut into the plastic sheath of your Ethernet cable, then Unwind and pair as shown below.

Use the TIA/EIA 568-B standard, which define pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity.



Connection Example

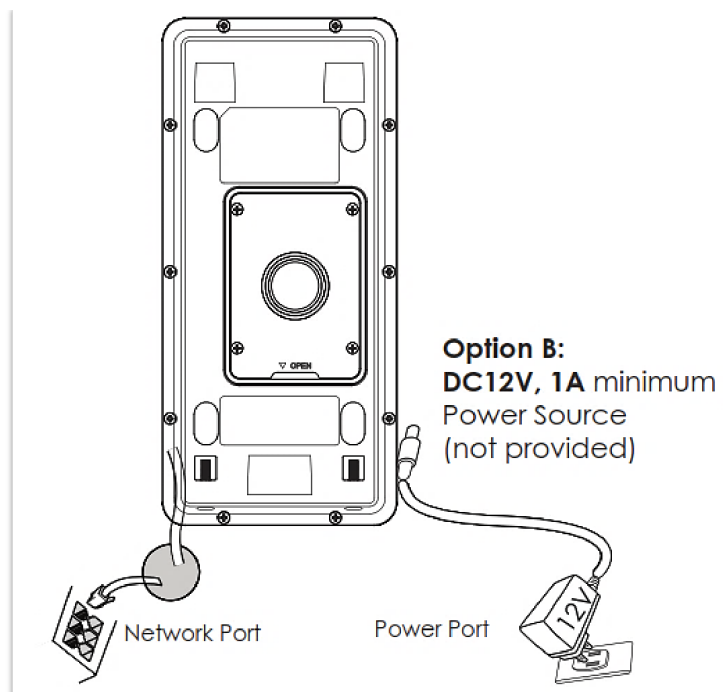
- Connect each wire of the cable to its associate on the Back Cover of the GDS371x to power the unit using PoE.

## 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 GDS371x since these wires are used to power the unit via Ethernet.



Powering the GDS371x

## GETTING TO KNOW GDS371x

The GDS371x has an embedded Web server to respond to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the GDS371x through Microsoft Internet Explorer or Mozilla Firefox.

Download WebControl Plug-in from the GDS371x 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 GDS371x to Network with DHCP Server


The GDS371x by default has a DHCP client enabled, it will automatically get IP address from DHCP server.

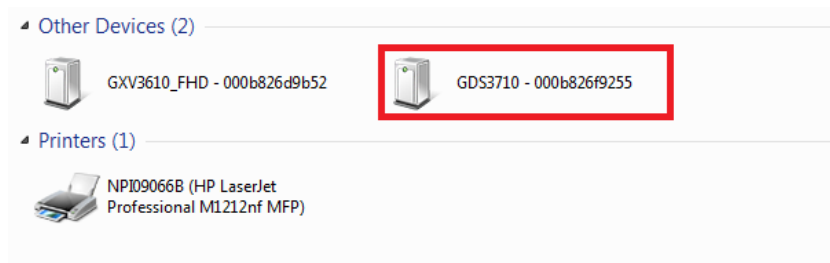
### Windows Platform

Two ways exist for Windows user to get access to the GDS371x:

#### UPnP

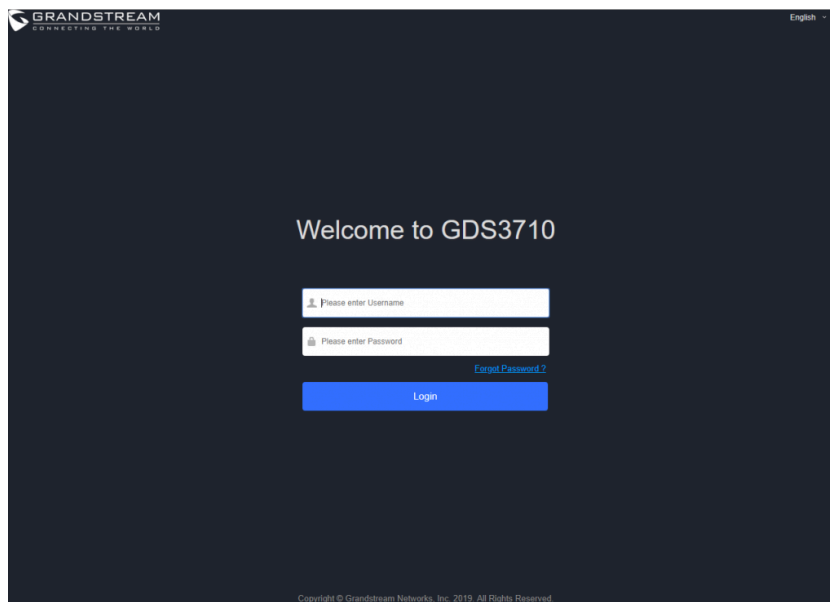
By default, the GDS371x has the UPnP feature turned ON. For customers using Windows network with UPnP turned on (most SOHO routers support UPnP), it is very easy to access the GDS371x, in this example we will take the GDS3710 as our testing unit:

1. Find the "Network" icon  Network on the windows Desktop.
2. Click the icon to get into the "Network", the GDS3710 will list as "Other Devices" shown like below. Refresh the pages if nothing displayed. Otherwise, the UPnP may not be active in the network.



*Detecting GDS371x via UPnP*

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



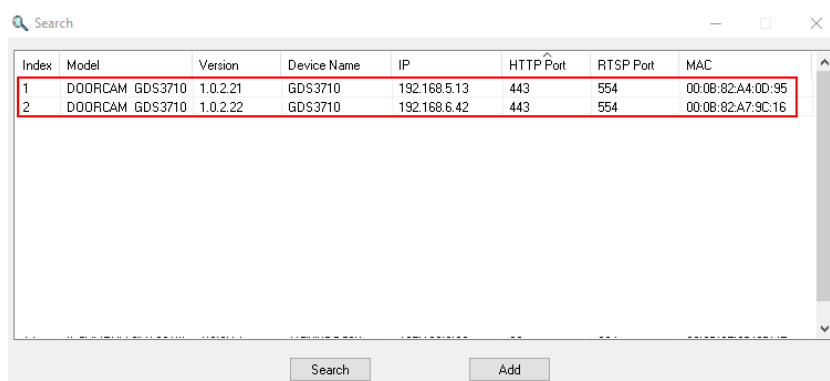
*GDS3710 Login Page*

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

## GS Search

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

- Download the GS Search utility tool from Grandstream website using the following link: [GS\\_Search](#)
- Double click on the downloaded file and the search window will appear.
- Click on  button to start the discovery for Grandstream devices.
- The detected devices will appear in the output field like below.



*GS Search Discovery*

- Double click on a device to access its webGUI.




## GDS Manager Utility Tool

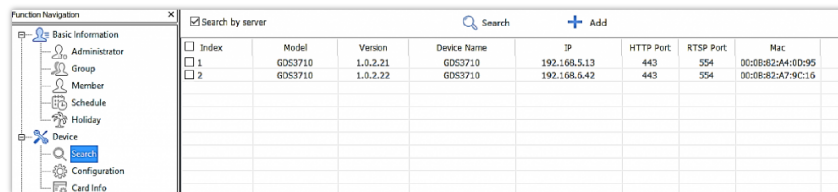
User can know the IP address assigned to the GDS371x from DHCP server log or using the Grandstream GDS Manager after installing this free utility tool provided by Grandstream. User can find instructions below, for using "GDS Manager" utility tool:

1. Download the GDS Manager utility tool from Grandstream website using the following link: [GDSManager Download](#)
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  Search button to start device detection

4. The detected devices will appear in the output field like below:



Index	Model	Version	Device Name	IP	HTTP Port	RTSP Port	Mac
1	GDS3710	1.0.2.21	GDS3710	192.168.5.13	443	554	00:0B:82:A4:0D:95
2	GDS3710	1.0.2.22	GDS3710	192.168.6.42	443	554	00:0B:82:A7:9C:16

*GDS3710x Detection*

5. Double click the column of the detected GDS371x, 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.

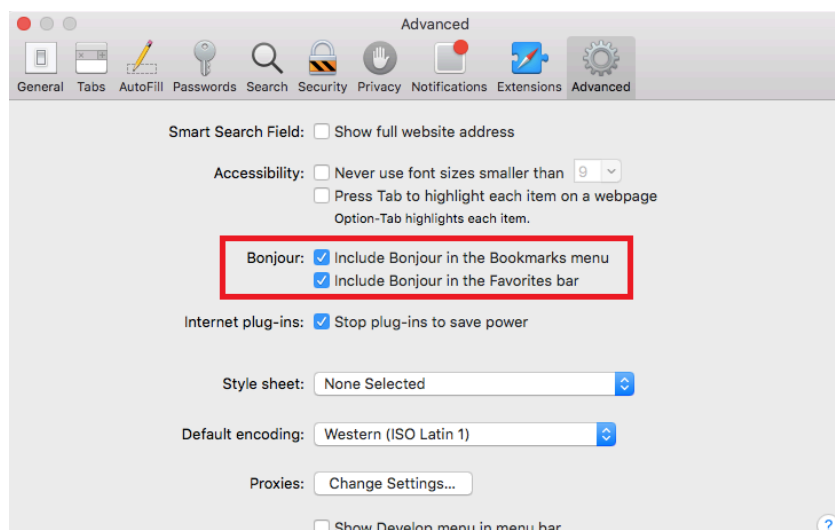
7. Enter the administrator user name and password to access the Web Configuration Interface, the default admin username is "admin" and the default random password can be found at the sticker on the GDS371x.

8. The plug-in can be downloaded from the GDS371x Web GUI.

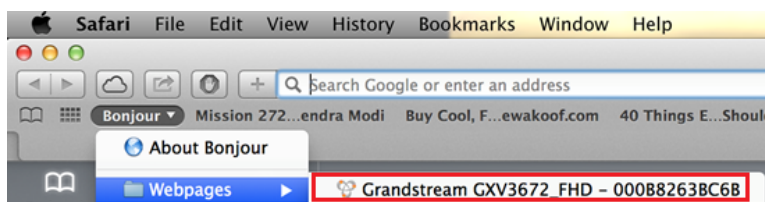
## Apple Platform

For Apple users, please turn on Bonjour of Safari to find and access the GDS371x.

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 GDS371x will be there.



Bonjour Setting Page

4. Click on the displayed GDS371x to access to the configuration page of the GDS371x.

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.

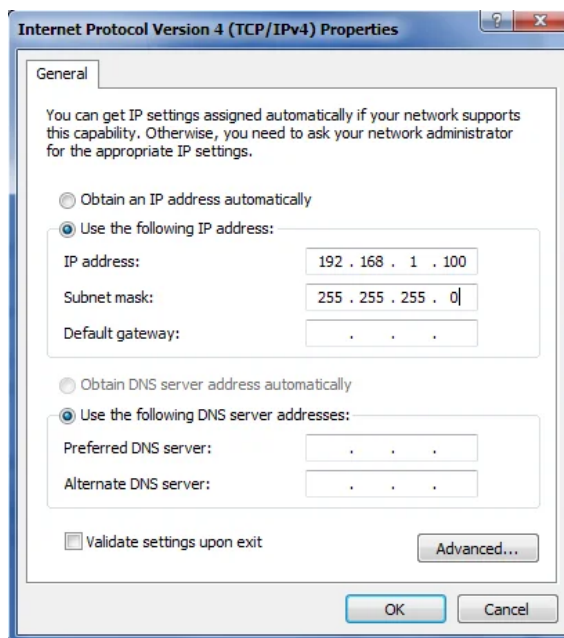


- iPhone/iPad (iOS) users are recommended to use Applications in Apple Store.
- Free or Paid applications from Apple Store like "IP Cam Viewer" is suggested and verified working with Grandstream GDS371x.
- Apple Store applications like "IP Cam Viewer" will support H.264 video codec.

### Connect to the GDS371x using Static IP

If there is no DHCP server in the network, or the GDS371x does not get IP from DHCP server, user can connect the GDS371x to a computer directly, using static IP to configure the GDS371x.

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 GDS371x 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:



*Static IP on Windows*

4. Power on the GDS371x, 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 GDS371x.
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 GDS371x.
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.

## **GDS371x APPLICATION SCENARIOS**

The GDS371x 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 GXV3x50 or GXV3x70, the GDS371x will meet your very basic intercom, open door and surveillance requirement.

This is the solution to upgrade the traditional analog Intercom and CCTV security system. All you need is a Power source, Switch or PoE Switch and Grandstream GXV33xx or GXV34xx video phones.

The equipment list can be found below:

- o GDS371x
- o GXV33xx or GXV34xx
- o PoE Switch with related Cat5e/Cat6 wiring

## Peering using SIP Server (UCM6XXX)

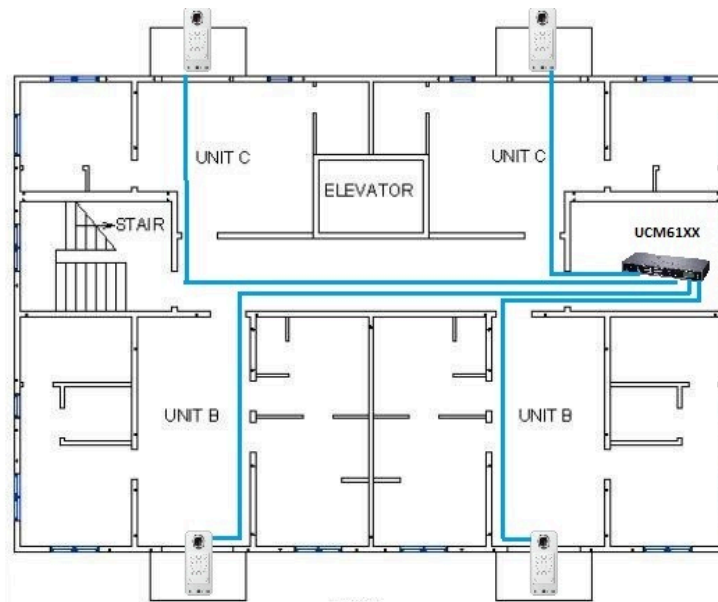
For large deployment, multiple GDS371x might be required, peered connection will not work in such case due to multiple connections. Such scenarios require an IPPBX or a SIP Proxy to accomplish the tasks.

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

- Several GDS371x
- UCM6XXX or another SIP Server
- GXV33xx or GXV34xx Video Phones
- PoE Switch with related Cat5e/Cat6 wiring
- Electronic Lock

If remote access to the GDS371x 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).



*Peering GDS371x with UCM6XXX*

## Using a Network Video Recorder (NVR)

For implementation with more than two GDS371Xs, if local video recording is required to store the record, then an NVR will be added to save all the video streams when people enter the door.

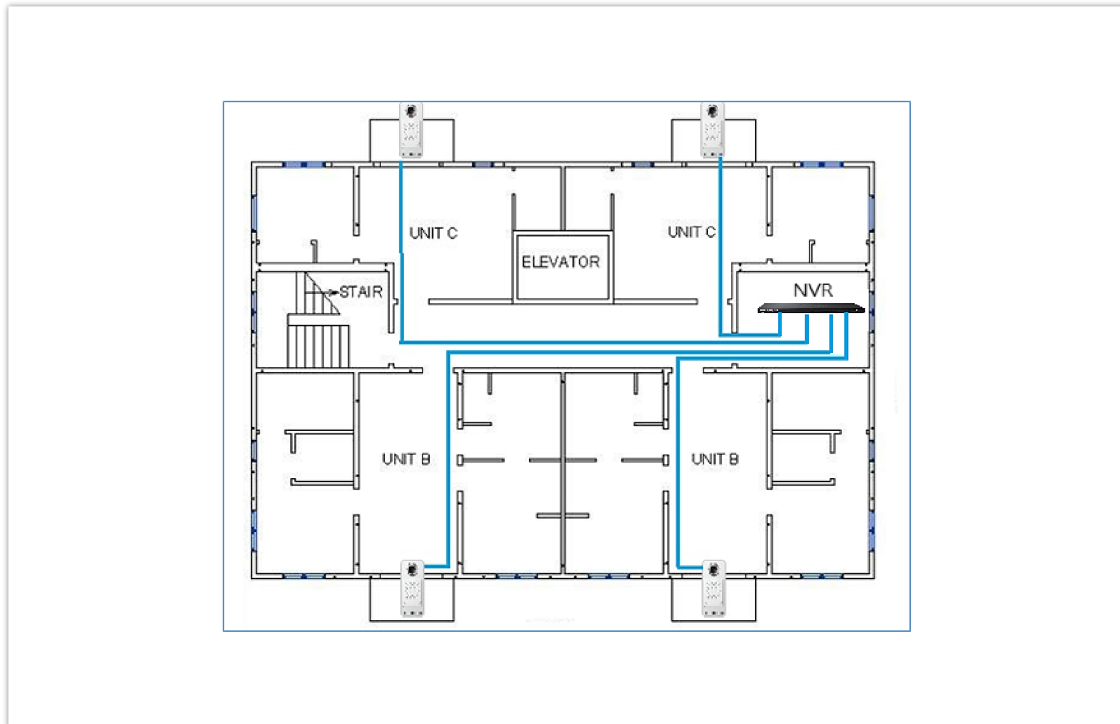
### Note

The RTSP Password defined on Access settings can be used to access Open Network Video Interface Forum devices.

Equipment List:

- Several GDS371x
- NVR supporting Onvif Profile S.
- PoE switches with Cat5e/Cat6 wiring.
- Router.
- Internet Access (Optical fiber, 3G, 4G, Cable or DSL).

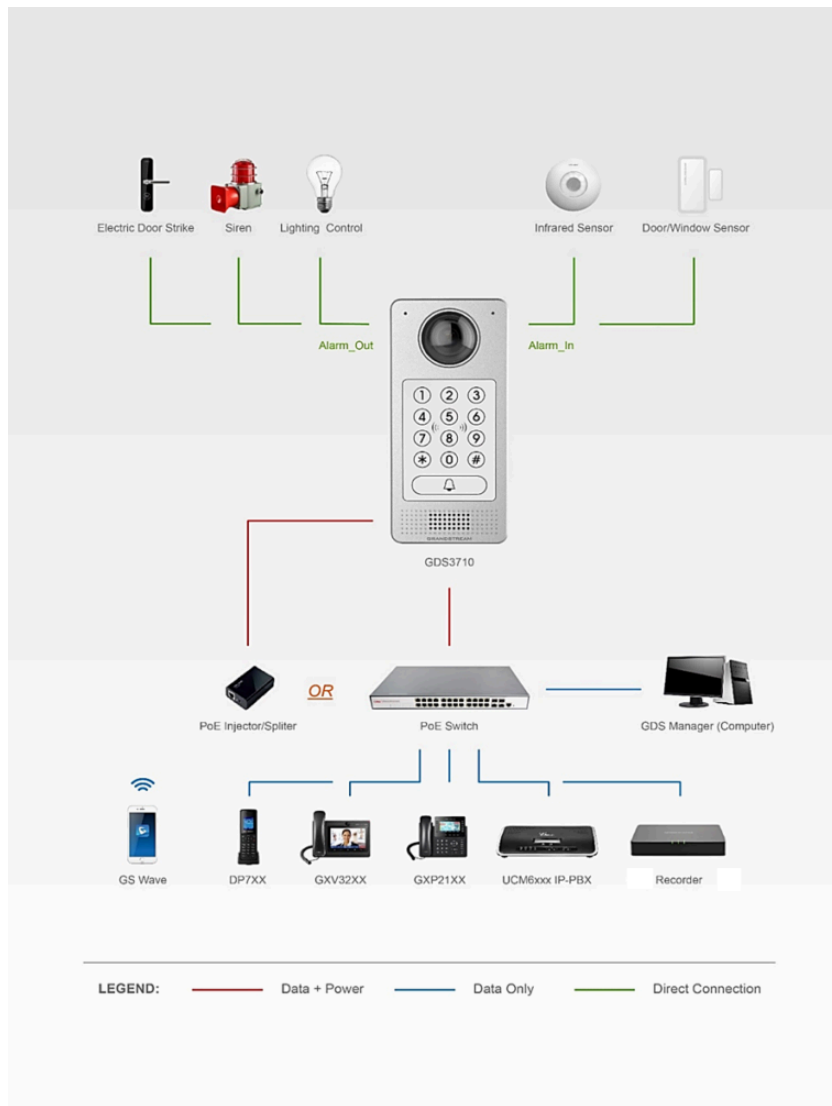
- iPhone or Android phone with 3rd party APP.



*Peering GDS3710 with an Onvif Profile S NVR.*

## **GDS371x PERIPHERAL CONNECTIONS**

Below is the illustration of GDS371x peripheral connections for related applications, We will take the GDS3710 as our testing unit.



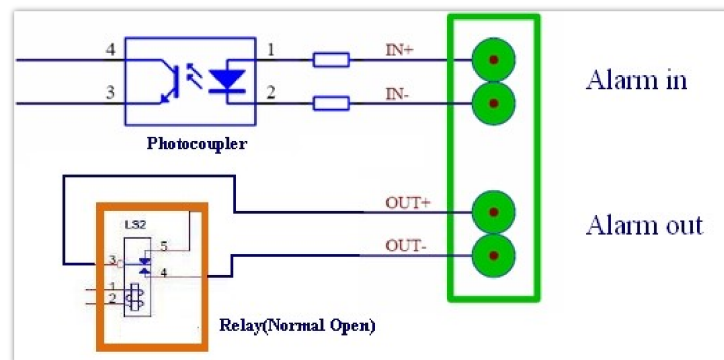
Peripheral Connections for GDS3710

## 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 GDS371x

### Notes:

- The Alarm\_In and Alarm\_Out circuit for the GDS371x should meet the following requirement:

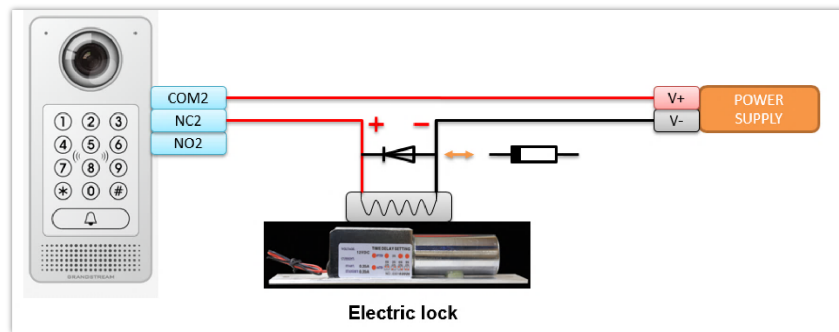
<b>Alarm Input</b>	3V < Vin < 15V, PINs (1.02KΩ)
--------------------	-------------------------------

<b>Alarm Output</b>	125VAC/0.5A, 30VDC/2A, Normal Open, PINs
---------------------	--

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

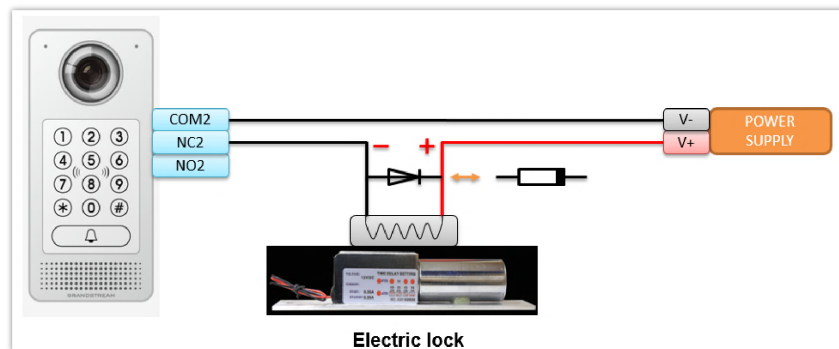
### Protection Diode

When connecting the GDS371x to a door strike it is recommended to set an EMF protection diode in reverse polarity for a secure use, below examples of deploying the GDS3710 for the protection diode.



Protection Diode – Example 1

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



Protection Diode – Example 2

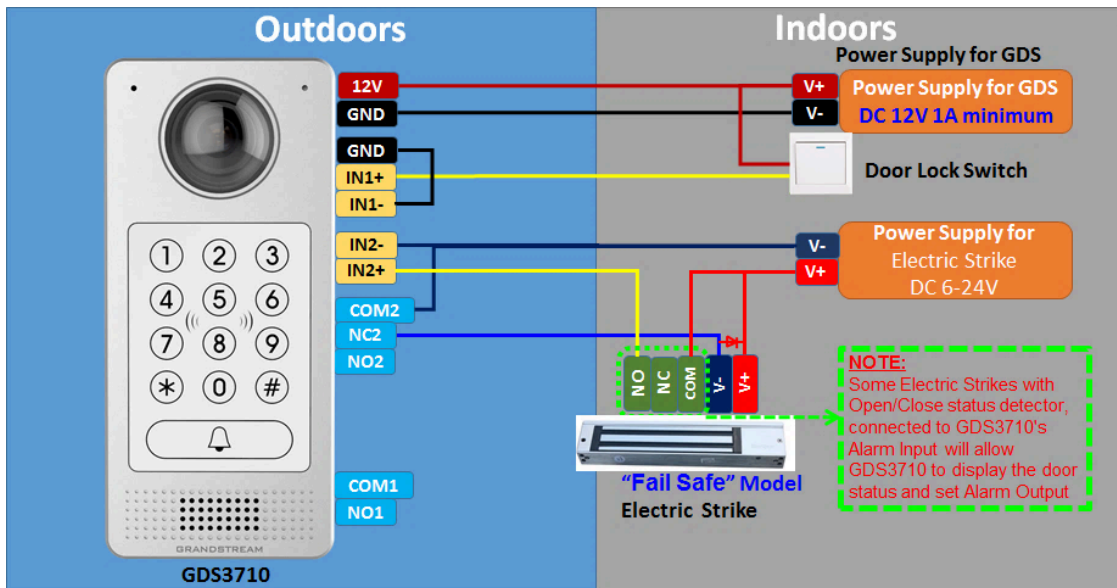
#### Note

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

### Connection Examples

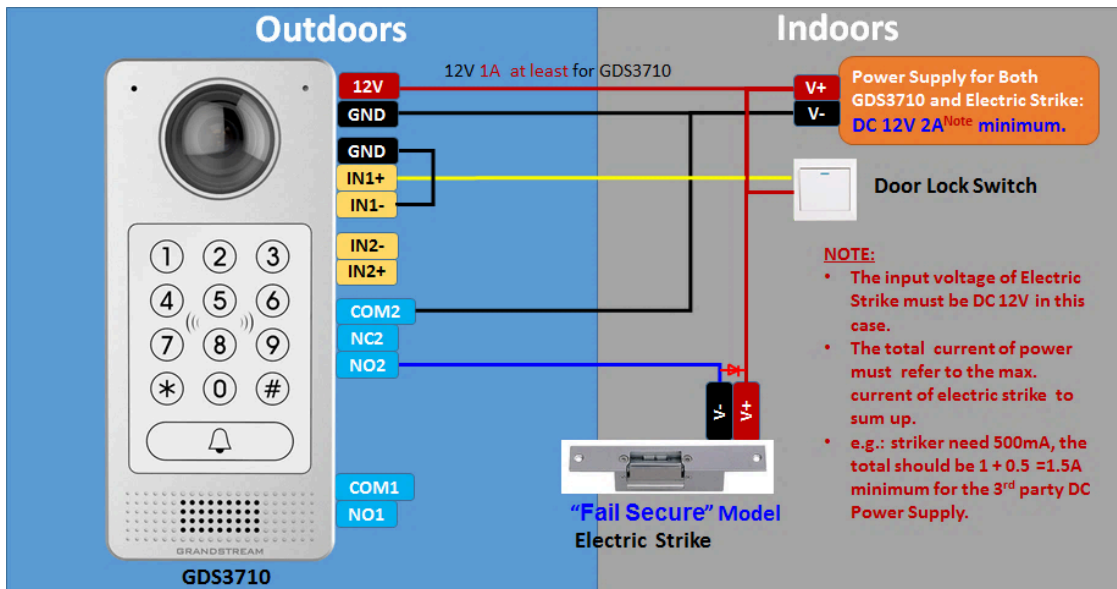
Below examples, show how to use wiring on the back cover of the GDS3710 to connect with external devices. The "NO" (Normal Open) model strike is used as example, "NC" (Normal Closed) should be similar and users need to decide which model (NO or NC) to be used on the door.

### Wiring Sample using 3<sup>rd</sup> Party Power Supply



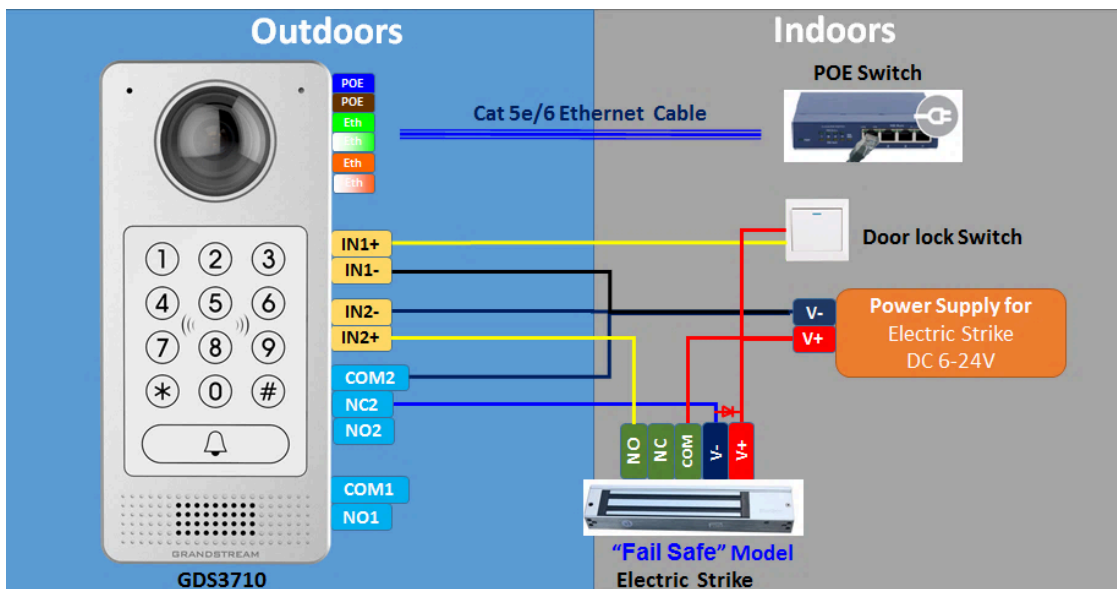
3<sup>rd</sup> party Power Supply Wiring Sample

**Wiring Sample using Power Supply for both GDS371x and Electric Strike**



Power Supply used for both GDS3710 and Electric Strike

**Wiring Sample using PoE to power GDS371x and 3<sup>rd</sup> Party Power Supply for Electric Strike**

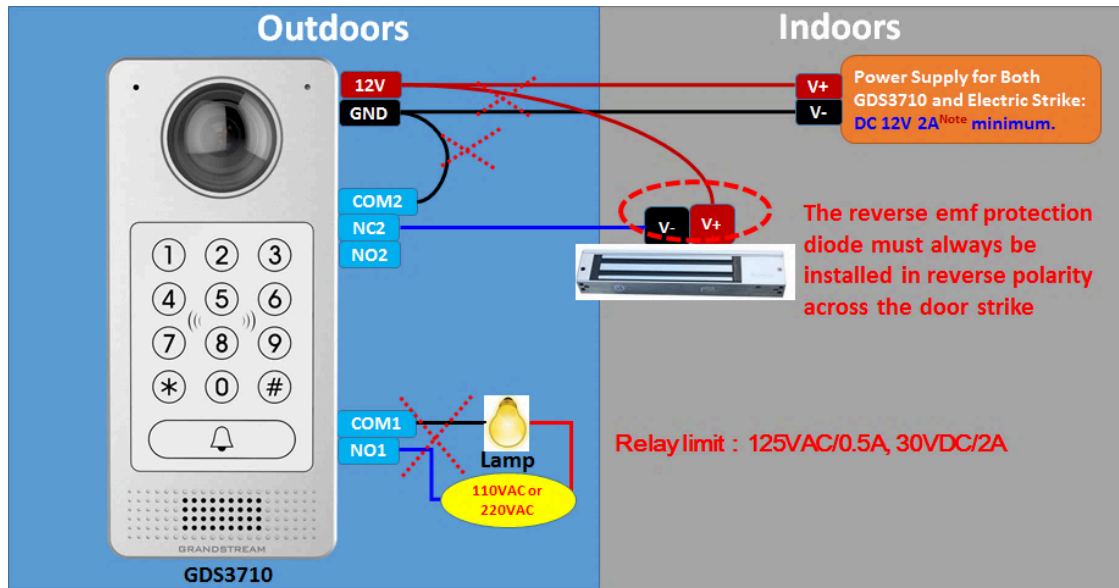


Power Supply used for both GDS3710 and Electric Strike



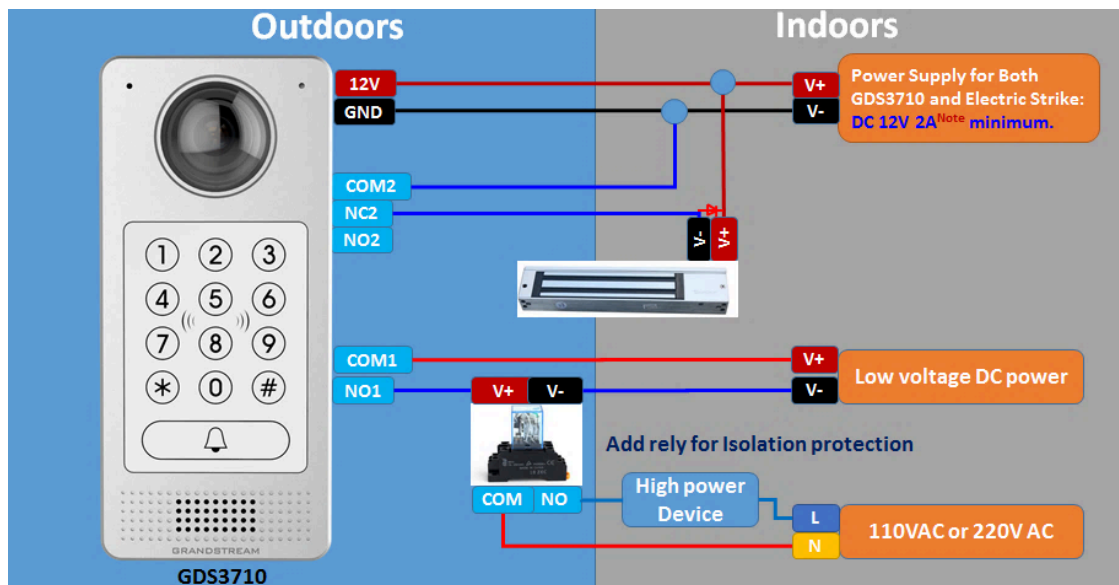
### Warning

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



Example to Avoid when Powering the Electric Strike

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

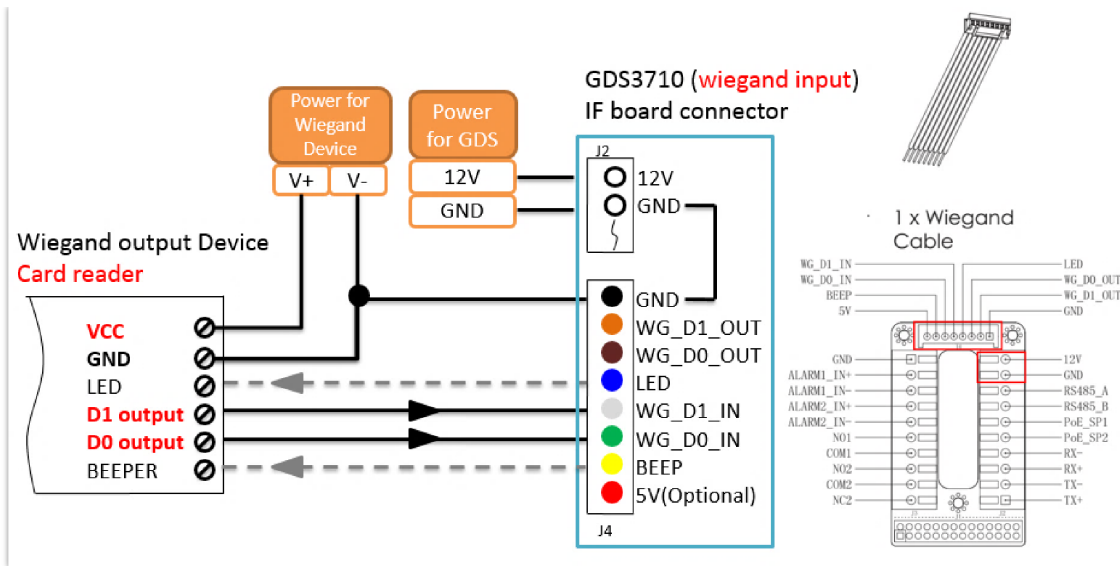


Electric Strike and High-Power Device Example

### Wiegand Module Wiring Examples

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

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

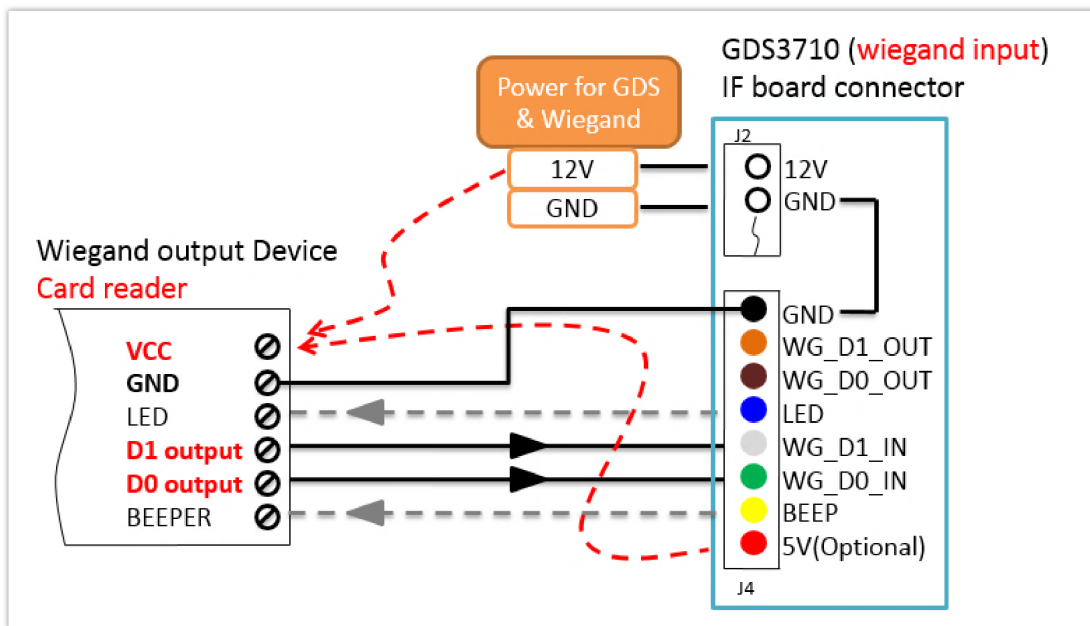


Wiegand Input Example with 3<sup>rd</sup> party Power Supply

Make sure to connect the GND of the Wiegand device and the GDS3710 Wiegand port.

For Wiegand input mode, LED and BEEP pins require that the Wiegand device support those interfaces. These two pins will not affect the Wiegand bus when not connected.

### Input example with power supply for both GDS371x and Wiegand device

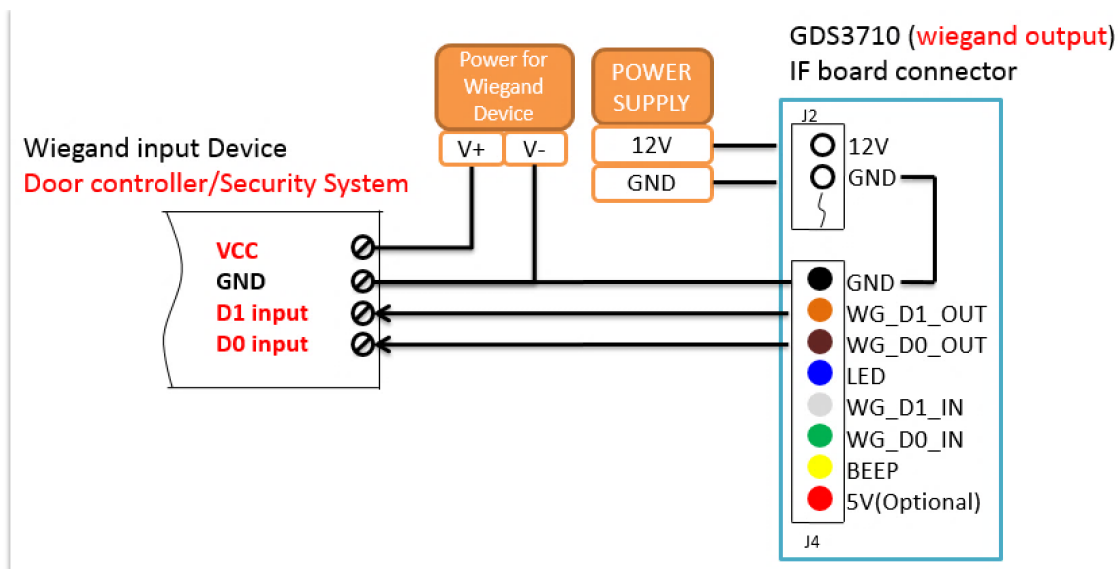


Wiegand Input Example with Power Supply for GDS3710 and Wiegand Device

If power source is **12VDC**, Wiegand device can share same power source of GDS3710. However, users need to check the max power consumption and the max capability of the power source.

If Wiegand device is using **5VDC**, GDS3710 Wiegand port can provide 5VDC with max 500mA to power up Wiegand device.

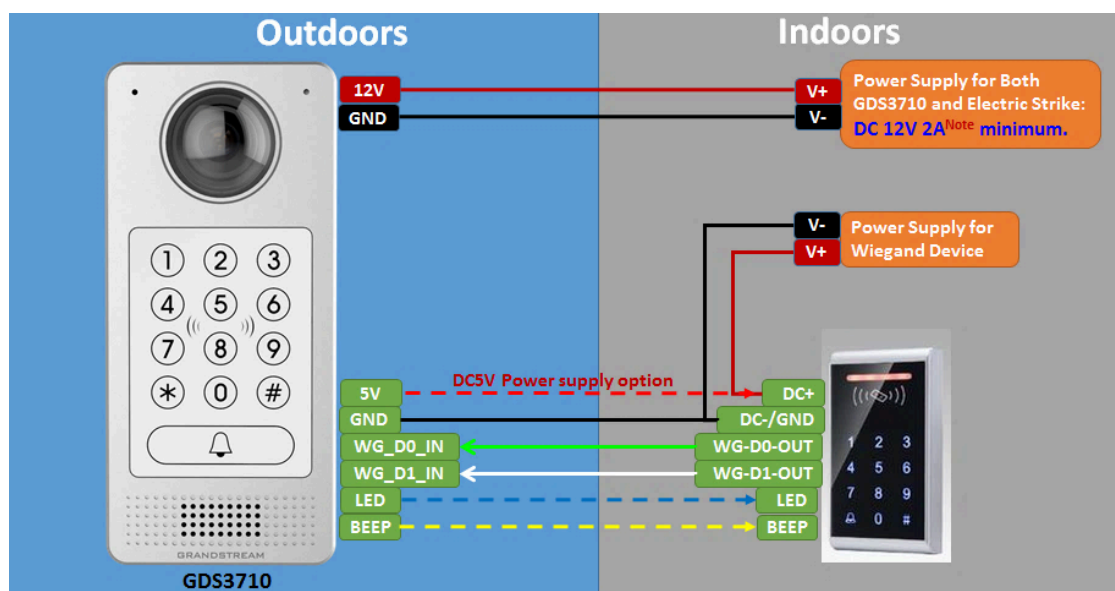
### Output example with 3<sup>rd</sup> party power supply for Wiegand device



Wiegand Output Wiring Example

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

### Wiegand RFID Card Reader Example



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 , Option valid only for the GDS3710 Model)

Once alarm triggered, the GDS371x will take snapshots when the abnormal open door happened, email and upload the snapshots to FTP or Central Server (when configured); call the configured alarm SIP phone, send the alarm output (if connected). User will only be able to disable the siren using the 3 methods mentioned above.

Detailed action information please refer to GDS37xx User Manual, "Alarm Action Settings" configuration.

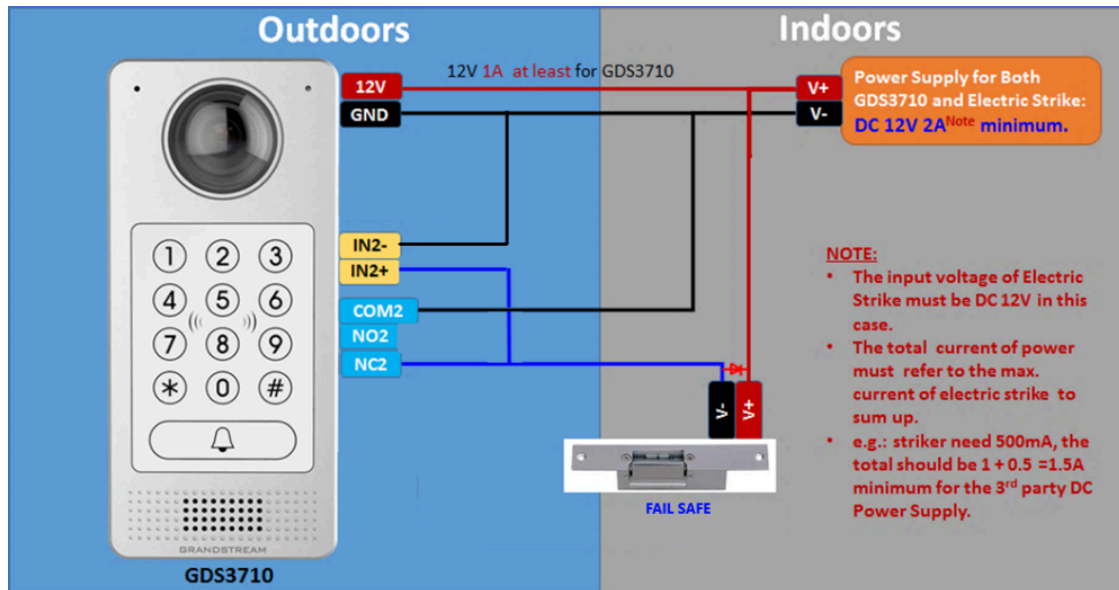
Below are some diagrams showing the correct wiring to enable this new security enhancement feature:

### GDS371x Connection: IN2 set as Normal Close and "Fail Safe" Electric Strike using 3<sup>rd</sup> Party Power Supply

#### Digit Input

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

*Digital Input set as Normal close*



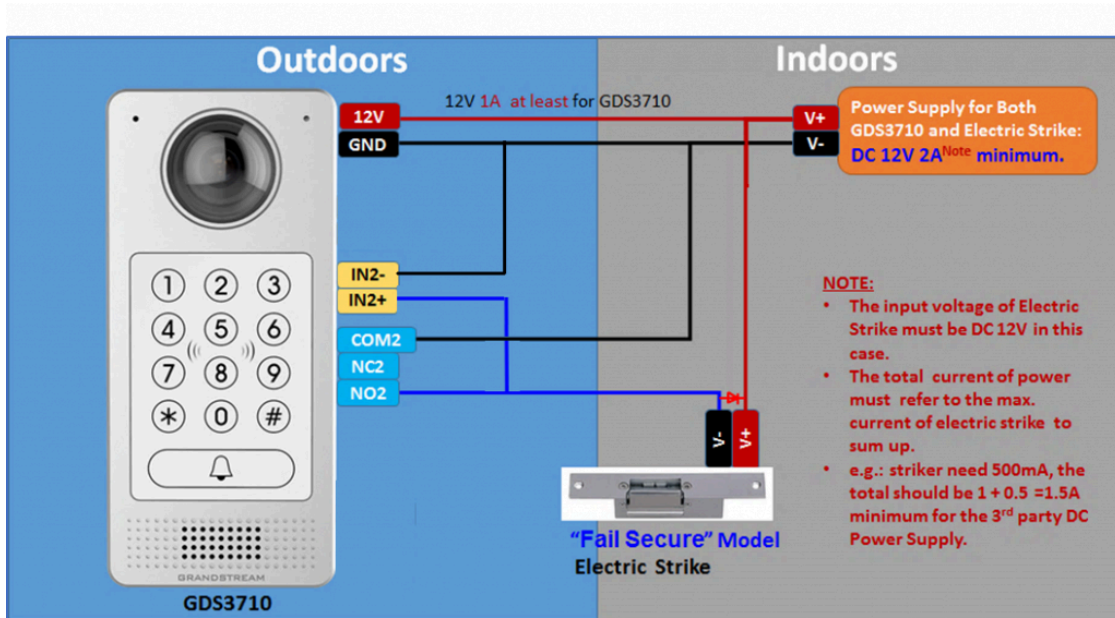
*Fail safe" Electric Strike using 3rd Party Power Supply*

### GDS371x Connection: IN2 set as Normal Open and "Fail Secure" Electric Strike using 3<sup>rd</sup> Party Power Supply

#### Digit Input

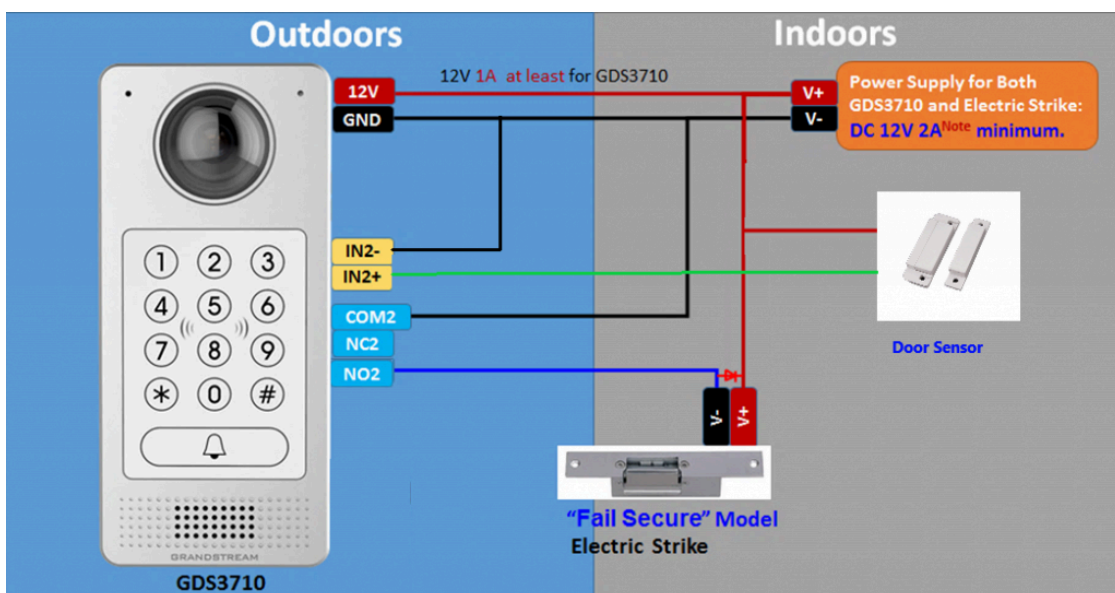
Digit Input 1	Abnormal Door Control
Digit Input 1 Abnormal Door Control Options	<input checked="" type="radio"/> Door 1 <input type="radio"/> Door 2
Digit Input 1 Status	Normal Open

*Digital Input set as Normal open*



"Fail Secure" Electric Strike using 3rd Party Power Supply

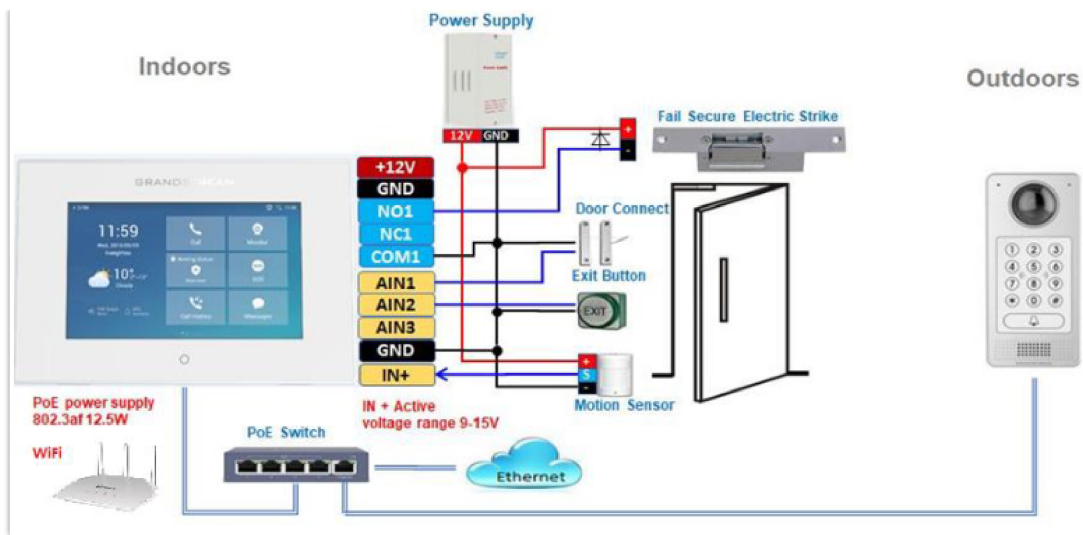
### GDS371x Connection: IN2 set as Normal Open and "Fail Secure" Electric Strike using 3<sup>rd</sup> Party Power Supply with Door sensor



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

### Secure Open Door Peering with GSC3570

Secure open door feature is a pairing scenario that is done between the GSC3570 control station and the GDS37xx door system, with GDS37xx installed outside, the GSC3570 is installed inside, the strike or lock is wired directly to the Alarm\_Out interface of GSC3570 to control the door from inside, therefore more secure compared to the strike wired directly to GDS37xx outside. Below is the application scene illustration:



GSC3570 secure open door via GDS3710

## Notes

Some considerations before configuring the Secure Open Door Peering with GDS37xx:

- GDS371x firmware 1.0.7.19 or above / GDS370x firmware 1.0.1.13 or above, are required to work with GSC3570.
- Only one door can be controlled by the GSC3570 since it has only one Relay Control circuit.
- If multiple doors need to be controlled by the GSC3570, then a SIP call is required, and the door strike/relay should be controlled by the related GDS37xx directly.
- The GSC3570 will turn on LCD when device in energy save mode (LCD Off) when secure open door event happened.
- When receiving an incoming call, a 3rd party audio/light strike device can be triggered by Door Open Port when wired properly on the GSC3570 side.
- When implementing secure open door, the door relay mode should be set to GSC3570 Relay.
- When configured correctly, the GSC3570 Secure Open Door will function with all GDS37xx open door mode: RFID card, Local PIN, Remote PIN (SIP Call or DTMF Open Door).
- RFID card can be used only on the GDS3710, and GDS3705 models.
- When using IP peering the SIP Transport must be set to "UDP"
- When using IP Peering, static IP address in same LAN must be used and the related Account need to configure "No" in the NAT Traversal.
- Remote open door without being in SIP direct IP is supported only on GDS3710/GDS3712 models.

Please refer to the following configuration guide to learn more about setting up Secure Open Door Peering with GDS37xx:  
[Peering GDS with GSC3570](#)

## One-Way Interlocking Mode

### Note

This configuration is exclusive to the GDS3710 Model.

This feature will allow GDS3710 to control two doors in one direction, with additional 3<sup>rd</sup> party window/door sensor installed accordingly (not provided by Grandstream). When configured and wired correctly, the two doors will operate under a controlling logic as below:

- 1) Only legal PIN or RFID card can open door when BOTH doors are detected closed. ( Only for GDS3710 Model )
- 2) When 1<sup>st</sup> door opened by valid user, the 2<sup>nd</sup> door is and will remain closed; the 2<sup>nd</sup> door will automatically open once detected the 1<sup>st</sup> door closed and programmed timer reached.
- 3) When 2<sup>nd</sup> door opening, the 1<sup>st</sup> door will NOT open even a valid PIN/RFID used. ( Only for GDS3710 Model )



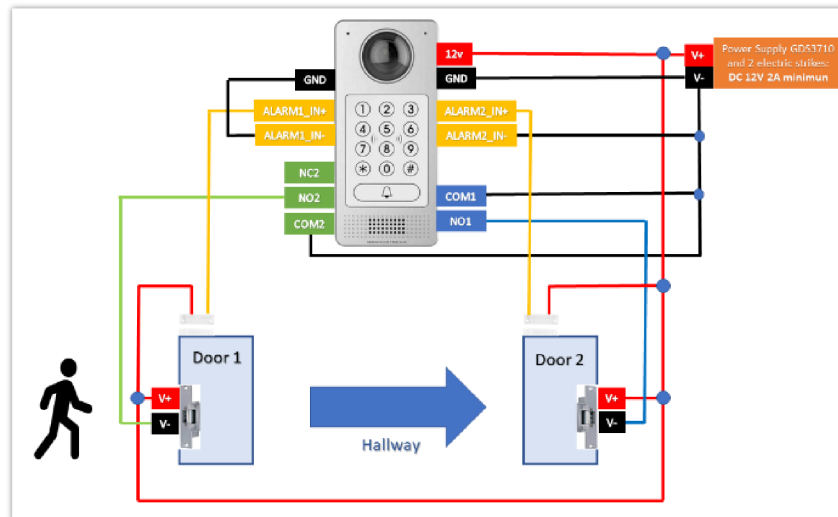
4) If entering 1<sup>st</sup> door and after 1<sup>st</sup> door closed and 2<sup>nd</sup> door opened, the person failed to enter 2<sup>nd</sup> door promptly (after 2<sup>nd</sup> door opening time out) will be locked in between two doors until next transaction happens or ask help (e.g.: call posted number or press button if there is one) from security staff to open door remotely (via SIP call into GDS3710 or GDSManager, for example).

This open door logic will make sure two doors are open in "One-Way" direction, at any given time only one door can be opened, and only one legal open door request is allowed to execute.

The hallway or scene between two doors could be monitored by installing Grandstream IP cameras.

This feature can be used in application scene like: College Dorm, Bank Branches, Government Offices, Medical Clinics, Private Clubs, etc., where there are two doors in place, high security and flow control is required (only one entry per time) but security guard may not be on site always.

Below is the illustrated drawing of the application scene as well as the wiring sample:



*One-Way Interlocking Mode Diagram Example*

#### Note

If required to use the same two doors for "Exit" direction, another GDS3710 is required and it can be configured in Door 2 to control "Exit" direction. The wiring/connection will be mirrored.

#### Web Configuration

This option can be found under device web UI → Door System Settings. Below example configuration screenshots are for reference only, customers need to test and get own parameters in field:

One-Way Interlocking Mode\_GDS3710\_Configuration\_1

## Notes

- Door 2 Delay before Unlock(s): Will be the total transit time from Door 1 to Door 2 right after the Door 1 is closed (this time will be "Door 1 unlock holding time").
- In above example, the Door1 unlock holding time is 2 seconds, the transit time of hallway is 6 seconds, therefore the Door 2 Delay before Unlock is set to 8 seconds.
- The transit time and unlock holding time will be decided and adjusted based on the actual application scene by the installer or system integrator.
- COM1 (ALMOUT1) only has two sockets for wiring, 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.

## Digital Input to Check Door Status (Door 1 & Door 2)

One-Way Interlocking Mode\_GDS3710\_Configuration\_2



Proceed to **Alarm Settings** → **Alarm Events Config** → **Digit Input**, configured as follow:

- **Digit Input 1: Door Status Check.** The DI will validate the current status of the Door, whether it is close or open, based on the sensor signal sending to the "Digit input 1".
- **Digit Input 1 Status:** If set to **Normal Open:** Configured door status check will be triggered when Digital Input Status switch from Close to Open, If set to **Normal Close:** Configured door status check will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 1 Status is "Disabled".
- **Digit Input 2: Door Status Check.** The DI will validate the current status of the Door, whether it is close or open, based on the sensor signal sending to the "Digit input 2".
- **Digit Input 2 Status:** If set to **Normal Open:** Configured door status check will be triggered when Digital Input Status switch from Close to Open, if set to **Normal Close:** Configured door status check will be triggered when Digital Input Status switch from Open to Close. By default, Input Digit 2 Status is "Disabled".

#### Note

- "Alarm Schedule" and "Alarm Action Profile" must be configured and selected otherwise the Digit Input channel will not be activated.
- There are two doors wired with window/door sensor separately, please make sure the door sensor is wired to correct Digit Input channel and refer to sample wiring diagram for reference [One-Way Interlocking Mode Diagram Example].

## Open Door via GDS37xx with or without a SIP Call

This feature needs related matching GDS37XX firmware to work. The minimum firmware version needed:

- **GDS3710: 1.0.7.19 or higher.**
- **GDS3705: 1.0.1.13 or higher.**

From GDS37XX side, the configuration is the same. Only difference is the number of doors be controlled: If using Local Relay controlled by GDS37XX, TWO DOORS can be controlled.

If using GSC3570 Relay, ONLY ONE DOOR can be controlled. The PIN and other settings are the same as SIP remote open door or GSC3570 secure open door for the GDS3710.

The difference will come out at the touch screen UI operation of GSC3570.

**Door System Settings**

Door Relay Options: Local Relay

ALMOUT1 Feature: Local Relay

ALMOUT1 Status: Webrelay

Control Options:  Door 1  Door 2

Wiegand Control:  Door 1  Door 2

Door 1 Delay before Unlock(s): 0

Door 2 Delay before Unlock(s): 0

Door 1 Unlock Holding Time(s): 5

Door 2 Unlock Holding Time(s): 5

Minimum Interval of Swiping Card(ms): 300

Call Mode: SIP Number

Doorbell Mode: Call Doorbell Number

Doorbell Call Out Account: Auto

Door Bell Call Mode: Serial Hunting

Number Called When Door Bell Pressed: 192.168.11.138:5060

Remote PIN to Open Door 1: \*\*\*\*\*

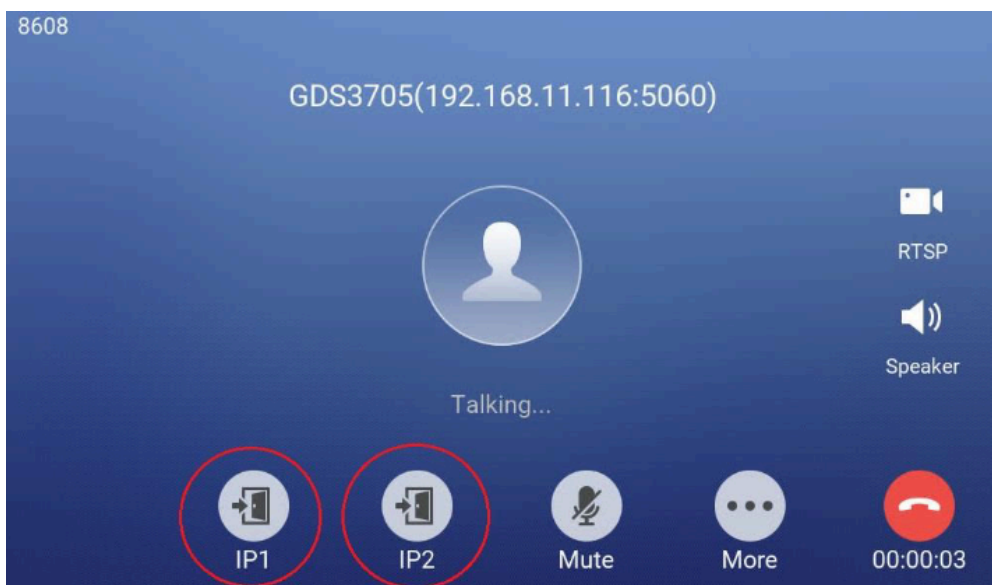
Remote PIN to Open Door 2: \*\*\*\*\*

Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
1	GDS	Account 1	Front_Door	873		Front_Door			
2	GDS	Account 1	Back_Door	877		Back_Door			
3	GDS	Account 1	GDS3710	192.188.11.125	192.188.11.125	IP			
4	GDS	Account 1	GDS3710	8606		SIP			
5	GDS	Account 1	GDS3705	192.188.11.116	192.188.11.116	IP1		IP2	***
6	GDS	Account 1							

GSC3570 Configuration Example

**Door opening with SIP Call:**

When GSC3570 established call with GDS37XX, the screen will display virtual open door button(s), and user will press the button to open door:

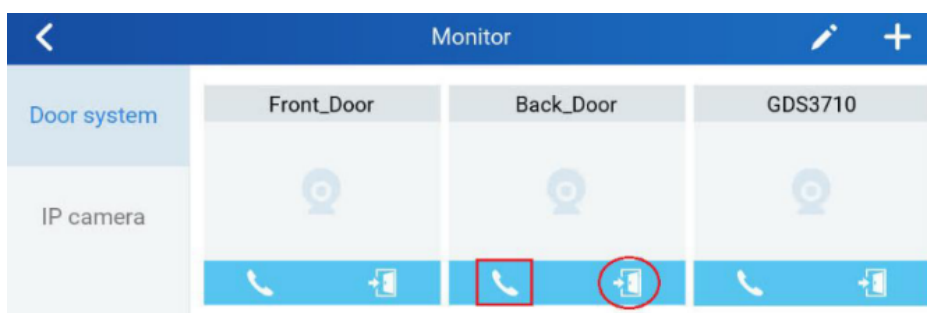


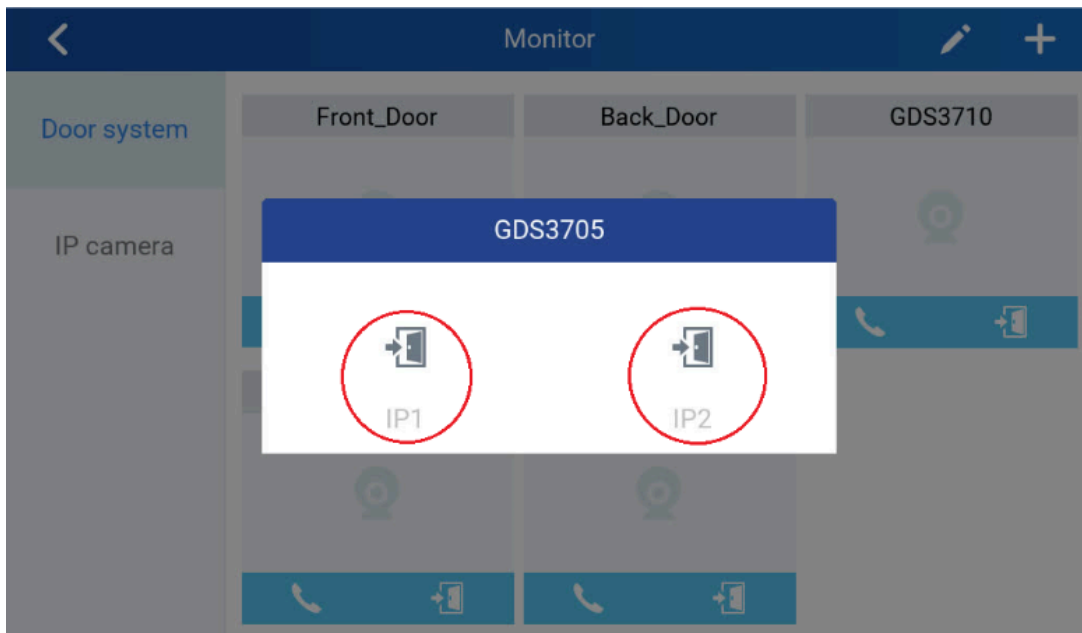
Open Door with SIP Call

**GSC3570 Open Door NO SIP Call:**

At the GSC3570 idle screen, press "Monitor →Door system", the related GDS37XX will be displayed. In the blue bar, left is a "Phone" icon and right is the "Open door" icon. The "Phone" icon will establish SIP call as previous firmware behaved.

Press "Open door" icon, the GSC3570 will open door directly and NO SIP CALL will be established. Depending on how many doors controlled, if one door configured, the door will open directly; if two doors configured, another screen will pop up to allow user to choose which door to open, as shown below:





When the door is successfully opened the following message will appear:

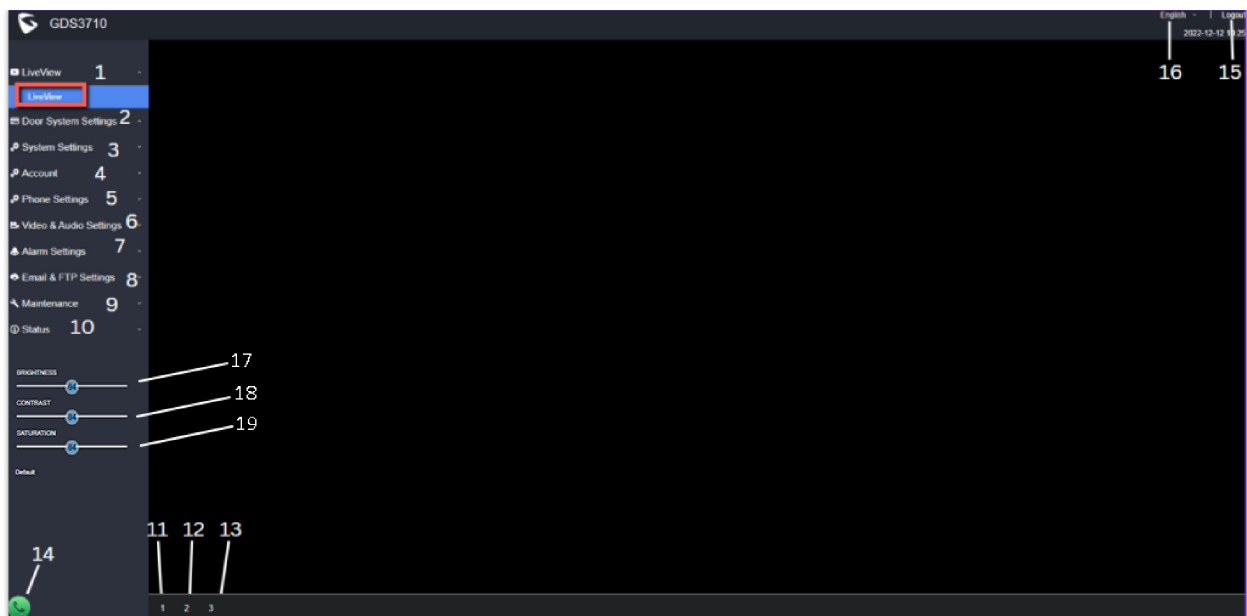


*Open Door without SIP Call*

## GDS371x HOME WEB PAGE

Once logged in successfully to the GDS371x, user will see the following page.

**Note:** the options displayed might differ from browser to another, and from a GDS model to another (GDS3710/GDS3712)



Home Page: Internet Explorer 11

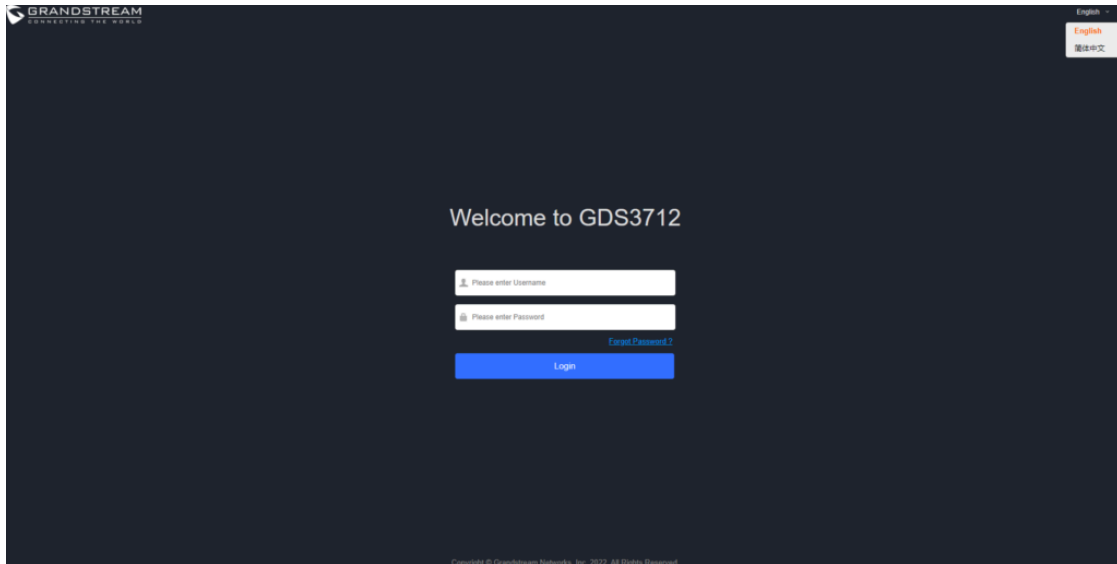
Number	Fields	Description
1	LiveView	Access to live view stream page.
2	Door System Settings	Access to “Door System Settings” page.
3	System Settings	Access to “System Settings” page.
4	Account	Access to “Account” configuration page.
5	Phone Settings	Access to “Phone Settings” configuration page.
6	Video & Audio Settings	Access to “Video & Audio settings” page.
7	Alarm Settings	Access to “Alarm settings” page.
8	Email & FTP Settings	Access to “Email & FTP Settings” page.
9	Maintenance	Access to “Maintenance” page.
10	Status	Click to enter “Status” page.
11	Stream 1	Play the primary stream.
12	Stream 2	Play the secondary stream.
13	Stream 3	Play the third stream.
14	Calling interface	Allows to dial an extension from the web interface and select an account to place the call
15	Logout	Logout from the web page.
16	Language	Select the webpage language.
17	Brightness	Adjusts the live preview brightness

18	Contrast	Adjusts the live preview contrast
19	Saturation	Adjusts the live preview saturation

*Home Page Description*

## GDS371x Configuration & Language Page

- Once the IP address of the GDS371x is entered on the user browser, the login web page will pop up allowing user to configure the GDS371x 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.



*GDS3712 Login Page*

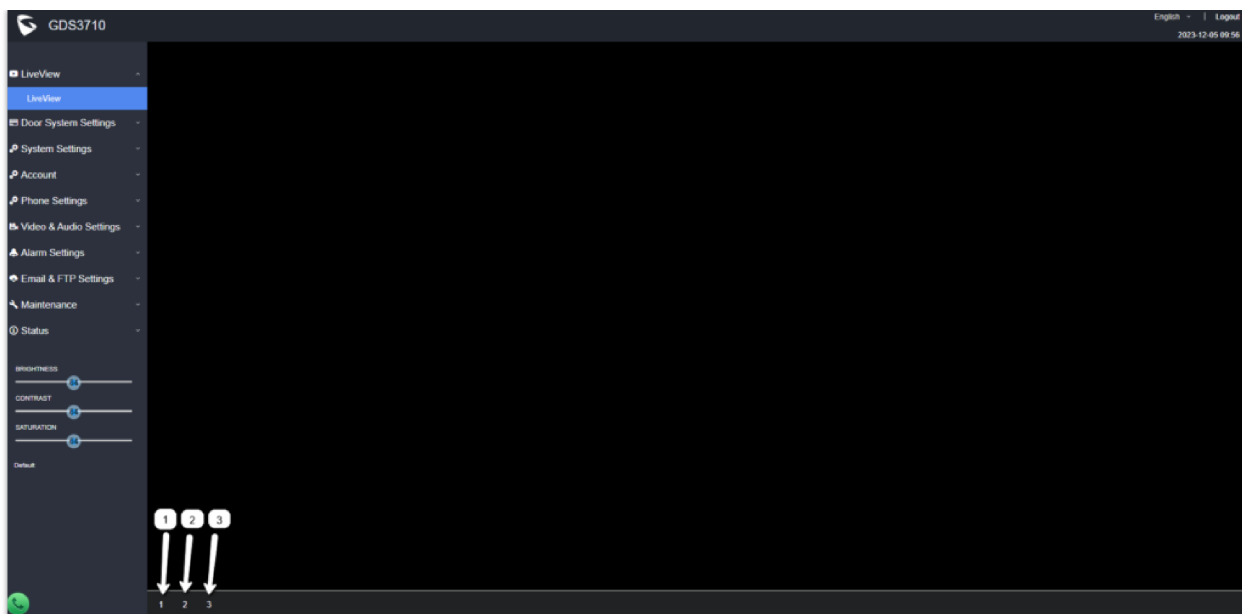
### Note

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

## GDS371x SETTINGS

### Live View Page

This page allows users to view the live video of the GDS371x using popular browsers like Chrome or Firefox immediately without downloading and installing any plugins.



Live View Page: Google Chrome

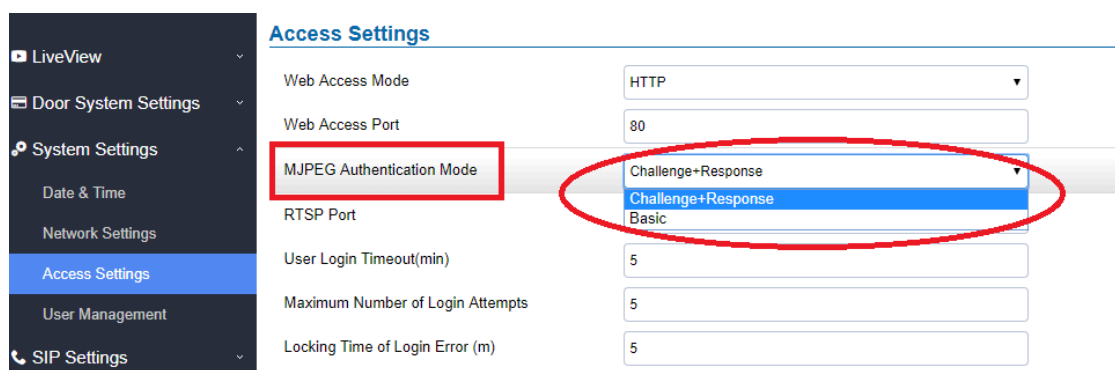
Three streams are available:

- **1 => Primary video stream:** 1920\*1080 resolution, recommended for continuous full HD recording.
- **2 => Secondary video stream:** 640\*480 resolution (1280 x 720 resolution for GDS3712), recommended for SIP/VoIP video calls (if used with GXV3470/GXV3480).
- **3 => 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 GDS371x 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 *JPEG Authentication Mode*, which can be set under following path:

**Web UI → System Settings → Access Settings**

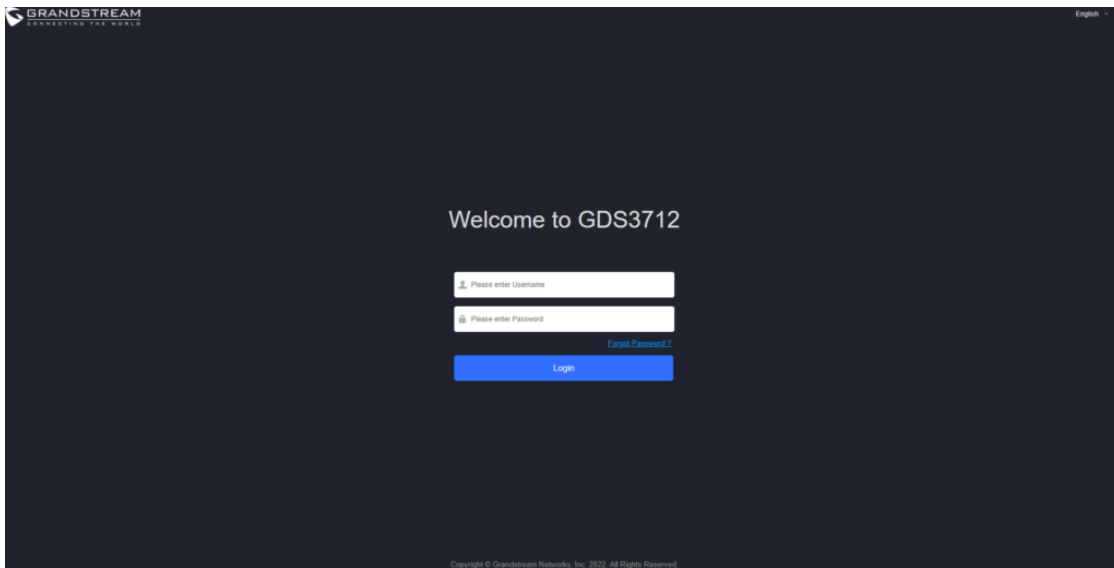


MJPEG Authentication Mode

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

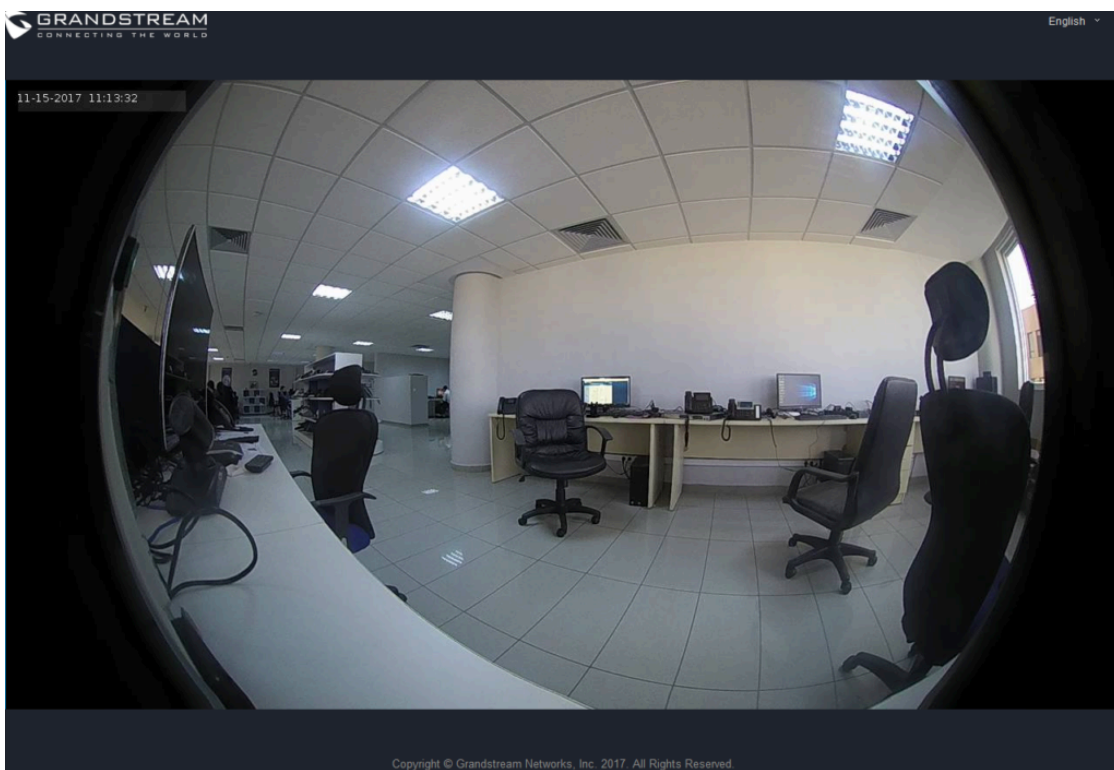
Please follow below steps in order to take a snapshot via HTTP commands on this mode:

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



*GDS3712 Admin credentials page*

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



*Snapshot view using secured MJPEG authentication Mode*

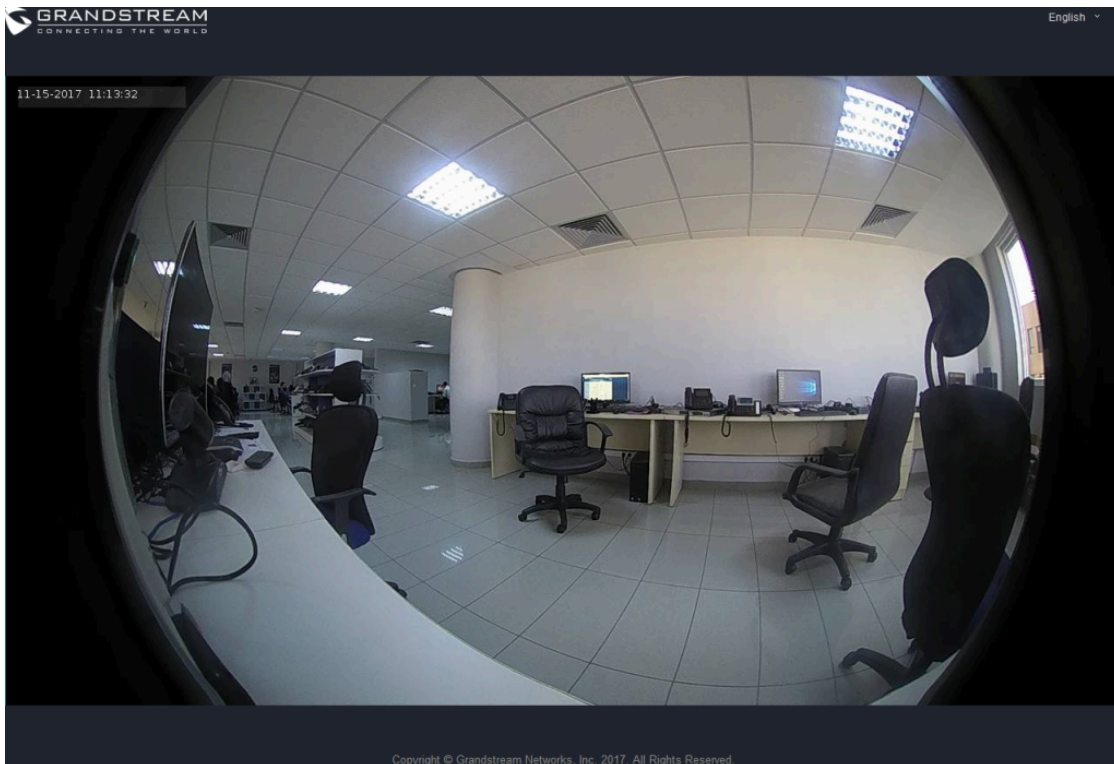
**Note**

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

**2). Basic MJPEG Authentication Mode:**

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

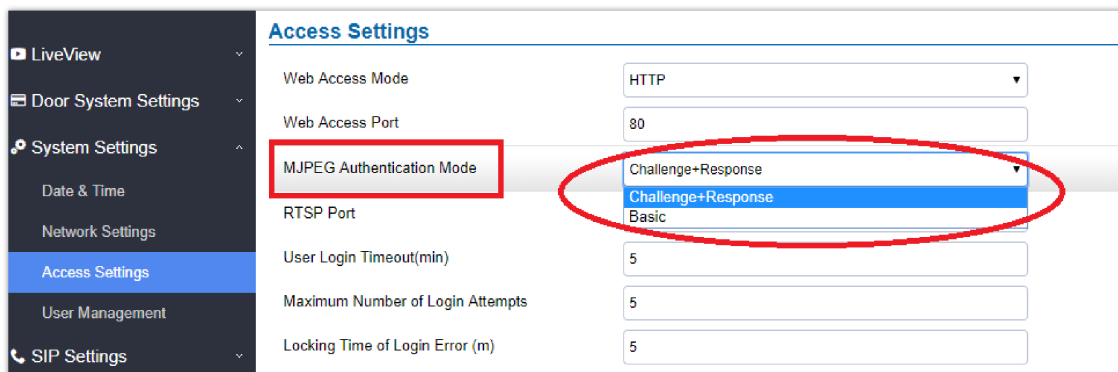
1. In browser type in: **http(s)://admin:password@IP\_Address\_GDS:Port/jpeg/view.html**
2. The browser will show one frame of the video (720p) as a snapshot.



## MJPEG Stream

The GDS371x 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 *JPEG Authentication Mode*, which can be set under following path:

**Web UI → System Settings → Access Settings**



*MJPEG Authentication Mode*

### Note

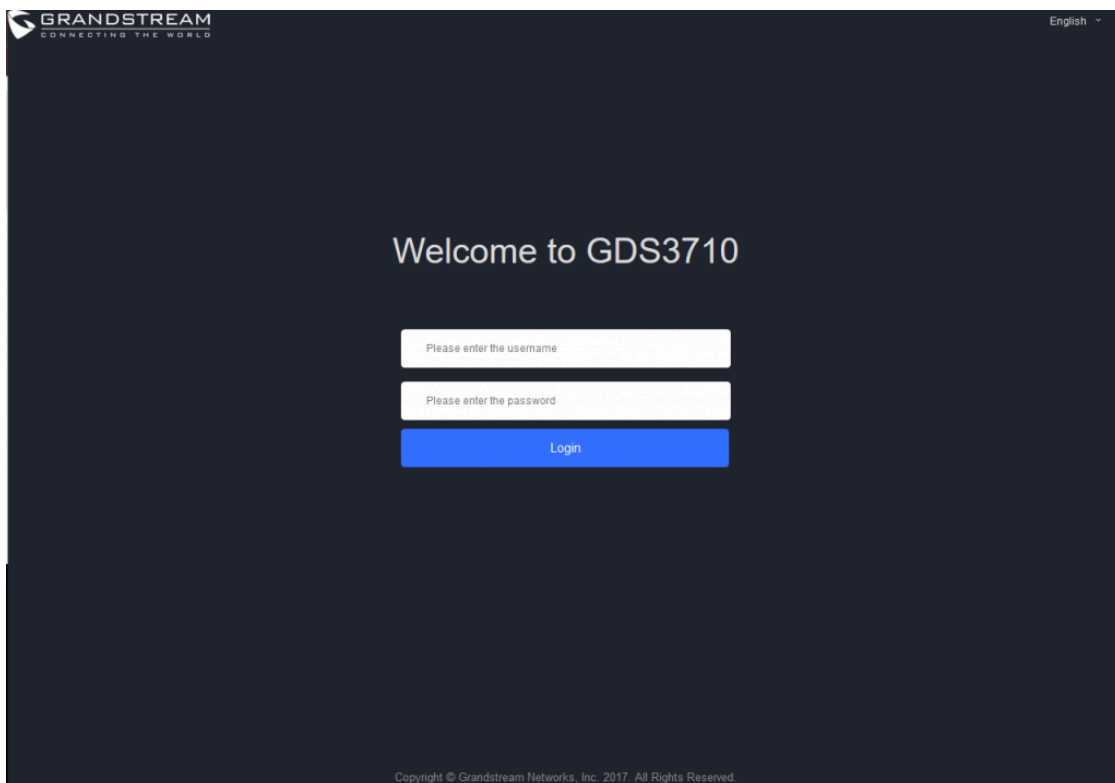
Please note that when the GDS371x device is added to UCM Remote Connect, then the MJPEG stream function will not work with the IP phone models such as the GRP26xx and GXP21xx, and the Wi-Fi phone models such as the WP820, in this case, it is recommended to use a video phone model such as the GXV34xx to stream video feed on the GXV34xx from the GDS371x.

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

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

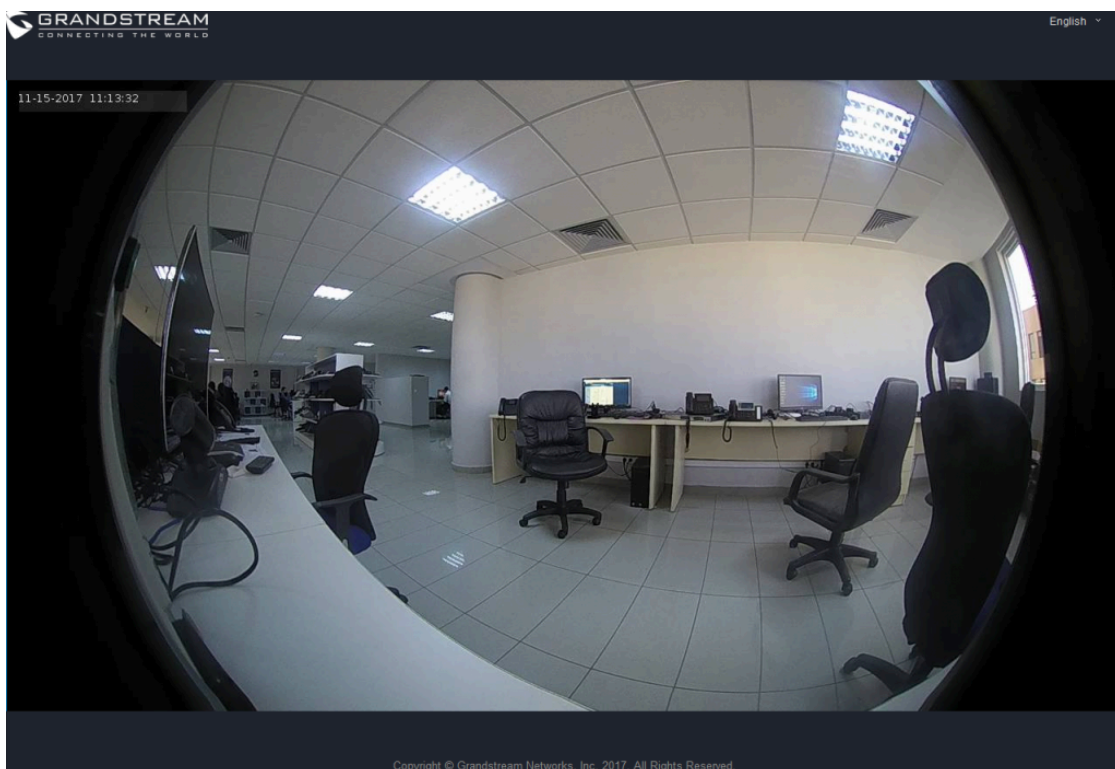
1. In browser type in: **http(s)://IP\_Address\_GDS:Port/jpeg/mjpeg.html**
2. The browser will pop up the window above asking for credentials, user needs to enter admin credential.





*MJPEG view admin credential*

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



*MJPEG live view using secured MJPEG Authentication Mode*

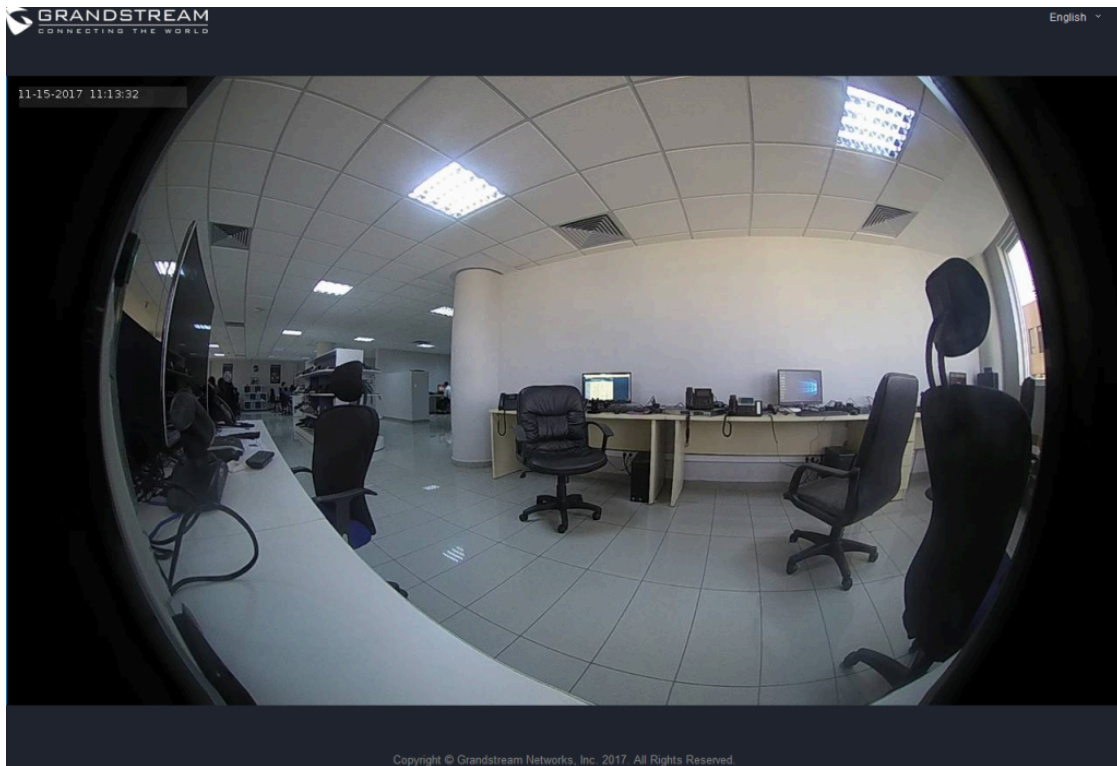
#### **Note**

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

#### **2). Basic MJPEG Authentication Mode:**

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

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



*MJPEG view using Basic MJPEG Authentication Mode*

**Note**

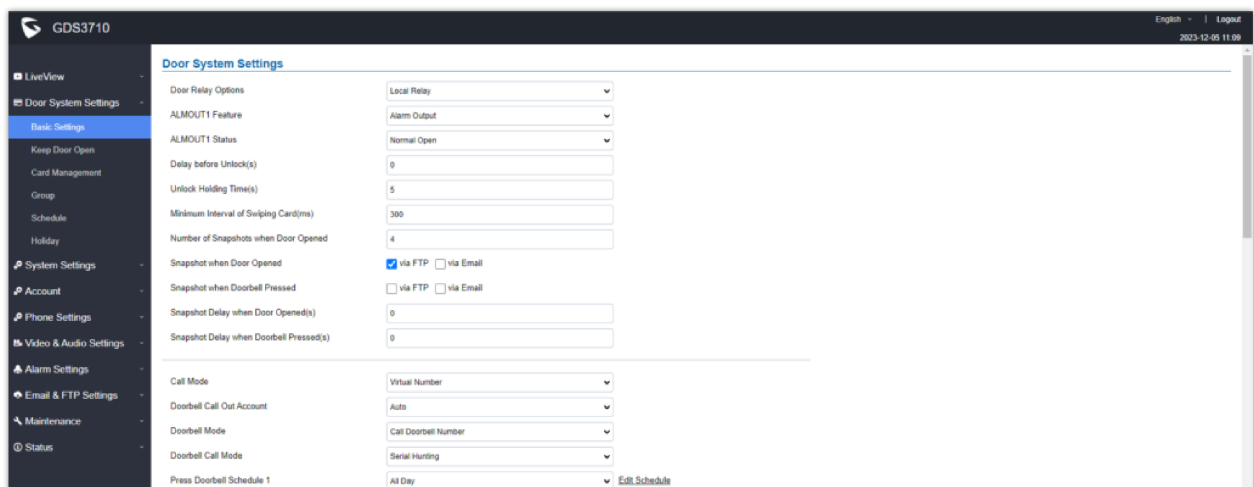
Similar command can be applied to open source application like **VLC MediaPlayer** to retrieve H.264 video stream with better quality: **rtsp://admin:password@IP\_GDS3710:Port/X**

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

**Door System Settings**

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

**Basic Settings**



*Door System Settings Page*

<p><b>Door Relay Options</b></p>	<p>This feature allows customers to integrate GDS37XX with 3rd party web relay to control door open over network, via script or other applications, to meet real application scene and enhance security. User need to input web relay IP address or domain name, as well as authentication information, to make this to work.</p> <p>There are four choices in the pull-down selection:</p>
----------------------------------	---

	<ul style="list-style-type: none"> <li>● <b>Local Relay:</b> Local Relay is the GDS371x controlling the relay. The strike is wired into the COM2 or COM1 port of the GDS371x depending 1 door or 2 door need to be controlled.</li> <li>● <b>Webrelay:</b> When Webrelay is selected, customers need to continue configure the webrelay IP address or domain name, together with credentials like Username and Password. When legal open door event happened, the configured web relay will get the communication from GDS371x, and will operate the strike to open door for the authenticated open door request.</li> <li>● <b>GSC3570 Relay:</b> When the Door relay is set to GSC3570, it gives the option to connect it to the GSC3570 device by entering the Phone number and door password.</li> <li>● <b>Send Wiegand Code on Remote Open Door Action:</b> When this mode is selected, The device will send PIN1/PIN2 code via the Wiegand interface when the remote HTTP API open door1/door2 has been executed.</li> </ul> <p><b>Note:</b> In web relay mode, the strike is wired to the web relay controller device.</p>
<b>Webrelay URL ON</b>	<p>When Door relay Option set to Webrelay, then enter the correct URL used by the third party controller so that the GDS3710 send the command to activate the relay.</p> <p>This adds an extra layer of security so when legal open door event happened, the configured web relay will get the communication from GDS3710, and will operate the strike to open door for the authenticated open door request or use that command to operate other industry application.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● Now there are two Webrelay URL fields available, with On or Off URL command allowed or other usage URL command allowed. Also allow Username and Password configured if the 3rdparty Webrelay requiring this security feature.</li> <li>● If some 3rdparty Webrelay only support one URL command, then just leave another Off URL blank, or put whatever there as long as it is NOT a URL command.</li> </ul>
<b>Webrelay URL OFF</b>	<p>When Door relay Option set to Webrelay, then enter the correct URL used by the third party controller so that the GDS3710 send the command to disable the relay.</p>
<b>Webrelay Username</b>	<p>Enter the web relay username.</p>
<b>Webrelay Password</b>	<p>Enter the web relay password.</p>
<b>ALMOUT1 Feature</b>	<p>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 the option “Open Door” is selected, will enable GDS3710 to control the operation of two doors via RFID, and local and remote PINs.</p>
<b>ALMOUT1 Status</b>	<p>Select Normal Open or Normal Close depending on the lock used.</p>
<b>Delay before Unlock (s)</b>	<p>Device will open door after specified delay (in seconds) when user issuing the authorization.</p>
<b>Unlock Holding Time (s)</b>	<p>Configures the lock holding time, in seconds (default value is 5 seconds). Device will hold the door unlocked for this specified duration. Range: 1-1800 seconds.</p>
<b>One-way Interlocking Doors Mode</b>	<p>This option allows to control two doors for access control in one-way mode. Once the card or PIN is fully validated by the GDS3710, it will check the status of both doors (using 3rd party window/door sensors - not provided by Grandstream - to verify if they are opened or closed), if both doors are closed the Door 1 will open allowing the person to pass through hallway, once the Door 1 is closed it will start counting and when the timeout is reached, the Door 2 will open granting access to the person in the facility.</p> <p><b>Note:</b> This feature is available only at for GDS3710.</p>
<b>Control Options</b>	<p>Configures weather to allow the two doors to be controlled by local RFID cards or PINs for access.</p>

	<b>Note:</b> This feature is available only at for GDS3710.
<b>Wiegand Control</b>	Configures weather to allow the two doors to be controlled by wiegand or keypad Input. <b>Note:</b> This feature is available only at for GDS3710.
<b>Door 1 Delay before Unlock(s)</b>	The device will open door 1 after the specified delay (in seconds) when user has issues the authorization.
<b>Door 2 Delay before Unlock(s)</b>	The device will open door 2 after the specified delay (in seconds) when user has issues the authorization.
<b>Door 1 Unlock Holding Time(s)</b>	The device will hold the door 1 unlocked for a while (1-1800 seconds)
<b>Door 2 Unlock Holding Time(s)</b>	The device will hold the door 2 unlocked for a while (1-1800 seconds)
<b>Minimum Interval of Swiping Card (ms)</b>	Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms. <b>Note:</b> option only available for GDS3710
<b>Number of Snapshots when Door Opened</b>	Define number of snapshot to be sent by the GDS (via FTP or Email) Maximum up to 4 screenshots.
<b>Snapshot when Door Opened</b>	User can choose to email the snapshot when door is opened without sending the snapshots via FTP to the FTP server.
<b>Snapshot when Doorbell Pressed</b>	User can choose to email the snapshot when doorbell pressed without sending the snapshots via FTP to the FTP server.
<b>Snapshot Delay when Door Opened(s)</b>	Configures the delay in seconds to the snapshots taken when Door Opened. The valid range is 0-10 seconds. Default value is 0, meaning there will be no delay for taking the snapshot when door opened.
<b>Snapshot Delay when Doorbell Pressed(s)</b>	Configures the delay in seconds to the snapshots taken when Doorbell pressed. The valid range is 0-10 seconds. Default value is 0, meaning there will be no delay for taking the snapshot when door pressed.
<b>Call Mode</b>	Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3710 keypad.
<b>Doorbell Call Out Account</b>	This option sets the account to be used to make call upon the doorbell trigger. If set to Auto, the GDS will use the first available account.
<b>Doorbell Mode</b>	Configures the action to be taken when the doorbell is pressed, three options are available: <ul style="list-style-type: none"> <li>● <b>Call Doorbell Number:</b> when Doorbell is pressed, a call will be made to the “Number Called When Door Bell Pressed”</li> <li>● <b>Control Doorbell Output (Digital Output 1):</b> when Door Bell is pressed electronic lock for Output 1 is opened with a time duration of (1s to 4s), <b>Option available Only on GDS3710 Model</b></li> <li>● <b>Both of Above:</b> When selected, both Call Doorbell Number and Control Doorbell Output options are enabled , <b>Option Available Only on GDS3710 Model</b></li> </ul>
<b>Door Bell Call Mode</b>	Select the ring strategy for the Numbers Called when pressing the Door Bell button to be either Serial or Parallel: <ul style="list-style-type: none"> <li>● <b>Serial Hunting:</b> the configured extensions and/or IP addresses will ring one after one by order.</li> <li>● <b>Parallel Hunting:</b> The configured extensions and/or IP addresses will ring simultaneously (up to 4 simultaneous SIP calls).</li> </ul>

<p><b>Press Doorbell Schedule [1-4]</b></p>	<p>Select the schedule when pressing the doorbell will call the configured destination.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>● Maximum 4 different “Schedule” can be configured.</li> <li>● “Doorbell” Call Number or IP address must be configured in related “Schedule”</li> <li>● The priority order of schedule is “Schedule 1, 2, 3, 4”. The device will first check and verify current time fits in “Schedule 1”, if yes it will dial out using the configured number in Number 1; if not it will check “Schedule 2” and dial out using the configured number in Number 2 if result matched, and continue to do such checking and verification in loop till end.</li> </ul>
<p><b>Number [1-4] Called When Door Bell Pressed</b></p>	<p>Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed:</p> <ul style="list-style-type: none"> <li>● <b>SIP Server mode:</b> <ul style="list-style-type: none"> <li>○ The field can be configured to store multiple one or multiple SIP extensions, if configured with multiple extensions (ex: 1001, 1002, 1003), separated with “,” the GDS3710 will ring one extension after the other in a <b>Serial Hunting Mode</b> (GDS will ring each extension by default 15 seconds, this can be changed on the Ring Timeout) or ring them simultaneously in <b>Parallel Hunting Mode</b>.</li> <li>○ When using UCM, users can also configure there a Ring Group extension (6400 for example) that will ring multiple extensions simultaneously, or one by one depending on the Ring Group ring strategy.</li> <li>○ If all phones are GXP21XX, the phone will stream the video frame by frame and users can open door either by pressing <b>Remote_PIN#</b> or by pressing Open Door button if already configured.</li> <li>○ If early media is enabled on phone side, user can send the PIN code using the Open-Door button before answering the call (Of course users can open the door also after answering the call).</li> </ul> </li> <li>● <b>Peering mode:</b> <ul style="list-style-type: none"> <li>○ User should configure multiple IP addresses of phones instead of SIP extensions, when Door Bell pressed the GDS3710 will ring the configured IP Addresses in <b>Serial or Parallel Mode</b> according to Doorbell Call Mode strategy.</li> <li>○ If early media is enabled, the GXV33XX will receive the video stream while it is ringing, and user can open door by pressing the Open-Door button if already configured (Of course users can open the door also after answering the call).</li> <li>○ GXP21XX phones receive the GDS3710 video using JPEG streaming this means that it will receive video if early media is enabled or disabled. <b>Note:</b> This field supports a Maximum of 256 characters.</li> </ul> </li> </ul>
<p><b>Maximum Number of Dialed Digits</b></p>	<p>Configure the maximum digits allowed to dial in the keypad. Once the configured condition is satisfied, the device will send out the number to call automatically without pressing #. It is disabled if set to 0.</p> <p><b>Note:</b> Configuration can be done only on the GDS3710.</p>
<p><b>No Key Input Timeout(s)</b></p>	<p>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.</p> <p><b>Note:</b> Configuration can be done only on the GDS3710.</p>
<p><b>Press Doorbell Schedule</b></p>	<p>Configure a schedule for the Doorbell button, once configured, the doorbell will turn ON/OFF based on configured schedule. Default setting is “All Day”.</p>
<p><b>Remote PIN to Open the Door</b></p>	<p>Configures PIN code stored in the GDS3710, remote SIP phone needs to input and match this PIN (the PIN is sent via DTMF while in call) so that the GDS3710 can open the door.</p> <p><b>Note:</b> For enhanced security, when the call is initiated from GDS then only the numbers existing in “White List” will be able to use DTMF PIN to open door remotely.</p>
<p><b>Local PIN Type</b></p>	<p>Three options are available: Private Card PIN, Unified PIN or Card and Private PIN.</p>

	<ul style="list-style-type: none"> <li>● <b>Private PIN:</b> Means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3710 to open the door [<i>*Virtual Number*Private PIN#</i>].</li> </ul> <p><b>Notes:</b></p> <ol style="list-style-type: none"> <li>1. When Local PIN type is set to <b>private PIN</b>, users can also open the door by swiping their cards.</li> <li>2. If “Disable Keypad SIP Number Dialing” is checked, users will be able to open door using private PIN with following sequence [<b>Private PIN</b>].</li> </ol> <p><b>Note:</b> Door can still be opened by Card and with the sequence [<i>*Virtual Number*Private PIN</i>]. For more details and conditions, refer to [Disable Keypad SIP Number Dialing].</p> <ul style="list-style-type: none"> <li>● <b>Unified PIN:</b> Means all members share a same PIN to unlock the door. Users need to enter the following sequence from the GDS3710 keypad to open the door [<i>*Local PIN to Open the Door#</i>].</li> </ul> <p><b>Notes:</b></p> <p>If “Disable Keypad SIP Number Dialing” is checked, users will be able to open door using Local PIN with following sequence [<i>Local PIN</i>].</p> <ul style="list-style-type: none"> <li>● <b>Card &amp; Private PIN:</b> Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence [<b>Swipe the card + * Private PIN#</b>]</li> </ul> <p><b>Note :</b> This feature is available to be configured only on the GDS3710 Model.</p>
<b>Local PIN to Open the Door</b>	<p>Configures PIN stored in GDS3710, input locally this PIN on the GDS3710 keypad will unlock the door.</p> <p>This feature needs Private PIN, means every member has a private PIN, the GDS will record who unlocked the door every time.</p> <p>Users need to enter the following sequence from the GDS3710 to open the door [<i>*Virtual Number*Private PIN#</i>].</p> <p><b>Note:</b> When local PIN type is set to private card PIN, users can also open the door by swiping their cards.</p>
<b>Local PIN to Open Door Schedule</b>	<p>Configure a schedule for the Local PIN to open the door. Once configured, the door opening ability using a local PIN with turn ON/OFF based on a configured schedule. The default setting is “All Day”.</p>
<b>Enable DTMF Open Door</b>	<p>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.</p>
<b>Enable Guest PIN</b>	<p>Enables password entry for guests.</p>
<b>Guest PIN</b>	<p>Configures the password that will be used by guests.</p>
<b>Guest PIN Start Time</b>	<p>Selects the start time when the Guest PIN start to take effect.</p>
<b>Guest PIN End Time</b>	<p>Selects the end time when the Guest PIN will stop working.</p>
<b>Disable Auto Answer</b>	<p>If checked, GDS3710 will not answer incoming calls automatically, users can press any key to answer the call. Default setting in unchecked.</p>
<b>Enable Doorbell Button to Hang up Call</b>	<p>If checked, Users can hang up an active call when pressing the doorbell button. Enabled by default.</p>
<b>Disable Keypad (except the Doorbell Button)</b>	<p>When checked the Keypad will be disabled, only Door Bell button can be pressed.</p>



<b>Enable On Hook After Remote Door Opened</b>	When checked calls will be disconnected automatically after the remote open door event.
<b>Onhook Timer After Remote Open Door(s)</b>	Defines the duration in seconds when the calls will be disconnected after the remote open door event. The valid range is 3-1800 The default value is 3 seconds.
<b>Enable HTTP API Remote Open Door</b>	Enabling this option allows to use HTTP API command to open the door remotely. <ul style="list-style-type: none"> <li>● <b>Disable:</b> to disable the option.</li> <li>● <b>Challenge + Response Authentication:</b> this option allows the use of a multi-step method to authenticate</li> <li>● <b>Basic Authentication:</b> this option uses a simple request to authenticate:</li> </ul> 1. Open the door command example: <i>https://admin:password@192.168.23.123/goform/apicmd?remotepin=12345&amp;type=1</i> 2. Close the door command example: <i>https://admin:password@192.168.23.123/goform/apicmd?remotepin=12345&amp;type=2</i> <b>Important note:</b> We will not be responsible for any security problems resulting from opening the HTTP API remote function, this option is disabled by default and the user should enable it while knowing how to mitigate the risk. <b>Note:</b> The option to send PIN via Wiegand when HTTP API open door executed is added on the new firmware upgrade for the GDS3710 Model.
<b>HTTP API Open Door Compatibility Mode</b>	If this option is enabled, HTTP API Open Door will be supported under HTTPS mode. Disabled by Default.
<b>Disable Keypad SIP Number Dialing</b>	When Keypad SIP number Dialing disabled, device will interpret each digit entry as private-password open door request after pressing #. <b>Notes:</b> <ul style="list-style-type: none"> <li>● “Local PIN Type” should choose “Private PIN”.</li> <li>● Dial keypad to make SIP call will NOT work (except for doorbell button call).</li> <li>● Private PIN must be <b>UNIQUE</b> among users, otherwise the door will still open but log will NOT tell who opened the door due to duplicated PIN and whoever user last matched in the database with the Private PIN will be shown in the log.</li> </ul>
<b>Card Issuing Mode Settings</b>	
<b>Enable Card Issuing Mode</b>	Enables RFID card issuing/program into the GDS3710. When selected sweeping an RFID card into the GDS3710 will add card information into.
<b>Card issuing State Expire Time(m)</b>	Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes).
<b>Light Settings</b>	
<b>Enable Key Blue Light</b>	When checked, the blue light will be activated when pressing the GDS3710 Keys.
<b>Enable Background Light</b>	When checked, the background light will turn on once clicking the GDS3710 Keys.
<b>Blue Light Brightness(Time Interval)</b>	This bar adjusts the brightness when blue LED is configured to light up at configured On/Off intervals. The valid range is 1-255, the default value is 90
<b>Blue Light Brightness(Key Pressed)</b>	This bar adjusts the brightness of blue LED when keypad is pressed. The valid range is 1-255, the default value is 90

<b>Doorbell Blue Light On/Off Time Interval Settings</b>	
<b>Enable Doorbell Blue Light on Time Interval</b>	When enabled, Doorbell LED will light based on the configured Start/End Time. For instance, this option can be used when GDS is deployed on dark environment, the GDS will be located easily using Doorbell LED.
<b>Keypad Blue Light On/Off Interval Settings</b>	
<b>Enable Keypad Blue Light on Time Interval</b>	When enabled, Keypad LED (except for Doorbell LED) will light based on the configured Start/End Time. For instance, this option can be used when GDS is deployed on dark environment, the GDS will be located easily using Keypad LED.
<b>Backlight Light On/Off Time Interval Settings</b>	
<b>Enable White Backlight on Time Interval</b>	If checked, the white background LED will light up based on the scheduled Start/End Time. This option also helps to illuminate any nearby areas around the GDS3710.
<b>Card and PIN open door schedule configuration module</b>	
<b>Central Mode</b>	If enabled, Group/Schedule/Holiday can only be synchronized from the Central (GDS Manager), local configuration will not be allowed. If disabled, only local configuration from GDS3710 is allowed.
<b>Key Sensitivity</b>	
<b>Key Sensitivity Level</b>	<p>Set the sensitivity level:</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> with this mode, the GDS3710 is using less sensitivity keypad parameters which applied to most usage scenes, especially in warm and high humidity places like tropic regions or places near seaside or riverside where high humidity weather condition exists, especially in Summer.</li> <li>• <b>High:</b> This option is designed for application scenes located in high latitude regions normally very cold and user might need to press the keypad with gloves. Due to the sensitivity is high, false positive might happen if such parameter used in different place like low latitude environment.</li> </ul> <p>Notes: Most application scenes the Default setting of this firmware is good enough for application. Please use Default setting unless the usage scene really needs high keypad lever sensitivity.</p> <p>If with default or low sensitivity keypad, the false-positive ghost call issue still happens frequently, which might indicate inappropriate wiring or installation, or maybe the hardware is faulty. Please contact Our Grandstream Support for assistance to resolve such a problem.</p>
<b>Key Tone Settings</b>	
<b>Key Tone Type</b>	<p>Configures the key tones for the GDS3710.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> Beeps will be played when pressing the GDS3710 keys.</li> <li>• <b>DTMF:</b> Tones will be played when pressing the GDS3710 keys.</li> <li>• <b>Mute:</b> No sound will be played when pressing keys.</li> </ul>
<b>Wiegand Settings</b>	
<b>Enable Wiegand Input</b>	This option needs to be enabled when GDS is connected to the wiegand. output device (RFID card reader for example)
<b>Wiegand Output</b>	This option is to be enabled when the GDS is the wiegand output device. (example: input device is a door controller)



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

GDS3710 support RFID for multiple users to open door, therefore every user has its own PIN. For environment with large number of users (limit is 2000), it's difficult for the GDS3710 to manage all these users, so a separate PC or Server should be involved for such kind of management and monitoring.

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

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

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

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

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

Door System Settings	
ALMOUT1 Feature	Open Door
ALMOUT1 Status	Normal Open
Control Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Wiegand Control	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Door 1 Delay before Unlock(s)	0
Door 2 Delay before Unlock(s)	0
Door 1 Unlock Holding Time(s)	5
Door 2 Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Number of Snapshots when Door Opened	4
Snapshot when Door Opened	<input checked="" type="checkbox"/> via FTP <input type="checkbox"/> via Email
Snapshot when Doorbell Pressed	<input type="checkbox"/> via FTP <input type="checkbox"/> via Email

*Alarm\_Out1 Feature*

### ◦ Interface for Door Control (which Door can be OPEN):

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

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

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

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

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

### ◦ Universal PIN for Operation of Doors:

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

Alarm\_Out1 Feature

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.

o **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" (For GDS3710) will be able to use DTMF PIN to open door remotely.

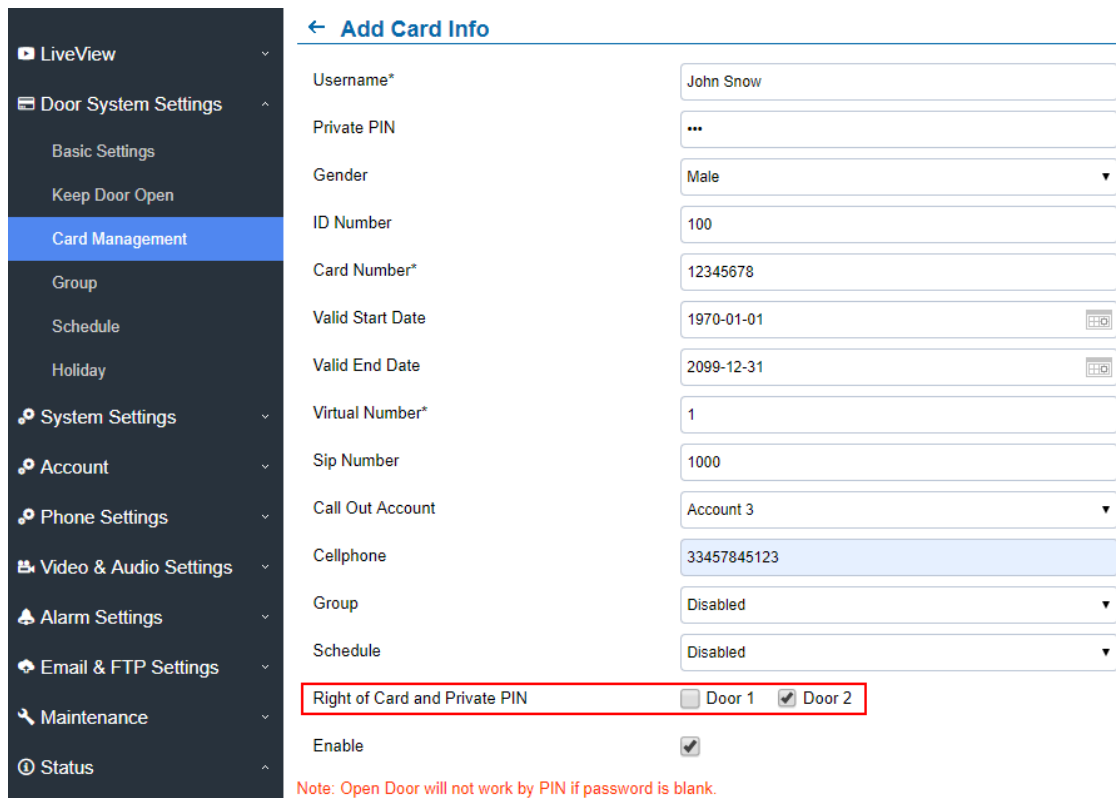
<ul style="list-style-type: none"> <li>LiveView</li> <li>Door System Settings <ul style="list-style-type: none"> <li>Basic Settings</li> <li>Keep Door Open</li> <li>Card Management</li> <li>Group</li> <li>Schedule</li> <li>Holiday</li> </ul> </li> <li>System Settings</li> <li>Account</li> <li>Phone Settings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

Universal Local PIN

o **Private PIN or Card & Private PIN:**

**Note**

This configuration is exclusive for the GDS3710 Model.



← Add Card Info

Username\* John Snow

Private PIN \*\*\*

Gender Male

ID Number 100

Card Number\* 12345678

Valid Start Date 1970-01-01

Valid End Date 2099-12-31

Virtual Number\* 1

Sip Number 1000

Call Out Account Account 3

Cellphone 33457845123

Group Disabled

Schedule Disabled

Right of Card and Private PIN  Door 1  Door 2

Enable

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

#### 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.

#### Note

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

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

## Keep Door Open

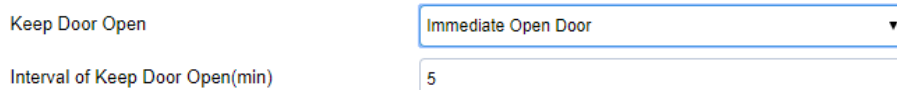
This feature allows users to set either an immediate or scheduled open door, this will allow usage scene like schools or similar private or public places where the door needs to keep open at specific time window and closed otherwise. Also handy for buildings or properties where a seminar needs to be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

The GDS3712 gives the option to configure Door1 and Door2 separately with either Immediate door open or Scheduled door open unlike the GDS3710 which has one configuration for both doors.

There are two modes under this section:

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

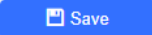
#### Keep Door Open



Keep Door Open Immediate Open Door

Interval of Keep Door Open(min) 5

#### Immediate Open Door

<b>Keep Door Open</b>	Select the Keep Door Open mode.
<b>Length(m) to Keep Door Open</b>	Set the amount of time in minutes where the door will keep opened. Click  to open door immediately.  Default is 5 minutes.

*Immediate Open-Door 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)**

**Keep Door Open**

**Door 1**

Keep Door Open	<input type="text" value="Schedule Open Door"/>
Schedule Start Time	<input type="text" value="2019-11-05 12:31:32"/>
Schedule End Time	<input type="text" value="2019-11-27 00:00:00"/>
Holiday Mode	<input type="text" value="holiday1"/> <a href="#">Edit Holiday</a>

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	0	
Sun																										
Mon																										
Tue																										
Wed																										
Thu																										
Fri																										
Sat																										
Holiday																										

**Door 2**

Keep Door Open	<input type="text" value="Disabled"/>
Emergency PIN to Disable Keep Door Open	<input type="text"/>

*Schedule Open Door*

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

*Schedule Keep Door Open*

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

Modify Schedule
✕

Sun	Period1	12 ▾	: 00 ▾	-	14 ▾	: 00 ▾
Mon	Period2	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Tue	Period3	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Wed	Period4	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Thu	Period5	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Fri	Period6	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
Sat	Period7	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾
	Period8	00 ▾	: 00 ▾	-	00 ▾	: 00 ▾

---

Copy
 Sun
  Mon
  Tue
  Wed
  Thu
  Fri
  Sat
  Select All

Save

Cancel

*Edit Schedule*

**Note**

A variety of schedules can be configured on the "Keep door open" settings, and users can choose which schedule they prefer to use.

## Emergency PIN

**Note**

This configuration is exclusive to the GDS3710 Model.

GDS3710

LiveView
Door System Settings
Keep Door Open
Card Management
Group
Schedule
Holiday

### Keep Door Open

Keep Door Open Disabled ▾

Emergency PIN to Disable Keep Door Open

Emergency PIN to Re-enable Keep Door Open

*Keep Door Open – Emergency PIN*

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

**Example:**

1. Fill in the password in Emergency PIN to Disable Keep Door Open, in our example: 2018
2. Open the door using either Immediate/Scheduled Keep Door open
3. enter the following Emergency Password sequence: \*2018#
4. After entering the sequence \*Emergency PIN to disable#, the GDS will close the door, and when entering the web GUI, the Keep Door Open section is switched automatically to "Disabled" Option.
5. In case the user wants to re-enable the keep door open option, he can enter the sequence \*Emergency PIN to re-enable#, in our example it will be \*2019#, the GDS will re-enable the open door when the PIN is provided.

**Note**

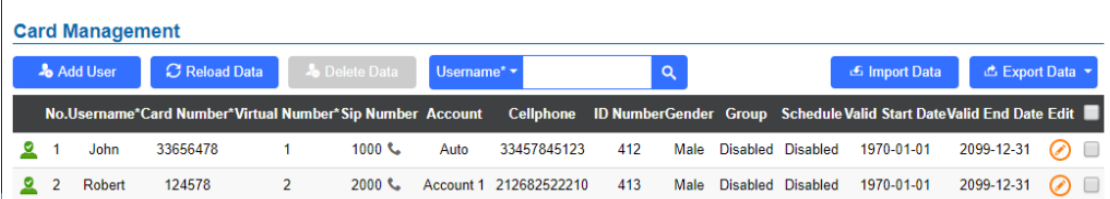
When ALMOUT1 Feature is set to Open Door then separated Keep Door Open features would be available on this page for each door.

## Card Management

### Note

This configuration is exclusive to the GDS3710 Model.

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



The screenshot shows the 'Card Management' interface. At the top, there are buttons for 'Add User', 'Reload Data', 'Delete Data', a search box for 'Username', 'Import Data', and 'Export Data'. Below these is a table with the following columns: No., Username, Card Number, Virtual Number, Sip Number, Account, Cellphone, ID Number, Gender, Group, Schedule Valid Start Date, Valid End Date, and Edit. Two rows of data are visible:

No.	Username	Card Number	Virtual Number	Sip Number	Account	Cellphone	ID Number	Gender	Group	Schedule Valid Start Date	Valid End Date	Edit	
1	John	33656478	1	1000	Auto	33457845123	412	Male	Disabled	Disabled	1970-01-01	2099-12-31	
2	Robert	124578	2	2000	Account 1	212682522210	413	Male	Disabled	Disabled	1970-01-01	2099-12-31	

Card Management

### Note

- The GDS3710 can add up to 2000 user cards.
- Press or 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 , the following page will pop up.

Card Info

<b>Username</b>	Configures the username to identify the user.
<b>Private PIN</b>	Specifies a PIN to unlock the door for this particular user.
<b>Gender</b>	Selects a gender, either Male or Female.
<b>ID Number</b>	Enters an ID number (This number is set by the admin to identify each user uniquely).
<b>Card Number</b>	Enters the RFID Card number (this is the number written on the RFID card. When "card issuing mode" is enabled, this field will be added automatically. Maximum number that can be entered is 2147483647.
<b>Valid Start Date</b>	Configures the start date of validity of the RFID card.
<b>Valid End Date</b>	Configures the End date of validity of the RFID card.
<b>Virtual Number</b>	When dialing directly from the keypad, the GDS accept only Virtual number to identify a user, once the Virtual number is typed followed by # key, the SIP Number will be dialed.
<b>SIP Number</b>	Configures the SIP Number which is mapped with virtual number. Once the virtual number is dialed the GDS3710 will send an INVITE to the SIP Number. <b>Note:</b> The SIP Number can be configured with an extension/phone number or IP address. Example: 192.168.5.124
<b>Call Out Account</b>	Select the Account from which the GDS3710 will call the User SIP Number when dialing from the keypad. Default is Auto.

<b>Cellphone</b>	Configures cellphone of the user.
<b>Group</b>	Specifies to which group the user will be added.
<b>Schedule</b>	Specifies the schedule that will be assigned to the user.
<b>Right of Card and Private PIN</b>	Select the doors that can be accessed by user.
<b>Enable</b>	When checked, the user's RFID and Private PIN will be active for door opening. If unchecked, the Private PIN nor RFID card swipe won't take effect.

### Card Info


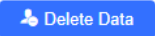





#### Notes

- Group overrides Schedule.
- If Schedule is set as "Disabled" the RFID Card will be accepted when swiped All Day.
- If user disabled, the related Card or PIN will fail to Open Door.
- Private PIN Open Door will not work if "Private PIN" is blank.

## Add Users Automatically

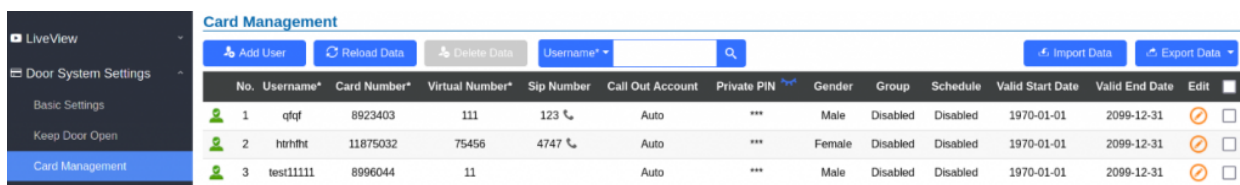
If [Enable Card Issuing Mode] is checked, the GDS3710 keypad will start blinking and once an RFID card is swiped, data stored on the card will be added into the GDS3710 card management page, user can still edit the entry added automatically by modifying some fields.







## Users Operation

- Click on  to edit the entry or show details of the entry.
- Select the entries and click on  to delete the selected users.
- Click  to refresh the data entered to the GDS3710.
- Users can use **Go to:**      to navigate through User Management pages.

## Show private PIN

The private PIN can be displayed easily from the card management page using the eye icon.



No.	Username*	Card Number*	Virtual Number*	Sip Number	Call Out Account	Private PIN 	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	qfjf	8923403	111	123 	Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	 <input type="checkbox"/>
2	htrhrt	11875032	75456	4747 	Auto	***	Female	Disabled	Disabled	1970-01-01	2099-12-31	 <input type="checkbox"/>
3	test11111	8996044	11		Auto	***	Male	Disabled	Disabled	1970-01-01	2099-12-31	 <input type="checkbox"/>

Hidden Private PIN



No.	Username*	Card Number*	Virtual Number*	Sip Number	Call Out Account	Private PIN	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	qfql	8923403	111	123	Auto		Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
2	htrhft	11875032	75456	4747	Auto		Female	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>
3	test11111	8996044	11		Auto	12345	Male	Disabled	Disabled	1970-01-01	2099-12-31	<input type="checkbox"/>

Visible Private PIN

To enable this feature, on the web UI, head to System Settings > Access Settings, switch the Web Access Mode to HTTPS and enable PIN/Password Display (HTTPS)

Access Settings	
Web Access Mode	HTTPS
Web Access Port	443
MJPEG Authentication Mode	Challenge+Response
RTSP Port	5554
User Login Timeout(min)	5
Maximum Number of Login Attempts	5
Locking Time of Login Error (m)	5
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input checked="" type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	22
GDSManager Configuration Password	*****
RTSP Password	*

PIN/Password display and HTTPS enabled

**Note**

- By default, this feature is disabled for security reasons.
- This feature only works when HTTPS is used as web UI access method.

**Group**

**Note**

This Configuration is exclusive for the GDS3710 Model.

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

**Note**

Users can create up to 50 groups.

**Add Group**
✕

Group Name

Schedule

Add Group

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

*Add Group*

The following screenshots display the list of the created groups.

**Group**

[+ Add](#)

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

*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.

**Schedule**

No.	Schedule Name	Holiday Name	Detail	Edit
1	schedule1	Disabled		
2	schedule2	Disabled		
3	schedule3	Disabled		
4	schedule4	Disabled		
5	schedule5	Disabled		
6	schedule6	Disabled		
7	schedule7	Disabled		
8	schedule8	Disabled		
9	schedule9	Disabled		
10	schedule10	Disabled		

*Edit Schedule Time*

### Holiday

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

Click on to edit the holidays or for holiday details.

**Holiday**

No.	Holiday Name	Detail	Edit
1	holiday1		
2	holiday2		
3	holiday3		
4	holiday4		
5	holiday5		
6	holiday6		
7	holiday7		
8	holiday8		
9	holiday9		
10	holiday10		

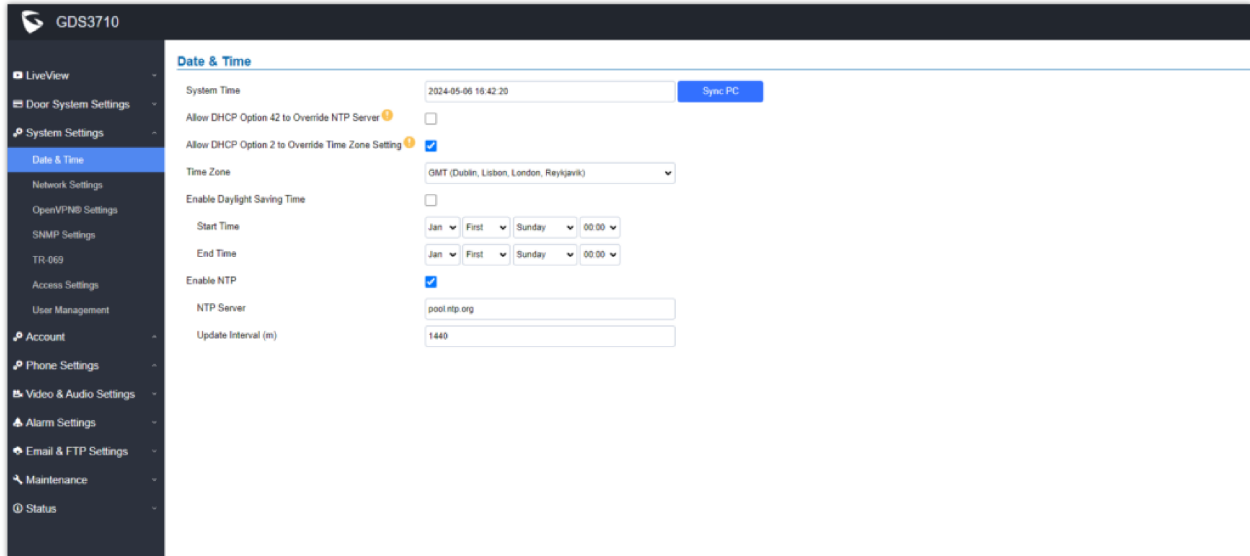
*Edit Holiday Time*

## System Settings

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

### Date & Time Settings

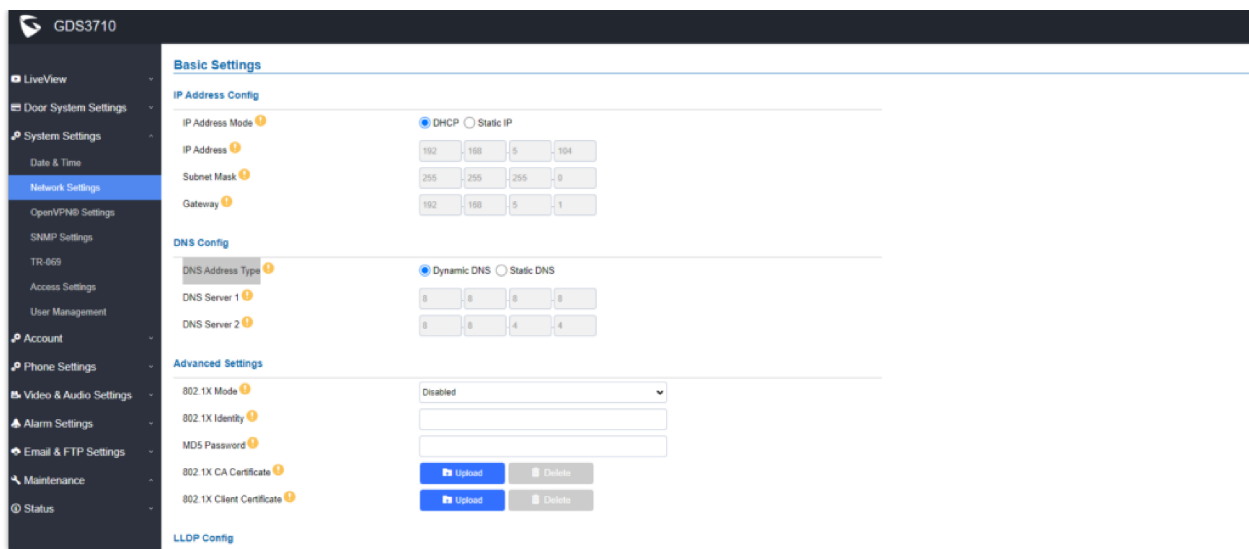
This page allows users to adjust system date and time of the GDS371x.



<b>System Time</b>	Displays the current system time.
<b>Allow DHCP Option 42 to override NTP server</b>	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it's set up on the LAN. The default setting is "Yes".
<b>Allow DHCP Option 2 to Override Time Zone Setting</b>	Allows the device to get provisioned for Time Zone from DHCP option 2 in the local server.
<b>Time Zone</b>	Selects from drop down menu the preferred time zone.
<b>Enable Daylight Saving Time</b>	Enables Daylight Saving Time.
<b>Start time</b>	Selects the Start time of DST.
<b>End Time</b>	Selects DST end time.
<b>Enable NTP</b>	Enables NTP to synchronize device time.
<b>NTP Server</b>	Configures the domain name of NTP server.
<b>Update Interval</b>	Configures the Interval (in minutes) to retrieve updates from the NTP server.

### Network Settings

This page allows users to configure network settings for the GDS371x



Network Settings Page

<b>IP Address Mode</b>	Selects DHCP or Static IP. Default DHCP. (Static recommended)
<b>IP Address</b>	Configures the Static IP of the GDS3710.
<b>Subnet Mask</b>	Configures the Associated Subnet Mask.
<b>Gateway</b>	Configures the Gateway IP address.
<b>DNS Address Type</b>	Specifies the DNS type used: Dynamic DNS or Static DNS.
<b>DNS Server 1</b>	Configures DNS Server 1 IP address.
<b>DNS Server 2</b>	Configures DNS Server 2 IP address.
<b>802.1X Mode</b>	Defines the 802.1X authentication mode, the supported options are: Disabled, EAP-MD5, EAP-TLS, EAP-PEAPv0/MSCHAPv2
<b>802.1X Identity</b>	Defines the identity for the 802.1X authentication
<b>MD5 Password</b>	Defines the password for the 802.1X authentication
<b>802.1X CA Certificate</b>	Uploads the CA certificate for the EAP-PEAPv0/MSCHAPv2 or EAP-TLS authentication mode, the supported file is .pem
<b>802.1X Client Certificate</b>	Uploads the client certificate for the EAP-TLS authentication mode, with the certificate and private key in .pem file
<b>Enable LLDP</b>	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is “Enabled”.
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assigns the VLAN Tag of the Layer 2 QoS packets. Default value is 0.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assigns the priority value of the Layer2 QoS packets. Default value is 0.

Notes

- If the GDS371x 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.

## OpenVPN® Settings

This page allows users to configure OpenVPN settings.

OpenVPN Settings page

<p><b>Enable OpenVPN®</b></p>	<p>Enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server.</p> <p><b>Note:</b> To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key. Additionally, the user must also set the SIP account to use "VPN" for the "NAT Traversal" (under Account → Network Settings).</p>
<p><b>OpenVPN® Server Address</b></p>	<p>Defines the URL/IP address for the OpenVPN® server.</p>
<p><b>OpenVPN® Port</b></p>	<p>Defines the network port for the OpenVPN® server. The default setting is <b>1194</b>.</p>
<p><b>OpenVPN® Transport</b></p>	<p>Determines network protocol used for OpenVPN® (UDP or TCP).</p> <p>The default setting is <b>TCP</b>.</p>

<b>OpenVPN® CA</b>	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Client Certificate</b>	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Client Key</b>	OpenVPN® Client key (*.key) required by OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
<b>OpenVPN® Cipher Method</b>	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Supported methods are: Blowfish, AES-128, AES-256 and Triple-DES.
<b>OpenVPN® Username</b>	Configures the OpenVPN® authentication username (optional).
<b>OpenVPN® Password</b>	Configures the OpenVPN® authentication password (optional).
<b>Additional Options</b>	<p>Additional options to be appended to the OpenVPN® config file, separated by semicolons. For example, <i>comp-lzo no; auth SHA256</i></p> <p><b>Note:</b> Please use this option with caution. Make sure that the options are recognizable by OpenVPN® and do not unnecessarily override the other configurations above.</p>

## SNMP Settings

This page configures the GDS371x SNMP parameters.

The screenshot shows the 'SNMP Settings' page in the GDS3710 web interface. The left sidebar contains a navigation menu with categories like 'LiveView', 'Door System Settings', 'System Settings', 'Account', 'Phone Settings', 'Video & Audio Settings', 'Alarm Settings', 'Email & FTP Settings', 'Maintenance', and 'Status'. The 'SNMP Settings' option is highlighted under 'System Settings'. The main content area displays the following configuration options:

- Enable SNMP:
- SNMP Version: Version 3
- SNMP Port: 161
- SNMPv1/v2c Community: (empty field)
- SNMP Trap Version: Version 3
- SNMP Trap IP Address: (empty field)
- SNMP Trap Port: 162
- SNMP Trap Interval: 5
- SNMPv1/v2c Trap Community: (empty field)
- SNMPv3 User Name: (empty field)
- SNMPv3 Security Level: noAuthUser
- SNMPv3 Authentication Protocol: None
- SNMPv3 Privacy Protocol: None
- SNMPv3 Authentication Key: (empty field)
- SNMPv3 Privacy Key: (empty field)
- SNMPv3 Trap User Name: (empty field)
- SNMPv3 Trap Security Level: noAuthUser
- SNMPv3 Trap Authentication Protocol: None

A 'Save' button is located at the bottom of the configuration area.

Field	Description
-------	-------------

<b>Enable SNMP</b>	Enable/Disable SNMP feature. The default setting is "disabled".
<b>Version</b>	Select the SNMP version.  <ul style="list-style-type: none"> <li>● Version 1</li> <li>● Version 2c</li> <li>● Version 3</li> </ul> The default setting is "Version 3"
<b>SNMP Port</b>	Defines the SNMP port. The default setting is "161".
<b>SNMPv1/v2c Community</b>	Enter the SNMPv1/v2c Community.
<b>SNMP Trap Version</b>	Select the SNMP Trap Version.  <ul style="list-style-type: none"> <li>● Version 1</li> <li>● Version 2c</li> <li>● Version 3</li> </ul> The default setting is "Version 3"
<b>SNMP Trap IP Address</b>	Enter the SNMP Trap IP Address.
<b>SNMP Trap Port</b>	Enter the SNMP Trap Port. The default setting is "162". <b>Note:</b>  <ul style="list-style-type: none"> <li>● starting from firmware 1.0.13.2, GDS371x receives real-time notifications when someone activates the doorbell. the device gets those notifications through the SNMP trap messages.</li> <li>● Starting from firmware 1.0.13.2, System Temperature object identifier is added to the MIB file of the GDS371x</li> </ul>
<b>SNMP Trap Interval</b>	Set the SNMP Trap Interval. The default setting is "5".
<b>SNMPv1/v2c Trap Community</b>	Enter the SNMPv1/v2c Trap Community.
<b>SNMPv3 Username</b>	Enter the SNMPv3 Username.
<b>SNMPv3 Security Level</b>	Select the SNMPv3 Security Level.  <ul style="list-style-type: none"> <li>● noAuthUser</li> <li>● authUser</li> <li>● privUser</li> </ul> The default setting is "noAuthUser".
<b>SNMPv3 Authentication Protocol</b>	Select the SNMPv3 Authentication Protocol.  <ul style="list-style-type: none"> <li>● None</li> <li>● MD5</li> <li>● SHA</li> </ul> The default setting is "None".

<b>SNMPv3 Privacy Protocol</b>	Select the SNMPv3 Privacy Protocol. <ul style="list-style-type: none"> <li>• None</li> <li>• DES</li> <li>• AES AES128</li> </ul>
<b>SNMPv3 Authentication Key</b>	Enter the SNMPv3 Authentication Key.
<b>SNMPv3 Privacy Key</b>	Enter the SNMPv3 Privacy Key.
<b>SNMPv3 Trap User Name</b>	Enter the SNMPv3 Trap User Name
<b>SNMPv3 Trap Security Level</b>	Select the SNMPv3 Trap Security Level. <ul style="list-style-type: none"> <li>• noAuthUser</li> <li>• authUser</li> <li>• privUser</li> </ul> <p>The default setting is "noAuthUser".</p>
<b>SNMPv3 Trap Authentication Protocol</b>	Select the SNMPv3 Trap Authentication Protocol. <ul style="list-style-type: none"> <li>• None</li> <li>• MD5</li> <li>• SHA</li> </ul> <p>The default setting is "None"</p>
<b>SNMPv3 Trap Privacy Protocol</b>	Select the SNMPv3 Trap Privacy Protocol. <ul style="list-style-type: none"> <li>• None</li> <li>• DES</li> <li>• AES AES128</li> </ul> <p>The default setting is "None".</p>
<b>SNMPv3 Trap Authentication Key</b>	Enter the SNMPv3 Trap Authentication Key.
<b>SNMPv3 Trap Privacy Key</b>	Enter the SNMPv3 Trap Privacy Key.

## TR-069

This page configures the GDS371x TR-069 parameters.

TR-069 settings page



<b>Enable TR-069</b>	Sets the device to enable the “CPE WAN Management Protocol” (TR-069). The default setting is “No”. <b>Note:</b> Reboot the device to make changes take effect.
<b>ACS URL</b>	Specifies URL of TR-069 ACS (e.g, http://acs.test.com), or IP address.
<b>ACS Username</b>	Enters username to authenticate to ACS.
<b>ACS Password</b>	Enters password to authenticate to ACS.
<b>Periodic Inform Enable</b>	Sends periodic inform packets to ACS. The default is “No”.
<b>Periodic Inform Interval (s)</b>	Configures to send periodic “Inform” packets to ACS based on a specified interval. The default setting is 86400.
<b>Connection Request Username</b>	Enters username for the ACS to connect to the device.
<b>Connection Request Password</b>	Enters the password for the ACS to connect to the device.
<b>Connection Request Port</b>	Enters the port for the ACS to connect to the device.
<b>CPE Cert File</b>	Enters Cert File for the device to connect to the ACS via SSL. <b>Note:</b> The CPE version has been updated to 1.0.5.7
<b>CPE Cert Key</b>	Uploads Cert Key for the device to connect to the ACS via SSL.

#### TR-069 settings

### Access Settings

This page configures the GDS371x access control parameters.

GDS3710

- LiveView
- Door System Settings
- System Settings
  - Date & Time
  - Network Settings
  - OpenVPN® Settings
  - SNMP Settings
  - TR069
  - Access Settings
  - User Management
- Account
- Phone Settings
- Video & Audio Settings
- Alarm Settings
- Email & FTP Settings
- Maintenance
- Status

### Access Settings

Web Access Mode <span style="color: orange;">!</span>	<input type="text" value="HTTPS"/>
Web Access Port <span style="color: orange;">!</span>	<input type="text" value="443"/>
MJPEG Authentication Mode	<input type="text" value="Challenge+Response"/>
RTSP Port	<input type="text" value="554"/>
User Login Timeout (min)	<input type="text" value="5"/>
Maximum Number of Login Attempts	<input type="text" value="5"/>
Locking Time of Login Error (m)	<input type="text" value="5"/>
Disable Web Access	<input type="checkbox"/>
Enable UPnP Discovery	<input checked="" type="checkbox"/>
Enable Anonymous LiveView	<input type="checkbox"/>
Enable PIN/Password Display (HTTPS)	<input type="checkbox"/>
Enable SSH	<input checked="" type="checkbox"/>
SSH Port	<input type="text" value="22"/>
Minimum TLS Version	<input type="text" value="TLS 1.1"/>
Maximum TLS Version	<input type="text" value="Unlimited"/>
GDSManager Configuration Password	<input type="password" value="*****"/>
RTSP Password	<input type="password" value="*****"/>

Access Settings Page

<b>Web Access Mode</b>	Selects the access mode to the webGUI either HTTP or HTTPS.
<b>Web Access Port</b>	Specifies the TCP port for Web Access, default 443.
<b>JPEG Authentication Mode</b>	<p>Allows 3rd party system integrator or developers to implement related application for users. By default, this feature is disabled and use more secured “Challenge+Response” mode.</p> <p>If enabled, user can send HTTP API with correct credentials to retrieve MJPEG video stream or JPEG snapshot from GDS3710.</p> <p>Notes:</p> <ol style="list-style-type: none"> <li>The MJPEG stream can be retrieved via the following URL  HTML based → <code>http(s)://admin:password@IP_GDS3710:Port/jpeg/mjpeg.html</code>  Stream → <code>http(s)://admin:password@ip:port/jpeg/stream</code></li> </ol> <p>The MJPEG stream retrieved via the methods above is running on the background and cannot be tuned. If users want more flexibility, they can use the three configurable video streams as shown on [Retrieving Video Streams].</p>
<b>RTSP Port</b>	Specifies RTSP port for media stream, default TCP port 554.
<b>User Login Timeout(min)</b>	If no action is made within this time the GDS371x will logout from the Web GUI, range is between 3 and 60.
<b>Maximum Number of Login Attempts</b>	Specifies the allowed login times error limit, if the unsuccessful login attempts exceed this value, the GDS371x webGUI will be locked for the time specified in Login Error Lock Time.
<b>Locking Time of Login Error (m)</b>	Specifies how long the GDS371x is locked before a new login attempt is allowed.
<b>Disable Web Access</b>	<p>Allow or deny the web access to the GDS371x. (HTTP API do not take effect when this option is enabled).</p> <p>Note: If both WebUI and SSH are disabled, GDS371x will get blocked and not be able to be accessed. Only two ways to get it back:</p>

	<p>1. Re-provisioned by ITSP or Service Provider (by adjusting the related parameters)</p> <p>2. Hard Reset (GDS371x has to be offline and uninstalled to perform this hard reset).</p>
<b>Enable UPnP Discovery</b>	UPnP (or mDNS) function for local discovery. Default setting is enabled.
<b>Enable Anonymous LiveView</b>	<p>1. When enabled, user can display the camera stream from GDS without admin credentials using the following URL scheme:  <code>http(s)://GDS371x_IP:port/videoview.html</code></p> <p>2. User can also retrieve a real-time snapshot without admin credentials using the following URL:  <code>http(s)://IP:port/anonymous/snapshot/view.html</code>  Or with:  <code>https://IP_GDS371x:Port/anonymous/snapshot/view.jpg</code></p> <p>3. To retrieve video stream via RTSP, users can use the following format: <code>rtsp://IP_GDS371x:Port/X</code> where X=0,4,8 for 1st, 2nd, 3rd streams respectively.</p> <p>4. To retrieve Anonymous MJPEG, user can use following URLs to retrieve the related MJPEG streams:  <code>http(s)://IP:Port/anonymous/jpeg/stream=X</code> (X=0, 1, 2, or default 3)  For example: <code>https://192.168.1.128/anonymous/jpeg/stream=3</code></p> <p><b>Notes:</b>  Except default value 3, the stream 0, 1, 2 mapped to the stream 1, 2, 3 in the “Video Setting” page.  Unless using default value 3, all other values require to choose “MJPEG” in the “Preferred Video Codec” in the “Preferred Video Codec”</p>
<b>Enable SSH</b>	Allows SSH access for remote secured configuration purposes (restart, upgrade, provision...)
<b>Enable PIN/Password Display (HTTPS)</b>	<p>If Enabled, this option allows to view system PIN/Password.</p> <p>Default setting is Disabled.</p>
<b>SSH Port</b>	<p>Specifies the SSH port.</p> <p>Default setting is 22.</p>
<b>Minimum TLS Version</b>	<p>Configures the minimum TLS version supported by the device.</p> <p>Minimum TLS version must be less than or equal to maximum TLS version.</p> <p>The Available options are : TLS 1.0, TLS 1.1, TLS 1.2  the default value is TLS 1.1</p>
<b>Maximum TLS Version</b>	<p>Configures the maximum TLS version supported by the device.</p> <p>Maximum TLS version must be greater than or equal to minimum TLS version.</p> <p>The Available options are : TLS 1.0, TLS 1.1, TLS 1.2, unlimited.  the default value is unlimited.</p>
<b>GDSManager Configuration Password</b>	<p>User can set in this field a custom admin password instead of using GDS371x webUI administrator’s credentials, and this custom admin password will be the one used when adding the GDS371x unit to GDSManager database.</p> <p>Default password is the Admin’s default random password of the GDS371x.</p>
<b>RTSP Password</b>	<p>This feature enhancement is based on field feedback from customers. Customer request NOT using admin password to view the RTSP video stream via 3rdparty applications like VLC Player or own development Scripts.</p> <p>Now customer can still use admin as username, but NOT use admin password and configure another RTSP password to view the live stream via own scripts or 3rd party application like VLC Media Player.</p> <p>For example, using VLC Media Player, if configure the RTSP password to be “1234” in GDS371x, then using following command can get the video stream:  <code>rtsp://admin:1234@192.168.11.128/4</code> (here it shows the 2ndstream as “4” used)</p> <p><b>FORMAT:</b>  <code>RTSP://admin:rtsp_password@IP_GDS371x:Port/X</code>  (X = 0, 4, 8 correspondent to Stream 1, 2, 3)</p>

The selected live video stream with audio will play out with some delay based on the computer processing power and network conditions.

Notes:

Please make sure the environment is secure before using this feature.

Please reminder user the privacy when using this feature.

## 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.

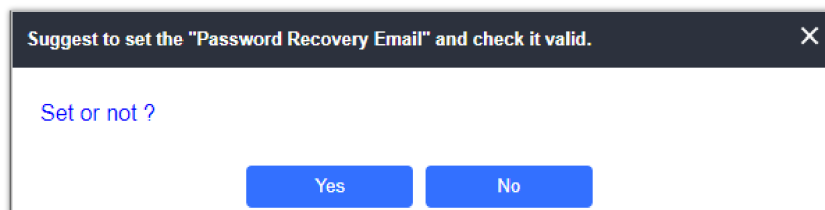
User Management Page

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

User Management

### 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.



Password Recovery Email

## Account

Starting from version 1.0.5.6, the GDS371x supports four SIP accounts and four 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:

GDS3710 English | Logout  
2021-08-18 15:41

**Account 2**

**SIP Basic Settings**

Account Active

SIP Server

Secondary SIP Server

Outbound Proxy

Backup Outbound Proxy

DNS Mode

SIP User ID

Authentication ID

Password

Display Name

TEL URI

**SIP Advanced Settings**

Registration Expiration(m)

Re-register before Expiration(s)

Local SIP Port

SIP Transport

Stream

Enable DTMF  RFC2833  SIP INFO

SIP Account Settings Page

SIP Basic Settings	
<b>Account Active</b>	This field indicates whether the account is active. Default setting is “Yes”.
<b>SIP Server</b>	Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.
<b>Secondary SIP Server</b>	Configures the FQDN or IP of the secondary SIP server from the VoIP service provider or local IPPBX. The Second SIP Server allows users to use a secondary SIP server if the primary SIP server is having problems ensuring service availability.
<b>Outbound Proxy</b>	Configures the IP address or the domain name of the outbound proxy, media gateway, or session border controller. It’s used by the GDS for firewall or NAT penetration in different network environments.  If a symmetric NAT is detected, STUN will not work and only an outbound proxy can provide a solution.
<b>Backup Outbound Proxy</b>	Configures the backup outbound proxy to be used when the “Outbound Proxy” registration fails. By default, this field is left empty.
<b>DNS Mode</b>	Configure which DNS mode will be used to translate the SIP Server FQDN (Default value is A Record): <ul style="list-style-type: none"> <li>● A Record.</li> <li>● SRV.</li> <li>● NAPTR/SRV.</li> </ul>
<b>SIP User ID</b>	Configures the SIP username or telephone number from ITSP. <b>Note:</b> Letters, digits and special characters including @ are supported.

<b>Authenticate ID</b>	Configures the Authenticate ID used by SIP proxy.
<b>Password</b>	Sets the Authenticate password used by SIP proxy. <b>Note:</b> For security reasons, the SIP password is invisible on the web UI.
<b>Display Name</b>	To allow user to input display name to be illustrated in far side SIP device(if having LCD display or similar hardware) so user will know what extension or device connected in SIP calling, to increase the usability.
<b>TEL URI</b>	Select "User=Phone" or "Enabled" from the dropdown list. If the SIP account has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable".
<b>SIP Advanced Settings</b>	
<b>Registration Expiration (m)</b>	Sets the registration expiration time. Default setting is 60 minutes. Valid range is from 1 to 64800 minutes.
<b>Re-register before Expiration (s)</b>	Specifies the time-frequency (in seconds) that the GDS371x sends a re-registration request before the Register Expiration. The default value is 0. The range is from 0-64800 seconds.
<b>Local SIP Port</b>	Sets the local SIP port. Default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4.
<b>SIP Transport</b>	Chooses the SIP transport protocol. UDP, TCP or TCP/TLS. Default setting is UDP.
<b>Check Domain Certificates</b>	When using SIP with TLS/TCP, the "Check Domain Certificates" parameter plays a role in determining whether the GDS371x device should verify the presented domain certificates for security purposes. <ul style="list-style-type: none"> <li>• If "Check Domain Certificates" is enabled, the device will validate that the domain of the presented certificate matches the expected domain. This is crucial for ensuring that the communication is secure and that the device is connecting to a legitimate SIP server.</li> <li>• If "Check Domain Certificates" is disabled, the device may not perform this validation, potentially accepting certificates from domains that do not match the expected one. This could introduce security risks, as it opens the possibility for man-in-the-middle attacks or connections to unauthorized servers.</li> </ul>
<b>Stream</b>	Select the Video stream to be used by the GDS371x when a call is made from this SIP Account. The default is Stream 2.
<b>Enable DTMF</b>	Specifies the mechanism to transmit DTMF digits. There are 2 supported modes: RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. SIP INFO uses SIP INFO to carry DTMF. Default setting is "RFC2833"
<b>DTMF Payload Type</b>	Configures the payload type for DTMF using RFC2833. The default value is 101. Range: 96~127.
<b>Unregister On Reboot</b>	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.
<b>NAT Traversal</b>	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". If set to "STUN" and STUN server is configured, the GDS will route according to the STUN

	<p>server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the unit will try to use public IP addresses and port number in all the SIP&amp;SDP messages.</p> <p>The GDS will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be “Keep-alive”. Configure this to be “No” if an outbound proxy is used. “STUN” cannot be used if the detected NAT is symmetric NAT. If the firewall and the SIP device behind the firewall are both able to use UPNP, it can be set to “UPNP”. Both parties will negotiate to use which port to allow SIP through.</p>
<b>Enable SRTP</b>	<p>Enable SRTP mode based on your selection from the drop-down menu.</p> <p>The default setting is “Disabled”, the two other modes are “Enabled but Not Forced” and “Enabled and Forced”.</p>
<b>SRTP Key Length</b>	<p>Defines the length of the Secure Real-time Transport Protocol (SRTP) encryption key used for securing communication, the options are: AES 128&amp;256 bit, AES 128 bit, and AES 256 bit</p>
<b>Special Feature</b>	<p>Configures GDS settings to meet different vendors’ server requirements.</p> <p>Users can choose from Standard, Broadsoft, Telefonica Spain, or metaswitch.</p> <p>The default setting is “Standard”.</p>
<b>Enable Local Call Features</b>	<p>Enables local call features for the GDS371x.</p> <p>Enabled by default.</p>
<b>Outbound Proxy Mode</b>	<p>In route: outbound proxy FQDN is placed in the routeing header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall.</p> <p>Always sent to SIP messages will always be sent to the Outbound proxy.</p> <p>Not in route: remove the Route header from SIP requests.</p>
<b>Enable RTCP</b>	<p>This option allows 3rd party Service Providers or Cloud Solutions to monitor the operation status of the GDS371x by using related SIP Calls.</p> <p>By default, it’s disabled. Users can choose either RTCP or RTCP-XR.</p>
<b>H.264 Payload Type</b>	<p>The H.264 payload type can now be configured to be compatible with 3rd party video phones, as well as other advanced SIP settings, to easy the system integration process. The default is 99.</p>
<b>Accept Incoming SIP from Proxy Only</b>	<p>When set to “Yes”, the SIP address of the Request URL in the incoming SIP message will be checked. If it doesn’t match the SIP server address of the account, the call will be rejected. The default setting is disabled.</p>
<b>Add MAC in User-Agent</b>	<p>This option is used with 3CX so that the GDS37xx can be compatible with 3CX auto-provisioning. The option adds the MAC address into User-Agent in the SIP Header.</p> <p>No: to disable the option</p> <p>Yes to all SIP: SIP messages will always behave User-Agent</p> <p>Yes except REGISTER: SIP messages will always behave User-Agent except for the REGISTER message</p>
<b>SIP URI Scheme When Using TLS</b>	<p>This option allows the GDS371x to work with the Cisco WebEX server as a SIP client. The two modes are SIP and SIPS.</p>
<b>Support SIP Instance ID</b>	<p>When enabled, the GDS371x will work with the Cisco WebEx server as a SIP client.</p>
<b>Vocoder Settings</b>	
<b>Preferred Vocoder 1</b>	<p>Selects the first audio codec by priority order (lowest is the highest priority). Supported codecs are PCMU, PCMA, G.722, and G.729A/B.</p>
<b>Preferred Vocoder 2</b>	<p>Selects the second audio codec by priority order (lowest is the highest priority). Supported codecs are PCMU, PCMA, G.722, and G.729A/B.</p>

<b>Preferred Vocoder 3</b>	Selects the third audio codec by priority order (lowest is the highest priority). Supported codecs are PCMU, PCMA, G.722, and G.729A/B.
<b>Preferred Vocoder 4</b>	Selects the fourth audio codec by priority order (lowest is the highest priority). Supported codecs are PCMU, PCMA, G.722, and G.729A/B.
<b>Codec Negotiation Priority</b>	Selects the negotiation Priority, whether it is for the Caller or the Callee, Set to Callee by Default.
<b>Voice Frame Per TX</b>	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.

## Phone Settings

The phone settings allow users to configure the GDS371x phone settings and the White list for all the SIP accounts.

## Phone Settings

This page allows users to configure the GDS371x phone settings.

The screenshot shows the 'Phone Settings' page. The left sidebar contains the following menu items: LiveView, Door System Settings, System Settings, Account, Phone Settings (selected), Account 1 White List, Account 2 White List, Account 3 White List, Account 4 White List, Video & Audio Settings, Alarm Settings, Email & FTP Settings, Maintenance, and Status. The main content area is titled 'Phone Settings' and includes the following settings:

- STUN Server: [Input field]
- Local RTP Port: 5004
- Use Random Port:
- Auto On-Hook Timer(s): 300
- Ringing Timeout(s): 15
- SIP TLS Certificate: [Input field]
- SIP TLS Private Key: [Input field]
- SIP TLS Private Key Password: [Input field with masked characters]
- Enable Direct IP Call:
- Enable two-way SIP Calling:
- SIP Proxy Compatibility Mode:
- SIP Packetization Compatibility Mode:
- Enable Multi-channel Call Mode:
- Allow Reset Via SIP NOTIFY:

Phone Settings Page

<b>STUN Server</b>	Configures the STUN server FQDN or IP. If the device is behind a non-symmetric router, STUN server can help to penetrate & resolve NAT issues.
<b>Local RTP Port</b>	Sets the local RTP port for media. Default setting is 5004. Range between 1024~65400.



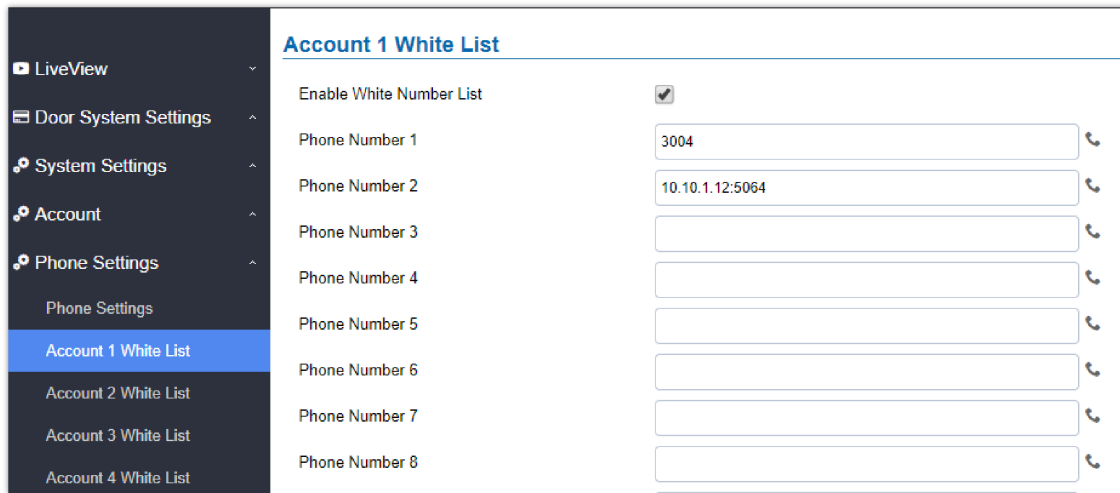
<b>Use Random Port</b>	Forces the GDS to use random ports for both SIP and RTP messages. This is usually necessary when multiple units are behind the same full cone NAT. The default setting is “Disabled” <b>Note:</b> This parameter must be set to “Disabled” for Direct IP Calling to work.
<b>Auto On-Hook Timer</b>	Configures the auto on-hook timer (in seconds) for automatic disconnecting the SIP call. Default setting is 300. Range between 0~65535.
<b>Ring Timeout(s)</b>	Specifies the Ring timeout, when no reply is returned from the called party after exceeding this field, the GDS will hang up the call. The value is in the range of 0s – 90s. By default; it is “30” seconds.
<b>DNS Cache Expiration Time(m)</b>	Configures the DNS Cache expiration Time, the default value is 30 , the range is 1-1440
<b>DNS Cache Duration(m)</b>	Configures the DNS Cache expiration Duration, the default value is 30 , the range is 1-1440
<b>SIP TLS Certificate</b>	Input the TLS certificate here for encryption.
<b>SIP TLS Private Key</b>	Input private key here for TLS security protection.
<b>SIP TLS Private Key Password</b>	Specifies the password for SIP TLS private Key.
<b>Enable Direct IP Call</b>	Accepts peer-to-peer IP call (over UDP only) without SIP server. Default is “Enabled”.
<b>Enable two-way SIP Calling</b>	Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.
<b>SIP Proxy Compatibility Mode</b>	Enables more proxy compatibility with cost of bandwidth, the SIP call will send audio no matter what.
<b>SIP Packetization Compatibility Mode</b>	When enabled, the GDS will have in SDP “packetization-mode = 0”. This is required when GDS is interacting with legacy video phones that only accepts this value to decode the RTP.
<b>Enable Multi-channel Call Mode</b>	This feature allows the device to receive multiple calls at the same time, with one active and others on hold (up to 4 calls maximum). The first call the blue LED light will light up keypad digit “1”, 2nd call will light up keypad digit “2”, and so on. On hold call will have related digit blinking while active call will have the digit blue LED solid light up. Call can be switched by pressing the blinking digits.
<b>Allow Reset Via SIP NOTIFY</b>	Allows to factory reset the devices directly through SIP Notify. If “Allow Reset Via SIP NOTIFY” is “check”, then once the GDS3710 receives the SIP NOTIFY from the SIP server with Event: reset, the GDS3710 will perform a factory reset after authentication. This authentication can be either with: 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 GDS371x. Default is unchecked (disabled).

*Phone Settings*

## 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 GDS371x. (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 200 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.



White List Page

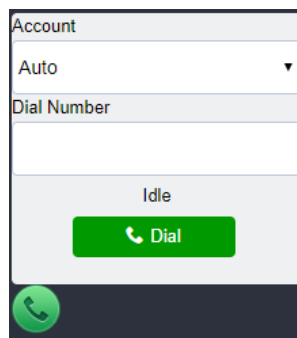
The table below gives a brief overview of the options:

<b>Enable White Number List</b>	Enables the White List feature.
<b>Phone Number 1 -200</b>	Adds a new phone number to the white list.

White List

## Click-To-Dial

The GDS371x 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.



Click-To-Dial

### Note

Only the whitelisted numbers can open door remotely using PIN Code when calling GDS3710

## 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

<b>Preferred Video Codec (Stream1)</b>	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.
<b>Profile</b>	Selects the H.264 profile. Three profiles are available: Baseline, Main Profile and High Profile. Default setting is "Main Profile".
<b>Resolution</b>	Specifies the resolution in pixels used at video image, 1080p or 720p.
<b>Bit Rate(kbps)</b>	Selects the video bit rate or bandwidth used.
<b>Frame Rate(fps)</b>	Selects the maximum frame rate used (more data if big frame used).
<b>Bit Rate Control</b>	Selects the constantly bit rate, or variable bit rate.
<b>Image Quality</b>	Selects the image quality used when Variable Bit Rate used.
<b>I-frame Interval</b>	Configures the I-frame interval (suggested 2~3 times of frame rate).
<b>Preferred Video Codec(Stream2)</b>	Selects the videos codecs, the codecs supported are H.264 and MJPEG supported. Default setting is H.264.

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

#### *Video Settings*

#### **Notes**

- H.264 suggested if the GDS371x 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 GDS371x provides three video streams, users can use them with flexibility. For example, the high-resolution stream for local recording, another low or high resolution for SIP video phone call or remote smartphone monitoring application, or vice versa depending application scenarios.
- Use below link to calculate bandwidth and storage before installation  
<http://www.grandstream.com/support/tools/bandwidth-storage-calc>

#### **Retrieving Video Streams**

- To retrieve video stream via RTSP, users can use the following format :

rtsp://admin:password@IP\_GDS3710:Port/X where X=0,4,8 for 1<sup>st</sup>, 2<sup>nd</sup>, 3<sup>rd</sup> streams respectively

- To retrieve MJPEG video stream via http, users can use the following format:

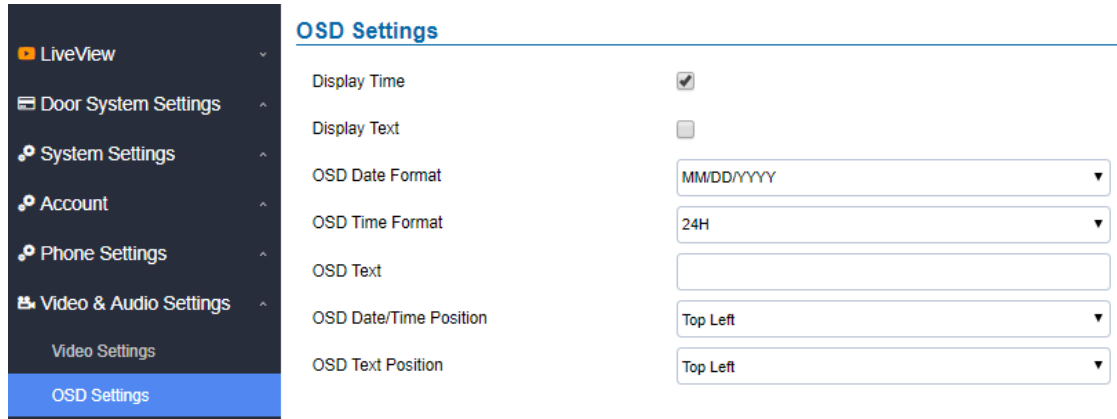
http(s)://admin:password@IP:port/jpeg/stream=X (X=Stream channel 0,1,2)

### Important Note

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

## OSD Settings

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



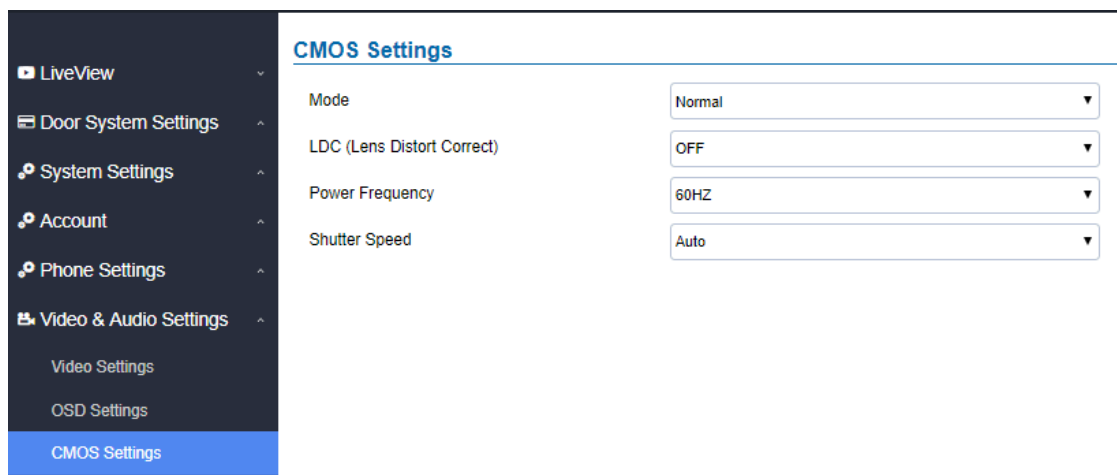
OSD Settings Page

<b>Display Time</b>	When checked, time will be displayed inside the video image.
<b>Display Text</b>	When checked, inputted text on "OSD Test" will be displayed on the video image.
<b>OSD Date Format</b>	OSD Date format, choose based on user preference.
<b>OSD Time Format</b>	OSD Time format, choose based on user preference.
<b>OSD Text</b>	Input a text (to identify the GDS3710) it will be shown on the screen. Maximum length is 32.
<b>OSD Date/Time Position</b>	Show the Date/Time position on the screen.
<b>OSD Text Position</b>	Show the text position on the screen.

OSD Settings

## CMOS Settings

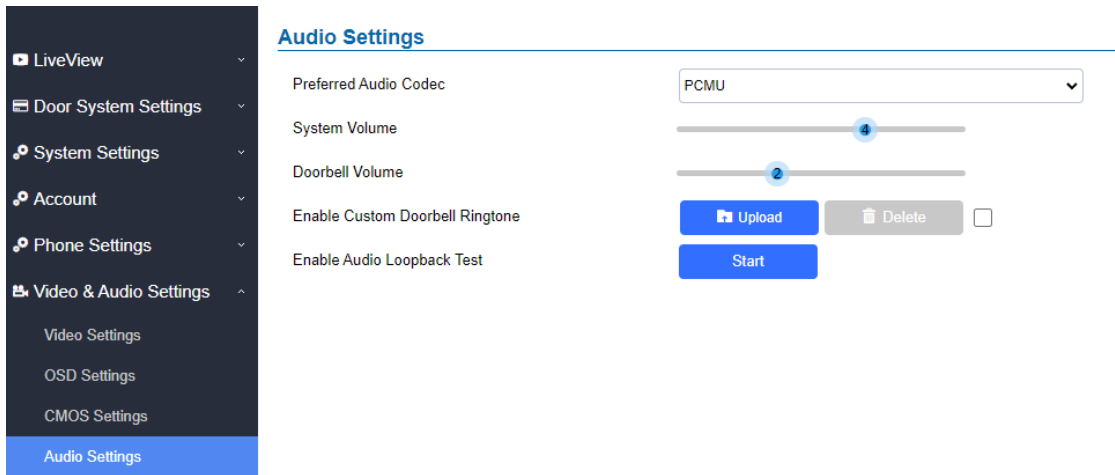
This page configures the CMOS parameters for different scenarios.



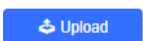
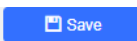

<b>Mode</b>	Pull down to choose "Normal, Low Light, WDR" for different light condition. Default "Normal".
<b>LDC</b>	Default "OFF". When "ON" the display will take a normal shape, but will lose some details located at corner of the original view.
<b>LDC Ratio</b>	Select LDC Ratio. Available options: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

## Audio Settings

This page allows users to configure the audio settings.



<b>Preferred Audio Codec</b>	Configures the audio codec. Three codecs are available: PCMU, PCMA and G.722 are supported.
<b>System Volume</b>	Adjusts the speaker volume connected.
<b>Doorbell Volume</b>	Adjusts the doorbell volume.
<b>Enable Custom Doorbell Ringtone</b>	User can check this option in order to use the custom Doorbell Ringtone. Default Ringtone is used when this option is disabled.
<b>Enable Audio Loopback Test</b>	When enabled, indicating the device is ready for an audio loopback test. Please remember to disable this mode once tested. <b>Note:</b> The OQA Speaker testing has been optimized starting from firmware version 1.0.11.23

- Click on  to upload the ringtone file, then press 
- Click on  to delete the existent custom ringtone.

- o 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:

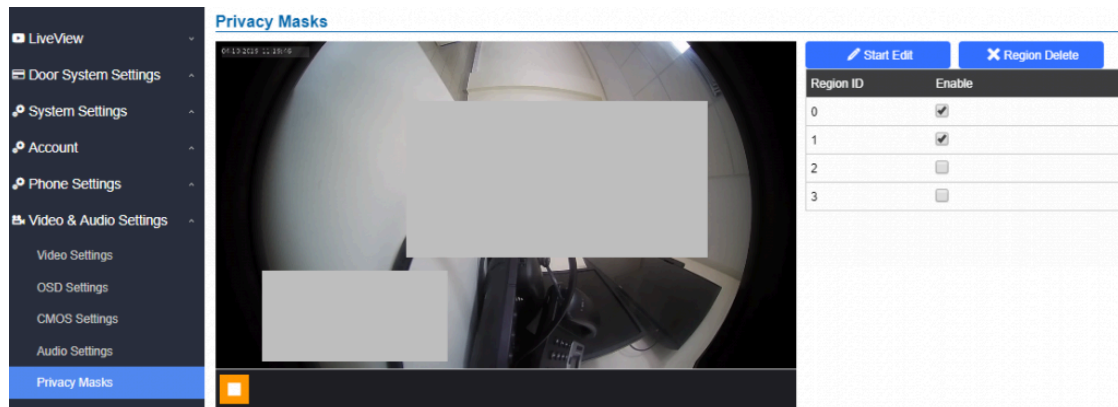
1. Sample Rate: 8K.
2. Channel: Dual-channel.

**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.



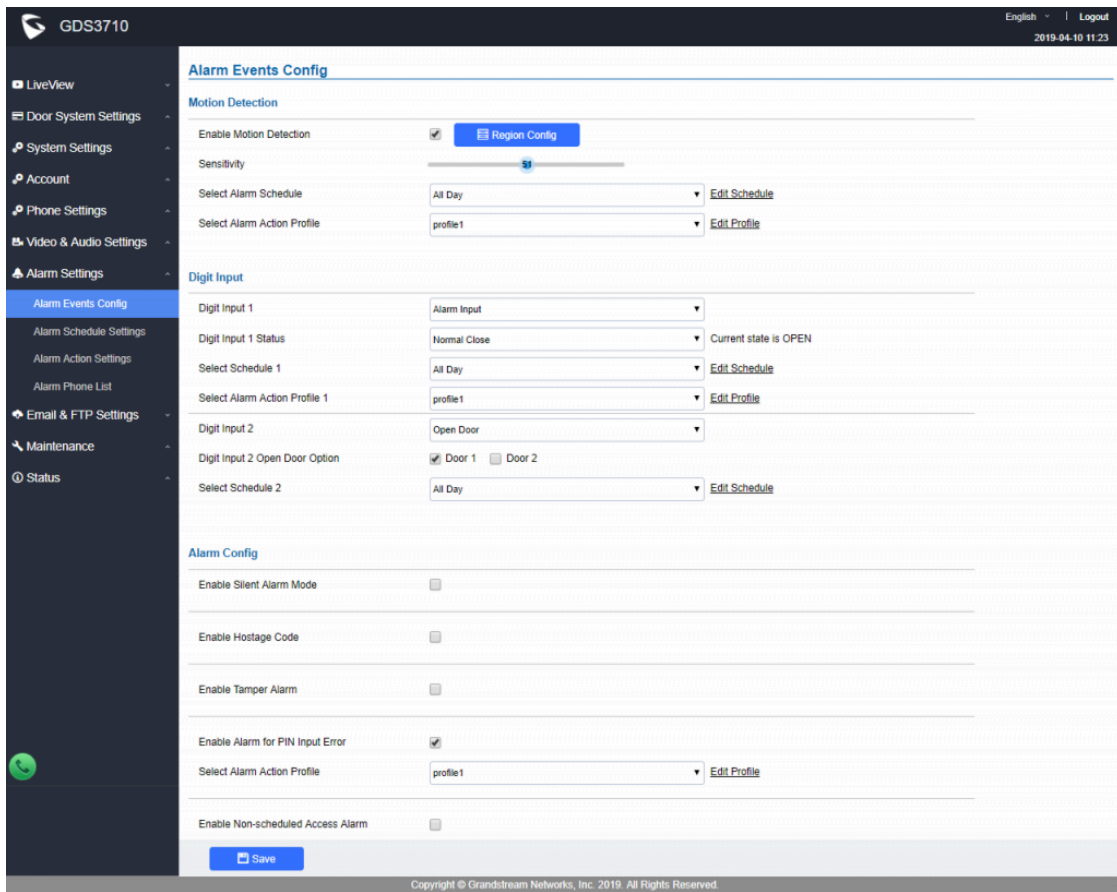
Privacy Masks Configuration Page

## Alarm Settings

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

## Alarm Events Config

This page allows users to configure GDS371x events to trigger programmed actions within a predefined schedule.

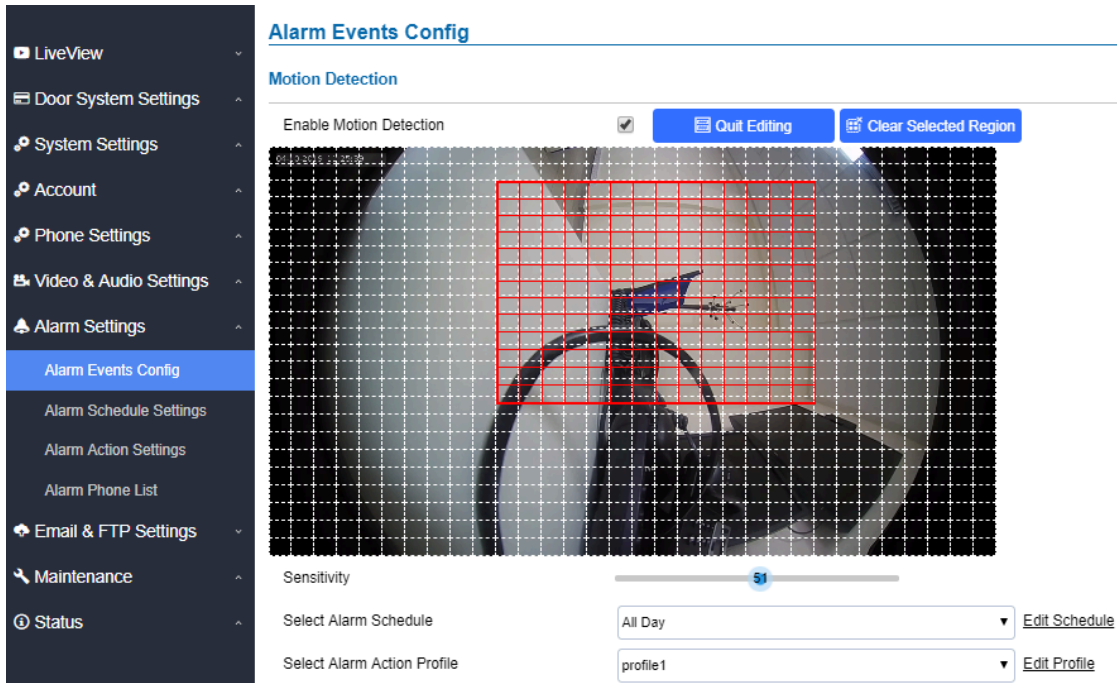


Events Page

Alarm can be triggered either by motion detection or by GDS371x input.

## Motion Detection

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



Region Config

<b>Enable Motion Detection</b>	Enables the motion detection feature.
<b>Region Config</b>	Configures the motion detection region.



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

*Motion Detection*

## Digital Input

### Digit Input

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

*Digital Input*

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

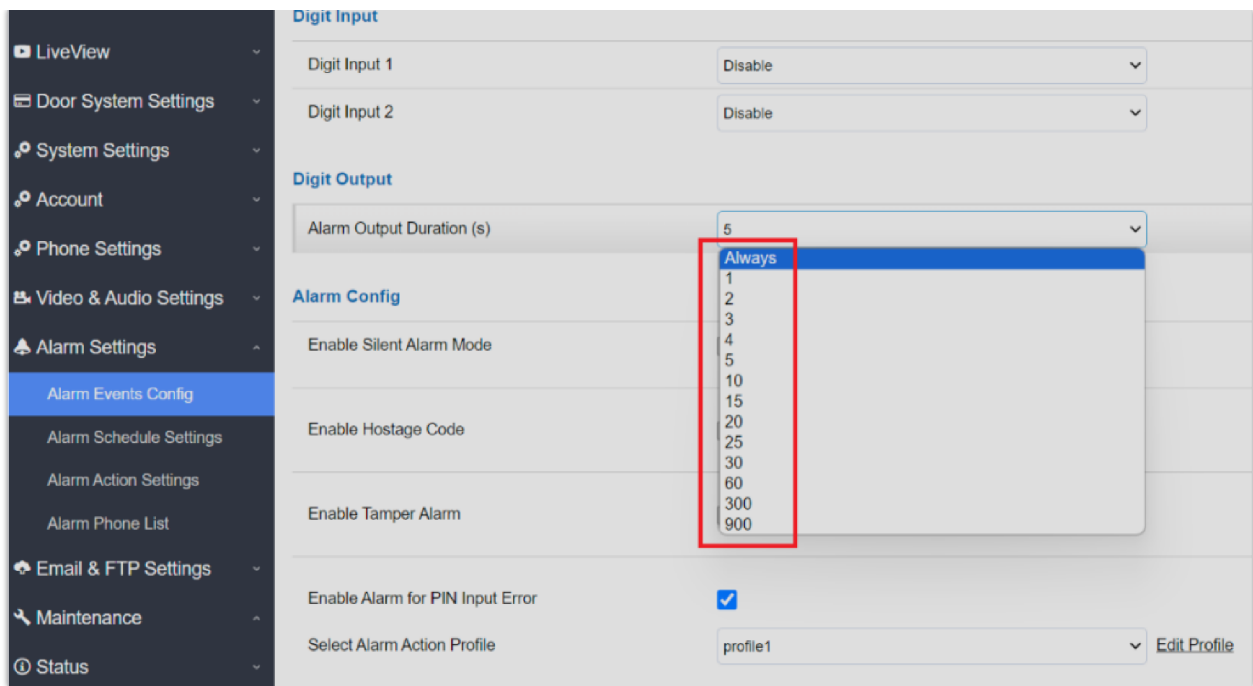
<b>Select Alarm Action Profile 1</b>	Selects the predefined Alarm Action for Profile 1.
<b>Digit Input 2</b>	<p>Selects the Input method (alarm Input or Door Open).</p> <p>Default disabled.</p> <p>Digital Input Port operates in 2 Modes:</p> <ol style="list-style-type: none"> <li>1. <b>Alarm Input:</b> Connect various of sensor to trigger alarm.</li> <li>2. <b>Open Door:</b> Connect a switch to open door from inside.</li> </ol> <p>If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.</p>
<b>Digit Input 2 Open Door Option</b>	When Digital Input is set to <b>Open door</b> then user can select the doors to be affected when Alarm IN 2 is triggered.
<b>Input Digit 2 Status</b>	<ul style="list-style-type: none"> <li>o If set to <b>Normal Open:</b> Configured alarm will be triggered when Digital Input Status switch from Close to Open.</li> <li>o If set to <b>Normal Close:</b> Configured alarm will be triggered when Digital Input Status switch from Open to Close.</li> </ul> <p>By default, Input Digit 2 Status is "Disabled".</p>
<b>Select Schedule 2</b>	Selects the predefined Alarm Schedule.
<b>Select Alarm Action Profile 2</b>	Selects the predefined Alarm Action for Profile 2.
<b>Alarm Output Duration(s)</b>	<p>Select the duration of the alarm output: 1/2/3/4/5/10/15/20/25/30 seconds. This option is hidden when <b>ALMOUT1 Feature</b> is set to Open Door.</p> <p><b>Note :</b> this configuration is exclusive for the GDS3710 Model.</p>

#### *Digital Input*

### **Digital Output**

The digital output field configures the duration of the alarm triggering, to achieve that, the following field can be defined:

- o **Alarm Output Duration (s):** The alarm output duration configures how long the alarm will be triggered. The valid range is 1-900 seconds. When 'Always' is selected in the pull-down menu, the alarm output will be triggered continuously until the administrator disables it.



## Enable Silent Alarm Mode

If Silently Alarm Mode is enabled, GDS371x 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.

### Note

On a triggered alarm call, the siren sound can be disabled by configuring the silent alarm mode.

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

### *Silently Alarm Mode*

## Hostage Code

### Note

This configuration is exclusive for the GDS3710 Model.

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 #"**.

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

<b>Select Alarm Action Profile</b>	Select the Alarm action to be taken when the hostage password is typed on the GDS3710 keypad.  <b>Note:</b> No sound alarm will be triggered in this mode.
------------------------------------	--

*Hostage Code Alarm*

## Tamper Alarm

Tamper alarm is anti-hack from Hardware level. When this option is checked, if the GDS371x is removed from the installation bracket, the built-in Howell Magnetic Switch will function and Tamper Alarm (if enabled and configured, default disabled) will be fired.

This embedded feature in the GDS37xx serves the purpose of enabling the device to detect the separation of these two components, similar to how security magnetic sensors detect the opening and closing of windows or doors.

<b>Enable Tamper Alarm</b>	When activating this mode, GDS371x will keep alarming until the alarm is dismissed.
<b>Select Alarm Action Profile</b>	Select the type of alarms actions to be triggered for the tamper alarm mode.

*Tamper Alarm*

## Keypad Input Error Alarm

**Note**

This configuration is exclusive for the GDS3710 Model.

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

*Keypad Input Error Alarm*

## Non-Scheduled Access Alarm

**Note**

This configuration is exclusive for the GDS3710 Model.

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

*Keypad Input Error Alarm*

No.	Schedule Name	Detail	Edit
1	schedule1		
2	schedule2		
3	schedule3		
4	schedule4		
5	schedule5		
6	schedule6		
7	schedule7		
8	schedule8		
9	schedule9		
10	schedule10		

Alarm Schedule

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

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

**Modify Schedule** ✕

Schedule Name:

Sun	Period1	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="23"/> : <input type="text" value="59"/>
Mon	Period2	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
Tue	Period3	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
Wed	Period4	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
Thu	Period5	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
Fri	Period6	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
Sat	Period7	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>
	Period8	<input type="text" value="00"/> : <input type="text" value="00"/> - <input type="text" value="00"/> : <input type="text" value="00"/>

Copy  Sun  Mon  Tue  Wed  Thu  Fri  Sat  Select All

Edit Schedule

## Non-authorized RFID Card Access Alarm

### Note

This configuration is exclusive to the GDS3710 Model.

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

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

Alarm action when illegal card swiped

## Alarm Action Settings

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

**Alarm Action Settings**

No.	Alarm Action Profile Name	Detail	Edit	Test						
1	profile1									
<div style="border: 1px solid gray; padding: 5px;"> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;"><input checked="" type="checkbox"/> Upload to Alarm Center</td> <td style="width: 50%;"><input checked="" type="checkbox"/> Audio Alarm</td> </tr> <tr> <td><input checked="" type="checkbox"/> Audio Alarm to SIP Phone</td> <td><input checked="" type="checkbox"/> Alarm Output</td> </tr> <tr> <td><input checked="" type="checkbox"/> Send Email</td> <td><input checked="" type="checkbox"/> Upload Snapshot</td> </tr> </table> </div>					<input checked="" type="checkbox"/> Upload to Alarm Center	<input checked="" type="checkbox"/> Audio Alarm	<input checked="" type="checkbox"/> Audio Alarm to SIP Phone	<input checked="" type="checkbox"/> Alarm Output	<input checked="" type="checkbox"/> Send Email	<input checked="" type="checkbox"/> Upload Snapshot
<input checked="" type="checkbox"/> Upload to Alarm Center	<input checked="" type="checkbox"/> Audio Alarm									
<input checked="" type="checkbox"/> Audio Alarm to SIP Phone	<input checked="" type="checkbox"/> Alarm Output									
<input checked="" type="checkbox"/> Send Email	<input checked="" type="checkbox"/> Upload Snapshot									
2	profile2									
3	profile3									
4	profile4									
5	profile5									
6	profile6									
7	profile7									
8	profile8									
9	profile9									
10	profile10									

Alarm Action

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

**Modify Alarm Action Profile** ✕

Alarm Action Profile Name

<input type="checkbox"/> Upload to Alarm Center	<input type="checkbox"/> Audio Alarm
<input type="checkbox"/> Audio Alarm to SIP Phone	<input type="checkbox"/> Alarm Output
<input type="checkbox"/> Send Email	<input type="checkbox"/> Upload Snapshot

Edit Alarm Action

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

<b>Upload to Alarm Center</b>	If selected, the GDS Manager will popup alarm window and sound alarm in the computer speaker.
<b>Audio Alarm to SIP Phone</b>	If selected, GDS371x will call pre-configured (video or audio) phone and will play sound alarm.
<b>Send Email</b>	If selected, an email with snapshot will be sent to the pre-configured email destination.
<b>Audio Alarm</b>	If selected, GDS371x will play alarm audio using built-in speaker.
<b>Alarm Output</b>	If selected, the alarm will be sent to the equipment (for example: Siren) connected to Alarm Output interface.
<b>Upload Snapshot</b>	If selected, snapshots at the moment where the event is triggered will be sent to preconfigured destination (e.g.: FTP or email).

Alarm Actions

## Alarm Phone List

This page allows users to configure the Alarm Phone List, which are phone numbers or extensions list that the GDS371x will call out when event is triggered (e.g.: doorbell pressed).

Alarm Phone List	
Alarm Call Out Account	Auto
Alarm Phone List 1	192.168.1.12:5060
Alarm Phone List 2	1004
Alarm Phone List 3	1003
Alarm Phone List 4	
Alarm Phone List 5	
Alarm Phone List 6	
Alarm Phone List 7	
Alarm Phone List 8	
Alarm Phone List 9	
Alarm Phone List 10	

*Alarm Phone List*

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

*Alarm Phone List*

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

## Email & FTP Settings

This page contains Email and FTP Settings.

### Email Settings

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

*Email Settings – SMTP Page*

SMTP Server	Configures the SMTP Email Server IP or Domain Name.
SMTP Server Port	Specifies the Port number used by server to send email.
From E-mail address	Specifies email address of alarm email sending from, usually client email ID.
Sender Email ID	Specifies sender’s User ID or account ID in the email system used.
Sender Email Password	Specifies sender’s password of the email account.
Alarm-To Email Address 1	Specifies the 1st email address to receive the alarm email.
Alarm-To Email Address 2	Specifies the 2nd email address to receive the alarm email.
SSL	Check if the SMTP email server requires SSL.
Email Subject	Customizes the warning email subject. The default template will be used if the field is left empty
Email Content	Customizes the warning email content. The default template will be used if the field is left empty

*Email Settings – SMTP Page*

**Notes**

- Click “Save” to save the email configuration information.
- E-Mail test successfully 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.



Picture Storage Settings

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

Picture Storage Settings

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

**Note**

- 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 GDS3710/GDS3712s 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:

FTP Filename with	Description
<b>CARD</b>	Meaning that open door operation is using RFID card.

<b>LPIN (Local PIN)</b>	Meaning that open door operation is via Local PIN (Private PIN, or Unified PIN, or Guest PIN).
<b>RPIN (Remote PIN)</b>	Meaning that open door operation is via remote PIN or DTMF PIN. (by local or remote SIP extensions, or GS_Wave/Cellphone, or GDSManager if installed in operation).
<b>RING</b>	Meaning the snapshot taken when somebody pressed the Door Bell button.

### FTP Filenames

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

[To Parent Directory]

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

### FTP filenames

## Maintenance Settings

This page shows the GDS371x Maintenance parameters.

## Upgrade

This page contains the upgrade and provisioning parameters of the GDS371x.

**Upgrade Via**

Selects the upgrade method (TFTP, HTTP, and HTTPS).

<b>Firmware Server Path</b>	Configures the IP address or the FQDN of the upgrade server.
<b>HTTP/HTTPS User Name</b>	The user name for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	The password for the HTTP/HTTPS server.
<b>Firmware File Prefix</b>	Enables your ITSP to lock configuration updates. If configured, only the firmware file with the matching encrypted prefix will be downloaded and flashed into the phone.
<b>Firmware File Postfix</b>	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.
<b>Upgrade via Manually Upload</b>	Allows manual uploading of firmware upgrade files.
<b>Upgrade via</b>	Selects the upgrade method (TFTP, HTTP, and HTTPS).
<b>Config Server Path</b>	Configures the IP address or the FQDN of the configuration server.
<b>HTTP/HTTPS User Name</b>	The user name for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	The password for the HTTP/HTTPS server.
<b>Config File Prefix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
<b>Config File Postfix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
<b>XML Config File Password</b>	Specifies the password for the configuration file.
<b>Validate Server Certificate</b>	Enable this option in order to validate certificate with trusted ones during TLS connection.
<b>Automatic Upgrade Interval</b>	Specifies the upgrade interval in minutes.
<b>Enable DHCP Option 66 Override Server</b>	Activates DHCP option 66 to override upgrade/config servers.
<b>3CX Auto Provision</b>	Enables 3CX Provision feature for auto provisioning.
<b>Enable DHCP Option 120 Override SIP Server</b>	Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is enabled.
<b>Automatic Upgrade</b>	Enables automatic upgrade and provisioning. Set schedule for provisioning for either every X minutes, every day or every week. Default is No.
<b>Randomized Automatic Upgrade</b>	Enable and define the start/End hours of the day and days of the week where the GDS will randomly checking for update.
<b>Disable SIP NOTIFY Authentication</b>	If this option is checked, the Device will not challenge NOTIFY with 401. Default setting is Enabled.

**LED Pattern:**

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

1. Doorbell button blue LED will flash when firmware files are downloading. (the call button will flash in the GDS3712)
2. Digit 1,2,3 blue LED will flash during upgrading from 0 to 25%, then stays on. (For the GDS3710)
3. Digit 4,5,6 blue LED will flash during upgrading from 25 to 50%, then stays on. (For the GDS3710)
4. Digit 7,8,9 blue LED will flash during upgrading from 50 to 75%, then stays on. (For the GDS3710)
5. Digit \*,0,# blue LED will flash during upgrading from 75 to 100%, then stays on. (For the GDS3710)
6. After all key's blue LEDs light on then flash twice then reboot itself to finish the upgrade process. (For the GDS3710)

**Reboot & Reset**

This page allows user to reboot and reset the GDS371x.

**Reboot & Reset**

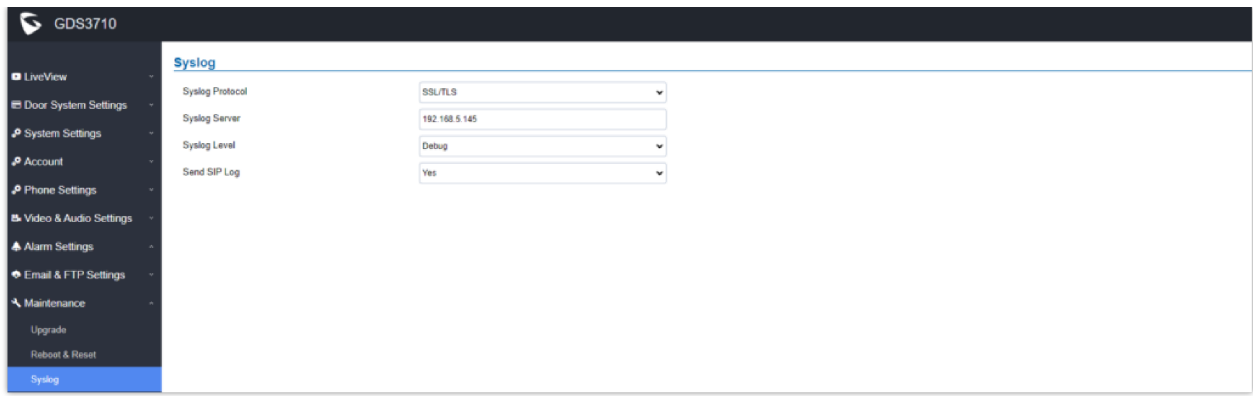
Reboot	<input type="button" value="Reboot"/>
Auto Reboot	<input type="checkbox"/> Everyday <input type="button" value="v"/> 00 <input type="button" value="v"/> : 00 <input type="button" value="v"/>
Reset	Retain Network Data Only <input type="button" value="v"/> <input type="button" value="Reset"/>

*Reset & Reboot Page*

<b>Reboot</b>	When clicked, the GDS371x will restart (soft reboot).
<b>Auto Reboot</b>	With this feature, user can configure convenient selected schedule for the device reboot by itself, per week or per day, to make a smooth performance.
<b>Reset</b>	There are two options for the reset function.
<b>Clear All Data</b>	All data will be reset, GDS3710 will be set to factory default.
<b>Retain Network Data Only</b>	All data will be erased except for Network data like IP address...
<b>Retain Only Card Information</b>	All data will be erased except for cards information. (Configuration available for the GDS3710 Only )
<b>Retain Network Data and Card Information</b>	All data will be erased except for Network Data and Card Information. (Configuration available for the GDS3710 Only )

*Reset & Reboot***Syslog**

This page allows users to configure SYSLOG to collect information to help troubleshooting issues with GDS371x.

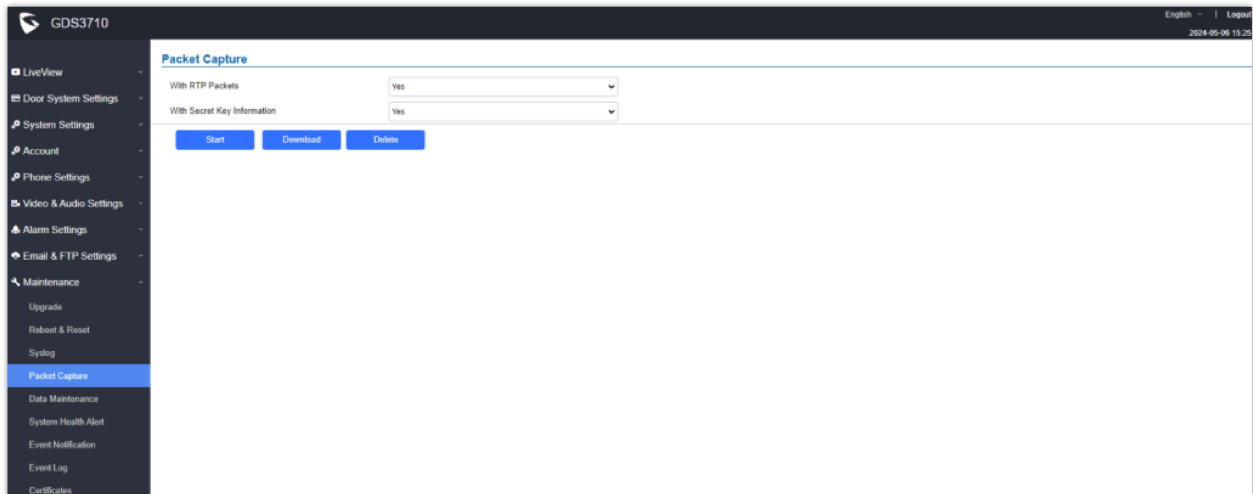


Syslog Page

<b>Syslog Protocol</b>	Selects the syslog protocol used: UDP or encrypted SSL/TLS. <b>Note:</b> The user can set the p-value "P82307" to "1" to save syslog settings and internal logs across a factory reset.
<b>Syslog Server</b>	Defines the IP address or FQDN of the syslog server
<b>Syslog Level</b>	Five levels of Debugging are available, None, Debug, Info, Warning, Error.
<b>Send SIP Log</b>	When enabled by selecting 'Yes' from the dropdown menu, the SIP log will be included in the syslog message. This is particularly useful when a secure link is employed, such as SSL/TLS.

## Packet Capture

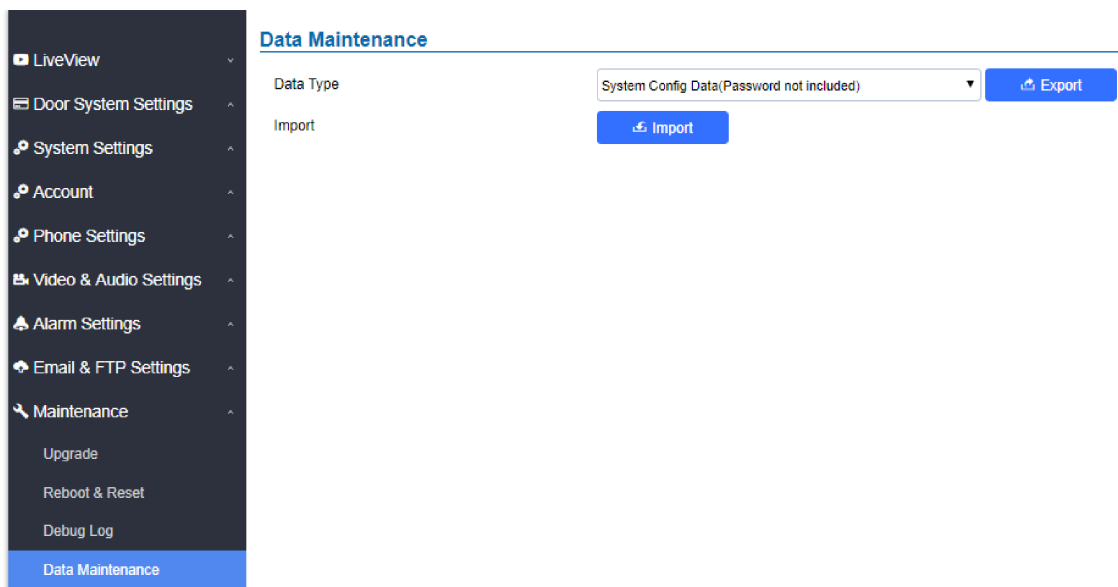
The packet capture feature allows administrators to trace the different changes related to the GDS371x device by running a packet capture, then downloading the .pcap output file and analyzing it.



<b>With RTP Packets</b>	Defines whether the packet capture file will include RTP information or not, this is recommended when troubleshooting media related issues such as audio issues...
<b>With Secret Key Information</b>	Configures whether the packet capture file will contain secret key information.

## Data Maintenance

This page allows users to manage the GDS371x configuration file by importing/exporting configuration files.



Data Maintenance Page

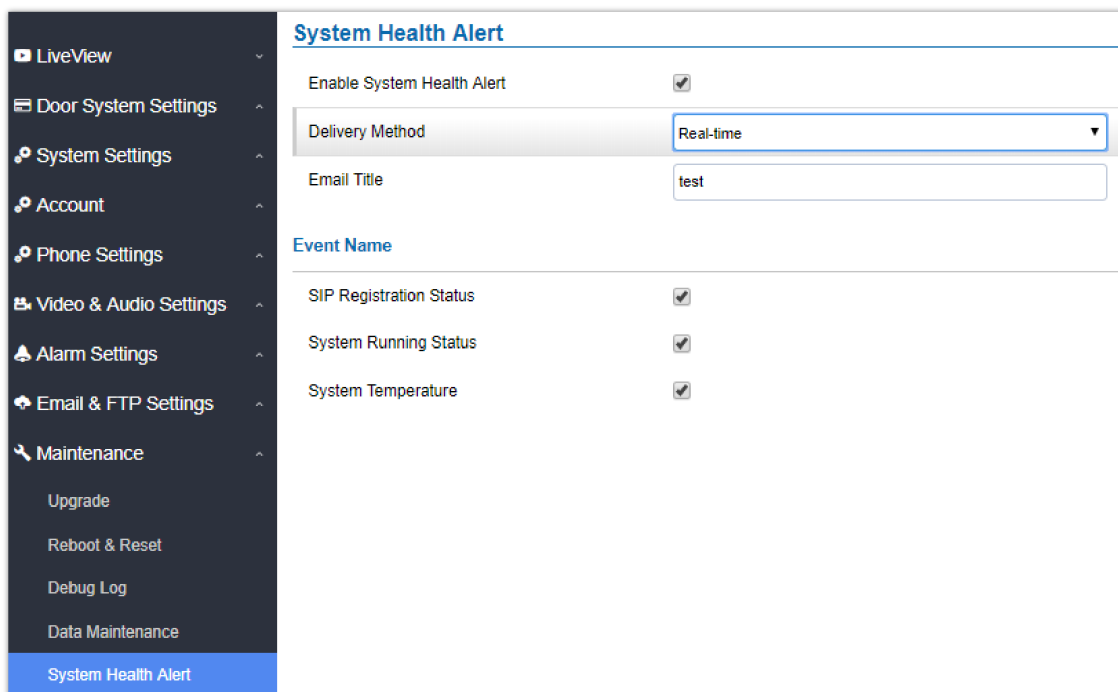
Click on  to save the GDS371x configuration in a predefined directory.

### 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.



System Health Alert Page

<b>Enable System Health Alert</b>	When this option is checked, then the GDS will send alert emails regarding the events selected under Event Name section using the already configured [Email Settings].
<b>Delivery Method</b>	When set to Realtime, the GDS will be sending successively alert emails every second. When set to Periodic, user can define the time interval between alert emails.

<b>Email Title</b>	Customize the Email title. Maximum length is 256 character.
<b>SIP Registration Status</b>	When checked, Email will contain Offline/Online indication for all 4 accounts.
<b>System Running Status</b>	When checked, Email will contain the system uptime.
<b>System Temperature</b>	When checked, Email will contain Temperature value of the system in °C and °F, as well as whether the temperature is normal or not.

## Event Notification

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

Examples:

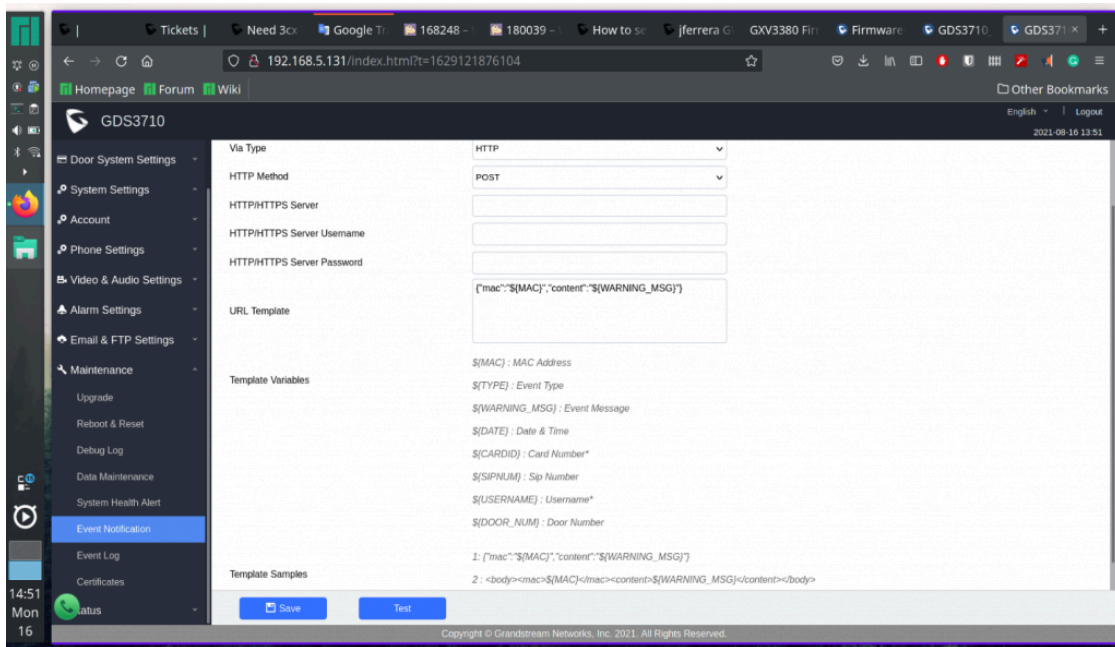
- After an RFID Card swiping, GDS3710 will send to the configured HTTP server the following HTTP POST containing "Use card open door" event:

```
POST / HTTP/1.1
Host: 192.168.6.107
Authorization: Basic Og==
Connection: keep-alive
Content-Length: 90
Date: 2017-11-09; Time: 14:07:27; Event describe: Use card open door. Card ID: 378690700.
```

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

```
POST/HTTP/1.1
Host:192.168.6.107
Authorization:BasicOg==
Connection:keep-alive
Content-Length:62
Date: 2017-11-09; Time: 14:13:12; Event describe: Phone call.
```

These HTTP POST messages can be used by a 3<sup>rd</sup> party software to integrate the GDS371x.



Log Manager Page

<b>Enable Event Notification</b>	Enables Event Notification feature
<b>Via Type</b>	Choose which protocol will be used to connect to the logs server (HTTP or HTTPS).
<b>HTTP Method</b>	Choose which HTTP(s) method will be used to send the logs to the server (POST or GET).
<b>HTTP/HTTPS Server</b>	Enter the IP address of domain name for the logs server.
<b>HTTP Server Username</b>	Configure the username of your HTTP(s) server
<b>HTTP Server Password</b>	Configure the password of your HTTP(s) server
<b>URL Template</b>	Specify the template for the event log messages that will be sent to the server.
<b>Template Variables</b>	<p>Customers can now populate the Event Notification template with additional information such as Event Type, Card ID, Username, etc., along with snapshots captured when a door is opened. Including more detailed information in the email, along with the snapshot, will enhance the management of door access events. This feature is particularly beneficial for customers with multiple doors on their premises, including, but not limited to, schools, gyms, hospitals, and office buildings.</p> <p>The supported template variables are:</p> <ul style="list-style-type: none"> <li>● <b>\${MAC}</b> : MAC Address</li> <li>● <b>\${TYPE}</b> : Event Type</li> <li>● <b>\${WARNING_MSG}</b> : Event Message</li> <li>● <b>\${DATE}</b> : Date &amp; Time</li> <li>● <b>\${CARDID}</b> : Card Number*</li> <li>● <b>\${SIPNUM}</b> : SIP Number</li> <li>● <b>\${USERNAME}</b> : Username*</li> <li>● <b>\${DOOR_NUM}</b> : Door Number</li> </ul>



## 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
- Unauthorized door opening attempt
- 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
- Admin Log

The screenshot shows the 'Event Log' interface. On the left is a dark sidebar menu with 'Event Log' highlighted. The main area displays a table of log entries with the following columns: No., Date & Time, Event Type, Username, Card Number, and (Account)Sip Number. The table contains 18 rows of data.

No.	Date & Time	Event Type	Username	Card Number	(Account)Sip Number
1	2019-04-10 08:06:02	System Up			
2	2019-04-10 08:14:55	Call Log(Door Bell Call)			(1)6400
3	2019-04-10 08:15:13	Visiting Log(Door 1)			(1)6400
4	2019-04-10 08:15:35	Call Log(Door Bell Call)			(1)4000
5	2019-04-10 08:15:50	Visiting Log(Door 1)			(1)4000
6	2019-04-10 08:16:44	Reboot			
7	2019-04-10 08:17:09	System Up			
8	2019-04-10 08:25:54	Call Log(Door Bell Call)			(1)4000
9	2019-04-10 08:26:09	Visiting Log(Door 1)			(1)4000
10	2019-04-10 08:31:52	System Up			
11	2019-04-10 08:40:37	Call Log(Door Bell Call)			(1)6400
12	2019-04-10 10:27:27	Call Log(Door Bell Call)			(1)3004
13	2019-04-10 10:27:42	Call Log(Door Bell Call)			(1)3004
14	2019-04-10 10:27:52	Call Log(Door Bell Call)			(2)3004
15	2019-04-10 10:28:16	Call Log(Door Bell Call)			(1)3004
16	2019-04-10 10:28:39	Call Out Log			(2)3004
17	2019-04-10 11:12:21	Call Log(Door Bell Call)			(1)3004
18	2019-04-10 11:12:35	Call Log(Door Bell Call)			(1)3004

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

### Notes

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

## Certificates

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

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

Certificates			
Trusted CA Certificates			
No.	Issued By	Expiration	
1			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
2			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
3			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
4			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
5			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
6			<input type="button" value="Upload"/> <input type="button" value="Delete"/>
Custom Certificate			
No.	Issued By	Expiration	
1			<input type="button" value="Upload"/> <input type="button" value="Delete"/>

*Upload Certificate files*

In order to upload your Trusted CA certificate:

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

Trusted CA Certificates			
No.	Issued By	Expiration	
1	-	2018-07-17 15:46:03	<input type="button" value="Upload"/> <input type="button" value="Delete"/>
2			<input type="button" value="Upload"/> <input type="button" value="Delete"/>

User could press  to delete one of the files.

In order to upload your Custom certificate:

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

Custom Certificate			
No.	Issued By	Expiration	
1			<input type="button" value="Upload"/> <input type="button" value="Delete"/>

User could press  to delete one of the files.

### Note

- 2nd generation certificates are supported on the GDS371x Models.
- The default method for downloading CFG files now uses HTTPS, streamlining the process of updating 2nd generation certificates without the need for manual configuration. This improvement enhances security and simplifies certificate management for a more seamless experience.

## Status

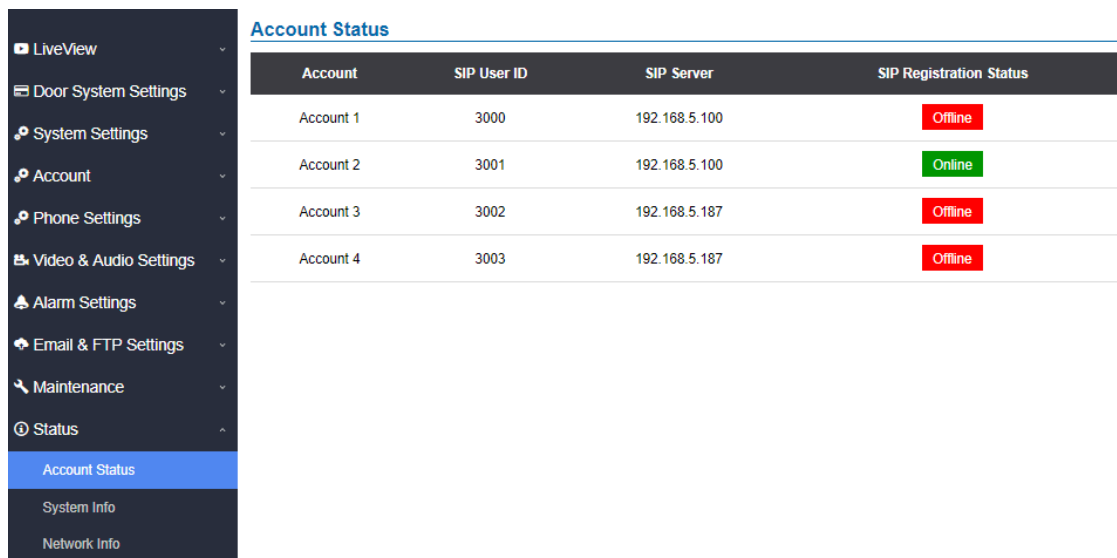
This page displays GDS371x system and network information.

## 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



Account	SIP User ID	SIP Server	SIP Registration Status
Account 1	3000	192.168.5.100	Offline
Account 2	3001	192.168.5.100	Online
Account 3	3002	192.168.5.187	Offline
Account 4	3003	192.168.5.187	Offline

*System Info Page*

## System Info

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

**System Info**

Product Model	GDS3710
Hardware Version	V1.7A
Part Number	9650001417A
Boot Version	1.0.0.59
Core Version	1.0.13.2
Base Version	1.0.13.2
Prog Version	1.0.13.2
CPE Version	1.0.5.5
Certificate Type	ECDSA+SHA384
System Uptime	20 hours 42 minutes

Firmware Status: [Check](#)

System Temperature: 39°C (102.2°F)

Tamper Sensor: Triggered

Door Ctrl: Untriggered

Digit Output: Untriggered

Digit Input 1: Untriggered

Digit Input 2: Untriggered

System Info Page

<b>Product Model</b>	Displays the Product Model.
<b>Hardware Version</b>	Displays the Hardware Version.
<b>Part Number</b>	Displays the Part Number.
<b>Boot Version</b>	Displays the Boot Version.
<b>Core Version</b>	Displays the Core Version.
<b>Base Version</b>	Displays the Base Version.
<b>Prog Version</b>	Displays the Prog Version.
<b>CPE Version</b>	Displays the Customer premise equipment version.
<b>Certificate Type</b>	Displays the security certificate type used.
<b>System Up Time</b>	Displays the time since the first boot of the GDS371x.
<b>SIP Registration Status</b>	Sows whether the SIP account is registered or not.
<b>Firmware Status</b>	Click the button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
<b>System Temperature</b>	Shows the current system temperature (in °C and °F). <b>Note:</b> the following parameter is added on the MIB file of the SNMP protocol.
<b>Tamper Sensor</b>	Shows if the Temper Sensor is triggered or not.
<b>Digit Output</b>	Shows if the Alarm Out is triggered or not. If ALMOUT1 Feature is set to Open Door, then two fields will show up indicating the state of both door 1 and door 2.
<b>Input Digit 1</b>	Shows if alarm IN 1 is triggered.

<b>Input Digit 2</b>	Shows if alarm IN 2 is triggered.
----------------------	-----------------------------------

*System Info page definitions*

## Network Info

This page displays the network system information of GDS3710.

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

*Network Info Page*

<b>MAC Address</b>	Displays the GDS3710 MAC Address.
<b>IP Address Mode</b>	Displays the IP address mode used.
<b>IP Address</b>	Displays the IP address of the GDS3710.
<b>Subnet Mask</b>	Displays the Subnet Mask used.
<b>Gateway</b>	Displays the GDS371x Gateway.
<b>DNS Server 1</b>	Displays the Preferred DNS Server.
<b>DNS Server 2</b>	Displays the secondary DNS Server.

*Network Info*

## CONNECTING GDS371x WITH GXV33XX

The GDS371x Door System offers a powerful integration with GXV33xx and allows users to open the door, initiates call to the GDS371x and gets real time audio/video stream.

The GXV33xx can be connected with the GDS371x 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:

<https://documentation.grandstream.com/knowledge-base/connecting-gds37xx-with-gxv33x/>

# CONNECTING GS WAVE WITH GDS371x DOOR SYSTEM

The GDS371x Door System can interact with the GS Wave softphone application to allow users to open door, initiate call to the GDS371x, 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 GDS371x to connect with Grandstream Wave Android™ version, please refer to following guide:

<https://documentation.grandstream.com/knowledge-base/connecting-gds3710-with-wave-lite-android-guide/>

- **GS Wave IOS:** For more details about needed steps for configuring the GDS371x to connect with Grandstream Wave iOS™ version, please refer to following guide:

<https://documentation.grandstream.com/knowledge-base/connecting-gds3710-with-wave-lite-ios-guide/>

## GDS371x HTTP API

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

For more details, please refer to following guide:

<https://documentation.grandstream.com/knowledge-base/gds37xx-http-api/>

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.

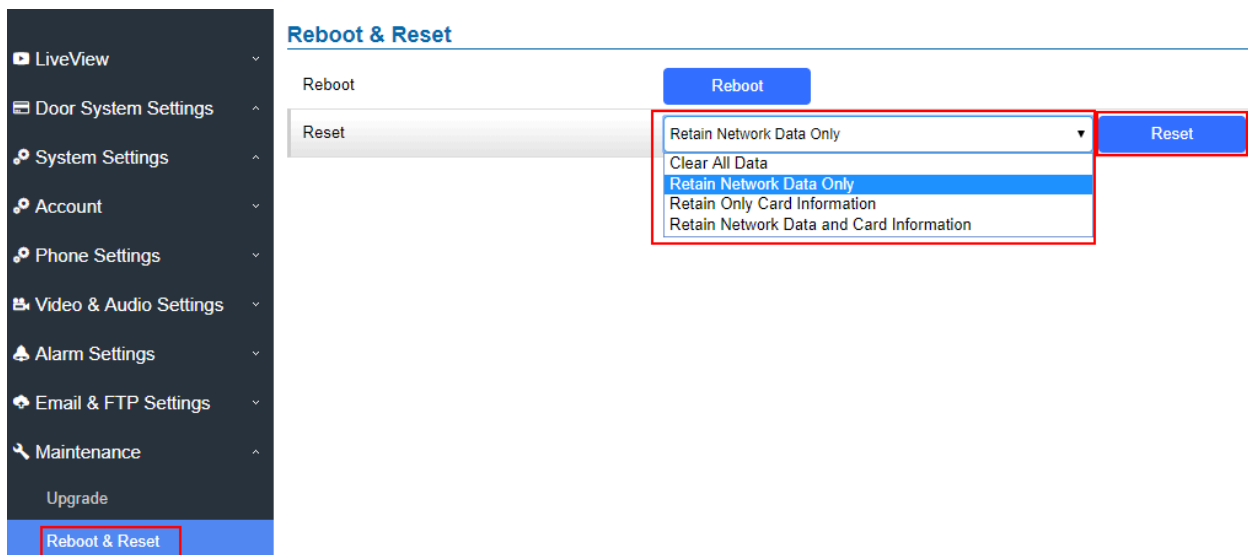
**Administrator Privilege** is required, and administrator authentication verification has to be executed before any operation to the related parameter configuration.

## FACTORY RESET

### Restore to Factory Default via Web GUI

To perform factory reset to the GDS371x via the Web GUI, please refer to following steps:

1. Access to GDS371x Web GUI using the using the shipped default password.
2. Navigate to **Maintenance → Reboot & Reset.**
3. Select the reset type from Rest drop down menu and press reset button as displayed on the following screenshot.



**Note**

Retaining Network Data and Card Information or Only Crad information options are available only on the GDS3710 Model.

## Hard Factory Reset

**Note**

Resetting the device on the Wiegand interface cable is supported only on the GDS3710 Model.

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**

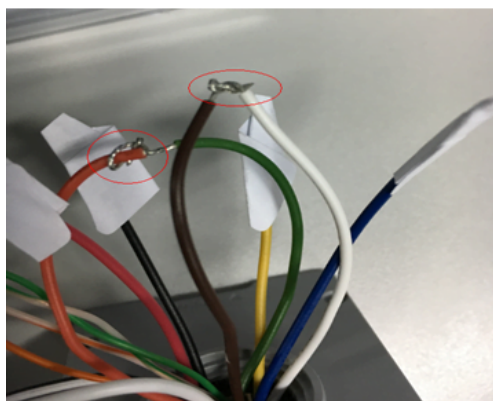
Power must **NOT** be lost while performing hard factory reset.



*Wiegand Interface Cable*

To perform hard factory reset to the GDS371x, 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.



*Wiegand Cable Connection*

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

### Notes

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

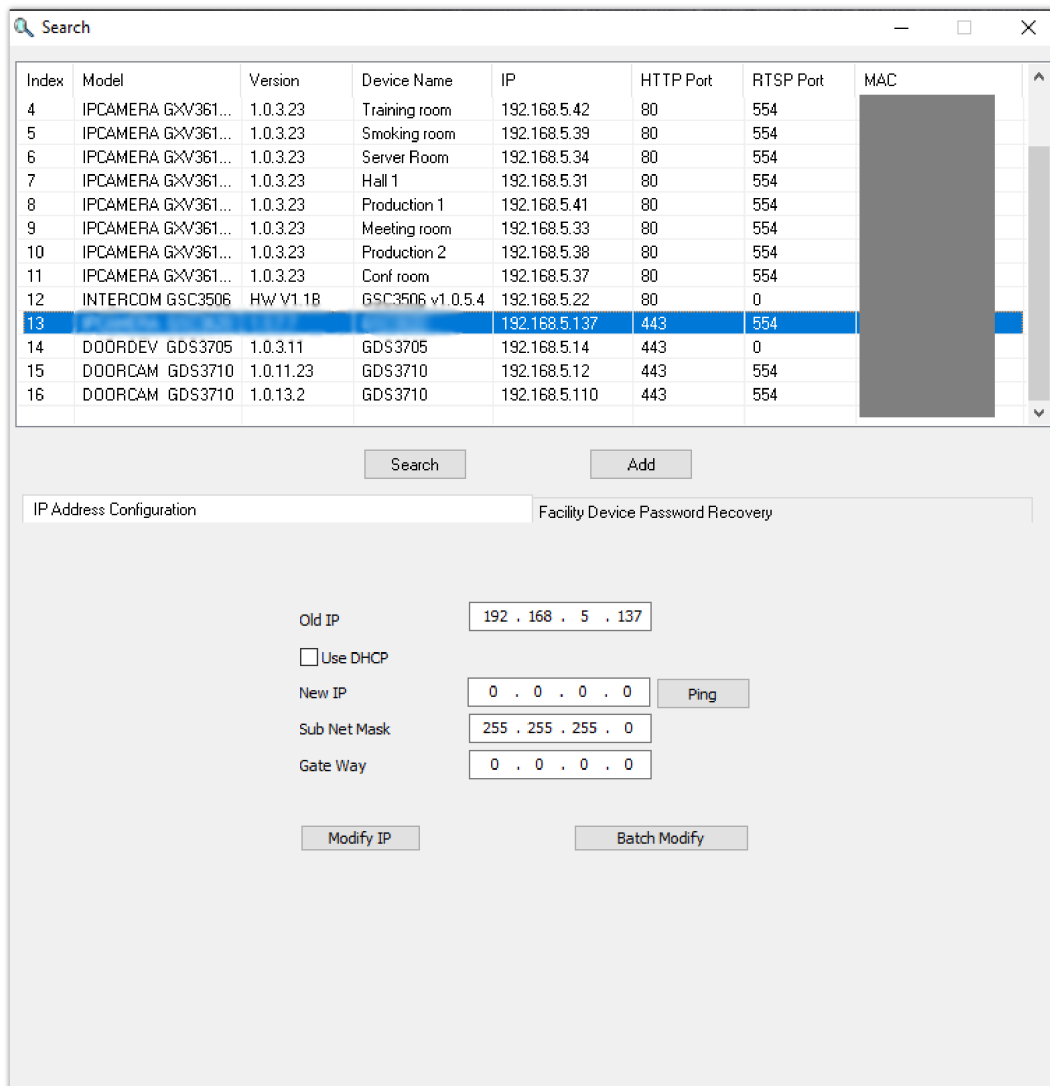
4. After 3 ~ 5 minutes the GDS3710 will finish performing the reset process, then the user can log into the GDS3710 web GUI using the shipped default password.

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

## Hard Factory Reset Using GS Search

The GDS37xx can be reset using the GS Search tool by following these steps :

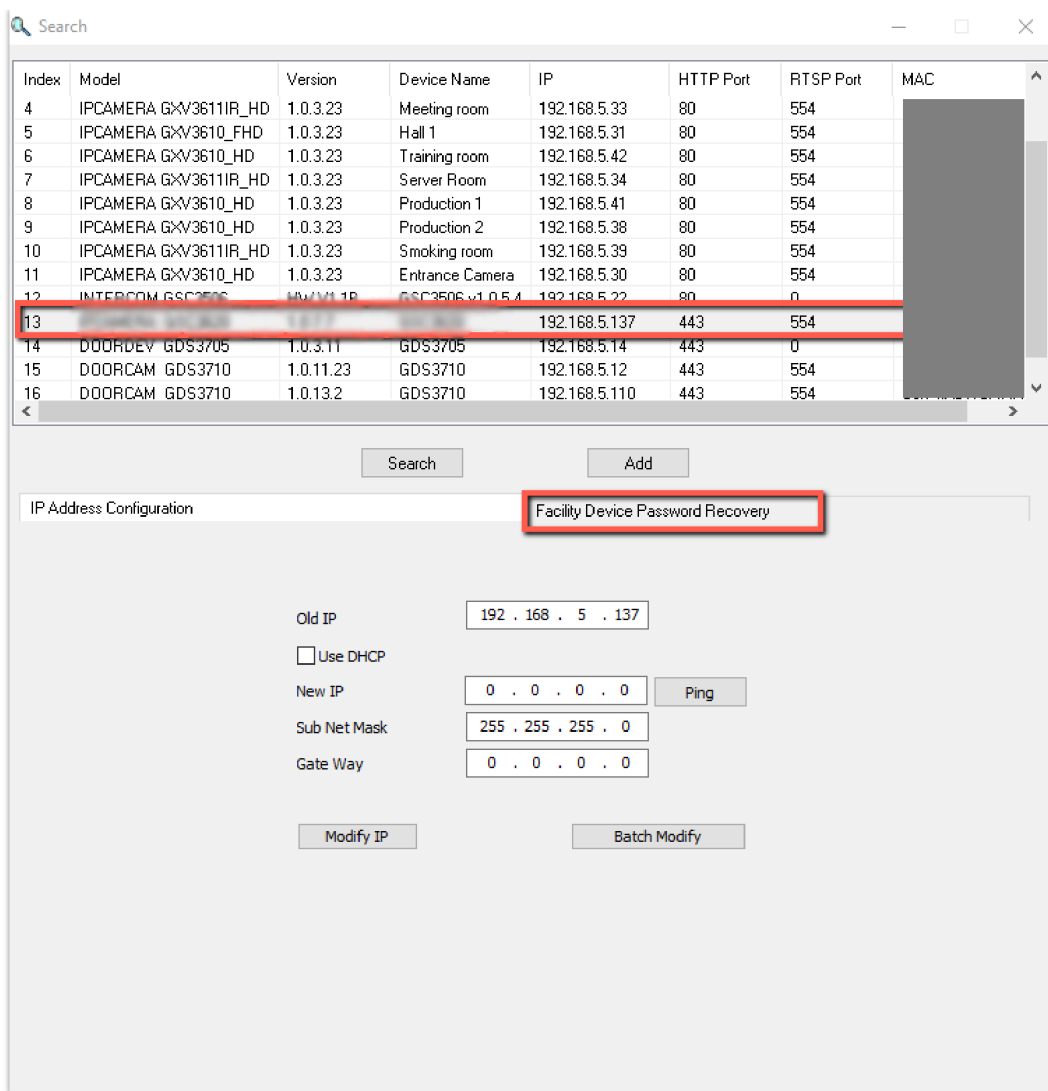
1. Open the GS Search tool that can be downloaded from the [Grandstream tools page](#).



GS Search main interface.

2. Select the device in question, in our example it is the GDS37xx, and then select Facility Device Password Recovery.





GS Search – Selecting the device to be reseted

3. Enter the Default password of the unit which can be found in the stick on the device body or in the package box.
4. Perform the reset of the device by clicking the Reset button option.

Search

Index	Model	Version	Device Name	IP	HTTP Port	RTSP Port
5	IPCAMERA GXV3610_FHD	1.0.3.23	Hall 1	192.168.5.31	80	554
6	IPCAMERA GXV3611IR_HD	1.0.3.23	Conf room	192.168.5.37	80	554
7	IPCAMERA GXV3610_HD	1.0.3.23	Training room	192.168.5.42	80	554
8	IPCAMERA GXV3610_HD	1.0.3.23	Production 2	192.168.5.38	80	554
9	IPCAMERA GXV3611IR_HD	1.0.3.23	Server Room	192.168.5.34	80	554
10	IPCAMERA GXV3611IR_HD	1.0.3.23	Meeting room	192.168.5.33	80	554
11	IPCAMERA GXV3611IR_HD	1.0.3.23	Smoking room	192.168.5.39	80	554
12	INTERCOM GSC3506	HW V1 1B	GSC3506 v1.0.5.4	192.168.5.22	80	0
13	IPCAMERA GDS3710	1.0.11.23	GDS3710	192.168.5.137	443	554
14	DOORCAM GDS3710	1.0.11.23	GDS3710	192.168.5.12	443	554
15	DOORDEV GDS3705	1.0.3.11	GDS3705	192.168.5.14	443	0
16	DOORCAM GDS3710	1.0.13.2	GDS3710	192.168.5.110	443	554

Search Add

IP Address Configuration Facility Device Password Recovery

Mac Address

IP Address

Default Password

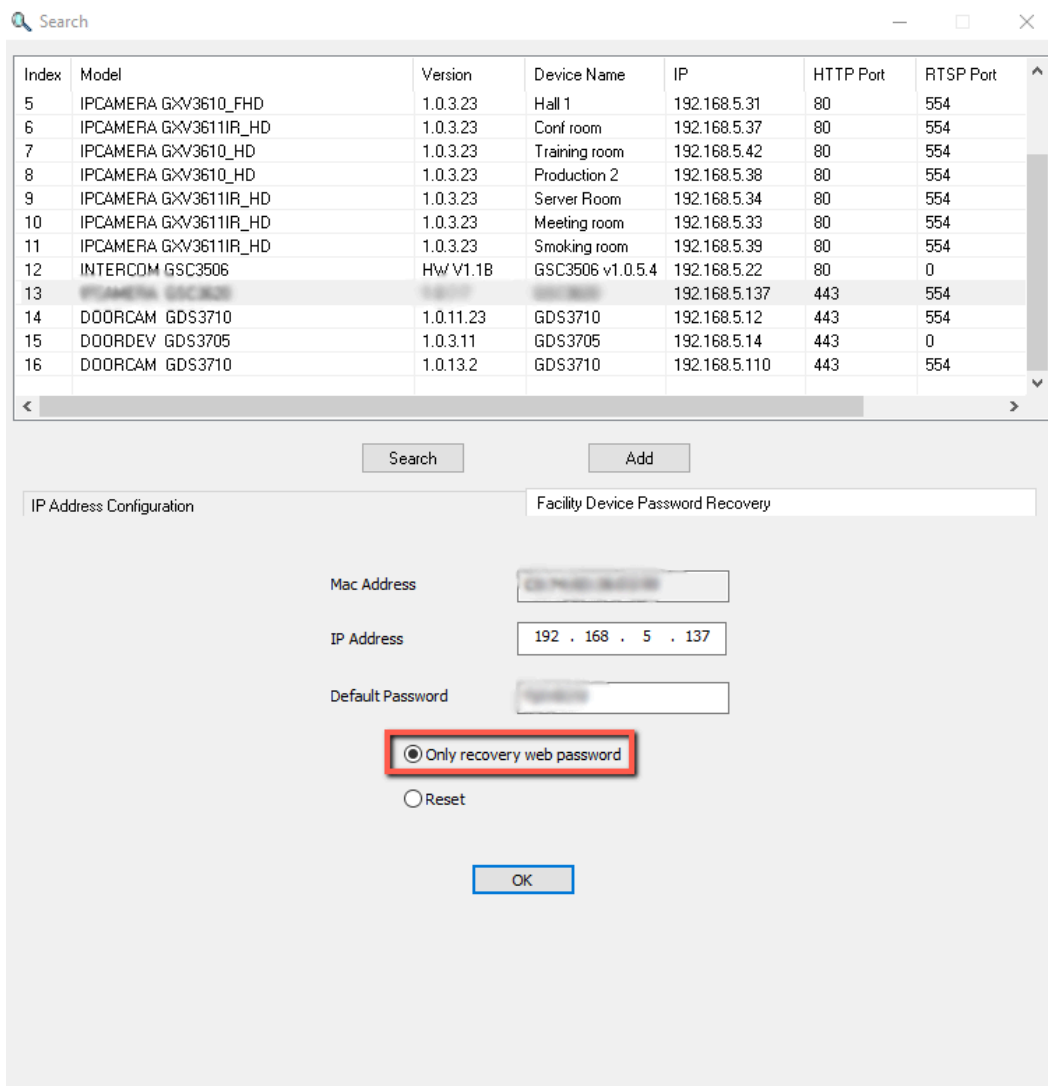
Only recovery web password

Reset

OK

GS Search – Resetting the device

5. You have the possibility to recover the initial default web password as well by selecting the option “only recover web password”



GS Search – Resetting the web password

## Restore to Factory Default Via SIP NOTIFY

1. Access your GDS37xx 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 GDS37xx 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).

9

## Restore factory password via special key combination

### Note

The following configuration is exclusive to the GDS3710 Model.

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

*Encoding rule*

### Notes

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: xwpzx6AA
- Decoding the default password to digits would be: 2423162426611

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

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

## 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 1.0.13.9

*Product name : GDS3712, GDS3710*

- Updated CPE version to 1.0.5.7 [[CPE Version](#)]
- Added schedule for enabling background light (GDS3710 Only). [[Enable White Backlight on Time Interval](#)]

### Firmware Version 1.0.13.5

*Product name : GDS3712, GDS3710*

- Changed "Zero Config" option wording to "3CX Auto Provision". [[3CX Auto Provision](#)]
- Added feature to allow device sending syslog debug messages after reset. [[Syslog Protocol](#)]
- Added SRTP requirement. [[SRTP Key Length](#)]
- Added support for Local Call Features. [[Enable Local Call Features](#)]
- Added SSL Key Log File. [[With secret key information](#)]
- Added support for DHCP Option 2. [[Allow DHCP Option 2 to Override Time Zone Setting](#)]
- Added support for packet capture. [[Packet Capture](#)]
- Enhanced Alarm Output duration to last longer or unlimited. [[Digital Output](#)]
- Added support for keypad blue LED light brightness to be adjusted. [[Blue Light Brightness\(Time Interval\)](#)] [[Blue Light Brightness\(Key Pressed\)](#)]
- Added support for the option "Send SIP Log". [[Send SIP Log](#)]
- Added feature to send "event type", "username" and "card ID" in the email with open door event. [[Template Variables](#)]
- Added support for 802.1X. [[802.1X Mode](#)] [[802.1X Identity](#)] [[MD5 Password](#)] [[802.1X CA Certificate](#)] [[802.1X Client Certificate](#)]

### Firmware Version 1.0.13.2

*Product name : GDS3712, GDS3710*

- Added support for HTTP API request when web access is set to HTTPS. [[HTTP API Open Door Compatibility Mode](#)]
- Added support to edit the interval of "Onhook Timer After Remote Open Door(s)". [[Onhook Timer After Remote Open Door\(s\)](#)]
- Added the ability to configure delay for the snapshots taken when "Door Opened" or "Doorbell Pressed". [[Snapshot Delay when Door Opened\(s\)](#)] [[Snapshot Delay when Doorbell Pressed\(s\)](#)]
- Added admin audit logging to the event log functionality [[Admin Log](#)].
- Added ability to define the TLS protocol level. [[Minimum TLS Version](#)] [[Maximum TLS Version](#)]
- Added support for System Temperature object identifier in the MIB file. [[System Temperature](#)]
- Added improvement for Alarm Email Subject and Text in GDS371x. [[Email Subject](#)] [[Email Content](#)]
- Added Emergency PIN to Re-enable Keep Door Open. [[Emergency PIN](#)]
- Added in WebUI the Certificate Type Information. [[Certificate type](#)]
- Added support for access with RTSP password in ONVIF. [[ONVIF](#)]
- Added support for 2nd generation certificate. [[Custom Certificate](#)]

- Added the use of HTTPS as default CFG file download method to update gen2 cert without manual configuration. [[Custom Certificate](#)]
- Added support for SNI extension on TLS. [[Check domain certificates](#)]
- Added support for SNMP trap when doorbell button pressed. [[SNMP trap port](#)]
- Added "BRIGHTNESS/CONTRAST/SATURATION" setting bar at LiveView page on WebUI. [[GDS371x HOME WEB PAGE](#)]

#### **Firmware Version 1.0.11.23**

*Product name : GDS3712, GDS3710*

- Added ability to disable alarm siren sound in triggered alarm call. [[Enable/Disable Silent Alarm Mode](#)]
- Added "Keep Door Open" to be configured to use multiple schedules and allow users to choose and apply which schedule to use. [[Schedule Open Door](#)]
- Added granular DIGITAL OUTPUT time duration (1s to 4s). [[Doorbell Mode](#)]
- Added sending PIN via Wiegand when HTTP API open door executed. [[Door Relay Options](#)]
- Added option that no "#" is required after PIN input to make the device behave like a traditional access controller when "Disable Keypad SIP Number Dialing" is selected. [[Local PIN Type](#)]
- Added firmware upgrade via manually uploading firmware files from the computer. [[Upgrade via Manually Upload](#)]
- Optimized speaker via OQA testing. [[Audio Testing](#)]
- Updated CPE version to 1.0.5.5 [[CPE Version](#)]

#### **Firmware Version 1.0.11.18**

- Added SNMP support. [[SNMP Settings](#)]

#### **Firmware Version 1.0.11.15**

- Added support of configuring different "Number Called When Door Bell Pressed" entries depending on the time frame or schedule. [[Basic Settings](#)]

#### **Firmware Version 1.0.11.13**

- Updated non-scheduled access alarm event log. [[Event Log](#)]

#### **Firmware Version 1.0.9.9**

- Added support for "SIP URI scheme When using TLS" and "Support SIP Instance ID". [[SIP](#)]
- Increased OSD text length to 32 [[OSD](#)]

#### **Firmware Version 1.0.9.6**

- Allow using "PIN#" format for Unified PIN when "Disable Keypad SIP Number Dialing" is enabled. [[Unified PIN](#)]
- Added support for Secondary SIP Server. [[secondary SIP server](#)]

#### **Firmware Version 1.0.7.26**

- Added support for Basic Authentication of HTTP API Remote Open Door. [[Basic Settings](#)]

#### **Firmware Version 1.0.7.24**

- Added MAC in User-Agent configuration. [[Account 1 – 4](#)]
- Added 'unauthorized card swiped on Wiegand reader' alert message in event Log. [[Event Log](#)]
- Added prompt to prevent empty alarm action profile name. [[Alarm Action Settings](#)]
- Added more template variables in Event Notification. [[Event Notification](#)]
- Improved private PIN management under the Card Management Web UI. [[Show private PIN](#)]
- Added option to choose HTTP method to either POST or GET in Event Notification. [[Event Notification](#)]

### **Firmware Version 1.0.7.23**

- Added support for Key Sensitivity Options. [Key Sensitivity Level]
- Added support for Scheduled Auto Reboot. [Auto Reboot]
- Increased whitelist up to 200 per Account. [Account [1-4] White List]
- Added support for One-Way Interlocking Mode. [One-Way Interlocking Mode]
- Added support for door opening with and without call when paired with GSC3570. [Open Door via GDS37xx with or without a SIP Call]

### **Firmware Version 1.0.7.19**

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

### **Firmware Version 1.0.7.14**

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

### **Firmware Version 1.0.7.11**

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

### **Firmware Version 1.0.7.10**

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

### **Firmware Version 1.0.7.8**

- Enhanced the failover mechanism based on DNS SRV. [DNS Mode]
- Include Holidays on Keep Door Open Schedule for Door 2. [[Holiday Mode](#)]

### **Firmware Version 1.0.7.7**

- Added siren alarming function when door opened abnormally. [Connection Examples]
- Added option to only accept incoming SIP call from Proxy/Server. [Accept Incoming SIP from Proxy Only]
- Added support for including Holidays at Keep Door Open schedule. [Keep Door Open]

Added reset/restore factory default password via special keypad combination operations. [FACTORY RESET]

### **Firmware Version 1.0.7.4**

- Added ability to separate webUI credentials from the GDSManager credentials. [GDSManager Configuration Password]
- Added G.729 audio codec support. [Technical Specifications] [Preferred Vocoder]

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

#### **Firmware Version 1.0.5.6**

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

#### **Firmware Version 1.0.5.2**

- Added Alarm\_Out port (COM1 interface) to 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. [JPEG Authentication Mode] [Live View Page]

#### **Firmware Version 1.0.3.32**

- Added LED lighting indication pattern for firmware upgrade process. [Upgrade]
- Increased the maximum allowed whitelist numbers to 30 records with 20-digit length for each number [Account [1-4] White List]
- Added Support for HTTP command to Open Door. [Enable HTTP API Remote Open Door]
- Added display device logs at GDS web UI. [Event Log]
- Added valid start/end dates for Card Management. [Card Management]
- Added "Test" button for Alarm Action. [Alarm Action]
- Added "Alarm IN/OUT Status" display at GDS "Status" page UI.
- [Added Self-defined Even Notification Message. [Event Notification]

#### **Firmware Version 1.0.3.31**

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

#### **Firmware Version 1.0.3.23**

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

#### **Firmware Version 1.0.3.13**

- Added option to disable alarm sound at phone side when event trigger SIP call to the phone. [Enable two-way SIP Calling]
- Increased maximum characters to 256 in "Number called when doorbell pressed" to allow serial hunting of SIP extensions or IP address with port or mixing of both, with each ring several seconds before going next. [Number Called When Door Bell Pressed]
- Added feature to capture snapshot when doorbell pressed. [Snapshot when Doorbell Pressed]
- Added feature to disable keypad input (lock keypad) and ONLY doorbell button can be pressed. [Disable Keypad (except the Doorbell Button)]
- Added option to disconnect call automatically after door open event. [Enable On Hook After Remote Door Opened]

- Issuing Mode automatically. [Card issuing State Expire Time(m)]
- Added ability for whitelist entries to open door using remote PIN. [Account [1-4] White List]

#### **Firmware Version 1.0.2.25**

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

#### **Firmware Version 1.0.2.22**

- No major changes.

#### **Firmware Version 1.0.2.21**

- Allow config and call IP address format on SIP field when dialing the Virtual Number. [SIP Number]
- Added "Silent Alarm" Mode. [Enable Silent Alarm Mode]
- Added option Backup/Restore including all passwords like SIP/FTP/Remote Access, etc. [Data Maintenance]
- Added schedule support for Card and PIN. [Schedule]
- Added LLDP support. [Enable LLDP]
- Added database automatic backup and synchronization.
- Modified WebGUI style.
- Added card information batch delete option in the WebGUI. [Users Operation]
- Added option to enable "Motion Detection", "Tamper Alarm" and backlight partially light. [Tamper Alarm] [Motion Detection] [Enable Background Light]
- Added card user limitation up to 2000 and Group Limit to 50. [Card Management]
- Added Card and PIN schedule configuration Central Mode. [Central Mode]
- Added LDC Ratio Control and Adjustment. [LDC Ratio]
- Expanded the range of Ring timeout. [Ring Timeout]
- Added option to disable Auto Answer. [Auto Answer]
- Updated the "DingDong" tone when doorbell pressed.
- Added function to check the default value.
- Added Factory Reset via special procedures. [Hard Factory Reset]
- Added file upload and download (card information, configuration etc.) can be executed after authentication. [Card Management]

#### **Firmware Version 1.0.2.13**

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

#### **Firmware Version 1.0.2.9**

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

### **Firmware Version 1.0.2.5**

- Added folder creation and file arrangement if multiple GDS3710s are uploading snapshots to FTP server.
- Added DTMF audio playing when key be pressed. [Key Tone Type]
- Separated volume control under Web GUI -> Audio Settings. [System Volume][Doorbell Volume]
- Added "Audio, Snapshot, Recording and File Path Saved" operation with icons at Live View webpage. [Live View Page]
- Added "show password" feature when the eye icon be clicked in the webGUI.
- Added prompt popup message when capture button clicked.
- Use different email title to separate the Motion Detection and Temperature Out of the Range alarm.
- Set initial value of "0" for Virtual Number and SIP number if user leaving the field empty. [Virtual Number][SIP Number]
- Added support open door remotely via GDS Manager utility (after GDS Manager version 1.0.0.78)
- Supported GXP color phone JPEG\_Over\_HTTP with encryption and authentication. This feature is pending on GXP/UCM6xxx firmware availability. Currently this feature does not support 3rd party PBX if SIP extension is used in Open Door configuration.
- Added SSH support with default TCP port 22. [Enable SSH][SSH Port]
- Added GS\_Wave (Android/iOS) Application support for Open Door. [CONNECTING GS WAVE WITH GDS3710 DOOR SYSTEM].
- Enhanced webGUI login process and added random default password.
- Enhance security by disable the DTMF to open door
- Added support of sending DTMF tone in SIP calling (RFC2833, SIP INFO). [Enable DTMF]

### **Firmware Version 1.0.1.19**

- This is the initial version for GDS371x.