

Grandstream Networks, Inc.

---

GDS3705

Audio Door Access System

**User Manual**



## **COPYRIGHT**

©2022 Grandstream Networks, Inc. <https://www.grandstream.com>

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

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

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

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

## **CAUTION**

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

## **WARNING**

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



## FCC Compliance Statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) The device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

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

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

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

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

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



## CE Declaration of Conformity

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

ETSI EN 300 330 V2.1.1 (2017-02);

ETSI EN 301 489-1 V2.1.1 (2017-02); ETSI EN 301 489-3 V2.1.1 (2017-03);

EN 60950-1: 2006+A11:2009+A1:2010+A12:2011+A2:2013: EN 62311: 2008



Manufacturer:

Grandstream Networks, Inc.

126 Brookline Ave, 3<sup>rd</sup> Floor Boston, MA 02215, USA

Channel Frequency: 125 KHz

Channel Number: 1

Antenna Type / Gain: Internal

Type of Modulation: ASK

Operation temperature: -30 °C ~ +60 °C

Storage temperature: -35 °C ~ +60 °C

Humidity: 10 ~ 90% non-condensing

## GNU GPL INFORMATION

GDS3705 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:

<https://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download>



## Table of Contents

<b>CHANGE LOG .....</b>	<b>14</b>
Firmware Version 1.0.1.21 .....	14
Firmware Version 1.0.1.16 .....	14
Firmware Version 1.0.1.11 .....	14
Firmware Version 1.0.1.6 .....	14
Firmware Version 1.0.1.3 .....	15
Firmware Version 1.0.0.41 .....	15
Firmware Version 1.0.0.37 .....	16
Firmware Version 1.0.0.36 .....	16
Firmware Version 1.0.0.35 .....	16
Firmware Version 1.0.0.31 .....	16
Firmware Version 1.0.0.28 .....	16
Firmware Version 1.0.0.26 .....	17
Firmware Version 1.0.0.20 .....	17
<b>DOCUMENT PURPOSE .....</b>	<b>18</b>
<b>WELCOME .....</b>	<b>19</b>
<b>PRODUCT OVERVIEW .....</b>	<b>20</b>
Feature Highlights .....	20
Technical Specifications .....	20
<b>GETTING STARTED .....</b>	<b>22</b>
Equipment Packaging .....	22
Description of the GDS3705 .....	23
Connecting and Setting up the GDS3705 .....	23
GDS3705 Wiring Connection .....	24
GDS3705 Back Cover Connections .....	25
Connection Example .....	25



Power GDS3705 using PoE .....	26
Power GDS3705 using PSU.....	26
<b>GETTING TO KNOW GDS3705 .....</b>	<b>27</b>
Connecting GDS3705 to Network with DHCP Server .....	27
Windows Platform .....	27
UPnP.....	27
GS Search.....	28
GDS Manager Utility Tool.....	29
Connect to the GDS3705 using Static IP .....	30
<b>GDS3705 APPLICATION SCENARIOS .....</b>	<b>32</b>
Peering Mode without SIP Server.....	32
Peering using SIP Server (UCM6XXX).....	32
<b>GDS3705 PERIPHERAL CONNECTIONS .....</b>	<b>34</b>
Alarm IN/OUT .....	35
Protection Diode .....	36
Connection Examples .....	36
Wiring Sample using 3 <sup>rd</sup> Party Power Supply .....	37
Wiring Sample using Power Supply for both GDS3705 and Electric Strike .....	37
Wiring Sample using PoE to power GDS3705 and 3 <sup>rd</sup> Party Power Supply for Electric Strike ....	38
Good Wiring Sample for Electric Strike and High-Power Device .....	39
Wiegand Module Wiring Examples .....	39
Input example with 3 <sup>rd</sup> party power supply for Wiegand device .....	39
Input example with power supply for both GDS3705 and Wiegand device .....	40
Output example with 3 <sup>rd</sup> party power supply for Wiegand device .....	41
Wiegand RFID Card Reader Example .....	41
Siren alarming when door opened abnormally .....	42
GDS3705 Connection: IN2 set as Normal Close and “Fail Safe” Electric Strike using 3 <sup>rd</sup> Party Power Supply.....	42
GDS3705 Connection: IN2 set as Normal Open and “Fail Secure” Electric Strike using 3 <sup>rd</sup> Party Power Supply.....	43



Open Door via GDS3705 with or without a SIP Call .....	44
<i>Door opening with SIP Call</i> .....	45
<i>Door opening without SIP Call</i> .....	45
Secure Open Door via GDS3705/GSC3570 Peering .....	46
<b>GDS3705 HOME WEB PAGE.....</b>	<b>49</b>
<b>GDS3705 SETTINGS.....</b>	<b>50</b>
Door System Settings .....	50
<i>Basic Settings</i> .....	50
<i>Using Alarm Out (COM 1) to Control a Second Door</i> .....	57
<i>Keep Door Open</i> .....	61
<i>Card Management</i> .....	63
<i>Add Users Manually</i> .....	63
<i>Add Users Automatically</i> .....	65
<i>Users Operation</i> .....	65
<i>Group</i> .....	66
<i>Schedule</i> .....	66
<i>Holiday</i> .....	67
System Settings .....	68
<i>Date &amp; Time Settings</i> .....	68
<i>Network Settings</i> .....	69
<i>OpenVPN® Settings</i> .....	70
<i>Access Settings</i> .....	72
<i>User Management</i> .....	73
<i>Factory Functions</i> .....	75
Account .....	76
<i>Account 1 - 4</i> .....	76
Phone Settings .....	81
<i>Phone Settings</i> .....	81
<i>Account [1-4] White List</i> .....	83
Audio Settings .....	84





Audio Settings.....	84
Alarm Config .....	85
Alarm Events Config .....	85
Input Digit.....	86
Alarm Output.....	87
Silently Alarm Mode .....	87
Hostage Code .....	88
Tamper Alarm .....	88
Keypad Input Error Alarm.....	88
Non-Scheduled Access Alarm.....	88
Alarm Schedule Settings .....	89
Alarm Action When Illegal Card Swiped .....	90
Alarm Action Settings .....	91
Alarm Phone List .....	92
Email Settings .....	93
Email Settings.....	93
Maintenance Settings .....	94
Upgrade .....	95
Reboot & Reset .....	96
Debug Log .....	97
Data Maintenance.....	97
System Health Alert .....	98
Event Notification.....	99
Event Log.....	100
Certificates .....	102
Status .....	103
Account Status.....	103
System Info.....	104
Network Info.....	105
<b>FACTORY RESET .....</b>	<b>107</b>
Restore to Factory Default Via Web GUI .....	107



Hard Factory Reset.....	107
Restore to Factory Default Via SIP NOTIFY.....	109
Reset Factory Password Via Special Key Combination Operation .....	110
<b>EXPERIENCING THE GDS3705 .....</b>	<b>112</b>

## Table of Tables

Table 1: GDS3705 Features in a Glance .....	20
Table 2: GDS3705 Technical Specifications .....	20
Table 3: Equipment Packaging .....	22
Table 4: GDS3705 Wiring Connection .....	24
Table 5: Door System Settings.....	51
Table 6: Immediate Door-Open Table .....	61
Table 7: Schedule Keep Door Open .....	62
Table 8: Card Info .....	64
Table 9: Add Group .....	66
Table 10: Date & Time.....	69
Table 11: Basic Settings .....	70
Table 12: Access Settings .....	72
Table 13: User Management.....	74
Table 14: User Management.....	76
Table 15: SIP Account Basic & Advanced Settings.....	77
Table 16: Phone Settings .....	82
Table 17: White List.....	84
Table 18: Audio Settings Page .....	84
Table 19: Input Digit .....	86
Table 20: Silently Alarm Mode.....	87
Table 21: Hostage Code Alarm .....	88
Table 22: Tamper Alarm .....	88
Table 23: Keypad Input Error Alarm .....	88
Table 24: Non-Scheduled Access Alarm .....	88
Table 25: Alarm Actions.....	92
Table 26: Alarm Phone List .....	93
Table 27: Email Settings - SMTP .....	94
Table 28: Upgrade.....	95
Table 29: Reset & Reboot .....	96
Table 30: System Health Alert.....	99
Table 31: System Info.....	104



Table 32: Network Info .....	106
------------------------------	-----

## Table of Figures

Figure 1: GDS3705 Package .....	22
Figure 2: GDS3705 Front View .....	23
Figure 3: GDS3705 Back View .....	23
Figure 4: GDS3705 Back Cover Connections .....	25
Figure 5: GDS3705 Back Cover .....	25
Figure 6: Connection Example.....	26
Figure 7: Powering the GDS3705 .....	26
Figure 8: Detecting GDS3705 via UPnP .....	27
Figure 9: GDS3705 Login Page .....	28
Figure 10: GS Search Discovery .....	29
Figure 11: GDS3705 Detection using GDS Manager .....	30
Figure 12: Static IP on Windows .....	31
Figure 13: Peering GDS3705 with UCM6XXX.....	33
Figure 14: Peripheral Connections for GDS3705 .....	34
Figure 15: Alarm_In/Out Circuit for GDS3705.....	35
Figure 16: Protection Diode - Example 1 .....	36
Figure 17: Protection Diode - Example 2 .....	36
Figure 18: 3 <sup>rd</sup> party Power Supply Wiring Sample .....	37
Figure 19: Power Supply used for both GDS3705 and Electric Strike .....	37
Figure 20: Wiring Sample using PoE to power GDS3705 and 3 <sup>rd</sup> party Power Supply for Electric Strike .....	38
Figure 21: Example to Avoid when Powering the Electric Strike .....	38
Figure 22: Electric Strike and High-Power Device Example .....	39
Figure 23: Wiegand Input Example with 3 <sup>rd</sup> party Power Supply.....	39
Figure 24: Wiegand Input Example with Power Supply for GDS3705 and Wiegand Device .....	40
Figure 25: Wiegand Output Wiring Example.....	41
Figure 26: Wiegand RFID Card Reader Example .....	41
Figure 27: Digital Input set as Normal close .....	42
Figure 28: "Fail safe" Electric Strike using 3rd Party Power Supply .....	43
Figure 29: Digital Input set as Normal open.....	43
Figure 30: "Fail Secure" Electric Strike using 3rd Party Power Supply .....	43
Figure 31: GDS3705 Configuration Example.....	44
Figure 32: GSC3570 Configuration Example.....	45
Figure 33: Open Door with SIP Call.....	45
Figure 34: Open Door without SIP Call.....	46
Figure 35: Open Door without SIP Call.....	46
Figure 36: GSC3570 secure open door via GDS3705 .....	47
Figure 37: GDS3505 Web GUI configuration for secure open door with GSC3570.....	48



Figure 38: GSC3570 Web GUI configuration for secure open with GDS3705 .....	48
Figure 39: Change Language Page .....	49
Figure 40: Door System Settings Page.....	50
Figure 41: Alarm_Out1 Feature .....	57
Figure 42: Universal Local PIN .....	58
Figure 43: Remote PIN to Open Door.....	59
Figure 44: Right of Card and Private PIN .....	60
Figure 45: Keep Door Open .....	61
Figure 46: Immediate Door Open .....	61
Figure 47: Schedule Door Open .....	62
Figure 48: Modify Schedule .....	62
Figure 49: Card Management .....	63
Figure 50: Card Info .....	64
Figure 51: Add Group.....	66
Figure 52: Groups List.....	66
Figure 53: Edit Schedule Time .....	67
Figure 54: Edit Holiday Time .....	68
Figure 55: Date & Time Page.....	68
Figure 56: Basic Settings Page.....	69
Figure 57: OpenVPN Settings page.....	71
Figure 58: Access Settings Page .....	72
Figure 59: User Management Page .....	73
Figure 60: Recover Password.....	74
Figure 61: Recover Password - Email Address .....	75
Figure 62 : Factory Functions Page.....	76
Figure 63: SIP Account Settings Page.....	77
Figure 64: Phone Settings Page .....	82
Figure 65: White List Page.....	83
Figure 66: Audio Settings Page .....	84
Figure 67: Events Page.....	85
Figure 68: Input Digit.....	86
Figure 69: Alarm Schedule.....	89
Figure 70: Edit Schedule.....	90
Figure 71: Enable Non-authorized RFID Card Access Alarm .....	90
Figure 72: Alarm action profile example for illegal card swipe.....	91
Figure 73: Alarm Action .....	91
Figure 74: Edit Alarm Action.....	92
Figure 75: Alarm Phone List.....	93
Figure 76: Email Settings - SMTP Page .....	94
Figure 77: Upgrade Page.....	95
Figure 78: Reset & Reboot Page .....	96
Figure 79: Debug Log Page .....	97



Figure 80: Data Maintenance Page .....	98
Figure 81: System Health Alert Page .....	98
Figure 82: Event Notification .....	100
Figure 83: Event Log.....	101
Figure 84: Upload Certificate files .....	102
Figure 85: Account Status Page .....	103
Figure 86: System Info Page.....	104
Figure 87: Network Info Page .....	105
Figure 88: Reset via Web GUI .....	107
Figure 89: Wiegand Interface Cable .....	108
Figure 90: Wiegand Cable Connection .....	108



## CHANGE LOG

This section documents significant changes from previous versions of user manual for GDS3705. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

### Firmware Version 1.0.1.21

- Cisco WebEx IOT: Added Web UI Option “SIP URI Scheme When Using TLS” and “Support SIP Instance ID” [Table 15: SIP Account Basic & Advanced Settings]
- Added support for configurable keypad blue light On/Off. [Table 5: Door System Settings]
- Added unauthorized card swiped on wired external 3rd party Wiegand reader will also have alert message in event Log [Event Log]
- Increased Whitelist Number to maximum 200 in each Account [Table 17: White List]
- Added prompt “Alarm Schedule Name” and “Alarm Action Profile Name” cannot be blank. [Alarm Config]
- 3CX IOT: Support “Add MAC in User-Agent” and Added “Codec Negotiation Priority” configuration [Table 15: SIP Account Basic & Advanced Settings]
- Added error prompt if illegal port value is set to web access [Table 12: Access Settings]

### Firmware Version 1.0.1.16

- Added open door without SIP call when paired with GSC3570. [Door opening without SIP Call]
- Added scheduled Auto Reboot. [Auto Reboot]
- Enhanced open door via 3<sup>rd</sup> party Webrelay ON/OFF URL. [Door System Settings]
- Added Alarm Action triggering when illegal card swiped. [Alarm Action When Illegal Card Swiped]
- Added enable/disable password display on Web UI when using HTTPs. [Enable PIN/Password Display (HTTPs)]
- Added secure open door with GDS3705/GSC3570 setup. [Secure Open Door via GDS3705/GSC3570 Peering]
- Added the time zone GMT-03:30 for Newfoundland. [Time Zone]

### Firmware Version 1.0.1.11

- Added OpenVPN® support. [OpenVPN® Settings]
- Added WebRelay Open Door Feature. [Door Relay Options]
- Increased Unlock Holding Time to 30 minutes. [Unlock Holding Time]
- Changed SIP Account Name to Display Name. [Display Name]
- Added reboot/resync via SIP Notify. [Disable SIP NOTIFY Authentication]

### Firmware Version 1.0.1.6

- Added support for failover mechanism based on DNS SRV. [DNS Mode]



- Added siren alarming function when door opened abnormally (special wiring required). [Siren alarming when door opened abnormally]
- Added including Holidays at Keep Door Open schedule. [Holiday Mode]
- Added reset/restore factory default password via special keypad combination operations. [Reset Factory Password]

### **Firmware Version 1.0.1.3**

- Added support for re-registration before expiration. [Re-register before Expiration (s)]
- Enhanced security and prevent ghost calls. [Accept Incoming SIP from Proxy Only]
- Added support for DHCP Option 42. [Allow DHCP Option 42 to override NTP server]
- Added support for Voice Frame Per TX at audio settings. [Voice Frame Per TX]
- Added support of separated webUI credentials for GDSManager. [GDSManager Configuration Password]
- Added support for G.729 audio codec. [Technical Specifications] [Preferred Vocoder]
- Added ability to enable multiple audio codecs simultaneously and specify priority of codecs. [Preferred Vocoder]
- Added support for randomize firmware upgrade and provisioning. [Upgrade]

### **Firmware Version 1.0.0.41**

- Added support for second door control via Alarm Output 1. [Using Alarm Out (COM 1) to Control a Second Door]
- Added support for “Normal Open” or “Normal Close” setting when Alarm Out1 is set to Open Door. [ALMOUT1 Status]
- Added option to specify digital input to be normal Open or normal Close. [Digit Input 1 Status]
- Added support for using Digit Only as Private PIN. [Local PIN Type]
- 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 disable WEB/SSH access. [Access Settings]
- Added option for calling out automatically without pressing #. [No Key Input Timeout(s)]
- Added option to disable SIP dialing from GDS keypad. [Disable Keypad SIP Number Dialing]
- Added option to set Schedule for “Local PIN to Open Door”. [Local PIN to Open Door Schedule]
- Added option to customize DTMF Payload. [DTMF Payload Type]
- Added RTCP/RTCP-XR for SIP Call. [Technical Specifications] [Enable RTCP]
- Added Boot version information into System status. [System Info]
- Enhanced security by only allowing numbers existing under “White List” to open the door remotely when call is initiated from GDS3705. [Remote PIN to Open the Door]
- Added option to synchronize Keep Door Open from GDSManager version 1.0.1.1 or later. [Central Mode]



### **Firmware Version 1.0.0.37**

- Added event log showing the users (Username) opening door via private PIN [Event Log]
- Added SIP NOTIFY to factory reset [Allow Reset Via SIP NOTIFY] [Restore to Factory Default Via SIP NOTIFY]
- Added option to disable outbound proxy route header [Outbound Proxy Mode]
- Added option to verify received SIP Message [Validate Incoming Messages]

### **Firmware Version 1.0.0.36**

- Added support for special character "@" in the SIP User ID. [SIP User ID]
- Added SIP password hided and not visible in the Web UI. [Password]
- Extended VLAN range from 0-4094. [Layer 2 QoS 802.1Q/VLAN Tag]
- Added ability to configure device with custom certificate signed by custom CA certificate [Certificates]
- Added option to display device temperature in Fahrenheit. [System Temperature]

### **Firmware Version 1.0.0.35**

- 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]
- Added support for Parallel Hunting when doorbell pressed. [Door Bell Call Mode]
- Added firmware check status button. [Firmware Status]
- Added Account section. [Account]
- Enhanced Event Notification Template Variables. [Event Notification]
- Added Random Port option. [Use Random Port]
- Added NAT Traversal option. [NAT Traversal]
- Added Doorbell Call Out Account. [Doorbell Call Out Account]
- Add ability to set schedule for Alarm IN door opening. [Input Digit]
- Added Account Status section. [Account Status]

### **Firmware Version 1.0.0.31**

- Added "Enabled but Not Forced; Enabled and Forced" under SRTP Configuration. [Enable SRTP]

### **Firmware Version 1.0.0.28**

- Added alarm notification of non-scheduled access users. [Non-Scheduled Access Alarm]
- Added support for HTTP command to Open Door [Enable HTTP API Remote Open Door]
- Added Keep Door Open section. [Keep Door Open]
- Added "Test" Button for Alarm Action. [Alarm Config]





## **Firmware Version 1.0.0.26**

- Added displaying logs at device Web UI. [Event Log]
- Added ability to upload Trusted CA certificate files. [Trusted CA certificate ]
- Added option to enable/disable certificate validation. [Validate Server Certificate]
- Added Ability to configure Start/End Valid date for users. [Card Management]
- Changed password recovery email option to user settings page. [User Management]
- Added UI showing Temperature/TamperSensor/DoorControl/DI/DO in the System Info Page [System Info]
- Added Support for system events notification via HTTP. [Event Notification]
- Added Factory Functions for Audio Loopback and Certificate Verification. [Factory Functions]

## **Firmware Version 1.0.0.20**

- This is the initial version for GDS3705.



## DOCUMENT PURPOSE

This document describes the basic concept and tasks necessary to use and configure your GDS3705. And it covers the topic of connecting and configuring the GDS3705, making basic operations and the call features. Please visit <https://www.grandstream.com/support> to download the latest “GDS3705 User Manual”.

This guide covers following topics:

- [Product Overview](#)
- [Getting Started](#)
- [Getting to Know GDS3705](#)
- [GDS3705 Application Scenarios](#)
- [GDS3705 Peripheral Connections](#)
- [GDS3705 Home Web Page](#)
- [GDS3705 Settings](#)
- [Factory Reset](#)
- [Experiencing the GDS3705](#)



## WELCOME

Thank you for purchasing Grandstream GDS3705 Audio Door Access System, an innovative IP based powerful door system. The GDS3705 Audio Door Access system features industry-leading SIP/VoIP for 2-way audio to SIP phones. It contains integrated PoE, HD loudspeaker, RFID card reader, and more.

GDS3705 IP Audio Door Access System can be managed by Grandstream's free windows-based management software: GDS Manager is a client/server based software which provided RFID card management and basic reports for the door entrance. GDS3705 is ideal for entry places such as banks, hotels, schools, office buildings, retail stores and small warehouses.




## PRODUCT OVERVIEW

### Feature Highlights

The following table contains the major features of the GDS3705.

**Table 1: GDS3705 Features in a Glance**

	<ul style="list-style-type: none"> <li>• 4 SIP accounts and 4 lines.</li> <li>• Broad interoperability with most 3<sup>rd</sup> party SIP/VoIP devices and leading SIP/NGN/IMS platforms.</li> <li>• 2 Channels Input/Output alarm.</li> <li>• RS485, Wiegand (26 bits) Input and Output.</li> <li>• RFID card reader.</li> <li>• Weather proof, 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 GDS3705.

**Table 2: GDS3705 Technical Specifications**

<b>Network Protocols</b>	TCP/IP/UDP, RTP/RTCP/RTCP-XR, HTTP/HTTPS local upload and mass provisioning using TR-069 (pending), ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, NTP, STUN, TLS, SRTP.
<b>SIP/VoIP Support</b>	Broad interoperability with most 3 <sup>rd</sup> 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).
<b>Security</b>	User and administrator level access control (pending), MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
<b>Upgrade / Provisioning</b>	Firmware upgrade via HTTP/HTTPS, mass provisioning using TR-069 (Pending) or AES encrypted XML configuration file.
<b>Audio Input</b>	Integrated dual microphones.
<b>Audio Output</b>	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.
<b>Keypad / Buttons</b>	12-Metal Keys plus a Metal doorbell button.
<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>	RS485, 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>Ingress Protection</b>	Weather proof, 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; Subpart C; MPE <b>CE:</b> EN 55032; EN 50130; EN 61000-3-2; EN 61000-3-3; EN 60950-1; EN 300 330; EN 301 489-1; EN 301 489-3; EN 62311 <b>RCM:</b> AS/NZS CISPR 22/24; AS/NZS 4268; AS/NZS 60950.1 <b>IC:</b> ICES-003; RSS310



## GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and information for obtaining the best performance using the GDS3705 Audio Access Door System.

### Equipment Packaging

**Table 3: Equipment Packaging**

<ul style="list-style-type: none"> <li>• 1 x GDS3705</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> <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 RFID Card (more can be purchased from Partner/reseller)</li> <li>• 1 x Key Fob (more can be purchased from Partner/reseller)</li> <li>• 1 x Frame Back Cover</li> <li>• 1 x Quick Installation Guide</li> <li>• 1 x GPL License</li> </ul>
---	--



**Figure 1: GDS3705 Package**

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

## Description of the GDS3705

Below figures show the component of the back and front view of GDS3705 IP Audio Access Door System:

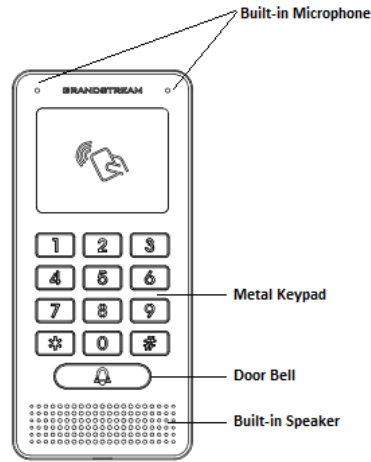


Figure 2: GDS3705 Front View

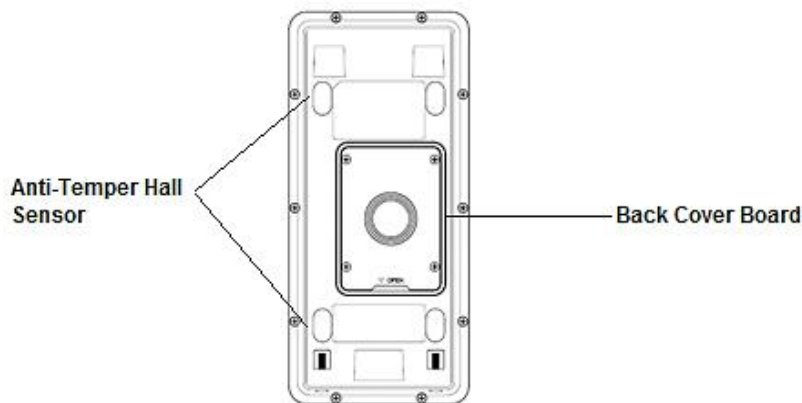


Figure 3: GDS3705 Back View

## Connecting and Setting up the GDS3705

The GDS3705 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 GDS3705.

## GDS3705 Wiring Connection

Table 4: GDS3705 Wiring Connection

Jack	Signal	Function	Note	
J2 (Basic) 3.81mm	TX+	Ethernet PoE 802.3af Class 3, 12.95W	Orange / White	Data
	TX-		Orange	
	RX+		Green / White	
	RX-		Green	
	PoE_SP2		Blue + Blue/White	Please twist these two wires together and connect to SP1, SP2 respectively even the PoE NOT used.
	PoE_SP1		Brown + Brown/White	
	RS485_B	RS485		
	RS485_A			
	GND	Power Supply	DC 12V, 1A Minimum	
	12V			
J3 (Advanced) 3.81mm	GND	Alarm GND		
	ALARM1_IN+	Alarm In	Vin<15V	
	ALARM1_IN-			
	ALARM2_IN+			
	ALARM2_IN-			
	NO1	Alarm Out	Relay: 30VDC/2A; 125VAC/0.5A	
	COM1			
	NO2	Electric Lock	For "Fail Secure" (Locked when Power Lost) Strike, connect <b>COM2 &amp; NO2</b> . For "Fail Safe" (Open when No Power) Magnetic Lock, connect <b>COM2 &amp; NC2</b> . <b>Relay: 30VDC/2A; 125VAC/0.5A</b>	
	COM2			
	NC2			
J4 (Special) 2.0mm	GND	Wiegand Power GND	Black	Both Input and Output MUST be connected
	WG_D1_OUT	Wiegand Output Signal	Orange	GDS3705 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 GDS3705 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.





## GDS3705 Back Cover Connections

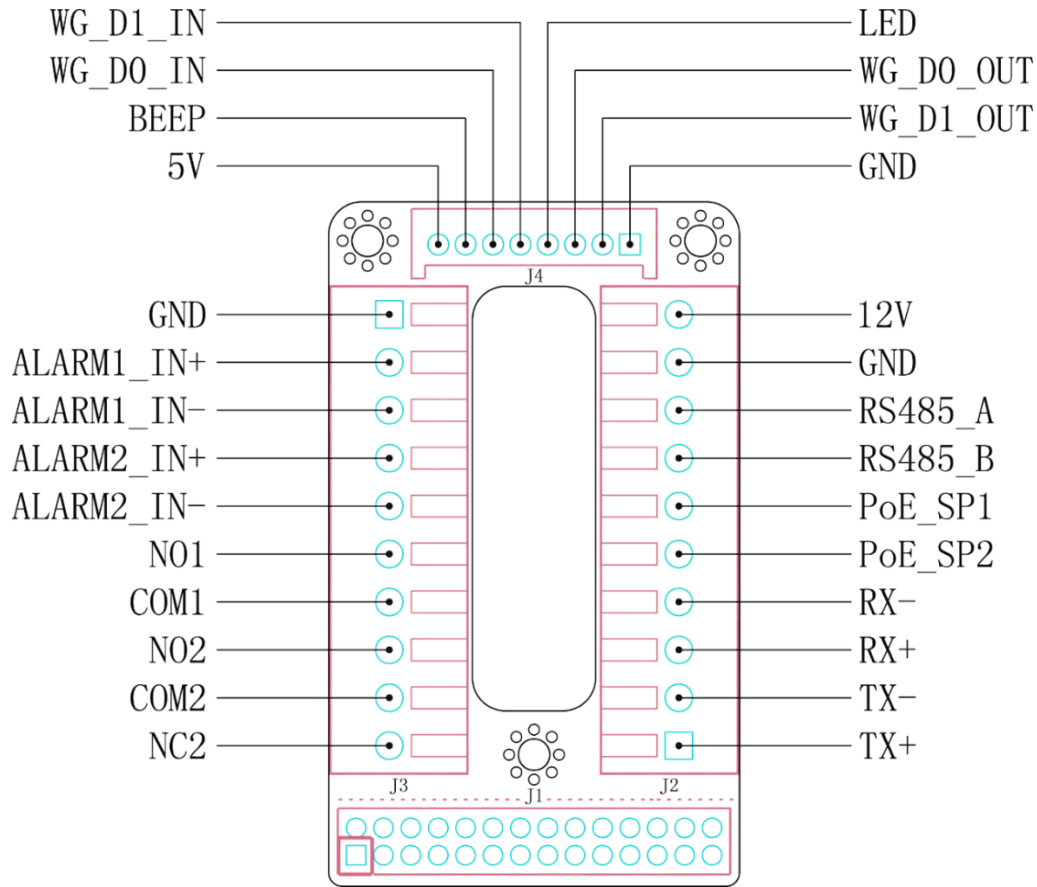


Figure 4: GDS3705 Back Cover Connections

## Connection Example

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

- Open the Back-Cover Board of the GDS3705 which should look like following figure.

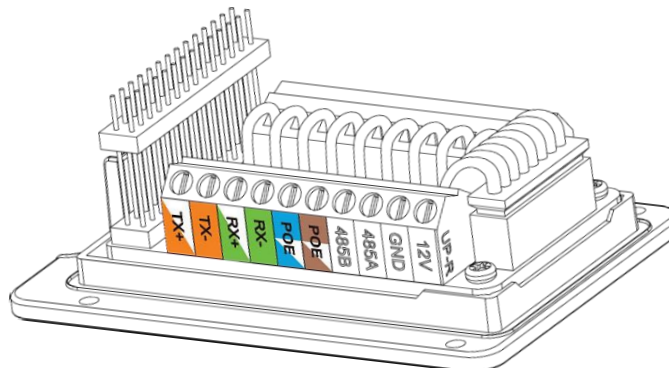


Figure 5: GDS3705 Back Cover

## Power GDS3705 using PoE

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



Figure 6: Connection Example

- Connect each wire of the cable to its associate on the Back Cover of the GDS3705 to power the unit using PoE.

## Power GDS3705 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 GDS3705 since these wires are used to power the unit via Ethernet.

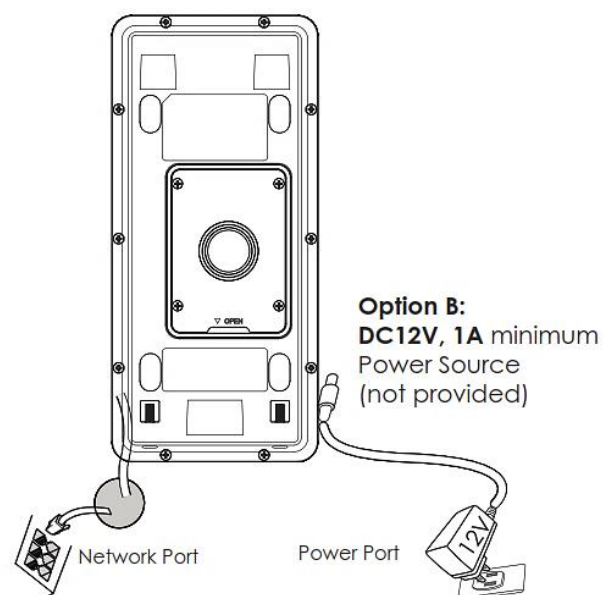


Figure 7: Powering the GDS3705

## GETTING TO KNOW GDS3705

The GDS3705 has an embedded Web server to respond to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the GDS3705 through all available Web browsers in the internet.

### Connecting GDS3705 to Network with DHCP Server

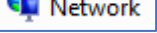
The GDS3705 by default has a DHCP client enabled, it will automatically get IP address from DHCP server.

### Windows Platform

Two ways exist for Windows users to get access to the GDS3705:

#### UPnP

By default, the GDS3705 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 GDS3705:

1. Find the “Network” icon  on the windows Desktop.
2. Click the icon to get into the “Network”, the GDS3705s will list as “Other Devices” shown like below. Refresh the pages if nothing displayed. Otherwise, the UPnP may not be active in the network.

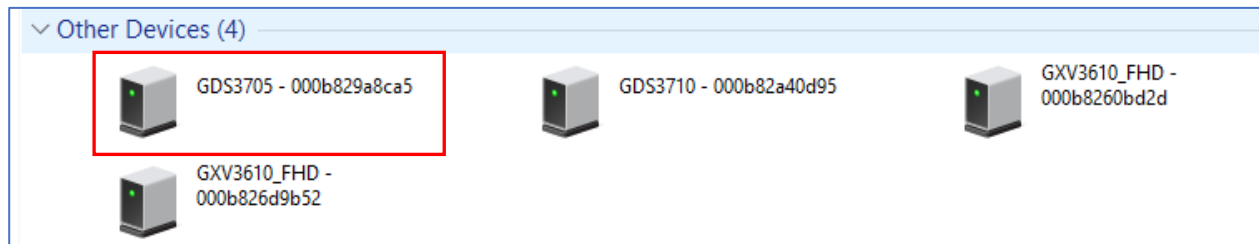
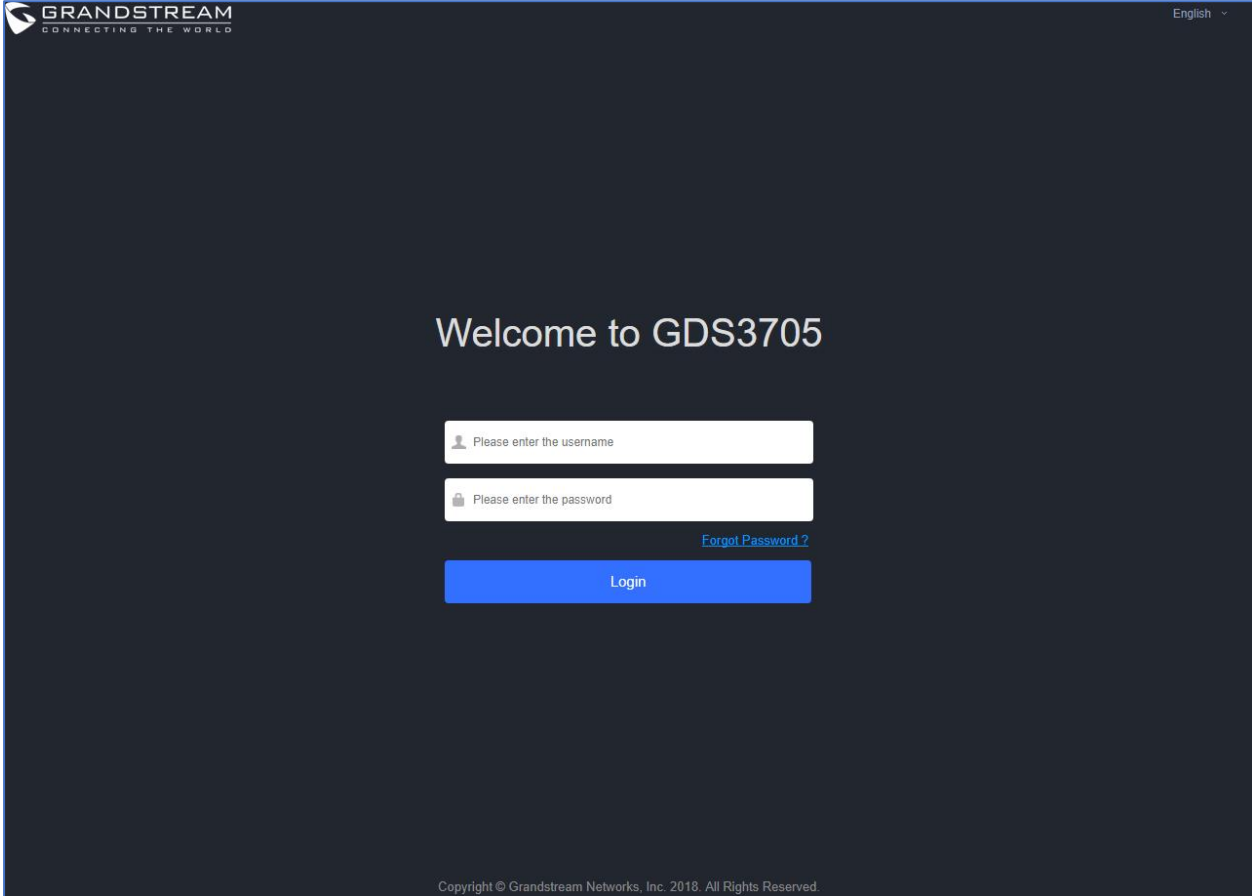


Figure 8: Detecting GDS3705 via UPnP


3. Click on the displayed icon of related GDS3705, the default browser (e.g.: Internet Explorer, Firefox or Chrome) will open and connect directly to the login webpage.

The screenshot shows the login interface for the GDS3705 device. At the top left is the Grandstream logo and tagline. At the top right is a language dropdown menu set to 'English'. The main heading is 'Welcome to GDS3705'. Below this are two input fields: the first is for the username with a user icon and the placeholder text 'Please enter the username'; the second is for the password with a lock icon and the placeholder text 'Please enter the password'. To the right of the password field is a blue link that says 'Forgot Password?'. Below the input fields is a blue 'Login' button. At the bottom of the page, there is a small copyright notice: 'Copyright © Grandstream Networks, Inc. 2018. All Rights Reserved.'

**Figure 9: GDS3705 Login Page**

## 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:  
[https://www.grandstream.com/sites/default/files/Resources/GS\\_Search.zip](https://www.grandstream.com/sites/default/files/Resources/GS_Search.zip)
- 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.

Index	Model	Version	Device Name	IP	HTTP Port	RTSP Port	MAC
1	DOORDEV GDS3705	1.0.0.20	GDS3705	192.168.5.182	443	0	00:0B:82:9A:8C:A5

Search

Add

**Figure 10: 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 GDS3705 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:  
<https://www.grandstream.com/sites/default/files/Resources/gdsmanager.zip>
2. Install and run the Grandstream GDS Manager, a client/server architecture application, the server should be running first, then GDSManager (client) later:



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

Function Navigation		<input checked="" type="checkbox"/> Search by server <input type="text"/> Search <input type="button" value="+ Add"/>						
<ul style="list-style-type: none"> <li>Basic Information</li> <li>Administrator</li> <li>Group</li> <li>Member</li> <li>Schedule</li> <li>Holiday</li> </ul>	<input type="checkbox"/> Index <input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2	Model GDS3710 GDS3705	Version 1.0.3.13 1.0.0.20	Device Name GDS3710 GDS3705	IP 192.168.5.13 192.168.5.182	Web Port 443 443	RTSP Port 554 554	Mac 00:0B:82:A4:0D:95 00:0B:82:9A:8C:A5

**Figure 11: GDS3705 Detection using GDS Manager**

- Double click the column of the detected GDS3705, the browser will automatically open and show the device's web configuration page.
- 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 GDS3705.

## Connect to the GDS3705 using Static IP

If there is no DHCP server in the network, or the GDS3705 does not get IP from DHCP server, user can connect the GDS3705 to a computer directly, using static IP to configure the GDS3705.

- The default IP, if no DHCP server, or DHCP request times out (after 3 minutes), is **192.168.1.168**
- Connect the Ethernet cable from GDS3705 to the computer network port directly.
- Configure the computer using Static IP: 192.168.1.XXX (1<XXX<255, except for 168) and configure the "Subnet mask" to "255.255.255.0". Leave the "Default Gateway" to "Blank" like below:

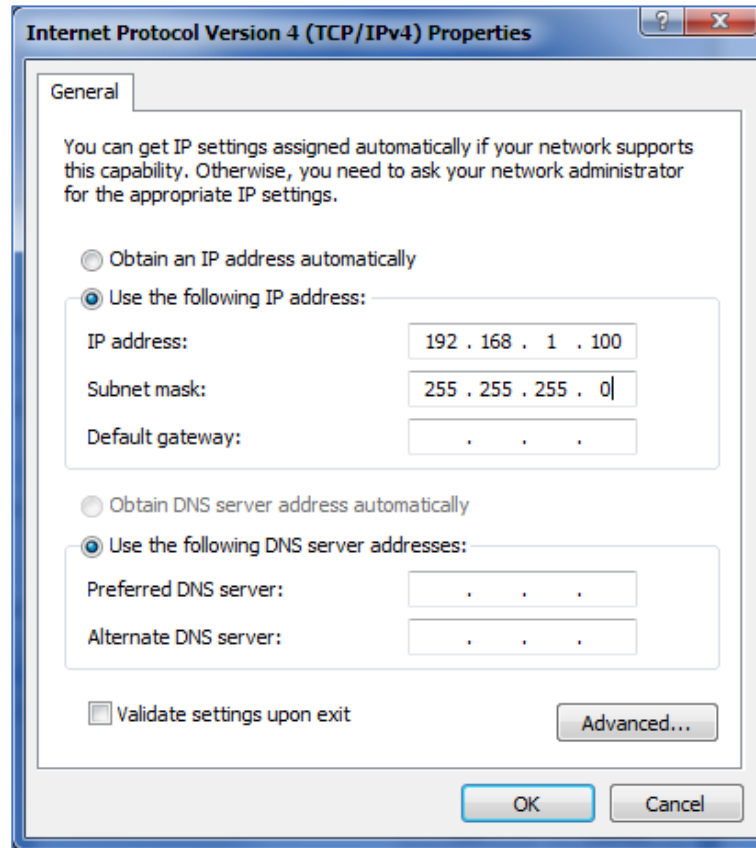


Figure 12: Static IP on Windows

4. Power on the GDS3705, 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 GDS3705.

## GDS3705 APPLICATION SCENARIOS

The GDS3705 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 audio phone GXP21XX/17XX/16XX series, the GDS3705 will meet your very basic intercom, and open-door requirements.

This is the solution to upgrade the traditional analogue Intercom system. All you need is a Power source, Switch or PoE Switch and Grandstream GXP21XX/17XX/16XX audio phones.

The equipment list can be found below:

- GDS3705
- GXP21XX/17XX/16XX
- PoE Switch with related Cat5e/Cat6 wiring

### Peering using SIP Server (UCM6XXX)

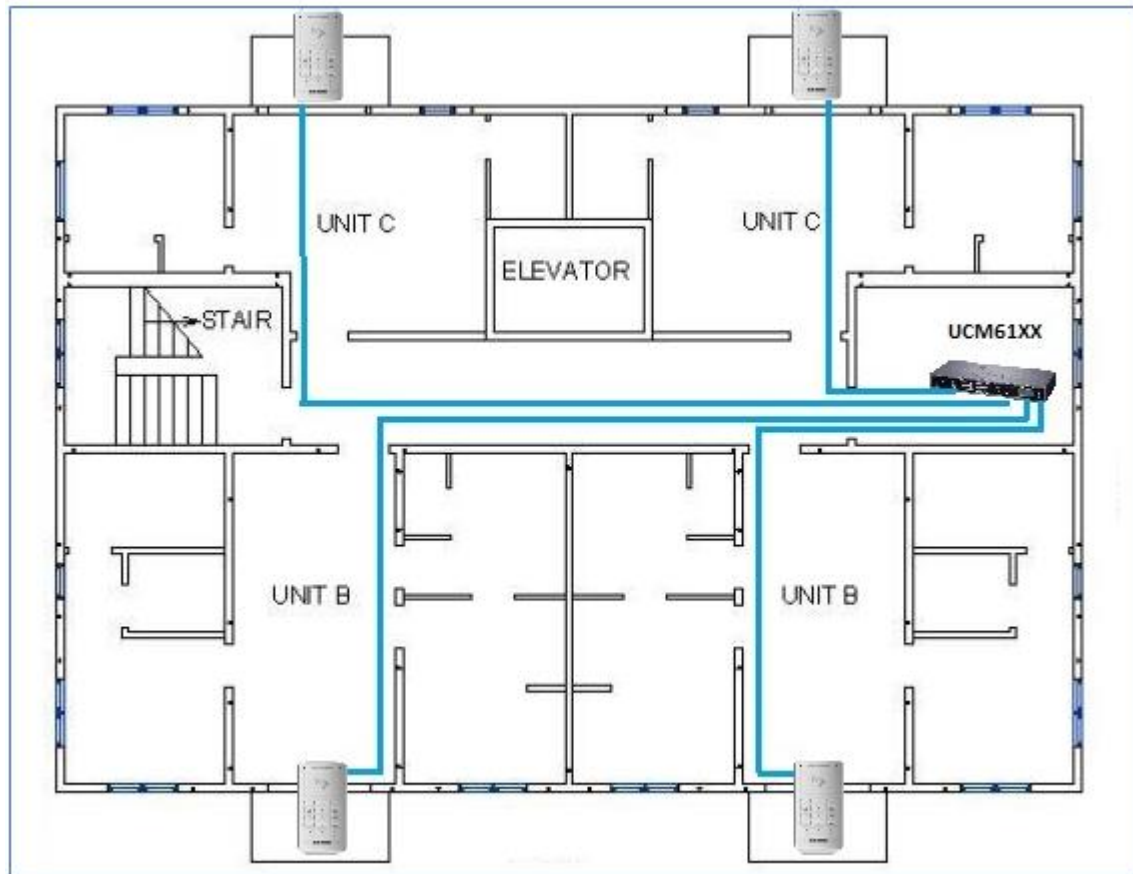
For large deployment, multiple GDS3705 units might be required, peered connection will not work in such case due to multiple connections. Such scenarios require an IPPBX or a SIP Proxy to accomplish the tasks.

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

- Several GDS3705
- UCM6XXX or another SIP Server
- GXP21XX/17XX/16XX audio Phones
- PoE Switch with related Cat5e/Cat6 wiring
- Electronic Lock







**Figure 13: Peering GDS3705 with UCM6XXX**

## GDS3705 PERIPHERAL CONNECTIONS

Below is the illustration of GDS3705 peripheral connections for related applications.



Figure 14: Peripheral Connections for GDS3705

## Alarm IN/OUT

Alarm\_In could use any 3rd party Sensors (like IR Motion Sensor).

Alarm\_Out device could use 3rd party Siren, Strobe Light, or Electric Door Striker, etc.

The figure below shows illustration of the Circuit for Alarm\_In and Alarm\_Out.

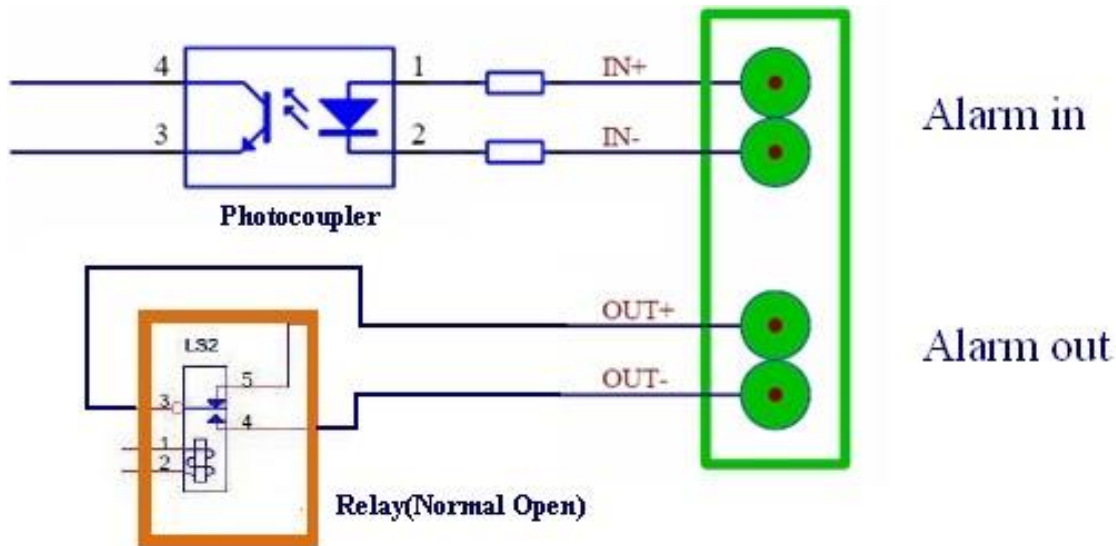


Figure 15: Alarm\_In/Out Circuit for GDS3705

### Notes:

- The Alarm\_In and Alarm\_Out circuit for the GDS3705 should meet the following requirement:

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

- The Alarm\_In circuit, if there is any voltage change between 3V and 15V, as specified in the table above, the GDS3705 Alarm\_In port will detect it and trigger the action and event.
- Higher voltage and wrong polarity connection are prohibited because this will damage the devices.

## Protection Diode

When connecting the GDS3705 to a door strike it is recommended to set an EMF protection diode in reverse polarity for a secure use, below examples of deployment for the protection diode.

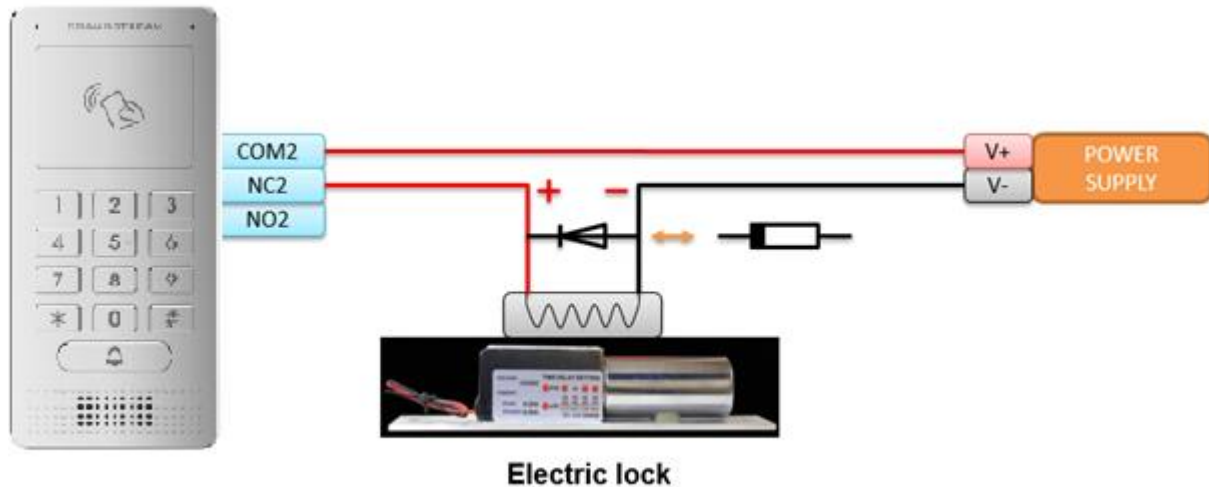


Figure 16: Protection Diode - Example 1

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

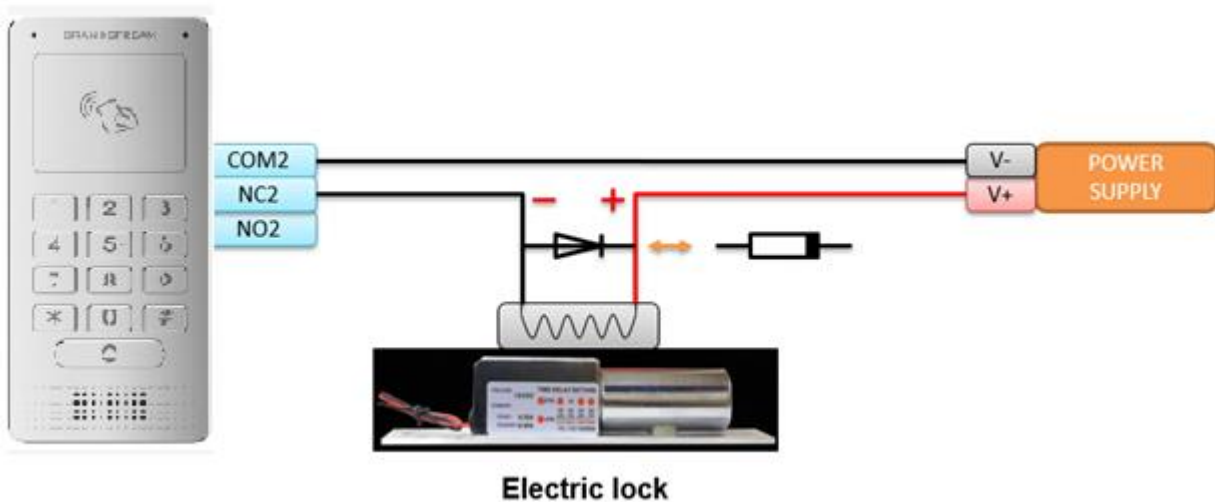


Figure 17: Protection Diode - Example 2

## Connection Examples

Below examples, show how to use wiring on the back cover of the GDS3705 to connect with external devices. The “NO” (Normal Open) model strike is used as example, “NC” (Normal Closed) should be similar and users need to decide which model (NO or NC) to be used on the door.

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

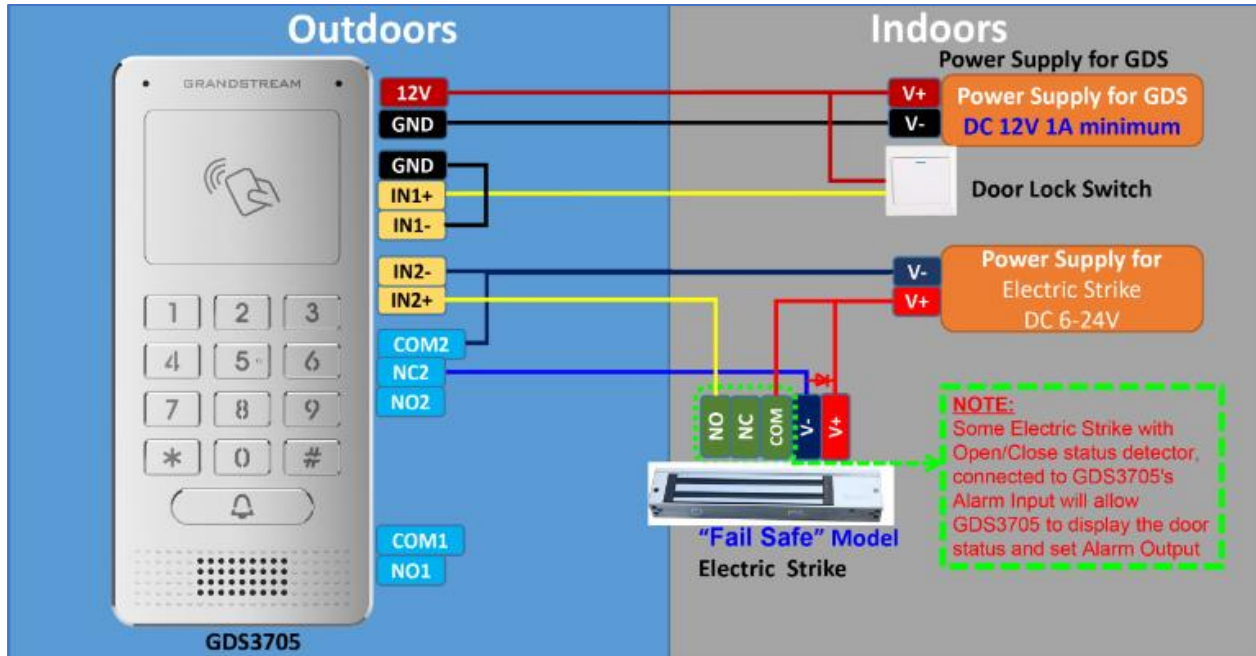


Figure 18: 3<sup>rd</sup> party Power Supply Wiring Sample

## Wiring Sample using Power Supply for both GDS3705 and Electric Strike

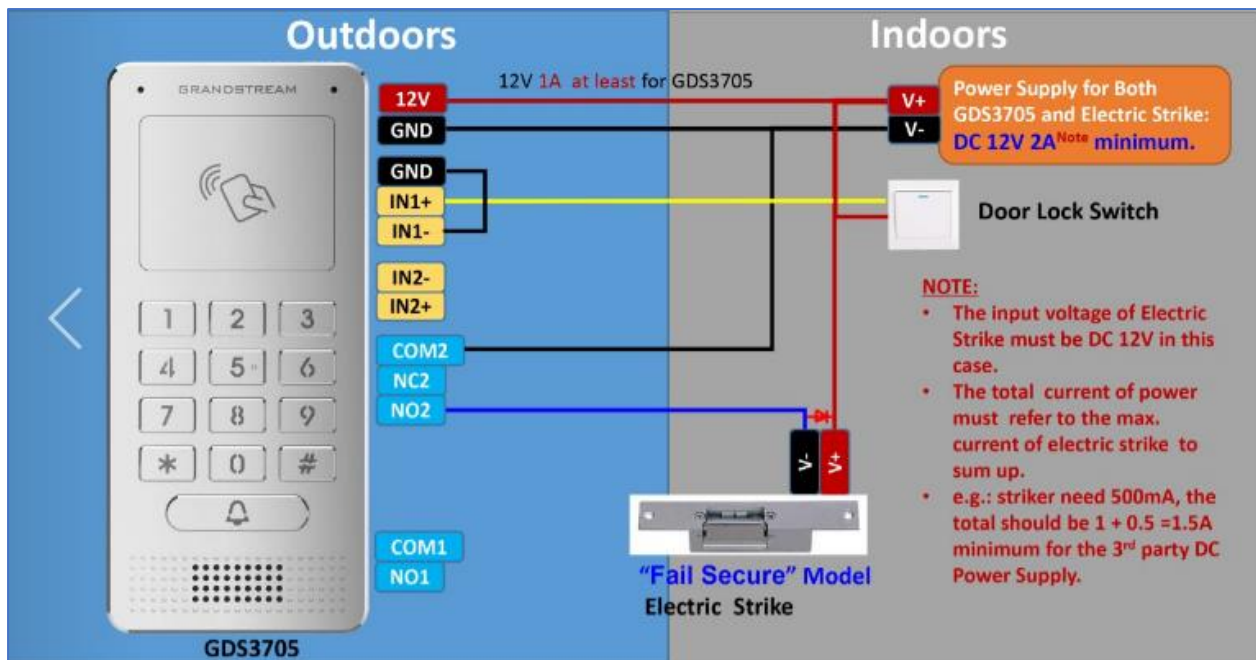


Figure 19: Power Supply used for both GDS3705 and Electric Strike

## Wiring Sample using PoE to power GDS3705 and 3<sup>rd</sup> Party Power Supply for Electric Strike

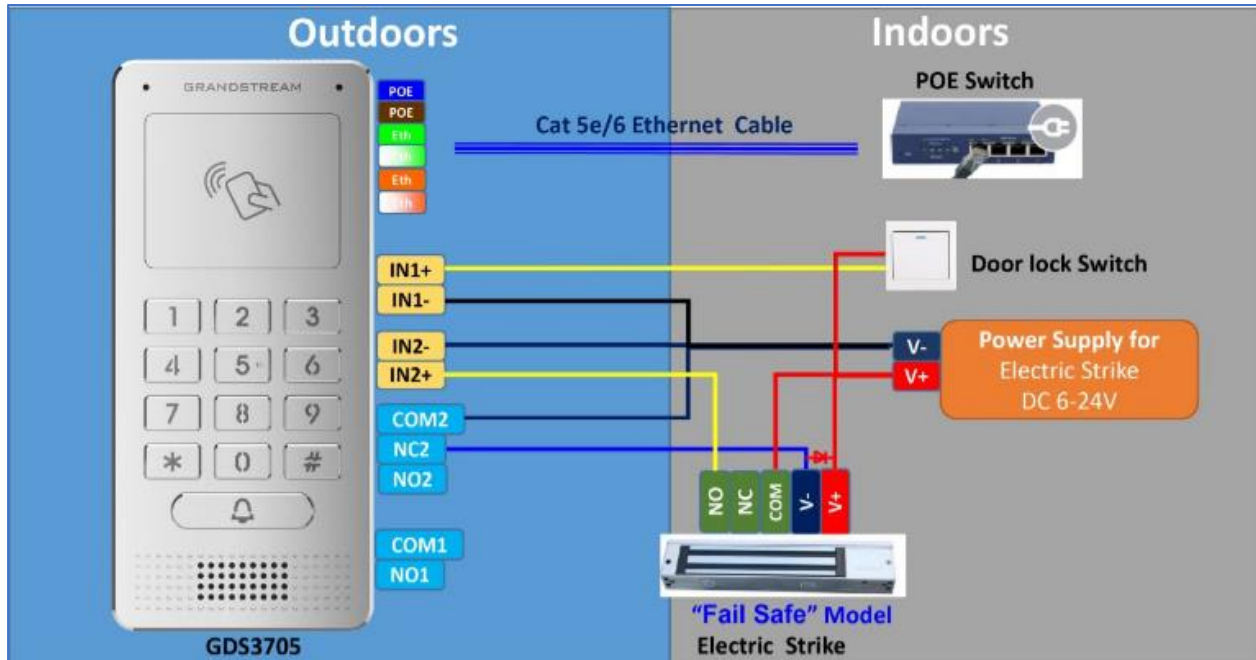


Figure 20: Wiring Sample using PoE to power GDS3705 and 3<sup>rd</sup> party Power Supply for Electric Strike

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

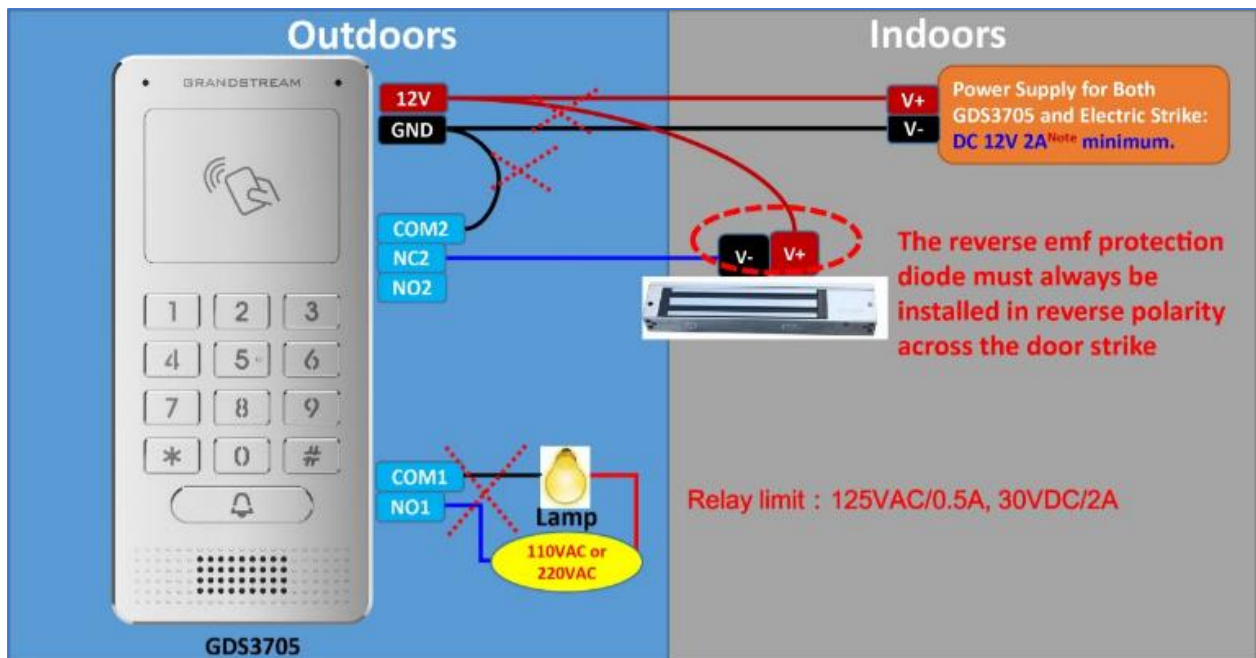


Figure 21: Example to Avoid when Powering the Electric Strike



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

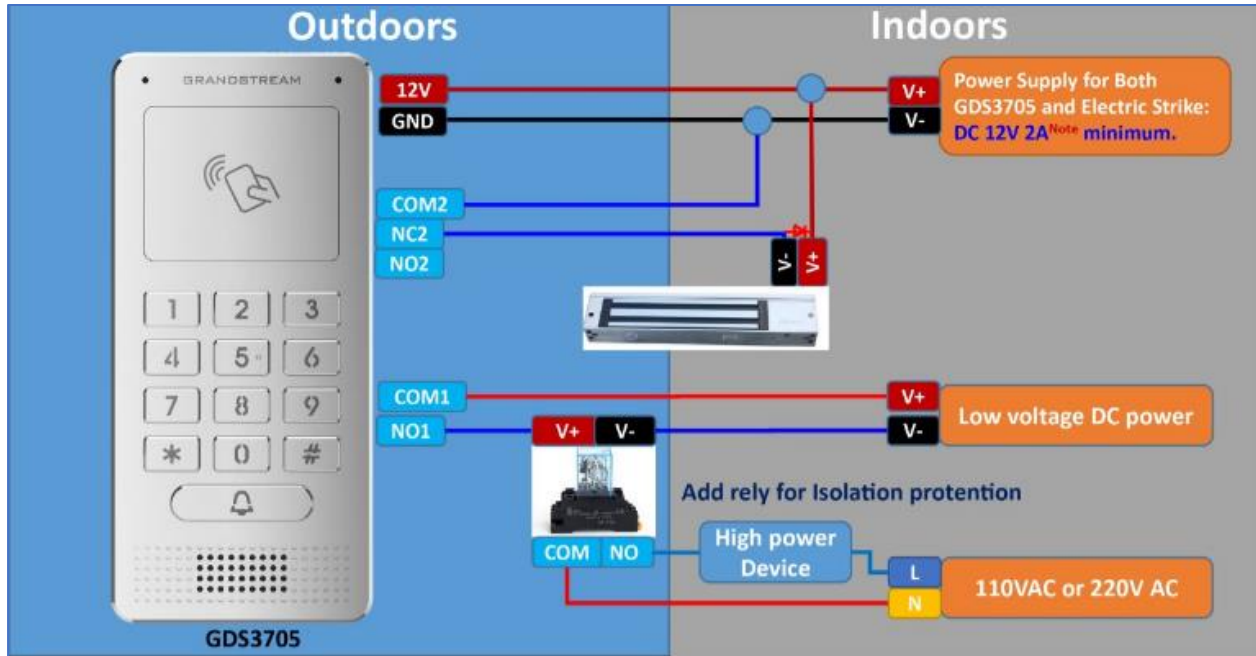


Figure 22: Electric Strike and High-Power Device Example

## Wiegand Module Wiring Examples

GDS3705 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 GDS3705.

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

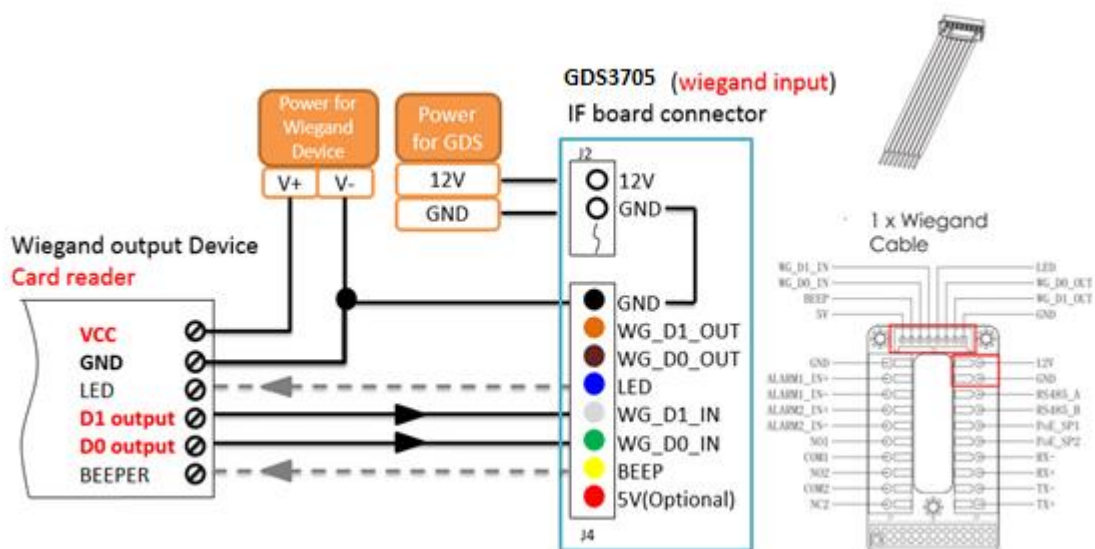


Figure 23: Wiegand Input Example with 3<sup>rd</sup> party Power Supply

Make sure to connect the GND of the Wiegand device and the GDS3705 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 GDS3705 and Wiegand device

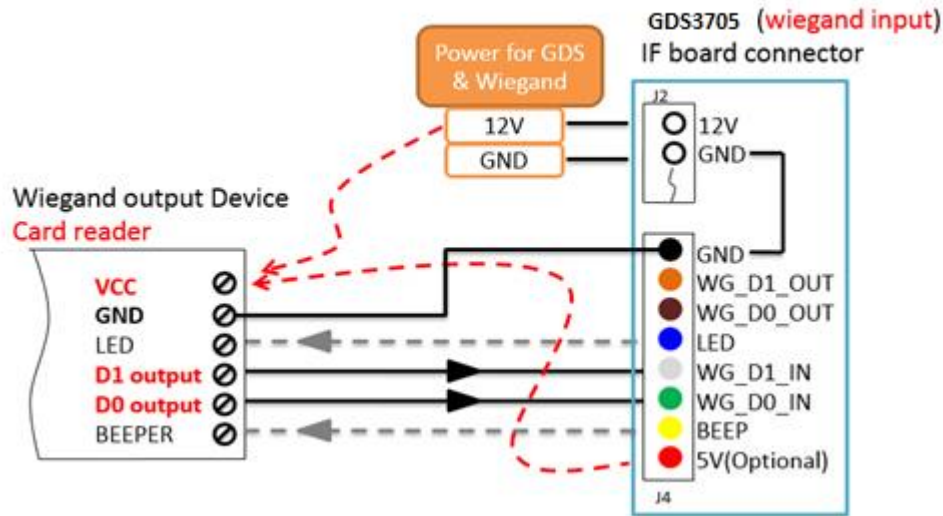


Figure 24: Wiegand Input Example with Power Supply for GDS3705 and Wiegand Device

If power source is **12VDC**, Wiegand device can share same power source of GDS3705. However, users need to check the max power consumption and the max capability of the power source.

If Wiegand device is using **5VDC**, GDS3705 Wiegand port can provide 5VDC with max 500mA to power up Wiegand device.



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

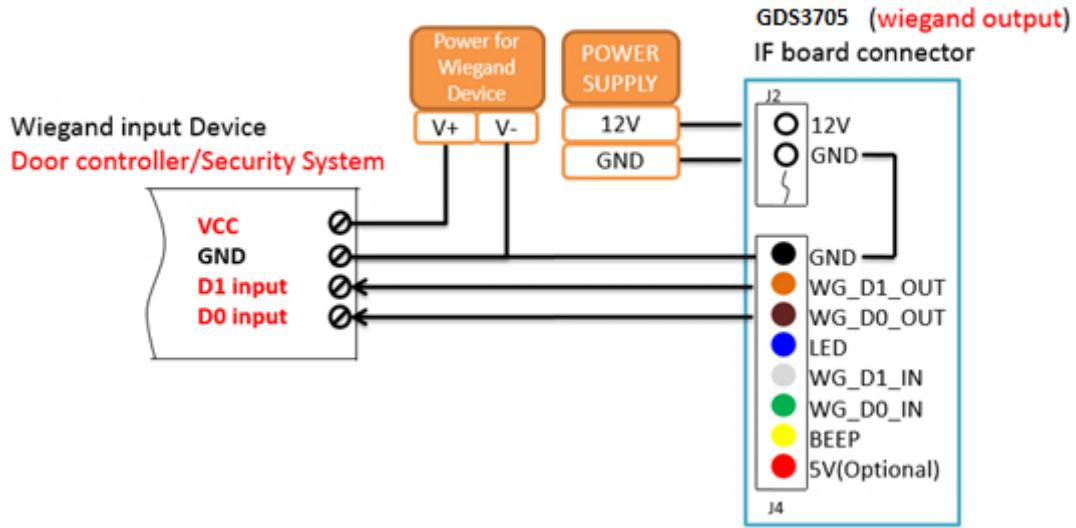


Figure 25: Wiegand Output Wiring Example

When the Wiegand output of the GDS3705 is connected, it acts as the signal receiver of the 3<sup>rd</sup> party Wiegand device, connecting to door controller. The major wiring is GND, D0, and D1. Because usually the door controller will consume big current and power, the power supply should be separated.

## Wiegand RFID Card Reader Example

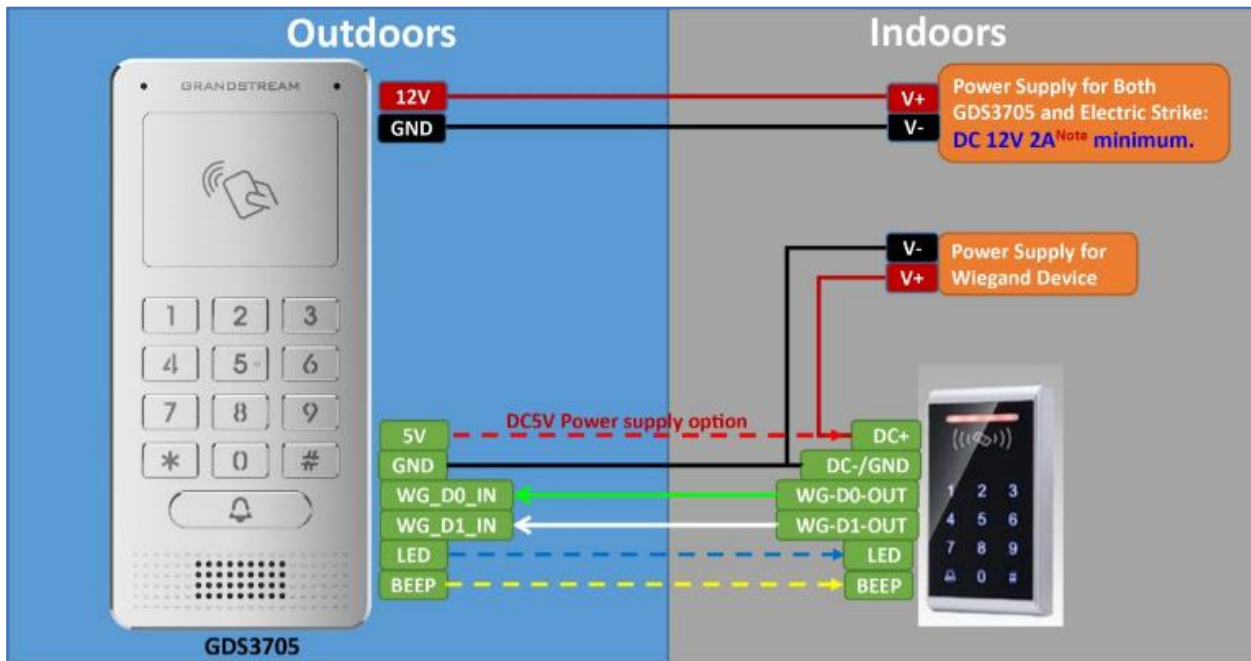


Figure 26: Wiegand RFID Card Reader Example

## Siren alarming when door opened abnormally

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

There are several ways to stop and disable the alarm:

- 1) Power cycle the GDS3705
- 2) Pick up the Alarm Phone Call (if configured)
- 3) Open Door using PIN (either public PIN or private PIN)

Once alarm triggered, the GDS3705 will play siren sound, send email to administrator (if configured SMTP); 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.

### GDS3705 Connection: IN2 set as Normal Close and “Fail Safe” Electric Strike using 3<sup>rd</sup> Party Power Supply

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

Figure 27: Digital Input set as Normal close

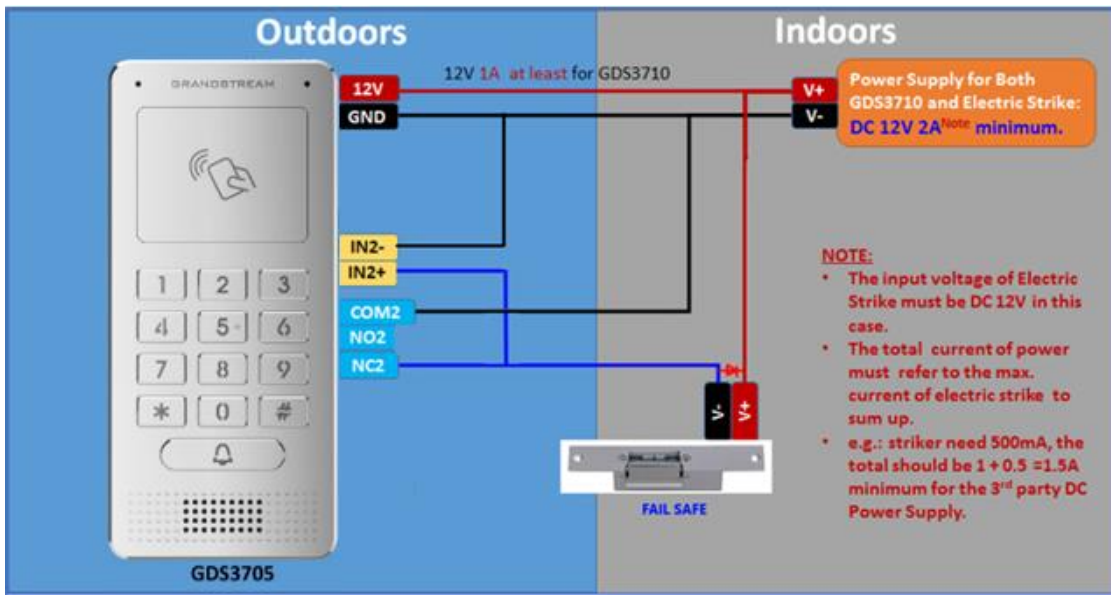


Figure 28: "Fail safe" Electric Strike using 3rd Party Power Supply

### GDS3705 Connection: IN2 set as Normal Open and "Fail Secure" Electric Strike using 3rd Party Power Supply

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

Figure 29: Digital Input set as Normal open

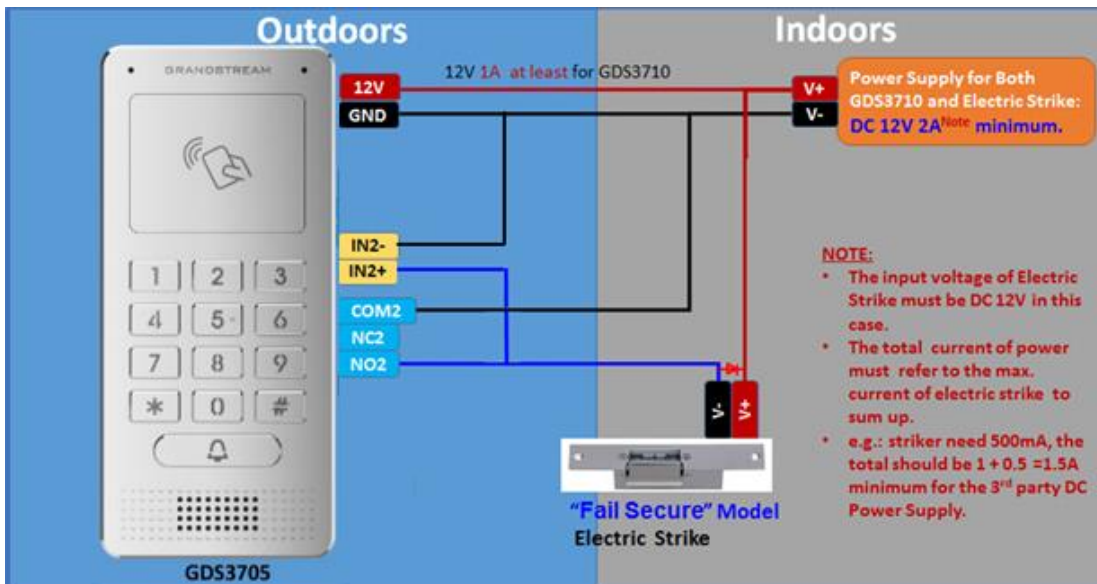


Figure 30: "Fail Secure" Electric Strike using 3rd Party Power Supply

## Open Door via GDS3705 with or without a SIP Call

This feature needs related matching GDS3705 firmware to work. The minimum firmware version needed:

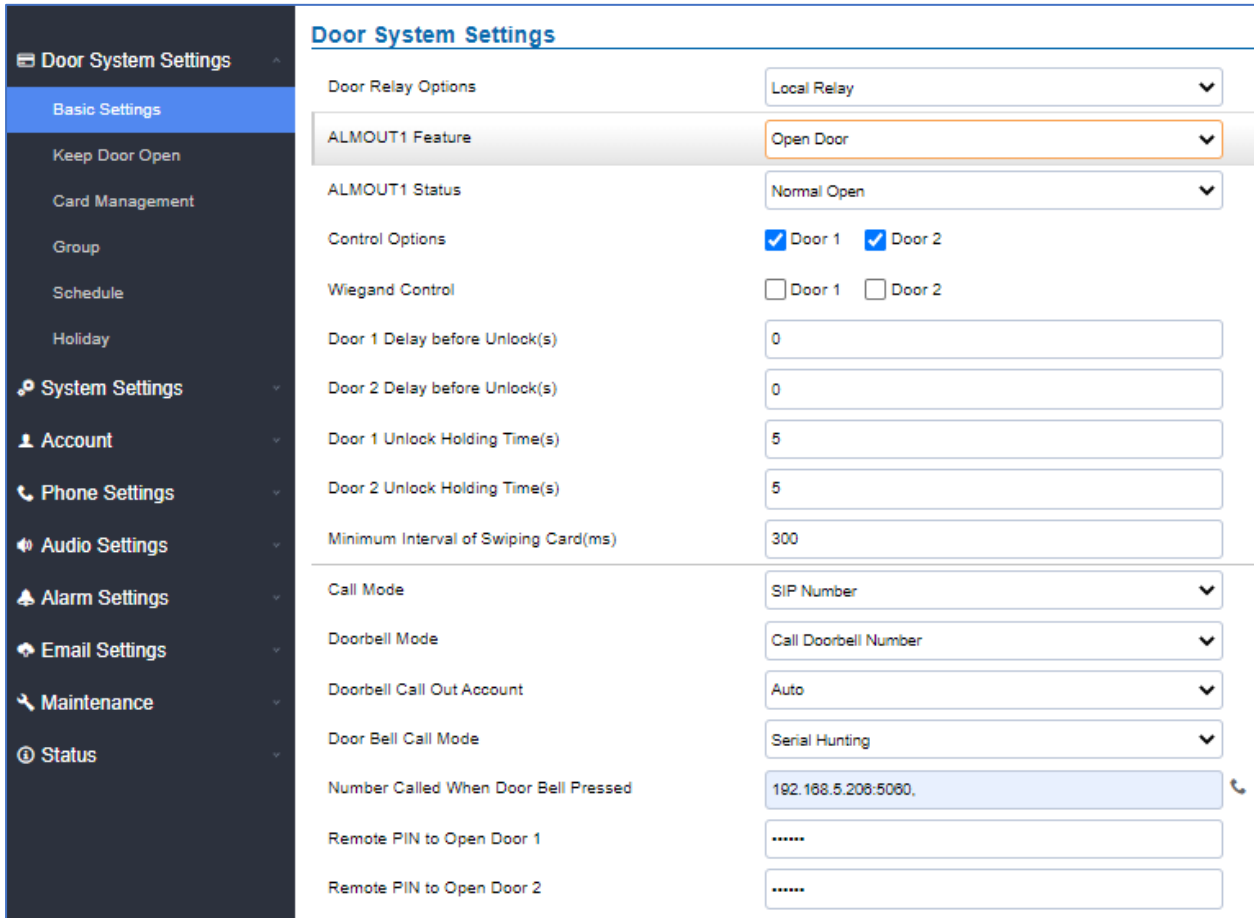
- **GDS3705: 1.0.1.16 or higher.**

From GDS3705 side, the configuration is the same. Only difference is the number of doors to be controlled:

If using Local Relay controlled by GDS3705, 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.

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



Door System Settings	
Door Relay Options	Local Relay
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 type="checkbox"/> Door 1 <input 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
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	192.168.5.208:5080
Remote PIN to Open Door 1	*****
Remote PIN to Open Door 2	*****

Figure 31: GDS3705 Configuration Example

Settings

Grandstream Door System

	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
External Service	1	GDS	Account 1	GDS3705	192.168.5.225	192.168.5.225	Door1	***	Door2	***
	2	GDS	Account 1							
Digital Output	3	GDS	Account 1							
	4	GDS	Account 1							
Alarm	5	GDS	Account 1							
	6	GDS	Account 1							
SOS	7	GDS	Account 1							
	8	GDS	Account 1							
IPC	9	GDS	Account 1							
	10	GDS	Account 1							

Save

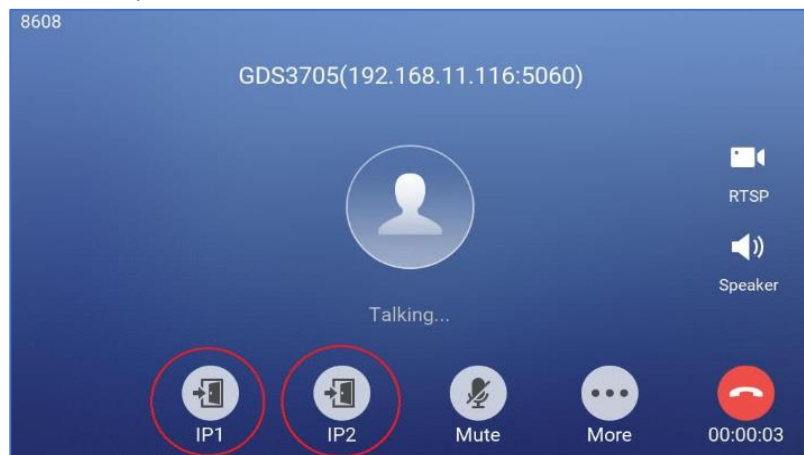
Save and Apply

Reset

**Figure 32: GSC3570 Configuration Example**

## Door opening with SIP Call

When GSC3570 established call with GDS3705, the screen will display virtual open door button(s), and user will press the button to open door:



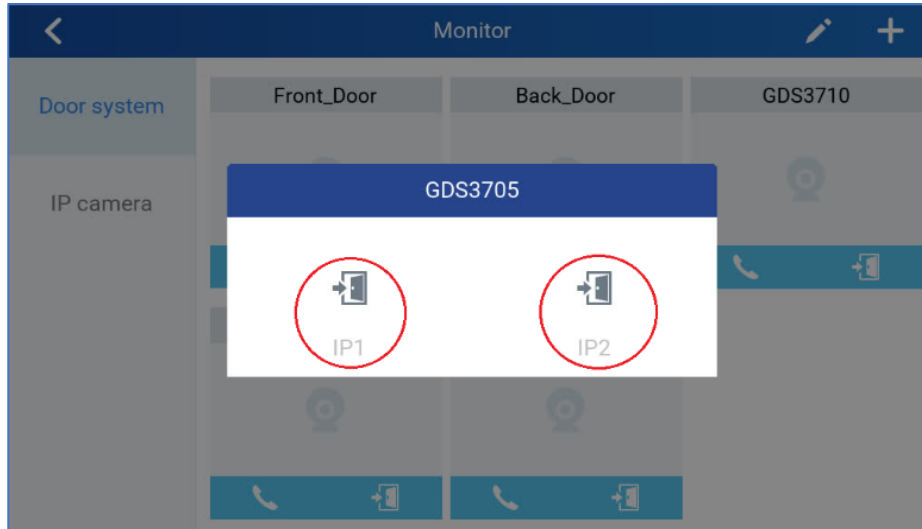
**Figure 33: Open Door with SIP Call**

## Door opening without SIP Call

At the GSC3570 idle screen, press “Monitor → Door system”, the related GDS305 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:



**Figure 34: Open Door without SIP Call**

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



**Figure 35: Open Door without SIP Call**

## Secure Open Door via GDS3705/GSC3570 Peering

This secure open door feature needs to include GSC3570 to make it a whole solution. The GDS3705/GSC3570 will be peering together in LAN/WAN via IP/SIP, the door lock/strike will be wired to GSC3570Alarm\_Out port and controlled by GSC3570. This way the strike control is inside the building with enhanced security. Below is a setup example:

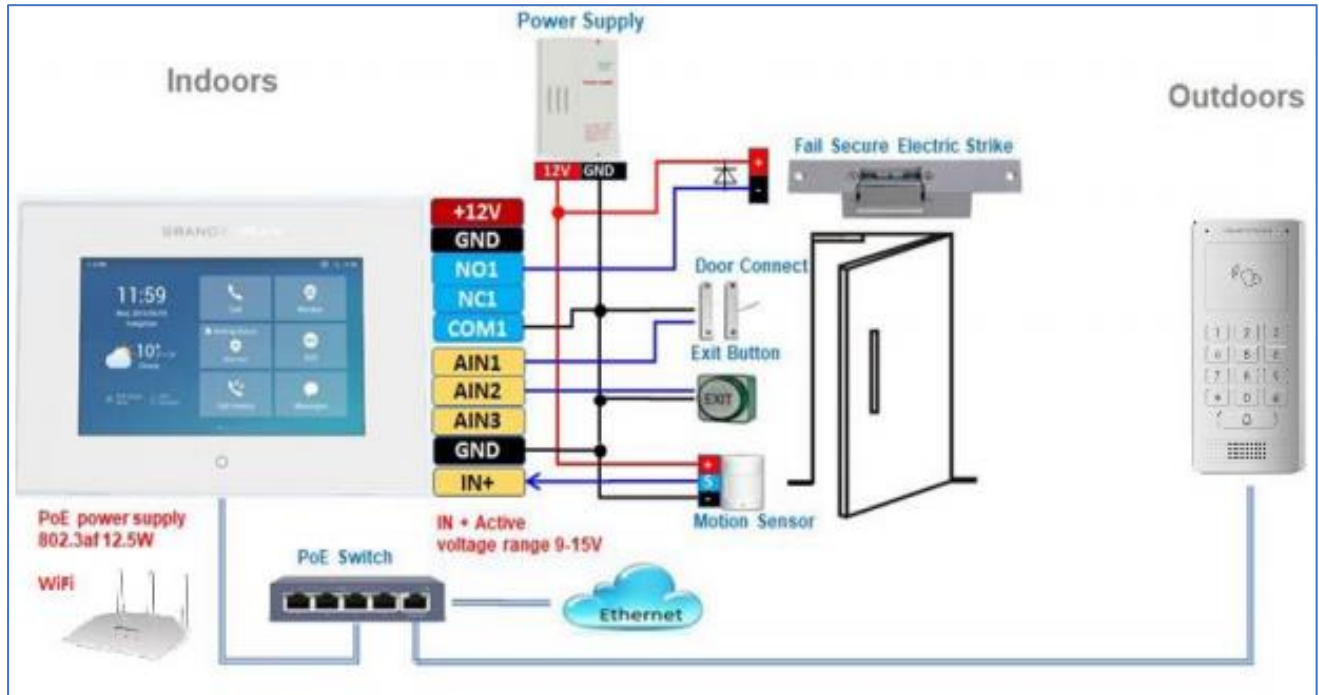


Figure 36: GSC3570 secure open door via GDS3705

**Note:** Minimum firmware required for this to work:

- Outdoor Device: GDS3705 firmware 1.0.1.116 and higher.
- Indoor Device: GSC3570 firmware 1.0.5.9 and higher.

For “Secure Open Door”, the GSC3570 is pairing with GDS3705. The GSC3570 controlling the relay/strike/lock from inside the building (Unlike GDS3705 installed outside), but only ONE door can be controlled because GSC3570 only has one Relay Control circuit build in. This pairing can be via LAN/WAN but LAN is recommended and actually most of the application scene are in LAN environment because most likely the GSC3570 and GDS37xx are in the same building.

For the GSC3570 and GDS37xx pairing, it can be used via SIP only (Cloud or UCM); IP only (No SIP proxy or UCM but static IP address) and Mixed (SIP and fallback to IP if Proxy failed).

### **GDS3705 Web Configuration**

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



**Door System Settings**

Basic Settings

Keep Door Open

Card Management

Group

### Door System Settings

Door Relay Options

GSC3570 Relay ▼

Open Door Account to Choose

Account 1 ▼

GSC3570 Phone Number

192.168.5.163

GSC3570 Door Password

\*\*\*\*\*

Figure 37: GDS3505 Web GUI configuration for secure open door with GSC3570

### GSC3570 Web Configuration

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

Grandstream Door System								
Settings	Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password
External Service	1	GDS ▼	Account 1 ▼	Front_Door	873		Front_Door	
	2	GDS ▼	Account 1 ▼	Back_Door	877		Back_Door	
Digital Output	3	GDS ▼	Account 1 ▼					
Alarm	4	GDS ▼	Account 1 ▼	GDS3705	8606	192.168.11.118	IP1	
	5	Other ▼	Account 1 ▼	GSC3620	192.168.11.203	192.168.11.203		

Figure 38: GSC3570 Web GUI configuration for secure open with GDS3705

### Notes:

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



## GDS3705 HOME WEB PAGE

- Once the IP address of the GDS3705 is entered on the user browser, the login web page will pop up allowing user to configure the GDS3705 parameters.
- When clicking on the “Language” drop down, supported languages will be displayed as shown in Figure below. Click to select the related webpage display language.

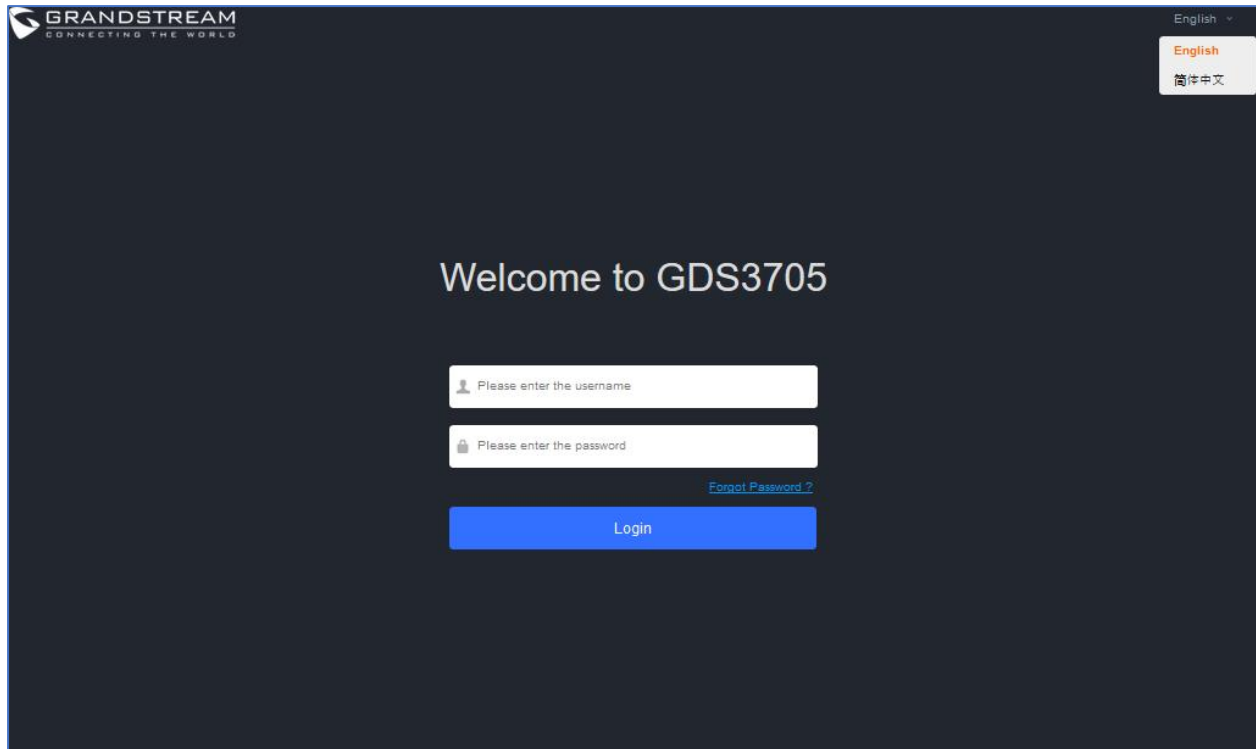


Figure 39: Change Language Page

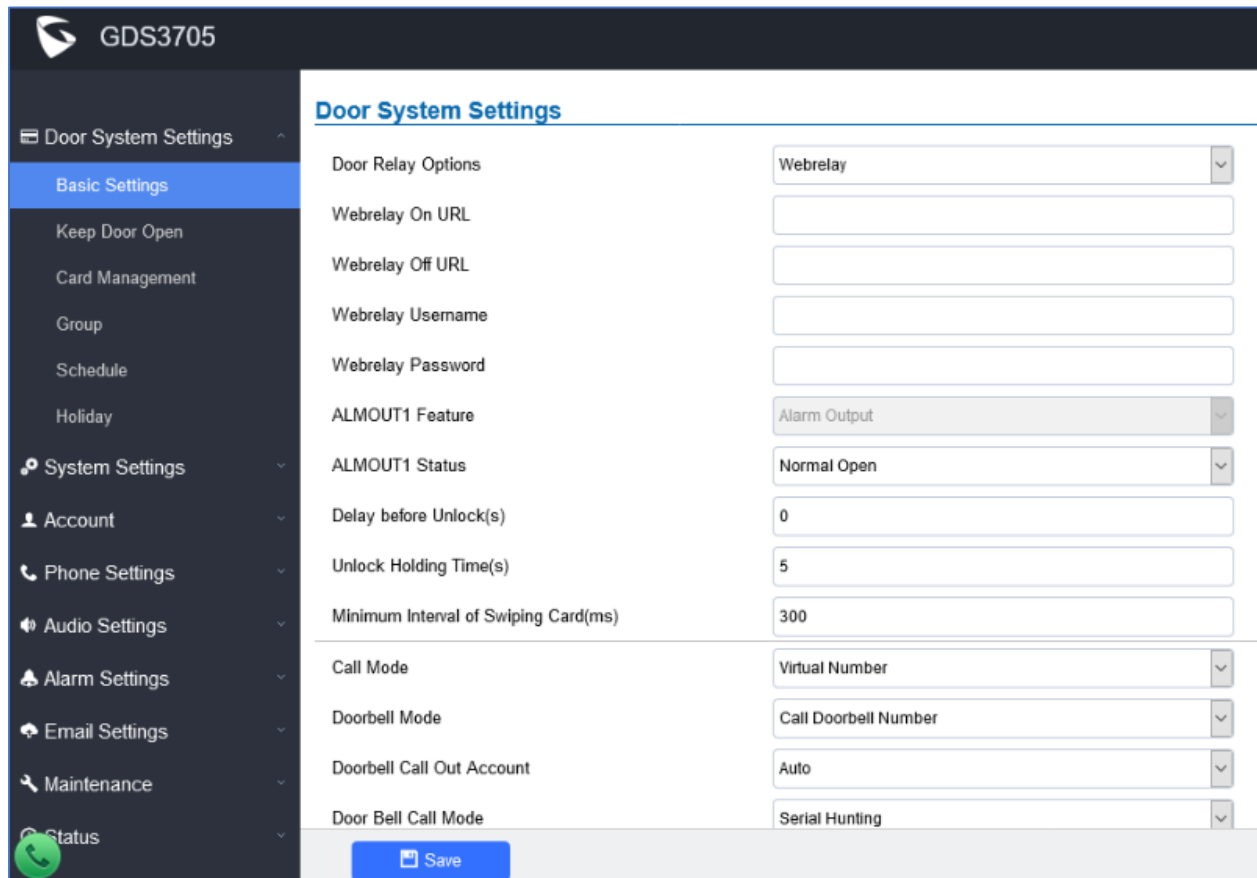
**Note:** Current firmware supports only English (default) and simplified Chinese.

# GDS3705 SETTINGS

## Door System Settings

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

### Basic Settings



Door System Settings	
Door Relay Options	Webrelay
Webrelay On URL	
Webrelay Off URL	
Webrelay Username	
Webrelay Password	
ALMOUT1 Feature	Alarm Output
ALMOUT1 Status	Normal Open
Delay before Unlock(s)	0
Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Call Mode	Virtual Number
Doorbell Mode	Call Doorbell Number
Doorbell Call Out Account	Auto
Door Bell Call Mode	Serial Hunting

[Save](#)

Figure 40: Door System Settings Page

**Table 5: Door System Settings**

<b>Door Relay Options</b>	<p>There are two choices in the pull-down selection: Local Relay and Webrelay.</p> <ul style="list-style-type: none"> <li>• <b>Local Relay:</b> Local Relay is the GDS3705 controlling the relay. The strike is wired into the COM2 or COM1 port of the GDS3705 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 GDS3705, and will operate the strike to open door for the authenticated open door request.</li> </ul> <p><b>Note:</b> In web relay mode, the strike is wired to the web relay controller device.</p> <p>For more details, please refer to the Webrelay documentation from this link: <a href="#">webrelay user manual</a></p>
<b>Webrelay URL ON</b>	<p>When Door relay Option set to Webrelay, then enter the correct URL used by the third party controller so that the GDS3705 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 GDS3705, 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 3<sup>rd</sup> party 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 3rd party controller so that the GDS3705 send the command to disable the relay.</p>
<b>Webrelay Username</b>	<p>Enter the web relay username.</p>



<b>Webrelay Password</b>	Enter the web relay password.
<b>ALMOUT1 Feature</b>	<p>This option allows to choose to use Alarm_Out (COM1) interface for either as alarm out with 3<sup>rd</sup> party device, or to control a second door “Door 2” (the two functions are mutual exclusive).</p> <p>When option “<b>Open Door</b>” is selected, will enable GDS3705 to control the operation of two doors via RFID, local and remote PINs.</p>
<b>ALMOUT1 Status</b>	Select Normal Open or Normal Close depending on the lock used.
<b>Delay before Unlock (s)</b>	Device will open door after specified delay (in seconds) when user issuing the authorization.
<b>Unlock Holding Time (s)</b>	<p>Configures the lock holding time, in seconds (default value is 5 seconds). Device will hold the door unlocked for this specified duration.</p> <p>Range: 1-1800 seconds.</p>
<b>Minimum Interval of Swiping Card (ms)</b>	Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms. Default 300 ms.
<b>Call Mode</b>	Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3705 keypad.
<b>Doorbell Mode</b>	<p>Configures the action to be taken when the doorbell is pressed, three options are available:</p> <ul style="list-style-type: none"> <li>• <b>Call Doorbell Number:</b> when Doorbell is pressed, a call will be made to the “<b>Number Called When Door Bell Pressed</b>”.</li> </ul> <p><i>*This option will be the only available when ALMOUT1 Feature is set to Open Door.</i></p> <ul style="list-style-type: none"> <li>• <b>Control Doorbell Output (Digital Output 1):</b> when Door Bell is pressed electronic lock for Output 1 is opened.</li> <li>• <b>Both of Above:</b> When selected, both Call Doorbell Number and Control Doorbell Output options are enabled.</li> </ul>
<b>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>Door Bell Call Mode</b>	<p>Select the ring strategy for the Numbers Called when pressing the Door Bell button to be either <b>Serial</b> or <b>Parallel</b>:</p> <ul style="list-style-type: none"> <li>• <b>Serial Hunting:</b> the configured extensions and/or IP addresses will ring one after one by order.</li> </ul>



	<ul style="list-style-type: none"> <li>• <b>Parallel Hunting:</b> The configured extensions and/or IP addresses will ring simultaneously (up to 4 simultaneous SIP calls).</li> </ul>
<b>Number Called When Door Bell Pressed</b>	<p>Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed:</p> <ul style="list-style-type: none"> <li>• <b>SIP Server mode:</b> <ul style="list-style-type: none"> <li>- The field can be configured to store multiple one or multiple SIP extensions, if configured with multiple extensions (ex: 1001, 1002, 1003), separated with “,” the GDS3705 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, 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 GDS3705 will ring the configured IP Addresses in <b>Serial or Parallel Mode</b> according to Doorbell Call Mode strategy.</li> </ul> </li> </ul> <p><b>Note:</b> This field supports a Maximum of 256 characters.</p>
<b>Remote PIN to Open the Door</b>	<p>Configures PIN code stored in the GDS3705, remote SIP phone needs to input and match this PIN (the PIN is sent via DTMF while in call) so that the GDS3705 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>



<b>Maximum Number of Dialed Digits</b>	Configure the maximum digits allowed to dial in the keypad. Once the configured condition satisfied, the device will send out the digit to call automatically without pressing #. Disabled if set to 0.
<b>No Key Input Timeout(s)</b>	Defines the timeout (in seconds) for no key entry. If no key is pressed after the timeout, the digits will be sent out without pressing #. The default value is 4 seconds. The valid range is from 1 to 15.
<b>Press Doorbell Schedule</b>	Configure a schedule for the Doorbell button, once configured, the doorbell will turn ON/OFF based on configured schedule. Default setting is "All Day".
<b>Local PIN Type</b>	<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 GDS3705 to open the door [<b>*Virtual Number*Private PIN#</b>].</li> </ul> <p><u>Notes:</u></p> <ol style="list-style-type: none"> <li>1. When Local PIN type is set to <b>private PIN</b>, users can also open the door by swiping their cards.</li> <li>2. If "Disable Keypad SIP Number Dialing" is checked, users will be able to open door using private PIN with following sequence [<b>Private PIN#</b>].</li> </ol> <p><b>Note:</b> Door can still be opened by <b>Card</b> and with the sequence [<b>*Virtual Number*Private PIN#</b>].</p> <p>For more details and conditions, refer to [<i>Disable Keypad SIP Number Dialing</i>].</p> <ul style="list-style-type: none"> <li>• <b>Unified PIN:</b> Means all members share a same PIN to unlock the door. Users need to enter the following sequence from the GDS3705 keypad to open the door [<b>*Local PIN to Open Door#</b>].</li> <li>• <b>Card &amp; Private PIN:</b> Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence [<b>Swipe the card + * Private PIN#</b>]</li> </ul>



<b>Local PIN to Open Door</b>	<p>Configures PIN stored in GDS3705, input locally this PIN on the GDS3705 keypad will unlock the door.</p> <p>This feature needs <b>Private PIN</b>, means every member has a private PIN, the GDS will record who unlocked the door every time.</p> <p>Users need to enter the following sequence from the GDS3705 to open the door [<b>*Virtual Number*Private PIN#</b>].</p> <p><b>Note:</b> When local PIN type is set to private card PIN, users can also open the door by swiping their cards.</p>
<b>Local PIN to Open Door Schedule</b>	<p>Configure a schedule for the Local PIN to open the door for “Unified PIN” mode only. Once configured, the door opening ability using local PIN with turn ON/OFF based on configured schedule. The schedule can ONLY be edited when “Central Mode” disabled.</p> <p><b>Notes:</b> If “Central Mode” enabled, the “Schedule” page cannot be edited. (a green “Central Model” label will display in top right corner of the UI).</p> <p>When “Central Mode” enabled, the “Schedule” will be edited in GDSManager and synchronized by pulling from GDSManager down to GDS3705 device.</p> <p>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>	Enables password entry for guests.
<b>Guest PIN</b>	Configures the password that will be used by guests.
<b>Guest PIN Start Time</b>	Selects the start time when the Guest PIN start to take effect.
<b>Guest PIN End Time</b>	Selects the end time when the Guest PIN will stop working.
<b>Disable Auto Answer</b>	<p>If checked, GDS3705 will not answer incoming calls automatically, users can press any key to answer the call.</p> <p>Default setting in unchecked.</p>
<b>Enable Doorbell Button to Hang up Call</b>	If checked, Users can hang up an active call when pressing the doorbell button. Enabled by default.
<b>Disable Keypad (except the Doorbell Button)</b>	When checked the Keypad will be disabled, only Door Bell button can be pressed.
<b>Enable On Hook After Remote Door Opened</b>	When checked calls will be disconnected automatically 5 seconds after the remote open door event.



<b>Enable HTTP API Remote Open Door</b>	<p>Enabling this option allows to use HTTP API command to open the door remotely.</p> <p><b>Important note:</b> We will not be responsible for any security problems resulting from opening the HTTP API remote function, this option is disabled by default and the user should enable it while knowing how to mitigate the risk.</p>
<b>Disable Keypad SIP Number Dialing</b>	<p>When Keypad SIP number Dialing disabled, device will interpret each digit entry as private-password open door request after pressing #.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• “Local PIN Type” should choose “Private PIN”.</li> <li>• Dial keypad to make SIP call will NOT work (except for doorbell button call).</li> <li>• Private PIN must be <b>UNIQUE</b> among users, otherwise the door will still open but log will NOT tell who opened the door due to duplicated PIN and whoever user last matched in the database with the Private PIN will be shown in the log.</li> </ul>
<b>Enable Card Issuing Mode</b>	<p>Enables RFID card issuing/program into the GDS3705. When selected sweeping an RFID card into the GDS3705 will add card information into. [Card Management]</p>
<b>Card issuing State Expire Time(m)</b>	<p>Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes).</p>
<b>Enable Key Blue Light</b>	<p>When checked, the blue light will be activated when pressing the GDS3705 Keys.</p>
<b>Enable Doorbell Blue Light</b>	<p>When enabled, Keypad LED will light based on the configured Start/End Time. For instance, this option can be used when GDS is deployed on dark environment, the GDS will be located easily using Keypad LED.</p>
<b>Enable Keypad Blue Light</b>	<p>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.</p>
<b>Central Mode</b>	<p>If enabled, Group/Schedule/Holiday/Keep Door Open, can only be synchronized from the Central (GDS Manager), local configuration will not be allowed.</p> <p>If disabled, only local configuration from GDS3705 is allowed.</p>





<b>Key Tone Type</b>	Configures the key tones for the GDS3705. <ul style="list-style-type: none"> <li>• <b>Default:</b> Beeps will be played when pressing the GDS3705 keys.</li> <li>• <b>DTMF:</b> Tones will be played when pressing the GDS3705 keys.</li> <li>• <b>Mute:</b> No sound will be played when pressing keys.</li> </ul>
<b>Enable Wiegand Input</b>	This option needs to be enabled when GDS is connected to the wiegand. output device (RFID card reader for example)
<b>Wiegand Output</b>	This option is to be enabled when the GDS is the wiegand output device. (example: input device is a door controller)

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

GDS3705 support RFID for multiple users to open door, therefore every user has its own PIN. For environment with 100 users and more, it's difficult for the GDS3705 to manage all these users and a separate PC or Server should be involved for such kind of management and monitoring.

In environments with more than 100 users the GDS3705, 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 1.0.0.41, 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 GDS3705 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 GDS3705 can be installed at Door2 with related cable wired into the control GDS3705 installed at Door1. The Door1 and Door2 can be configured to be open by programmed RFID cards, PINs either separately or both.

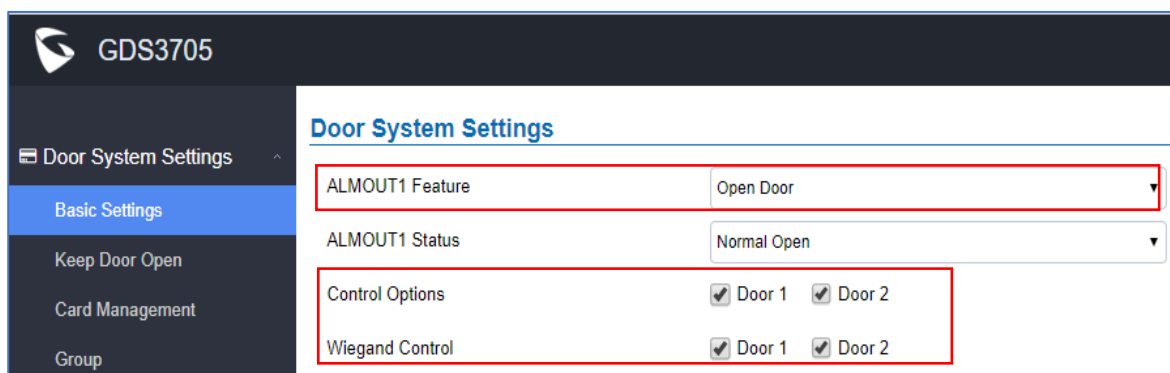


Figure 41: Alarm\_Out1 Feature

- **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.

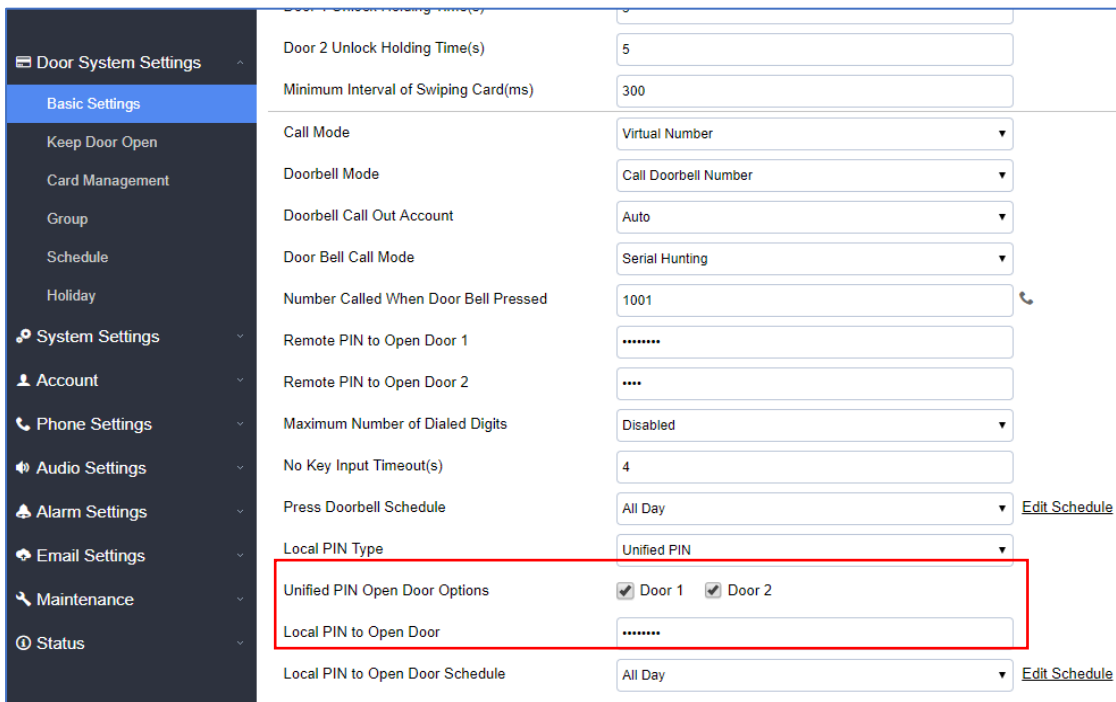
Unlike default COM2 which is designed for strike control and having three connecting sockets, the COM1 only has two connecting sockets. Therefore correct lock mode has to be configured to make the strike working as expected.

For above example, the GDS3705 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. Therefor 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:**



<b>Door System Settings</b>	Door 2 Unlock Holding Time(s)	5
<b>Basic Settings</b>	Minimum Interval of Swiping Card(ms)	300
Keep Door Open	Call Mode	Virtual Number
Card Management	Doorbell Mode	Call Doorbell Number
Group	Doorbell Call Out Account	Auto
Schedule	Door Bell Call Mode	Serial Hunting
Holiday	Number Called When Door Bell Pressed	1001
<b>System Settings</b>	Remote PIN to Open Door 1	*****
<b>Account</b>	Remote PIN to Open Door 2	****
<b>Phone Settings</b>	Maximum Number of Dialed Digits	Disabled
<b>Audio Settings</b>	No Key Input Timeout(s)	4
<b>Alarm Settings</b>	Press Doorbell Schedule	All Day <a href="#">Edit Schedule</a>
<b>Email Settings</b>	Local PIN Type	Unified PIN
<b>Maintenance</b>	Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
<b>Status</b>	Local PIN to Open Door	*****
	Local PIN to Open Door Schedule	All Day <a href="#">Edit Schedule</a>

**Figure 42: Universal Local PIN**

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

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

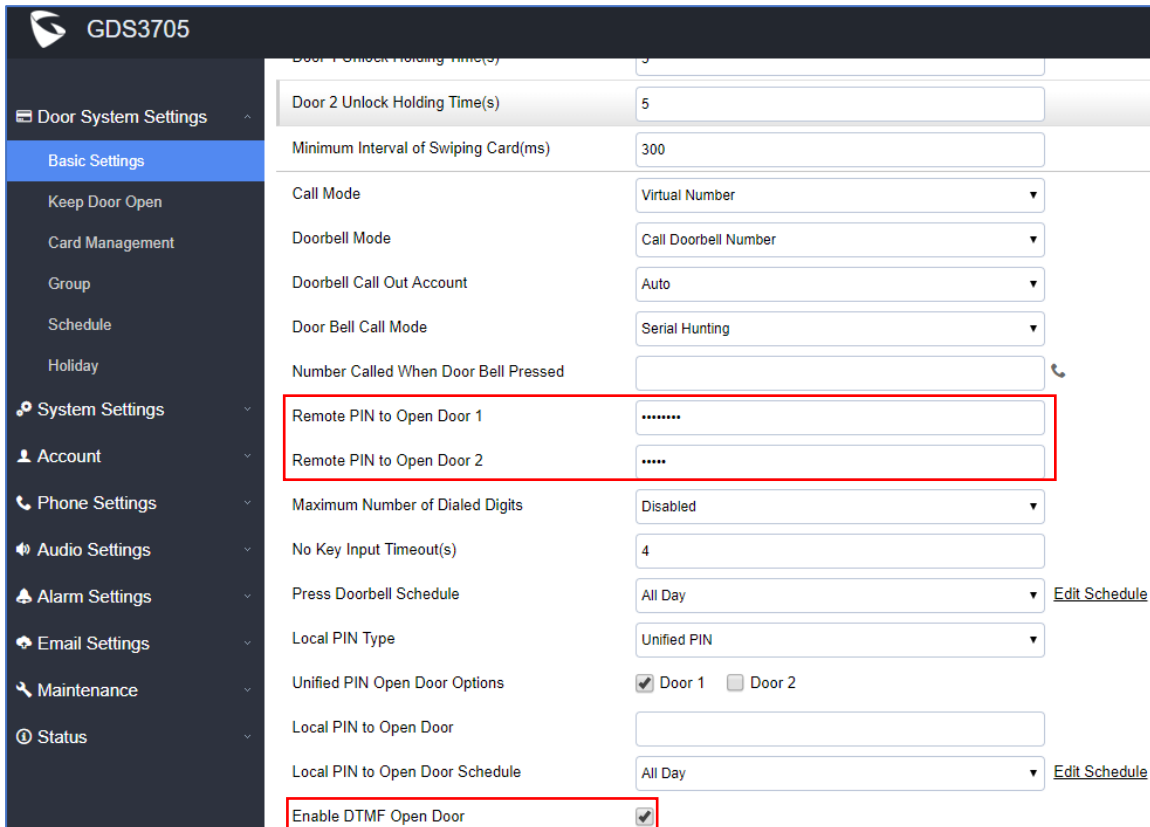
- **Remote PIN to Operation of Doors:**

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

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

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

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



GDS3705	
Door 1 Unlock Holding Time(s)	5
Door 2 Unlock Holding Time(s)	5
Minimum Interval of Swiping Card(ms)	300
Call Mode	Virtual Number
Doorbell Mode	Call Doorbell Number
Doorbell Call Out Account	Auto
Door Bell Call Mode	Serial Hunting
Number Called When Door Bell Pressed	
Remote PIN to Open Door 1	*****
Remote PIN to Open Door 2	*****
Maximum Number of Dialed Digits	Disabled
No Key Input Timeout(s)	4
Press Doorbell Schedule	All Day <a href="#">Edit Schedule</a>
Local PIN Type	Unified PIN
Unified PIN Open Door Options	<input checked="" type="checkbox"/> Door 1 <input type="checkbox"/> Door 2
Local PIN to Open Door	
Local PIN to Open Door Schedule	All Day <a href="#">Edit Schedule</a>
Enable DTMF Open Door	<input checked="" type="checkbox"/>

**Figure 43: Remote PIN to Open Door**

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

← Add Card Info

Username\*

John Snow

Private PIN

...

Gender

Male ▼


ID Number

123


Card Number\*

89978456

Valid Start Date

1970-01-01 

Valid End Date

2099-12-31 

Virtual Number\*

1

Sip Number

1001

Call Out Account

Auto ▼

Cellphone

561545020

Group

Disabled ▼

Schedule

Disabled ▼

Right of Card and Private PIN

☒ Door 1
 ☒ Door 2

Enable

☒

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

**Figure 44: Right of Card and Private PIN**

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

**Notes:**

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

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

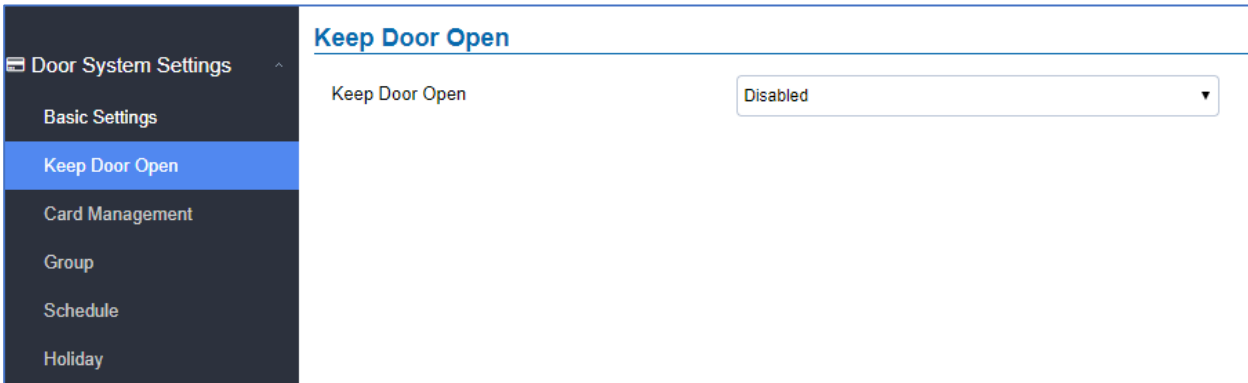


Figure 45: Keep Door Open

There are two modes under this section:

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

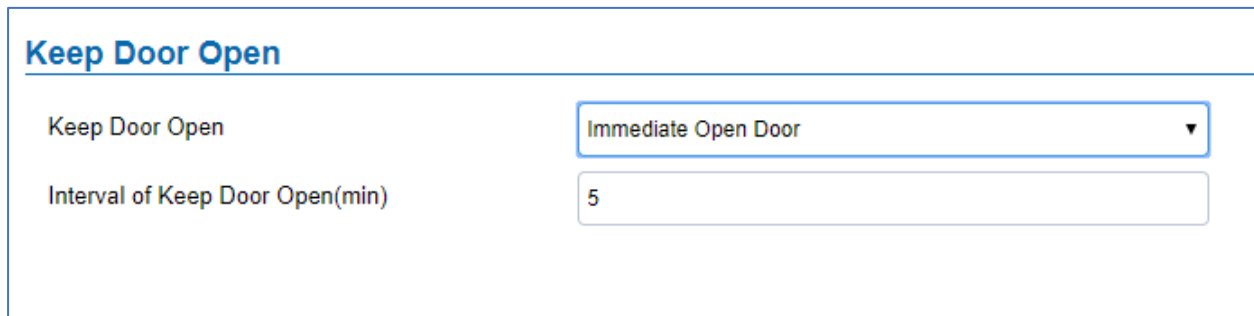
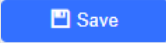


Figure 46: Immediate Door Open

Table 6: Immediate Door-Open Table

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

### 2- Schedule Open Door (Repeated Action)



**Keep Door Open**

**Door 1**

Keep Door Open Schedule Open Door

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

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

Holiday Mode holiday1 [Edit Holiday](#)

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

**Door 2**

Keep Door Open Disabled

Emergency PIN to Disable Keep Door Open

**Figure 47: Schedule Door Open**

**Table 7: Schedule Keep Door Open**

<b>Keep Door Open</b>	Select the Keep Door Open mode.
<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>Holiday Mode</b>	Users can specify which Holiday Schedule to be included into the Keep Door Open schedule

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

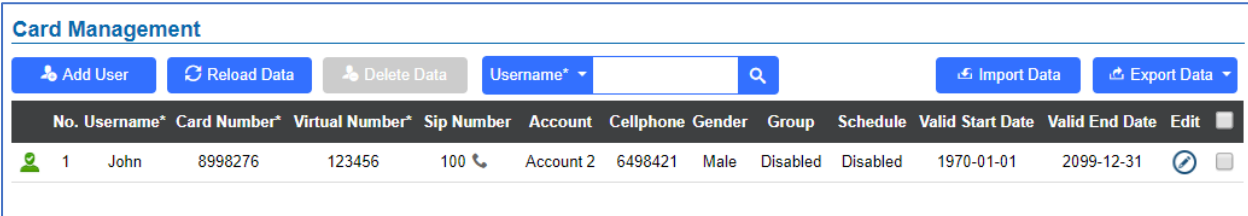
Save Cancel

**Figure 48: Modify Schedule**



## Card Management

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





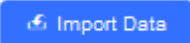


No.	Username*	Card Number*	Virtual Number*	Sip Number	Account	Cellphone	Gender	Group	Schedule	Valid Start Date	Valid End Date	Edit
1	John	8998276	123456	100	Account 2	6498421	Male	Disabled	Disabled	1970-01-01	2099-12-31	

Figure 49: Card Management

### Notes:



- The GDS3705 can add up to 2000 card user.
- Press  or  to import / export users' configuration file, information and data stored on the GDS3705.
- 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.
- Use  to search for an entry on the Cards list.

## Add Users Manually

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



← Add Card Info

Username*	<input type="text" value="John Snow"/>
Private PIN	<input type="text" value="..."/>
Gender	<input type="text" value="Male"/> ▼
ID Number	<input type="text" value="123"/>
Card Number*	<input type="text" value="89978456"/>
Valid Start Date	<input type="text" value="1970-01-01"/> 
Valid End Date	<input type="text" value="2099-12-31"/> 
Virtual Number*	<input type="text" value="1"/>
Sip Number	<input type="text" value="1001"/>
Call Out Account	<input type="text" value="Auto"/> ▼
Cellphone	<input type="text" value="561545020"/>
Group	<input type="text" value="Disabled"/> ▼
Schedule	<input type="text" value="Disabled"/> ▼
Right of Card and Private PIN	<input checked="" type="checkbox"/> Door 1 <input checked="" type="checkbox"/> Door 2
Enable	<input checked="" type="checkbox"/>

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

Figure 50: Card Info

Table 8: 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 filed will be added automatically.
<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 GDS3705 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 SIP account that will be used to call the <b>SIP Number</b> extension, when choosing Auto, the unit will use the first available SIP account.
<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.


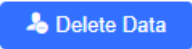

#### Notes:

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

### Add Users Automatically

If *[Enable Card Issuing Mode]* is checked, the GDS3705 keypad will start blinking and once an RFID card is swiped, data stored on the card will be added into the GDS3705 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 GDS3705.





- Users can use Go to:       to navigate through User Management pages.

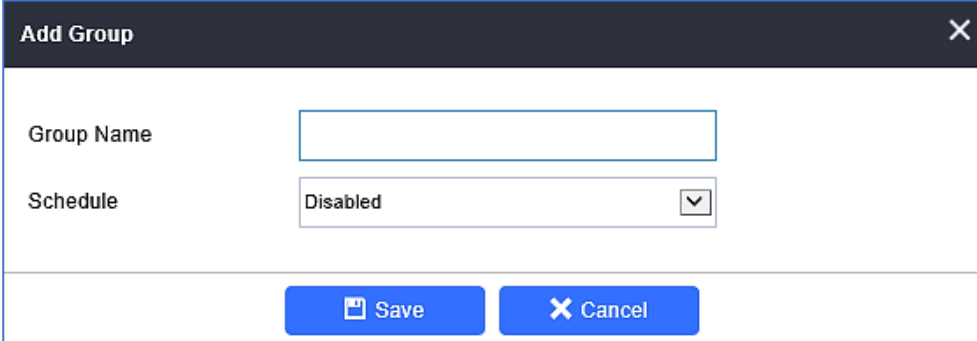
## Group

The Group page permits to manage the groups which will contains multiple users, click on



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

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



**Add Group** [X]

Group Name

Schedule  [v]



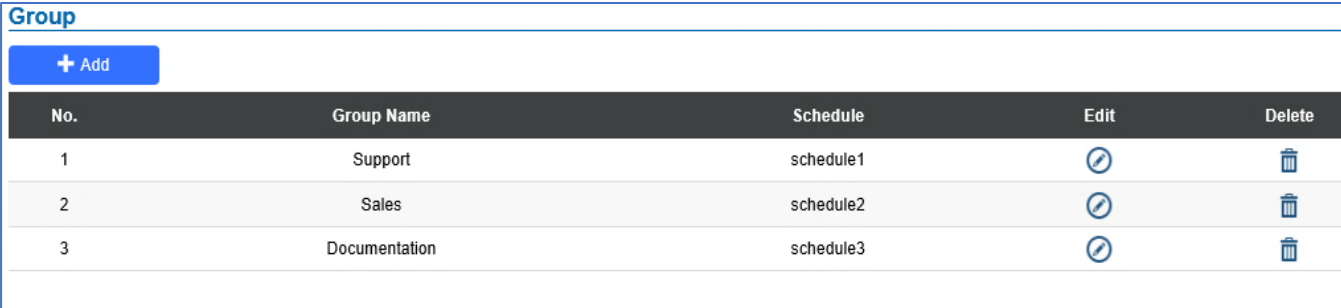
 Save  Cancel

Figure 51: Add Group


Table 9: Add Group

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

The following screenshots display the list of the created groups.



**Group**











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

Figure 52: Groups List

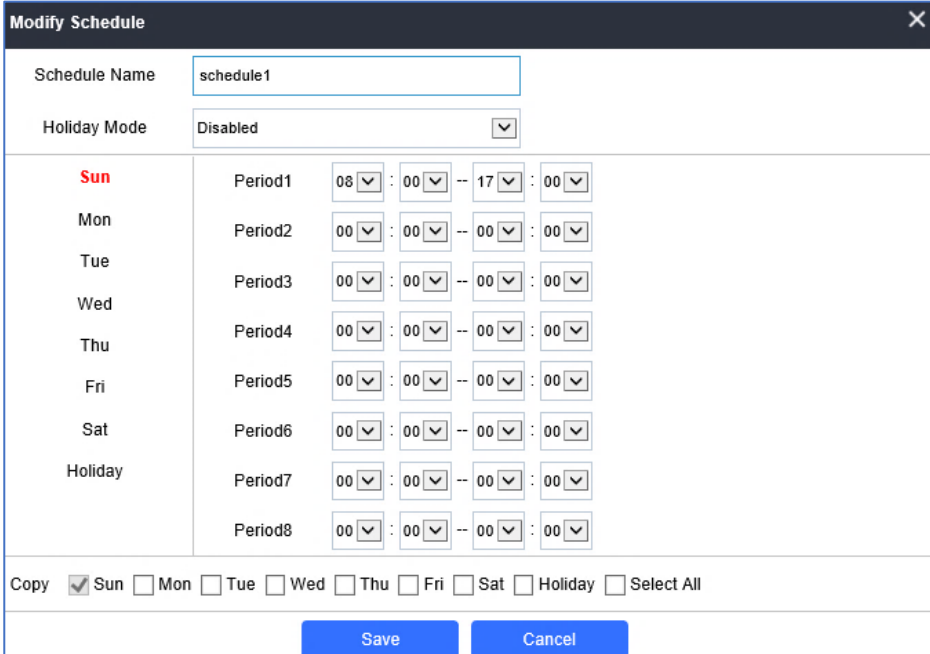
## Schedule

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, GDS3705 will not allow users to access.

Click on  to edit a schedule or  for schedule details.



**Note:** The GDS3705 supports up to 10 schedules.



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



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

**Save** **Cancel**

**Figure 53: Edit Schedule Time**

## Holiday

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

Click on  to edit the holidays or  for holiday details.

Schedule Name

holiday1

Duration1

-

+

«

»

Sep

2017

»

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

Today

OK

Save

Cancel


Figure 54: Edit Holiday Time

## System Settings

This page allows users to configure date and time, network settings as well as access method to the GDS3705 and password for accessing the Web GUI.

### Date & Time Settings

This page allows users to adjust system date and time of the GDS3705.


**GDS3705**

Door System Settings

System Settings

**Date & Time**

Network Settings

Access Settings

User Management

Factory Functions

Account

Phone Settings

Audio Settings

Date & Time

System Time

2019-08-08 09:43:16

Sync PC

Allow DHCP Option 42 to override NTP server

☐

Time Zone

GMT (Dublin, Lisbon, London, Reykjavik)

▼

Enable Daylight Saving Time

☐

Start Time

Jan

First

Sunday

00:00

End Time

Jan

First

Sunday

00:00

Enable NTP

☒

NTP Server

pool.ntp.org

Update Interval(m)

1440

Figure 55: Date & Time Page

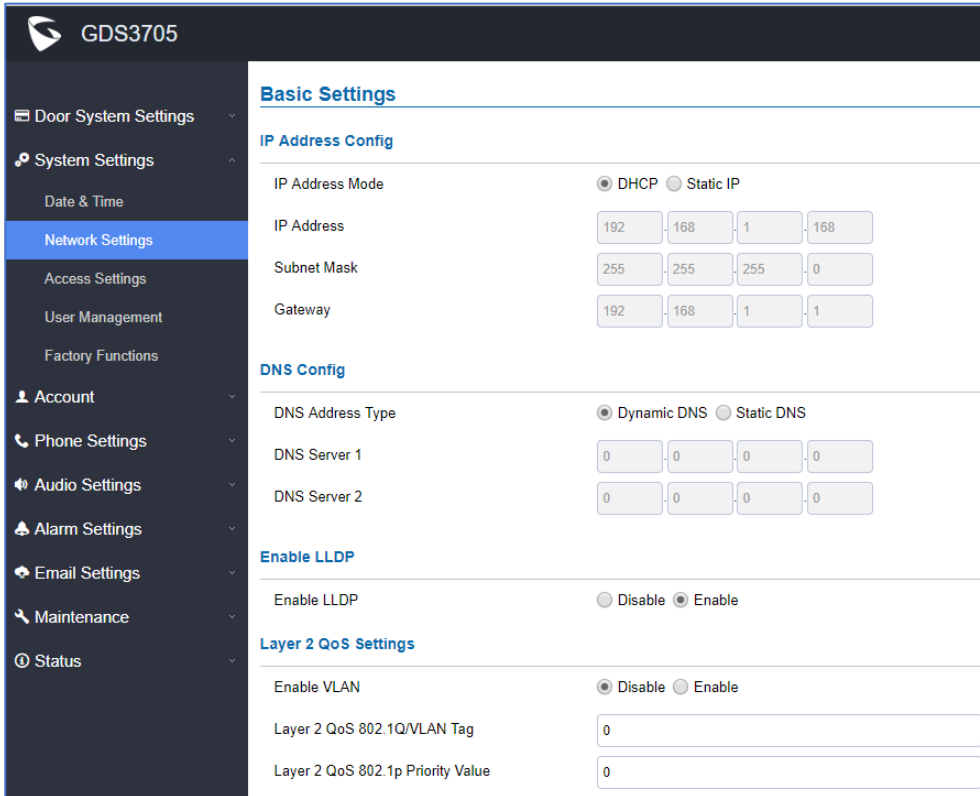


**Table 10: Date & Time**

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

## Network Settings

This page allows users to set either a static or DHCP IP address to access the GDS3705.



The screenshot shows the 'Basic Settings' page for the GDS3705 device. The left sidebar contains a navigation menu with options: Door System Settings, System Settings, Date & Time, Network Settings (highlighted), Access Settings, User Management, Factory Functions, Account, Phone Settings, Audio Settings, Alarm Settings, Email Settings, Maintenance, and Status. The main content area is titled 'Basic Settings' and includes the following sections:

- IP Address Config**:
  - IP Address Mode: ☒ DHCP ☐ Static IP
  - IP Address: 192.168.1.168
  - Subnet Mask: 255.255.255.0
  - Gateway: 192.168.1.1
- DNS Config**:
  - DNS Address Type: ☒ Dynamic DNS ☐ Static DNS
  - DNS Server 1: 0.0.0.0
  - DNS Server 2: 0.0.0.0
- Enable LLDP**:
  - Enable LLDP: ☐ Disable ☒ Enable
- Layer 2 QoS Settings**:
  - Enable VLAN: ☒ Disable ☐ Enable
  - Layer 2 QoS 802.1Q/VLAN Tag: 0
  - Layer 2 QoS 802.1p Priority Value: 0

**Figure 56: Basic Settings Page**

**Table 11: Basic Settings**

<b>IP Address Mode</b>	Selects DHCP or Static IP. Default DHCP. (Static recommended)
<b>IP Address</b>	Configures the Static IP of the GDS3705.
<b>Subnet Mask</b>	Configures the Associated Subnet Mask.
<b>Gateway</b>	Configures the Gateway IP address.
<b>DNS Address Type</b>	Specifies the DNS type used: Dynamic DNS or Static DNS.
<b>DNS Server 1</b>	Configures DNS Server 1 IP address.
<b>DNS Server 2</b>	Configures DNS Server 2 IP address.
<b>Enable LLDP</b>	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is "Enabled".
<b>Enable VLAN</b>	Controls the VLAN. Default setting is "Disabled"
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assigns the VLAN Tag of the Layer 2 QoS packets. Valid range: 0-4096. 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 GDS3705 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.

## OpenVPN® Settings

This page allows users to configure OpenVPN settings.



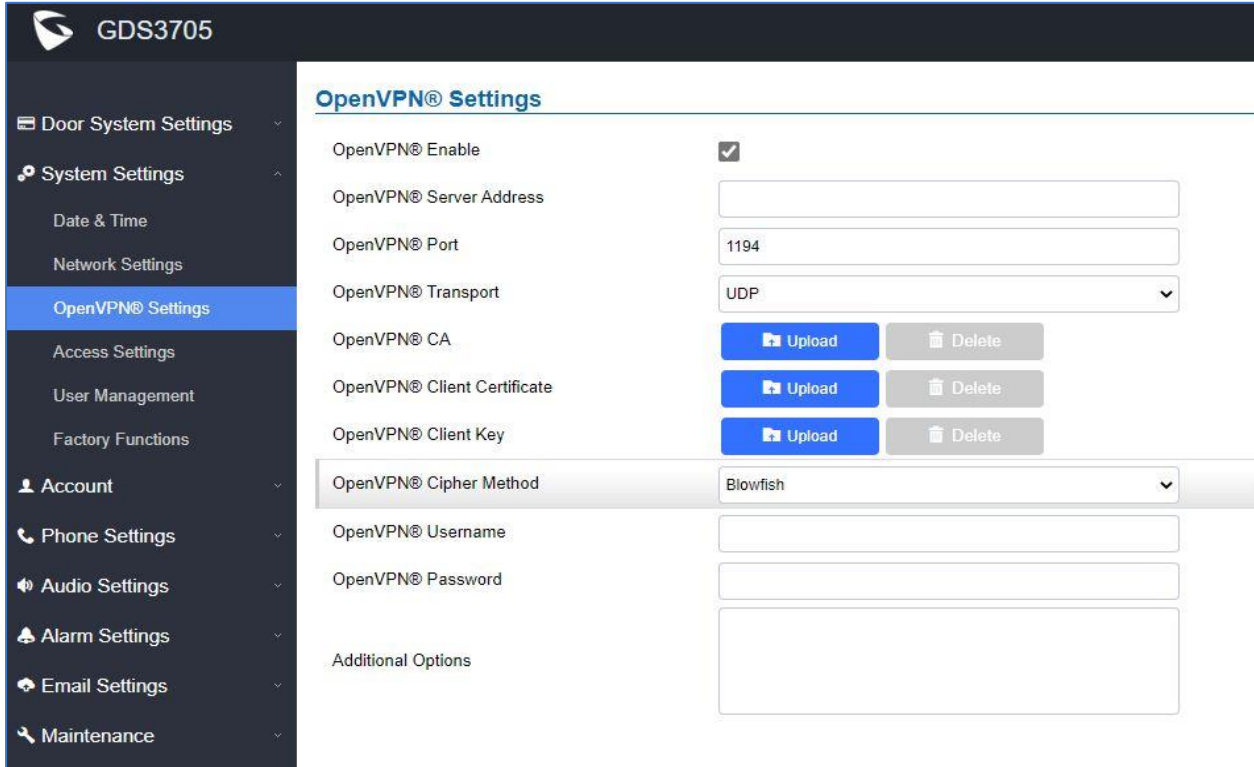


Figure 57: OpenVPN Settings page

<b>Enable OpenVPN®</b>	Enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server. <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).
<b>OpenVPN® Server Address</b>	Defines the URL/IP address for the OpenVPN® server.
<b>OpenVPN® Port</b>	Defines the network port for the OpenVPN® server. The default setting is <b>1194</b> .
<b>OpenVPN® Transport</b>	Determines network protocol used for OpenVPN® (UDP or TCP). The default setting is <b>TCP</b> .
<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).

## OpenVPN® Password

Configures the OpenVPN® authentication password (optional).

## Access Settings

This page configures the GDS3705 access control parameters.

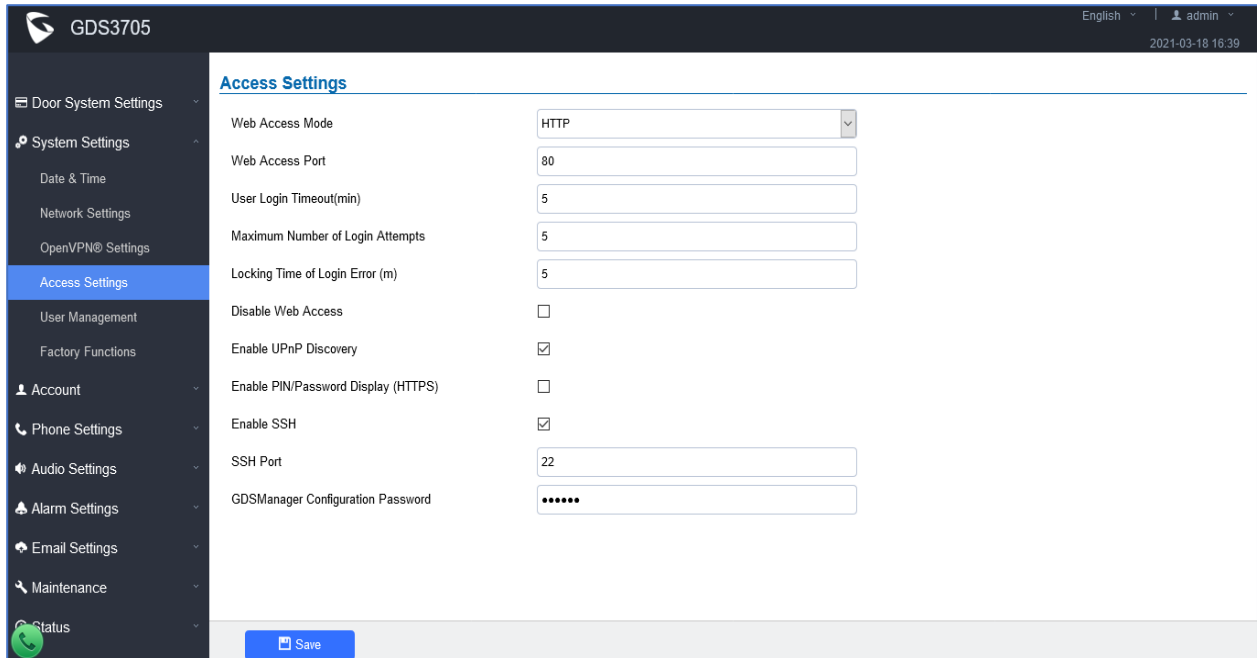


Figure 58: Access Settings Page

Table 12: Access Settings

<b>Web Access Mode</b>	Selects the access mode to the webGUI either HTTP or HTTPS.
<b>Web Access Port</b>	Specifies the TCP port for Web Access, default 443.
<b>User Login Timeout(min)</b>	If no action is made within this time the GDS3705 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 GDS3705 webGUI will be locked for the time specified in <b>Locking Time of Login Error</b> .
<b>Locking Time of Login Error (m)</b>	Specifies how long the GDS3705 is locked before a new login attempt is allowed.
<b>Disable Web Access</b>	<p>Allow or deny the web access to the GDS3705. (HTTP API do not take effect when this option is enabled).</p> <p><b>Note:</b> If both Web UI and SSH are disabled, GDS3705 will get blocked and not be able to be accessed. Only two ways to get it back:</p>





	<ol style="list-style-type: none"> <li>1. Re-provisioned by ITSP or Service Provider (by adjusting the related parameters)</li> <li>2. Hard Reset (GDS3705 has to be offline and uninstalled to perform this hard reset).</li> </ol>
<b>Enable UPnP Discovery</b>	UPnP (or mDNS) function for local discovery. Default setting is enabled.
<b>Enable PIN/Password Display (HTTPS)</b>	<p>Once enabled, there will be an “eye” icon displayed in the web UI, putting the cursor to the “eye” icon, the related password or PIN will be displayed at the web UI. Once mouse cursor moved away, the PIN/Password will be displayed as dot “.” as usual.</p> <p><b>Note:</b> This feature ONLY works in HTTPS mode. Due to the insecurity of HTTP, PIN/Password will NOT be displayed. PIN/Password can ONLY be displayed in HTTPS mode.</p>
<b>Enable SSH</b>	Selects to Enable/Disable SSH access. Default setting is enabled.
<b>SSH Port</b>	Specifies the SSH port. Default setting is 22.
<b>GDSManager Configuration Password</b>	User can set in this field a custom admin password instead of using GDS3705 webUI administrator's credentials, and this custom admin password will be the one used when adding the GDS3705 unit to GDSManager database.

## User Management

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

User Management

Password Recovery Email is not configured. Please input Password Recovery Email address and configure a valid SMTP service in Email Settings Page

Change Password
 

Old Password

New Password

Confirm New Password

Change Recover Email
 

Password Recover Email Address

[Email Settings](#)

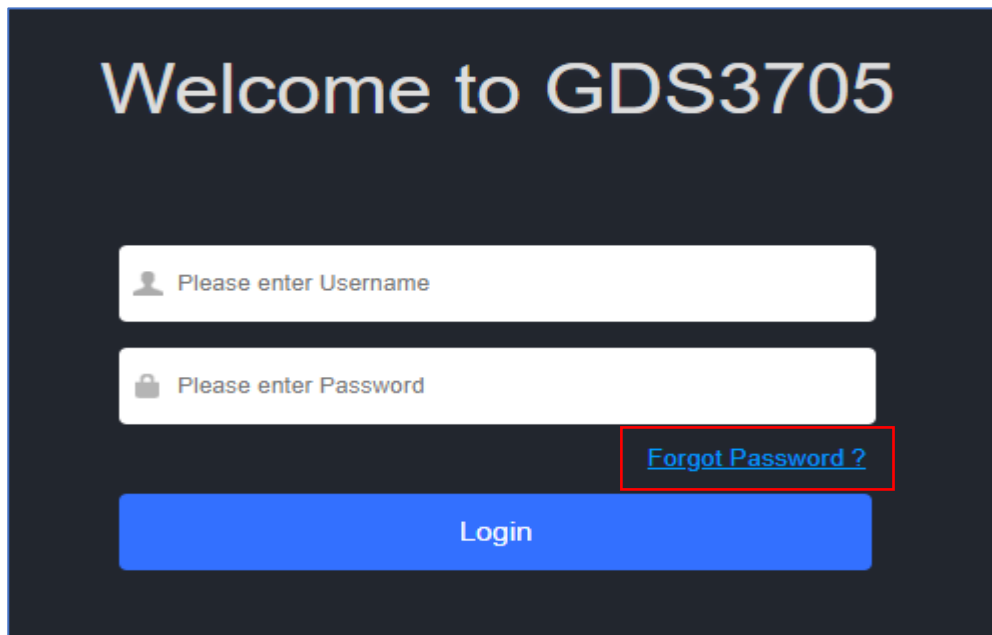
Figure 59: User Management Page



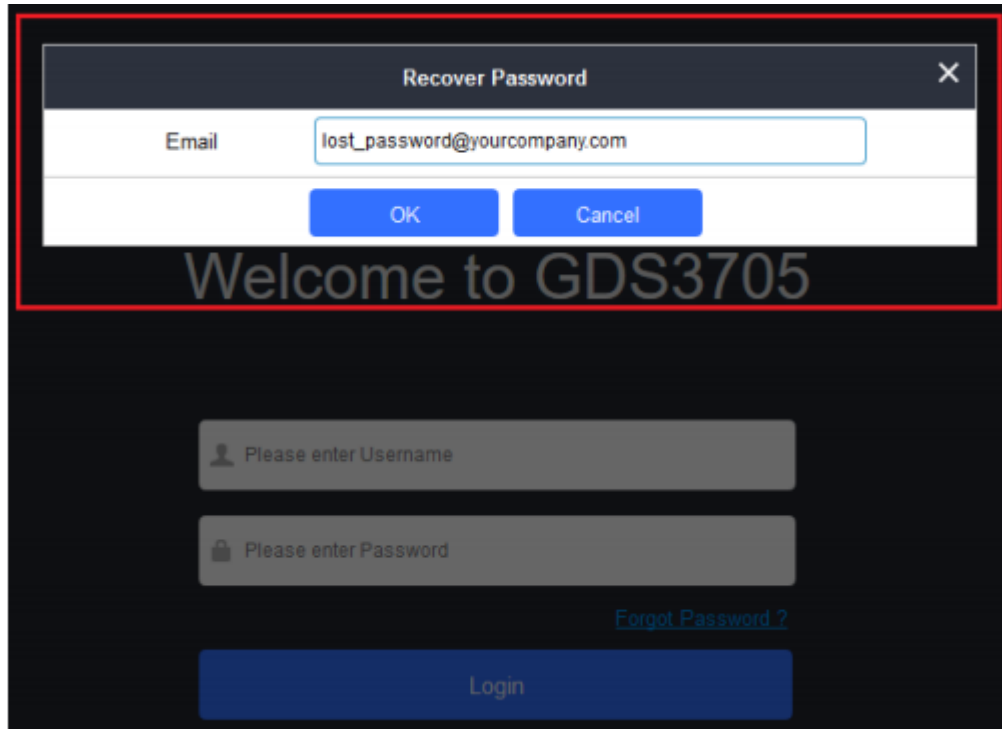
**Table 13: User Management**

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

To recover lost password, users can from the login page click on [Forgot Password?](#)


**Figure 60: Recover Password**

Click the link will pop up the following page to ask to input the “Email Address” for the Recover Password to be sent to:



**Figure 61: Recover Password - Email Address**

If the “Password Recover Email Address” and related SMTP is configured correctly, then click the “OK” button, the device will email the administrator password to the inputted email address, if the email address entered matches the pre-configured “Password Recover Email Address” inside the device and the device with working SMTP service configured.

Otherwise the device will prompt the following message at top of the UI page to advise user to configure the related parameters or service, to make this feature working. User can still click “Cancel” to omit these setting and continue the UI operation, but this is bad operation behavior.

**Invalid Email Address without User Bound!**

Grandstream strongly suggest user to configure a working email address as “Password Recover Email Address” and configure a good SMTP service to the device. So, if something happened, the administrator can get the password recover email to unlock the device.

## Factory Functions

Users could access factory functions in order to diagnosis the hardware and software of the unit like verifying the audio loopback and certificates verification.



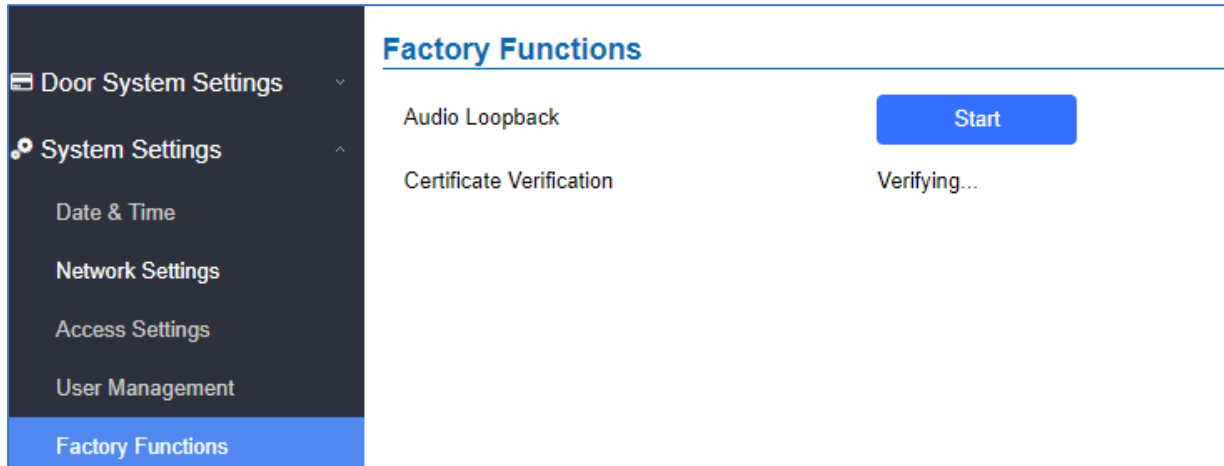


Figure 62 : Factory Functions Page

Table 14: User Management


<b>Audio Loopback</b>	Press <b>Start</b> button and speak to the GDS3705. If you can hear your voice, your audio is working fine. Press <b>Stop</b> to exit audio loopback mode.
<b>Certificate Verification</b>	This is used to validate certificate chain for the server's certificate.

## Account

The GDS3705 supports 4 SIP accounts and 4 lines, this section covers the configuration of basic and advanced SIP settings for each SIP account.

### Account 1 - 4

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


GDS3705

- Door System Settings
- System Settings
- Account
  - Account 1
  - Account 2
  - Account 3
  - Account 4
- Phone Settings
- Audio Settings
- Alarm Settings
- Email Settings
- Maintenance
- Status

### Account 1

#### SIP Basic Settings

Account Active	<input checked="" type="checkbox"/>
SIP Server	<input type="text" value="192.168.5.53"/>
Secondary SIP Server	<input type="text"/>
Outbound Proxy	<input type="text"/>
Backup Outbound Proxy	<input type="text"/>
DNS Mode	<div>A Record ▾</div>
SIP User ID	<input type="text" value="4003"/>
Authentication ID	<input type="text" value="4003"/>
Password	<input type="password" value="*****"/>
Display Name	<input type="text" value="4003"/>
TEL URI	<div>Disabled ▾</div>

#### SIP Advanced Settings

Registration Expiration(m)	<input type="text" value="60"/>
Re-register before Expiration(s)	<input type="text" value="0"/>
Local SIP Port	<input type="text" value="5060"/>

**Figure 63: SIP Account Settings Page**

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

SIP Basic Settings	
<b>Account Active</b>	This field indicates whether the account is active. Default setting is “Yes”.
<b>SIP Server</b>	Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.
<b>Secondary SIP Server</b>	Configures the FQDN or IP of the Secondary SIP server from VoIP service provider or local IPPBX.
<b>Outbound Proxy</b>	Configures the IP address or the domain name of the outbound proxy, media gateway, or session border controller. It's used by the GDS for firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and only an outbound proxy can provide a solution.
<b>Backup Outbound Proxy</b>	Configures the backup outbound proxy to be used when the “Outbound Proxy” registration fails. By default, this field is left empty.



<b>DNS Mode</b>	<p>Configure which DNS mode will be used to translate the SIP Server FQDN (Default value is <b>A Record</b>):</p> <ul style="list-style-type: none"> <li>• <b>A Record.</b></li> <li>• <b>SRV.</b></li> <li>• <b>NAPTR/SRV.</b></li> </ul> <p><b>Note:</b> Service providers can use DNS SRV feature to provide smooth service transition backup in case service down.</p>
<b>SIP User ID</b>	<p>Configures the SIP username or telephone number from ITSP.</p> <p><b>Note:</b> Letters, digits and special characters including @ are supported.</p>
<b>Authentication ID</b>	<p>Configures the Authenticate ID used by SIP proxy.</p>
<b>Password</b>	<p>Sets the Authenticate password used by SIP proxy.</p> <p><b>Note:</b> For security reasons, the SIP password is invisible on the web UI.</p>
<b>Display Name</b>	<p>The GDS3705 is an audio only device, unlike GDS3710, user cannot see who is at the door. Adding this "Display Name" will also allow user receiving calls from GDS3705 knowing where the call is coming from (e.g.: which door or extension the call is made), improve user experience when user is using a IP phone with LCD display.</p>
<b>TEL URI</b>	<p>Select "User=Phone" or "Enabled" from the dropdown list.</p> <p>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".</p>



SIP Advanced Settings	
<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 GDS3705 sends re-registration request before the Register Expiration. The default value is 0. Range is from 0 to 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. Default settings is UDP.
<b>Enable DTMF</b>	Specifies the mechanism to transmit DTMF digits. There are 2 supported modes: <ul style="list-style-type: none"> <li>• <b>RFC2833</b> sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.</li> <li>• <b>SIP INFO</b> uses SIP INFO to carry DTMF. Default setting is "RFC2833"</li> </ul>
<b>DTMF Payload Type</b>	Configures the payload type for DTMF using RFC2833. Default value is 101. Range: 96~127.
<b>Enable Keep Alive</b>	Checks to help NAT resolution, sending alive packets.
<b>Unregister On Reboot</b>	Allows the SIP user's registration information to be cleared when the GDS3705 reboots. The SIP REGISTER message will contain "Expires: 0" to unbind the connection
<b>NAT Traversal</b>	<p>This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, STUN, Keep-alive, UPnP, Auto or VPN. The default setting is "No".</p> <p>If set to "STUN" and STUN server is configured, the GDS3705 will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the unit will try to use public IP addresses and port number in all the SIP&amp;SDP messages.</p> <p>The GDS will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be "Keep-alive". Configure this to be "No" if an outbound proxy is used. "STUN" cannot be used if the detected NAT is symmetric NAT. Set this to "VPN" if OpenVPN is used.</p>
<b>Enable SRTP</b>	Enable SRTP mode based on your selection from the drop-down menu. The default setting is "Disabled", the two other modes are "Enabled but Not Forced" and "Enabled and Forced".



<b>Special Feature</b>	Configures GDS settings to meet different vendors' server requirements. Users can choose from Standard, Broadsoft or Telefonica Spain. The default setting is "Standard".
<b>Outbound Proxy Mode</b>	<b>In route:</b> outbound proxy FQDN is placed in route header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall. <b>Always sent to:</b> SIP messages will always be sent to Outbound proxy. <b>Not in route:</b> remove the Route header from SIP requests.
<b>Validate Incoming Messages</b>	Specifies if the device will check the incoming SIP messages caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
<b>Enable RTCP</b>	This option allows 3 <sup>rd</sup> party Service Provider or Cloud Solution to monitor the operation status of the GDS3705 by using related SIP Calls. By default, it's disabled. Users can choose either RTCP or RTCP-XR.
<b>Accept Incoming SIP from Proxy Only</b>	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 "No"
<b>SIP URI Scheme When Using TLS</b>	This option allows the GDS3705 to work with Cisco WebEX server as SIP client. The two modes are SIP and SIPS.
<b>Support SIP Instance ID</b>	When enabled, the GDS3705 will work with Cisco WebEX server as SIP client.
<b>Custom SIP Headers</b>	
<b>Use P-Access-Network-Info Header</b>	Enables / disables the use of P-Access-Network-Info header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "Yes"
<b>Add MAC in User-Agent</b>	if <b>Yes except REGISTER</b> , the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header; If <b>Yes to ALL SIP</b> , the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP message including REGISTER will attach the MAC address to the User-Agent header;





	If <b>No</b> , neither will the MAC header be included in the register or unregister message nor the MAC address be attached to the User-Agent header for any outgoing SIP message. The default setting is “No”.
<b>Vocoder Settings</b>	
<b>Preferred Vocoder</b>	Select multiple audio codecs by priority order (lowest is the highest priority). Supported codecs are: PCMU, PCMA, G.722 and G.729A/B.
<b>Voice Frame Per TX</b>	<p>Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the “ptime” value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality.</p> <p>The default setting is 2.</p> <p>Range is from 1-64.</p>

**Note:** This new CISCO WEBEX COMPATABLE feature is implemented so the GDS3705 can be running in Cisco WebEx Service. When enabled and configured, the GDS3705 will register and work in Cisco WebEx Service.

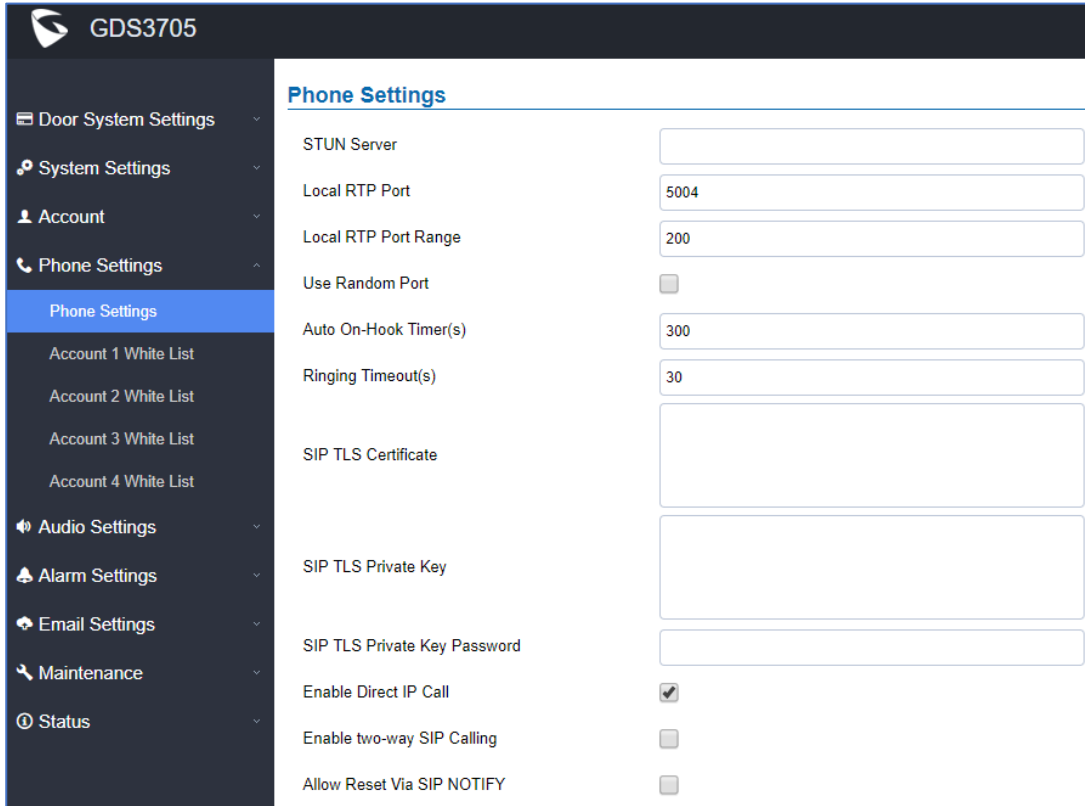
## Phone Settings

The phone settings allow users to configure the GDS3705 phone settings and the White list for all the SIP accounts.

### Phone Settings

This page allows users to configure the GDS3705 phone settings.





**Figure 64: Phone Settings Page**

**Table 16: Phone Settings**

<b>STUN Server</b>	Configures the STUN server FQDN or IP. If the device is behind a non-symmetric router, STUN server can help to penetrate & resolve NAT issues.
<b>Local RTP Port</b>	Sets the local RTP port for media. Default setting is 5004.
<b>Local RTP Port Range</b>	Define the range of local RTP port from 48 to 10000
<b>Use Random Port</b>	Forces the GDS3705 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.
<b>Ring Timeout(s)</b>	Specifies the Ring timeout, when no reply is returned from the called party after exceeding this field, the GDS3705 will hang up the call. The value is in the range of 0s – 90s. By default; it is “30” seconds.
<b>SIP TLS Certificate</b>	Copy/Paste 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>Allow Reset Via SIP NOTIFY</b>	<p>Allows to factory reset the devices directly through SIP Notify.</p> <p>If "Allow Reset Via SIP NOTIFY" is "check", then once the GDS3705 receives the SIP NOTIFY from the SIP server with Event: reset, the GDS3705 will perform a factory reset after authentication.</p> <p>This authentication can be either with:</p> <ul style="list-style-type: none"> <li>The admin password if no SIP account is configured on the GDS3705.</li> <li>The SIP User ID and Password credentials of the SIP account if configured on the GDS3705.</li> </ul> <p>Default is unchecked (disabled).</p>

## 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 GDS3705. (The call will be automatically answered when calling from a phone set on the white list, and all other inbound calls will be blocked), the user can configure up to 30 white phone numbers per SIP account.

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

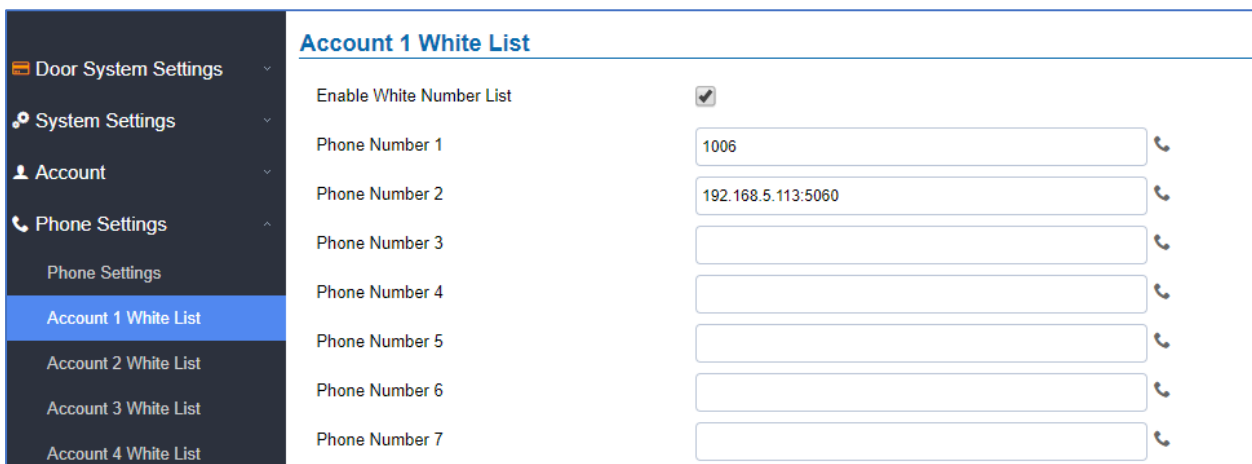


Figure 65: White List Page



The table below gives a brief overview of the options:

**Table 17: White List**

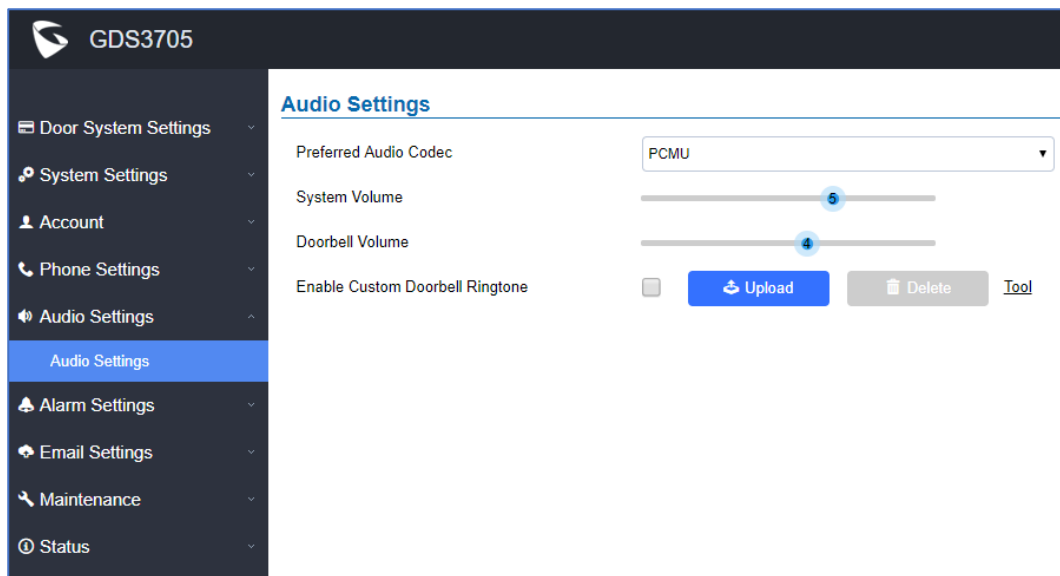
<b>Enable White Number List</b>	Enables the White List feature.
<b>Phone Number 1 - 200</b>	Adds a new phone number to the white list.

## Audio Settings

The audio settings allow users to configure the audio codecs and Volume related settings.

### Audio Settings

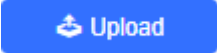
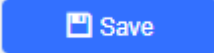

This page allows users to configure the audio settings.



**Figure 66: Audio Settings Page**

**Table 18: Audio Settings Page**

<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>Tool</b>	This button will redirect user to our Grandstream Ringtone Generator tool in our website.

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

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

## Alarm Config

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

## Alarm Events Config

This page allows users to configure GDS3705 events to trigger programmed actions within predefined schedule.

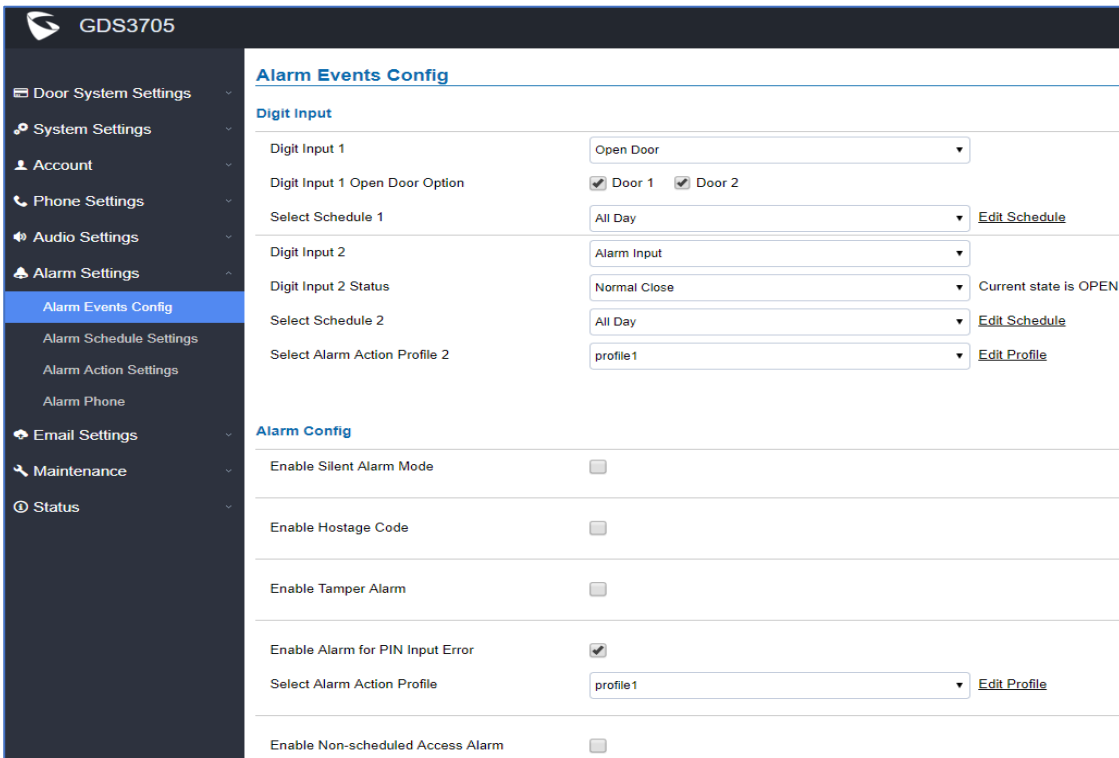


Figure 67: Events Page



## Input Digit

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

Figure 68: Input Digit

Table 19: Input Digit

<b>Digital Input 1</b>	<p>Selects the Input method (alarm Input or Door Open). Default disabled.</p> <p>Digital Input Port operates in 3 Modes:</p> <ol style="list-style-type: none"> <li><b>Alarm Input:</b> Connect various of 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> When enabled (special wiring required, see below wiring diagram), abnormal open door will be detected and therefore trigger siren alarm.</li> </ol> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If Digital Input port is connected to a switch, it will not work during the time of power outage, device booting or firmware upgrading.</li> <li>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). Please refer to XXX for diagrams showing the correct wiring to enable this feature.</li> </ul>
<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>Digit Input 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 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>Digit Input 2 Status</b>	<ul style="list-style-type: none"> <li>• If set to <b>Normal Open</b>: Configured alarm will be triggered when Digital Input Status switch from Close to Open.</li> <li>• If set to <b>Normal Close</b>: Configured alarm will be triggered when Digital Input Status switch from Open to Close.</li> </ul> <p>By default, Input Digit 2 Status is "Disabled".</p>
<b>Select Schedule 2</b>	Selects the predefined Alarm Schedule.
<b>Select Alarm Action Profile 2</b>	Selects the predefined Alarm Action for Profile 2.
<b>Alarm Output Duration(s)</b>	<p>Select the duration of the alarm output: 5/10/15/20/25/30 seconds.</p> <p>This option is hidden when <b>ALMOUT1 Feature</b> is set to Open Door.</p>

## Alarm Output

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

## Silently Alarm Mode

If Silently Alarm Mode is enabled, GDS3705 will disable alarm sound and background light for specified alarms types (Digital Input) when they are triggered.

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

Table 20: Silently Alarm Mode

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



## Hostage Code

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

**Table 21: Hostage Code Alarm**

<b>Enable Hostage Code</b>	Enable/Disable the Hostage password mode.
<b>Hostage Code</b>	Configures the password for the hostage mode.
<b>Select Alarm Action Profile</b>	Select the Alarm action to be taken when the hostage password is typed on the GDS3705 keypad.  <b>Note:</b> No sound alarm will be triggered in this mode.

## Tamper Alarm

Tamper alarm is anti-hack from Hardware level. When this option is checked, if the GDS3705 is removed from the installation board, it will trigger configured alarm actions. There is an embedded mechanism on the GDS3705 that allows it to detect when the unit is removed.

**Table 22: Tamper Alarm**

<b>Enable Tamper Alarm</b>	When activating this mode, GDS3705 will keep alarming until the alarm is dismissed.
<b>Select alarm Action Profile</b>	Select the type of alarms actions to be triggered for the tamper alarm mode.

## Keypad Input Error Alarm

**Table 23: Keypad Input Error Alarm**

<b>Enable Alarm for PIN Input Error</b>	Enable/Disable the Input Error Alarm, GDS3705 will trigger alarm actions at every 5 incorrect attempts.
<b>Select Alarm Profile</b>	Select the type of alarms actions to be triggered after 5 incorrect attempts.

## Non-Scheduled Access Alarm

**Table 24: Non-Scheduled Access Alarm**

<b>Enable Non-scheduled Access Alarm</b>	When enabling this feature, GDS3705 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.

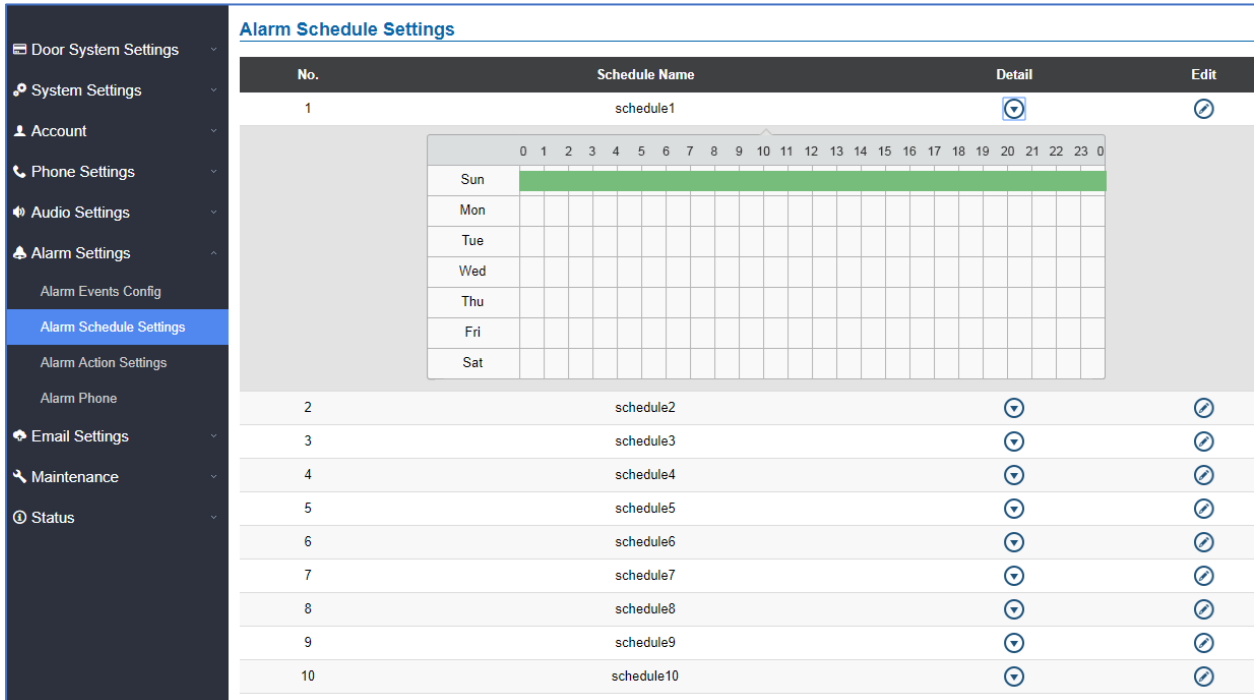




## Alarm Schedule Settings


This page specifies the configuration of Alarm Schedule.

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



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		

Figure 69: Alarm Schedule

GDS3705 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

<b>Sun</b>	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

Save

Cancel

Figure 70: Edit Schedule

**Note:**

Schedule Name cannot be blank

## Alarm Action When Illegal Card Swiped

This option can be enabled from the web GUI, under **Alarm Settings** → **Alarm Event Config**

Enable Non-authorized RFID Card Access Alarm

☒

Select Alarm Action Profile

▼

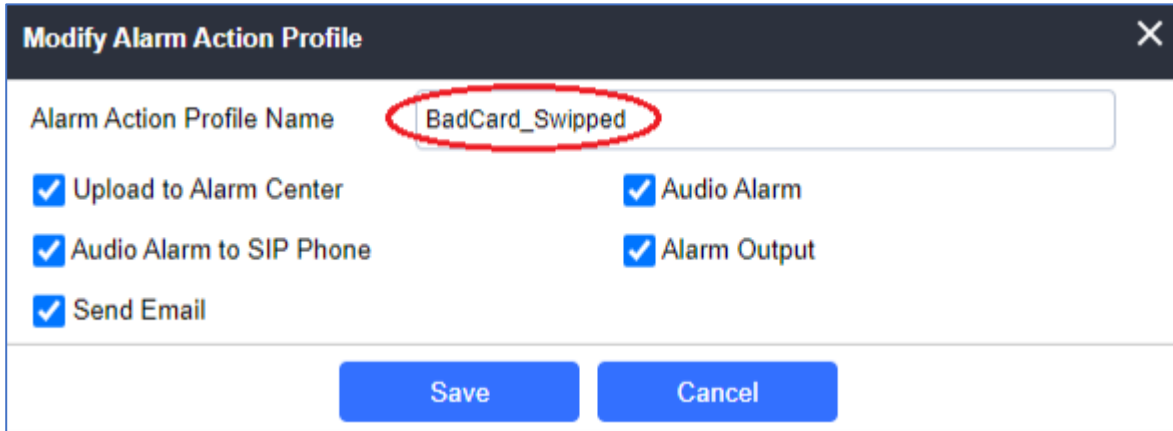
[Edit Profile](#)

Save

Figure 71: Enable Non-authorized RFID Card Access Alarm

Any illegal card swiped trying to access the door will trigger alarm based on user's configuration, like below:





**Modify Alarm Action Profile**

Alarm Action Profile Name: BadCard\_Swipped

☒ Upload to Alarm Center      ☒ Audio Alarm  
☒ Audio Alarm to SIP Phone      ☒ Alarm Output  
☒ Send Email

**Figure 72: Alarm action profile example for illegal card swipe**

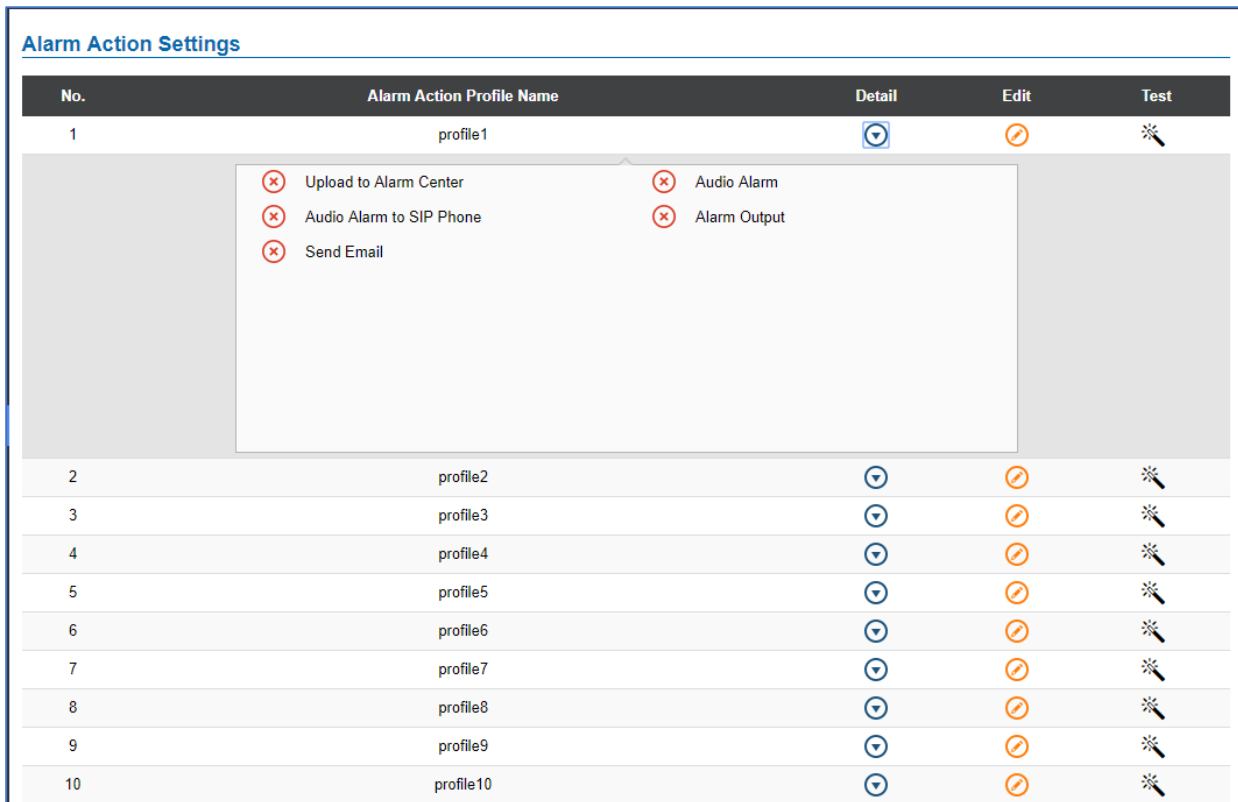
User will get email, snapshot, etc., based on the Alarm Action Profile configured, to enhance the security of access control.

**Note:**

Alarm Action Profile Name” cannot be blank

## 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.

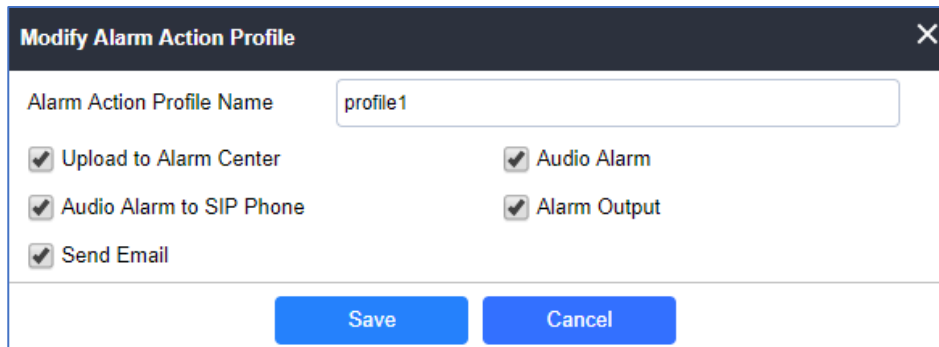


No.	Alarm Action Profile Name	Detail	Edit	Test
1	profile1	<div> <input checked="" type="checkbox"/> Upload to Alarm Center      <input checked="" type="checkbox"/> Audio Alarm  <input checked="" type="checkbox"/> Audio Alarm to SIP Phone      <input checked="" type="checkbox"/> Alarm Output  <input checked=""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


**Figure 73: Alarm Action**



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



**Figure 74: Edit Alarm Action**

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

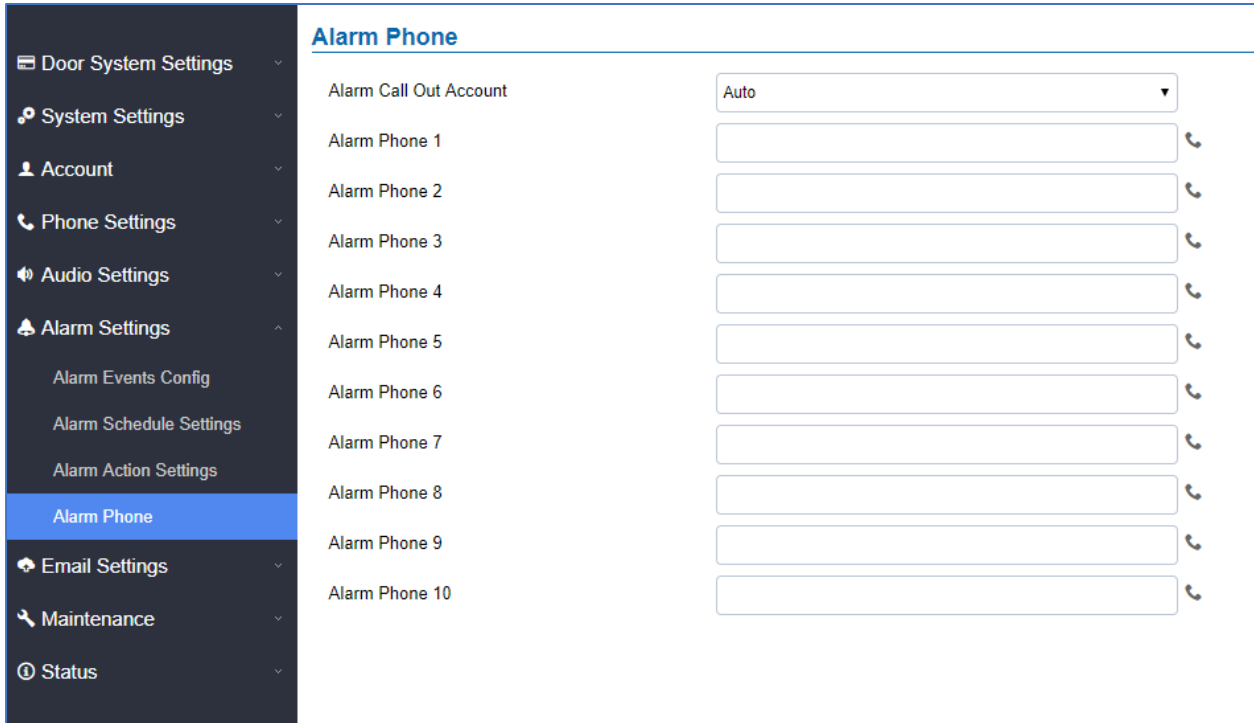
**Table 25: Alarm Actions**

<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, GDS3705 will call pre-configured phone and will play sound alarm.
<b>Send Email</b>	If selected, an email will be sent to the pre-configured email destination.
<b>Audio Alarm</b>	If selected, GDS3705 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.

## Alarm Phone List

This page allows users to configure the Alarm Phone List, which are phone numbers or extensions list that the GDS3705 will call out when event is triggered (e.g.: doorbell pressed), the administrator can configure up to 10 phone numbers to be called and specify the SIP account to trigger the alarm call.





**Figure 75: Alarm Phone List**

**Table 26: Alarm Phone List**

<b>Alarm Call Out Account</b>	Define the SIP account that will be used to trigger the alarm call, when choosing Auto, the unit will use the first available SIP account.
<b>Alarm Phone 1-10</b>	Add the phone numbers to be called into the alarm list.

Once the event is triggered (Door Bell Pressed...), the GDS3705 will call the first number, once time out is reached and no answer is returned from the first number, the GDS3705 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.

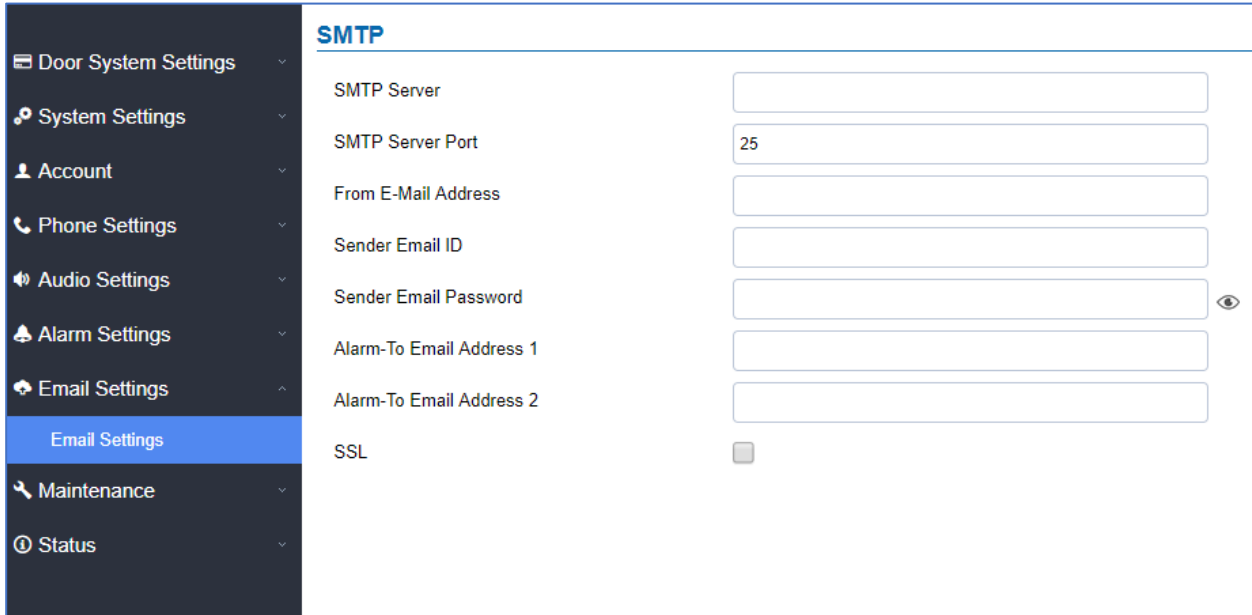
## Email Settings

This page contains Email Settings.

### Email Settings

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





**Figure 76: Email Settings - SMTP Page**

**Table 27: Email Settings - SMTP**

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

**Notes:**

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

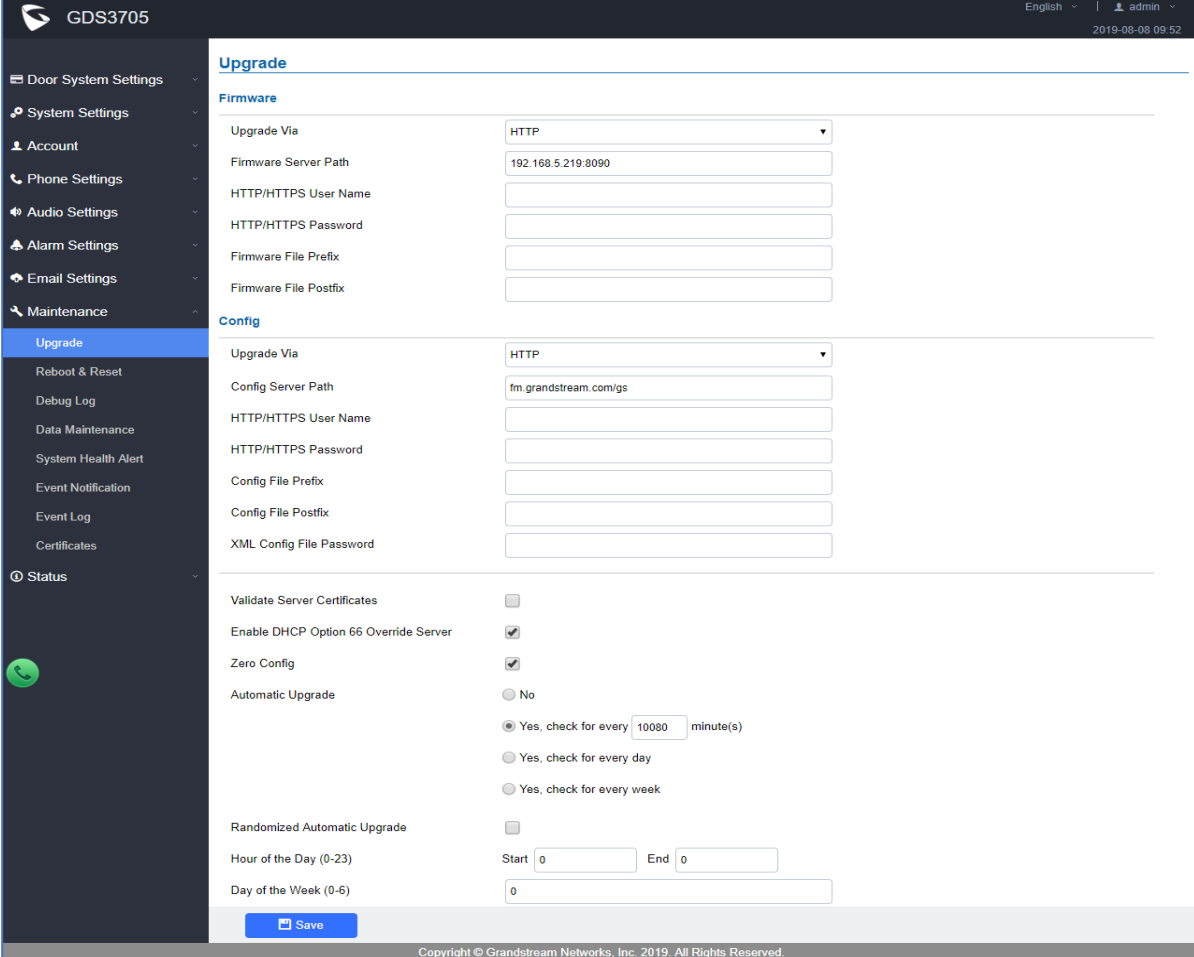
## Maintenance Settings

This page shows the GDS3705 Maintenance parameters.



## Upgrade

This page contains the upgrade parameters of the GDS3705.



**Figure 77: Upgrade Page**

**Table 28: Upgrade**

<b>Upgrade Via</b>	Selects the upgrade method (HTTP, HTTPS).
<b>Firmware Server Path</b>	Configures the IP address or the FQDN of the upgrade server.
<b>Config Server Path</b>	Configures the IP address or the FQDN of the configuration server.
<b>HTTP/HTTPS User Name</b>	User name if needed by remote provisioning HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	Password to authenticate with remote provisioning HTTP/HTTPS server.
<b>Firmware File Prefix</b>	Prefix that will be added when requesting firmware file.
<b>Firmware File Postfix</b>	Postfix that will be added when requesting firmware file.
<b>Config File Prefix</b>	Prefix that will be added when requesting config file.



<b>Config File Postfix</b>	Postfix that will be added when requesting config file.
<b>XML Config File Password</b>	Specifies the password for the configuration file.
<b>Validate Server Certificate</b>	Enable this option to validate certificate with trusted ones during TLS connection.
<b>Automatic Upgrade Interval(m)</b>	Specifies the upgrade interval in minutes.
<b>Enable DHCP Option 66 Override Server</b>	Activates DHCP option 66 to override upgrade/config servers.
<b>Zero Config</b>	Enables Zero Config feature for auto provisioning.
<b>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.

## Reboot & Reset

This page allows user to reboot (scheduled or immediate) and reset the GDS3705.

**Reboot & Reset**

Reboot

Reboot

Auto Reboot

☐

Everyday

00

:

00

Reset

Retain Network Data Only

Reset

**Figure 78: Reset & Reboot Page**

**Table 29: Reset & Reboot**

<b>Reboot</b>	When clicked, the GDS3705 will restart (soft reboot).
<b>Auto Reboot</b>	With this feature, users can configure convenient selected schedule for the device to reboot by itself, per week or per day.
<b>Reset</b>	There are two options for the reset function.
<b>Clear All Data</b>	All data will be reset, GDS3705 will be set to factory default.
<b>Retain Network Data Only</b>	All data will be erased except for Network data like IP address...





<b>Retain Only Card Information</b>	All data will be erased except for cards information.
<b>Retain Network Data and Card Information</b>	All data will be erased except for Network Data and Card Information.

## Debug Log

This page allows user to configure SYSLOG to collect information to help troubleshooting issues with GDS3705.

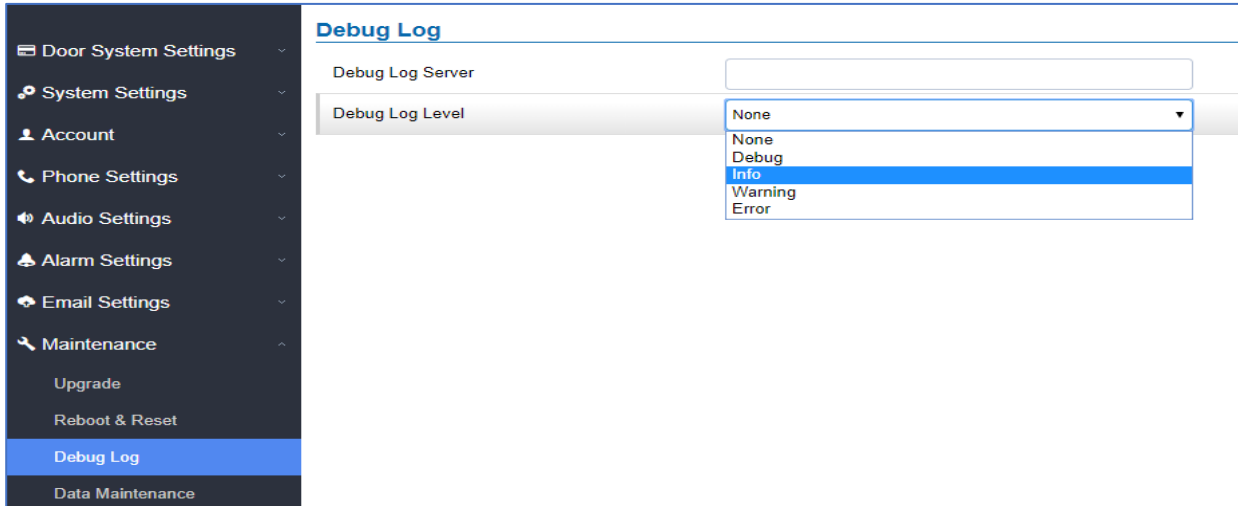


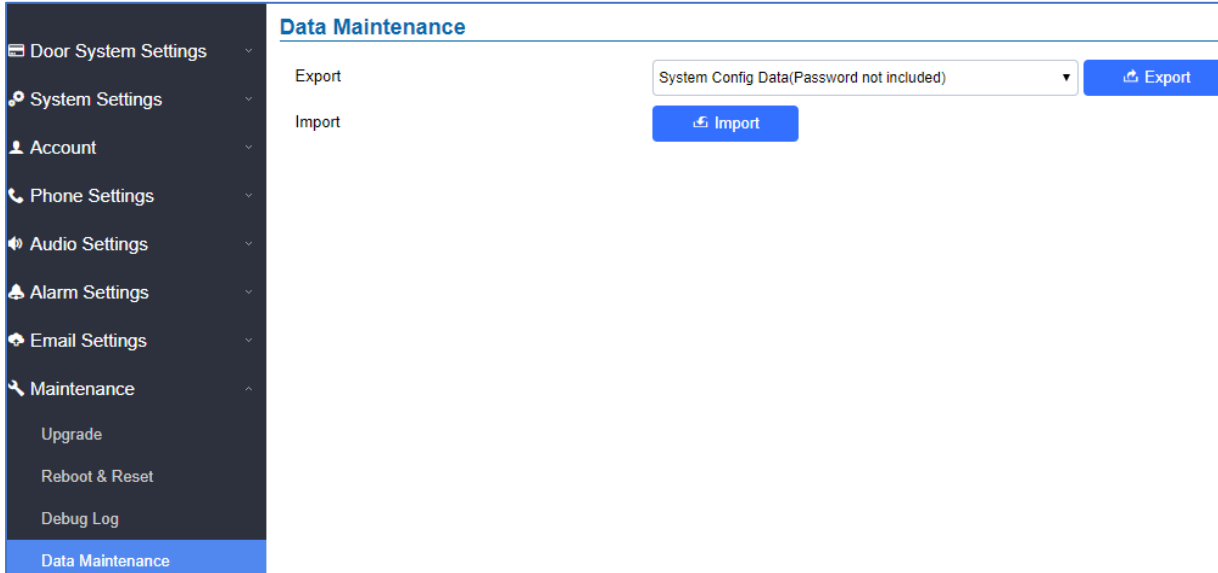
Figure 79: Debug Log Page

### Notes :

- Five levels of Debugging are available, None, Debug, Info, Warning, Error.
- Once the Syslog Server and the level entered, press “Save” and then Reboot the GDS3705 to apply the settings.

## Data Maintenance

This page allows users to manage the GDS3705 configuration file by importing / exporting the configuration files.



**Data Maintenance**

Export System Config Data(Password not included) **Export**

Import **Import**

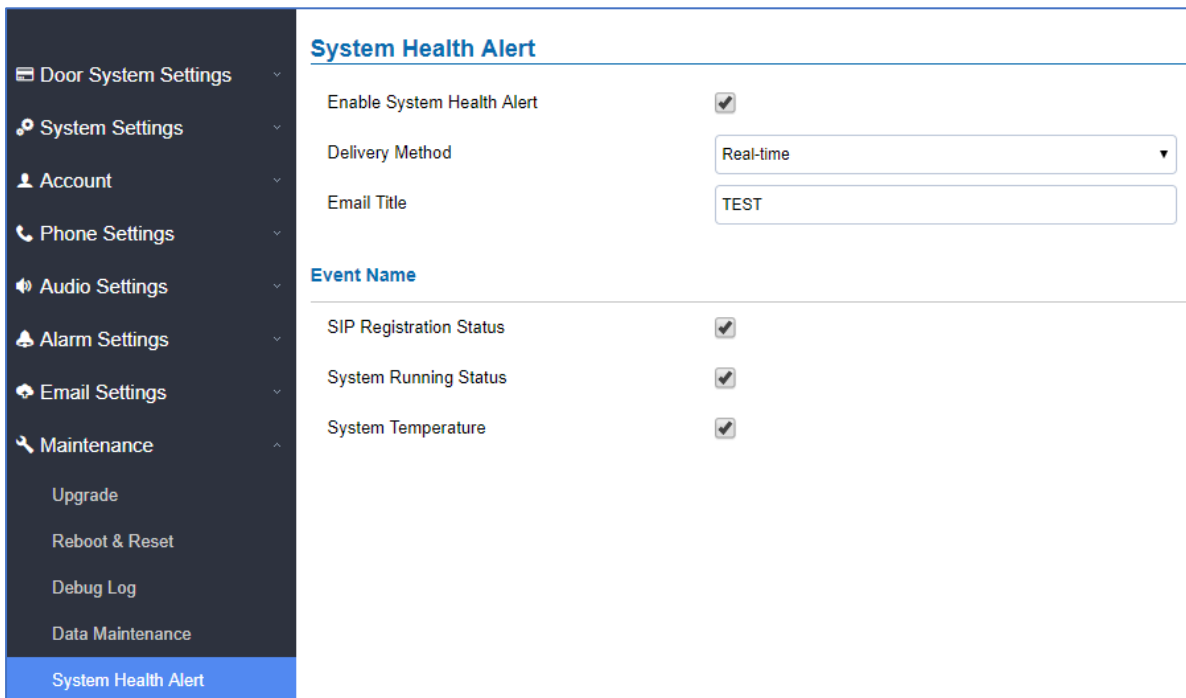
**Figure 80: Data Maintenance Page**

Click on **Export** to save the GDS3705 configuration in a predefined directory.

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

## System Health Alert

This page allows users to enable real-time or periodic email notifications about the GDS system status: Registration, Running Status and Temperature. This will require **Email Settings** already configured.



**System Health Alert**

Enable System Health Alert ☒

Delivery Method Real-time

Email Title TEST

**Event Name**

SIP Registration Status ☒

System Running Status ☒

System Temperature ☒

**Figure 81: System Health Alert Page**



**Table 30: System Health Alert**

<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>	There are two options: <ul style="list-style-type: none"> <li>• Real-Time: the GDS will be sending successively alert emails every second.</li> <li>• Periodic: a Time Interval of 1~10080 minutes between each email can be configured.</li> </ul>
<b>Email Title</b>	This would be the Email Subject title. Maximum characters number is 256.
<b>Event Name</b>	SIP Registration Status: When checked, Email will contain Offline/Online indication for all 4 accounts.
	System Running Status: When checked, Email will contain the system uptime.
	System Temperature: When checked, Email will contain Temperature value of the system in °C and °F, as well as whether the temperature is normal or not.

## Event Notification

This page allows users to configure the event notification details that will be used by GDS3705 to communicate to an HTTP server and Log Events. When the feature Enable and Configured, all the event logs will be uploaded to server: RFID open door, PIN open door, SIP Call, Alarm, etc...

For instance, the GDS3705, after an RFID Card swiping, 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.**

Or, the GDS3705, after making a Call, when doorbell pressed, will send to the configured HTTP server the following HTTP POST containing "Phone call" event:



**POST/HTTP/1.1**

**Host:192.168.6.107**

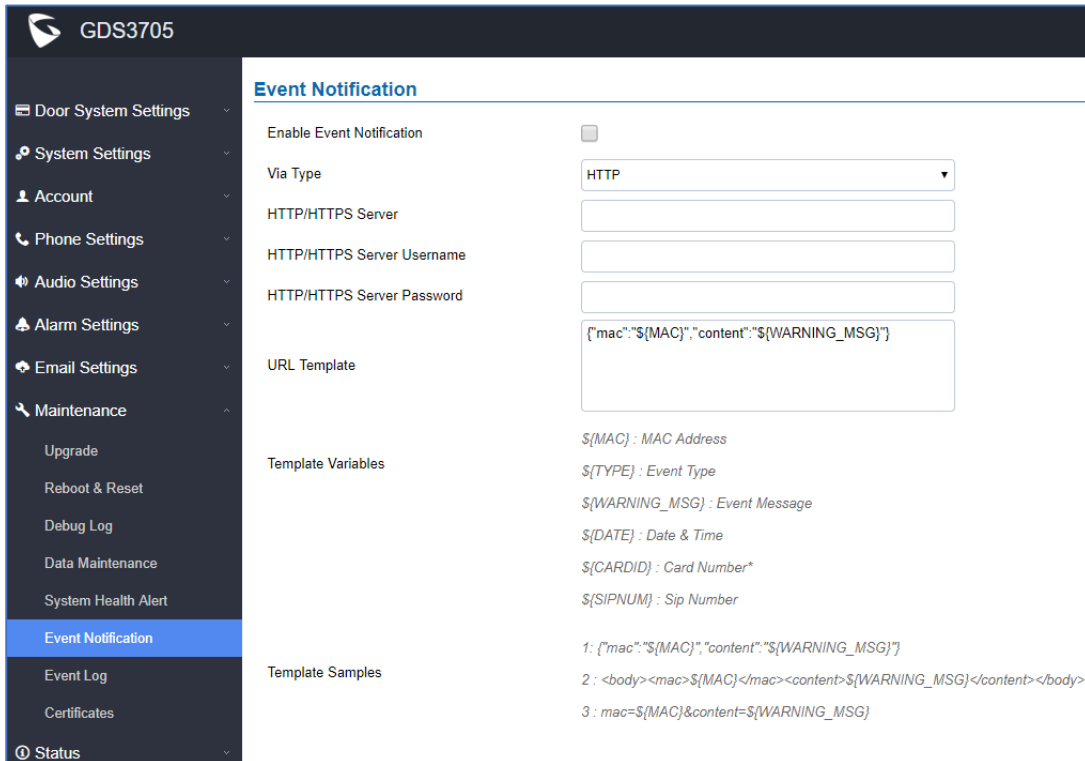
**Authorization:BasicOg==**

**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 GDS3705.



**GDS3705**

**Event Notification**

Enable Event Notification ☐

Via Type

HTTP/HTTPS Server

HTTP/HTTPS Server Username

HTTP/HTTPS Server Password

URL Template

Template Variables

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

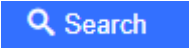
Template Samples

1: ["mac":"\${MAC}","content":"\${WARNING\_MSG}"]  
 2: <body><mac>\${MAC}</mac><content>\${WARNING\_MSG}</content></body>  
 3: mac=\${MAC}&content=\${WARNING\_MSG}

**Figure 82: Event Notification**

## Event Log

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

To get logs for a specific date interface, select the Start Time and End Time, then select which Event type you want to check using the drop-down list, and click on  to display the records.

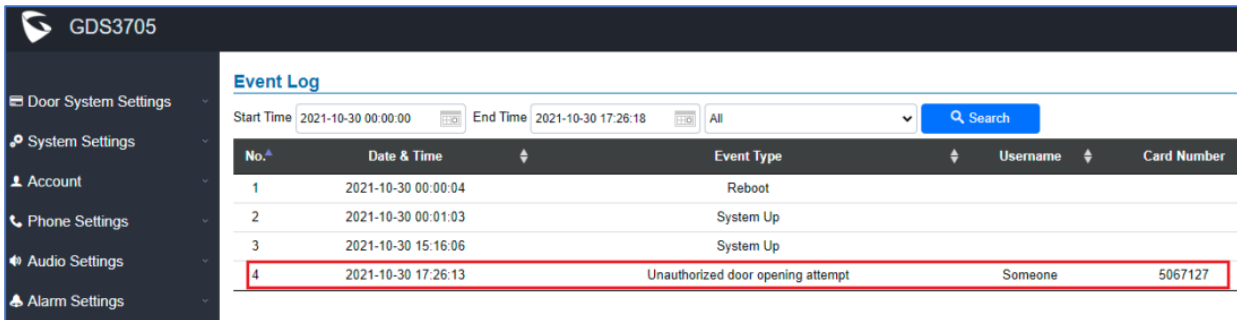
The following Event Types are included for filtering:

OpenDoor (via card, Pin or DI, Card+PIN, remote PIN.).

- Open Door via Card



- Visiting Log
- Open Door via PIN
- Open Door via DI
- Open door by SI
- Call Log
- Open Door via Card and PIN
- Open Door via Remote PIN
- 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
- Unauthorized door opening attempt



No.	Date & Time	Event Type	Username	Card Number
1	2021-10-30 00:00:04	Reboot		
2	2021-10-30 00:01:03	System Up		
3	2021-10-30 15:16:06	System Up		
4	2021-10-30 17:26:13	Unauthorized door opening attempt	Someone	5067127

**Figure 83: Event Log**

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

**Notes:**

- The maximum size of log storage space of GDS3705 is about 3M.
- 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.
- This feature Unauthorized door opening attempt only works when RFID card swiped at the GDS3705. If 3rd party card reader installed and wired into the Wiegand port of GDS3705, the illegal card swiped would not be able to be logged in the Event Log. With this feature implemented, the illegal RFID card swiped via the 3rd party card reader will also be logged and alerted in the Event Log of the GDS3705, as shown in above screenshot.















## 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			 Upload	 Delete
2			 Upload	 Delete
3			 Upload	 Delete
4			 Upload	 Delete
5			 Upload	 Delete
6			 Upload	 Delete

**Custom Certificate**








No.	Issued By	Expiration		
1			 Upload	 Delete


Figure 84: Upload Certificate files

In order to upload your Trusted CA certificate:


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

**Trusted CA Certificates**

No.	Issued By	Expiration		
1	-	2018-07-17 15:46:03	 Upload	 Delete
2			 Upload	 Delete


User could press  Delete to delete one of the files.

In order to upload your Custom certificate:

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



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.

## Status

This page displays GDS3705 accounts, 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**

Door System Settings

System Settings

Account

Phone Settings

Audio Settings

Alarm Settings

Email Settings

Maintenance

Status

Account Status

Account Status

Account	SIP User ID	SIP Server	SIP Registration Status
Account 1	1007	192.168.5.114	Online
Account 2	1008	192.168.5.114	Online
Account 3	1009	192.168.5.114	Online
Account 4	1010	192.168.5.114	Offline

Figure 85: Account Status Page

## System Info

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

System Info	
Product Model	GDS3705
Hardware Version	V1.0A
Part Number	9630001610A
Boot Version	1.0.0.41
Core Version	1.0.0.41
Base Version	1.0.0.41
Prog Version	1.0.0.41
System Uptime	9 minutes
Firmware Status	<div>Press check button and reload page to check firmware availability.</div> <div>Check</div>
System Temperature	39°C (102.2°F)
Tamper Sensor	Triggered
Door 1 Ctrl	Untriggered
Door 2 Ctrl	Untriggered
Digit Input 1	Untriggered
Digit Input 2	Untriggered

**Figure 86: System Info Page**

**Table 31: System Info**

<b>Product Model</b>	Displays the Product Model.
<b>Hardware Version</b>	Displays the Hardware Version.
<b>Part Number</b>	Displays the Part Number.
<b>Boot Version</b>	Displays the Boot Version.
<b>Core Version</b>	Displays the Core Version.
<b>Base Version</b>	Displays the Base Version.
<b>Prog Version</b>	Displays the Prog Version.
<b>System UpTime</b>	Displays the time since the first boot of the GDS3705.
<b>Firmware Status</b>	Click the <div>Check</div> button to check whether the firmware in the firmware server has an updated version, if so, update immediately.



<b>System Temperature</b>	Shows the current system temperature ( in °C and °F)
<b>Tamper Sensor</b>	Shows if the Tamper Sensor is triggered or not.
<b>Door Control</b>	Shows if the door control is triggered or not (in case door is opened for example it will show triggered
<b>Door 1 Ctrl</b>	Shows if Door 2 is opened.
<b>Door 2 Ctrl</b>	Shows if Door 2 is opened.
<b>Input Digit 1</b>	Shows if Alarm-IN 1 is triggered.
<b>Input Digit 2</b>	Shows if Alarm-IN 2 is triggered.
<b>Digit Output</b>	Shows if digital output is triggered.

## Network Info

This page displays the network system information of GDS3705.

Door System Settings

System Settings

Account

Phone Settings

Audio Settings

Alarm Settings

Email Settings

Maintenance

Status

Account Status

System Info

Network Info

### Network Info

MAC Address	00:0B:82:8B:5E:EF
IP Address Mode	Static IP
IP Address	192.168.5.187
Subnet Mask	255.255.255.0
Gateway	192.168.5.1
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4

Figure 87: Network Info Page



**Table 32: Network Info**

<b>MAC Address</b>	Displays the GDS3705 MAC Address.
<b>IP Address Mode</b>	Displays the IP address mode used.
<b>IP Address</b>	Displays the IP address of the GDS3705.
<b>Subnet Mask</b>	Displays the Subnet Mask used.
<b>Gateway</b>	Displays the GDS3705 Gateway.
<b>DNS Server 1</b>	Displays the Preferred DNS Server.
<b>DNS Server 2</b>	Displays the secondary DNS Server.



## FACTORY RESET

### Restore to Factory Default Via Web GUI

To perform factory reset to the GDS3705 via the Web GUI, please refer to following steps:

1. Access to GDS3705 Web GUI using the using the shipped default password.
2. Navigate to **Maintenance → Reboot & Reset**.
3. Select the reset type from Rest drop down menu and press reset button as displayed on the following screenshot.

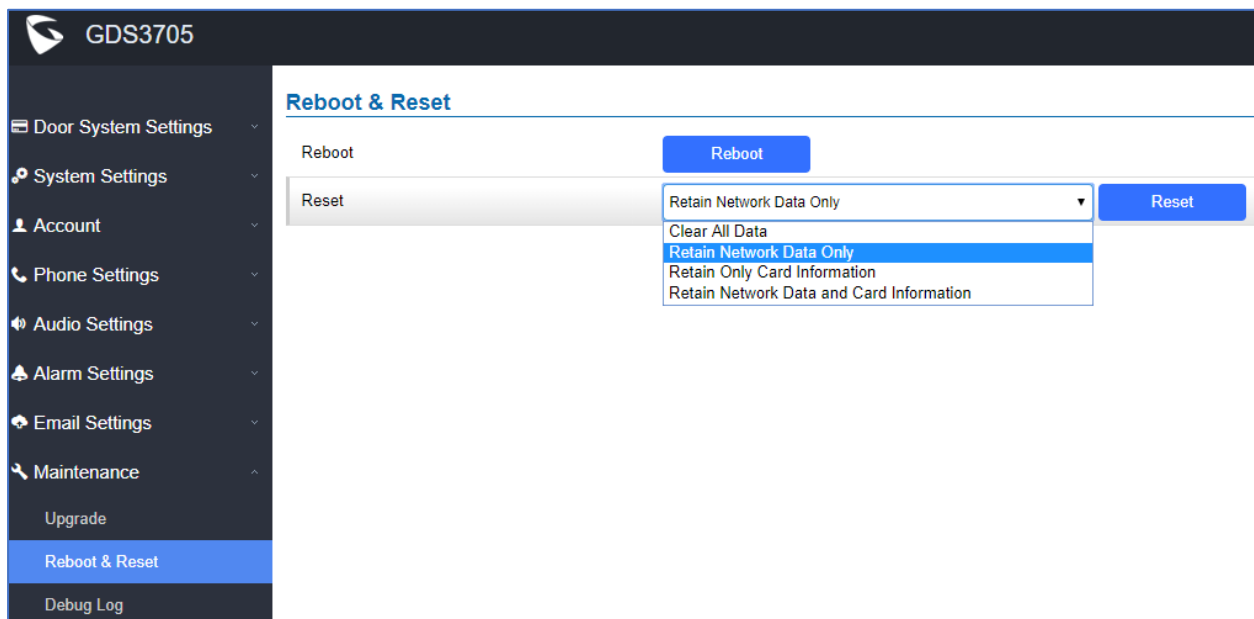


Figure 88: Reset via Web GUI

### Hard Factory Reset

Some users did not keep the revised password safely and forgot the changed password. Due to GDS3705 did NOT have built-in reset button (Grandstream purposely designed this way to enhance security), this will make the GDS3705 inaccessible even for the true owner who lost the changed password.

Below is a photo of the normal connection of the provided Wiegand cable.

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





Figure 89: Wiegand Interface Cable

To perform hard factory reset to the GDS3705, please refer to following steps:

1. Power OFF the GDS3705.
2. Take the provided Wiegand cable, connect (or shorting) the related color wires as illustrated on the following picture. Please make sure the connection is correct and solid:
  - Connect **WHITE** and **BROWN** cable together.
  - Connect **GREEN** and **ORANGE** cable together.

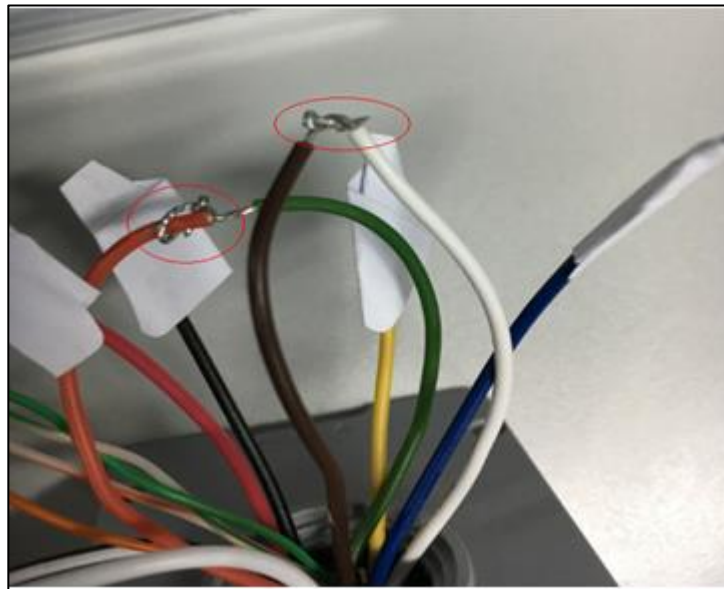


Figure 90: Wiegand Cable Connection

3. Power ON the GDS3705. 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 GDS3705 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 GDS3705 will play short beep quickly three times illustrating error. Nothing will happen and the GDS3705 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 GDS3705 will finish performing the reset process, then the user can log into the GDS3705 web GUI using the shipped default password.
  5. User must power OFF the GDS3705, unplug the Wiegand cable, power ON the GDS3705 again and make sure the GDS3705 is running correctly.

## Restore to Factory Default Via SIP NOTIFY

1. Access your GDS3705 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 GDS3705 will perform factory reset after authentication phase.

**Note:** 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).



## Reset Factory Password Via Special Key Combination Operation

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

### NOTE:

1. MAC address of the GDS3705 (check the sticker at back of the device)
2. Default password of the GDS3705 (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 GDS3705 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, GDS3705 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.
- 7) After successful password reset, operator will then be able to log into the GDS3705 webUI with default password, all the configuration inside the device will be the same and will NOT be changed.

**For example:**

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

*Device with last 6 MAC address: **33DDDD***

*Decoding the last 6 MAC to digits would be: **334444***

*Default password is: **xwpxz6AA***

*Decoding the default password to digits would be: **2423162426611***

- 1) Enter **\*\*\*334444\*\*#** via keypad, get into the password reset mode, the keypad backlight will flash quickly.
- 2) Within 60 seconds, enter **2423162426611#**, the device will play one long beep then reboot itself.
- 3) Wait the device finishing boot up, log in the webUI using the default password, **xwpxz6AA**



## EXPERIENCING THE GDS3705

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

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

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

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

