

Grandstream Networks, Inc.

GDS3705

Audio Door Access System

User Manual



COPYRIGHT

©2018 Grandstream Networks, Inc. <http://www.grandstream.com>

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

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

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

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

CAUTION

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

WARNING

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



FCC Compliance Statement

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

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

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

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

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

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

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



CE Declaration of Conformity

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

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

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

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



Manufacturer:

Grandstream Networks, Inc.

126 Brookline Ave, 3rd Floor Boston, MA 02215, USA

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

GNU GPL INFORMATION

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



Table of Contents

CHANGE LOG	13
Firmware Version 1.0.0.35	13
Firmware Version 1.0.0.31	13
Firmware Version 1.0.0.28	13
Firmware Version 1.0.0.26	13
Firmware Version 1.0.0.20	14
DOCUMENT PURPOSE	15
WELCOME	16
PRODUCT OVERVIEW	17
Feature Highlights	17
Technical Specifications	17
GETTING STARTED	19
Equipment Packaging	19
Description of the GDS3705	20
Connecting and Setting up the GDS3705	20
GDS3705 Wiring Connection	21
GDS3705 Back Cover Connections	22
Connection Example	22
<i>Power GDS3705 using PoE</i>	<i>23</i>
<i>Power GDS3705 using PSU</i>	<i>23</i>
GETTING TO KNOW GDS3705	24
Connecting GDS3705 to Network with DHCP Server	24
<i>Windows Platform</i>	<i>24</i>
UPnP	24
GS Search	25
GDS Manager Utility Tool	26



Connect to the GDS3705 using Static IP.....	27
GDS3705 APPLICATION SCENARIOS	29
Peering Mode without SIP Server.....	29
Peering using SIP Server (UCM6XXX).....	29
GDS3705 PERIPHERAL CONNECTIONS	31
Alarm IN/OUT	32
Protection Diode	33
Connection Examples	33
<i>Wiring Sample using 3rd Party Power Supply</i>	<i>34</i>
<i>Wiring Sample using Power Supply for both GDS3705 and Electric Strike</i>	<i>34</i>
<i>Wiring Sample using PoE to power GDS3705 and 3rd Party Power Supply for Electric Strike....</i>	<i>35</i>
<i>Good Wiring Sample for Electric Strike and High-Power Device</i>	<i>36</i>
Wiegand Module Wiring Examples.....	36
<i>Input example with 3rd party power supply for Wiegand device</i>	<i>36</i>
<i>Input example with power supply for both GDS3705 and Wiegand device</i>	<i>37</i>
<i>Output example with 3rd party power supply for Wiegand device</i>	<i>38</i>
<i>Wiegand RFID Card Reader Example</i>	<i>38</i>
GDS3705 HOME WEB PAGE.....	39
GDS3705 SETTINGS.....	40
Door System Settings	40
<i>Basic Settings</i>	<i>40</i>
<i>Keep Door Open</i>	<i>45</i>
<i>Card Management</i>	<i>47</i>
<i>Add Users Manually</i>	<i>47</i>
<i>Add Users Automatically</i>	<i>49</i>
<i>Users Operation</i>	<i>49</i>
<i>Group</i>	<i>50</i>
<i>Schedule</i>	<i>50</i>
<i>Holiday</i>	<i>51</i>



System Settings	52
<i>Date & Time Settings</i>	52
<i>Network Settings</i>	53
<i>Access Settings</i>	54
<i>User Management</i>	56
<i>Factory Functions</i>	58
Account	59
<i>Account 1 - 4</i>	59
Phone Settings	61
<i>Phone Settings</i>	61
<i>Account [1-4] White List</i>	63
Audio Settings	64
<i>Audio Settings</i>	64
Alarm Config	64
<i>Alarm Events Config</i>	64
<i>Input Digit</i>	65
<i>Alarm Output</i>	66
<i>Silently Alarm Mode</i>	66
<i>Hostage Code</i>	67
<i>Tamper Alarm</i>	67
<i>Keypad Input Error Alarm</i>	67
<i>Non-Scheduled Access Alarm</i>	67
<i>Alarm Schedule Settings</i>	68
<i>Alarm Action Settings</i>	69
<i>Alarm Phone List</i>	71
Email Settings	72
<i>Email Settings</i>	72
Maintenance Settings	73
<i>Upgrade</i>	73
<i>Reboot & Reset</i>	74
<i>Debug Log</i>	75
<i>Data Maintenance</i>	76



<i>Event Notification</i>	77
<i>Event Log</i>	78
<i>Trusted CA Certificates</i>	79
Status	80
<i>Account Status</i>	80
<i>System Info</i>	81
<i>Network Info</i>	82
FACTORY RESET	84
Restore to Factory Default Via Web GUI	84
Hard Factory Reset	84
EXPERIENCING THE GDS3705	87



Table of Tables

Table 1: GDS3705 Features in a Glance	17
Table 2: GDS3705 Technical Specifications	17
Table 3: Equipment Packaging	19
Table 4: GDS3705 Wiring Connection	21
Table 5: Door System Settings.....	41
Table 6: Immediate Door-Open Table	46
Table 7: Schedule Keep Door Open	46
Table 8: Card Info	48
Table 9: Add Group	50
Table 10: Date & Time.....	52
Table 11: Basic Settings	53
Table 12: Access Settings	55
Table 13: User Management.....	56
Table 14: User Management.....	58
Table 15: SIP Account Basic & Advanced Settings.....	60
Table 16: Phone Settings	62
Table 17: White List.....	63
Table 18: Audio Settings.....	64
Table 19: Input Digit	66
Table 20: Silently Alarm Mode.....	66
Table 21: Hostage Code Alarm	67
Table 22: Tamper Alarm	67
Table 23: Keypad Input Error Alarm	67
Table 24: Non-Scheduled Access Alarm	67
Table 25: Alarm Actions.....	70
Table 26: Alarm Phone List	71
Table 27: Email Settings - SMTP	72
Table 28: Upgrade.....	74
Table 29: Reset & Reboot	75
Table 30: System Info.....	82
Table 31: Network Info	83



Table of Figures

Figure 1: GDS3705 Package	19
Figure 2: GDS3705 Front View	20
Figure 3: GDS3705 Back View	20
Figure 4: GDS3705 Back Cover Connections	22
Figure 5: GDS3705 Back Cover	22
Figure 6: Connection Example.....	23
Figure 7: Powering the GDS3705	23
Figure 8: Detecting GDS3705 via UPnP	24
Figure 9: GDS3705 Login Page	25
Figure 10: GS Search Discovery	26
Figure 11: GDS3705 Detection using GDS Manager	27
Figure 12: Static IP on Windows	28
Figure 13: Peering GDS3705 with UCM6XXX.....	30
Figure 14: Peripheral Connections for GDS3705	31
Figure 15: Alarm_In/Out Circuit for GDS3705.....	32
Figure 16: Protection Diode - Example 1	33
Figure 17: Protection Diode - Example 2.....	33
Figure 18: 3 rd party Power Supply Wiring Sample	34
Figure 19: Power Supply used for both GDS3705 and Electric Strike	34
Figure 20: Wiring Sample using PoE to power GDS3705 and 3 rd party Power Supply for Electric Strike .	35
Figure 21: Example to Avoid when Powering the Electric Strike	35
Figure 22: Electric Strike and High-Power Device Example.....	36
Figure 23: Wiegand Input Example with 3 rd party Power Supply.....	36
Figure 24: Wiegand Input Example with Power Supply for GDS3705 and Wiegand Device	37
Figure 25: Wiegand Output Wiring Example.....	38
Figure 26: Wiegand RFID Card Reader Example	38
Figure 27: Change Language Page.....	39
Figure 28: Door System Settings Page.....	40
Figure 29: Keep Door Open	45
Figure 30: Immediate Door Open	45
Figure 31: Schedule Door Open	46
Figure 32: Modify Schedule	47
Figure 33: Card Management	47
Figure 34: Card Info	48
Figure 35: Add Group.....	50
Figure 36: Groups List.....	50
Figure 37: Edit Schedule Time	51
Figure 38: Edit Holiday Time	51
Figure 39: Date & Time Page.....	52



Figure 40: Basic Settings Page.....	53
Figure 41: Access Settings Page	55
Figure 42: User Management Page	56
Figure 43: Recover Password.....	57
Figure 44: Recover Password - Email Address	57
Figure 45 : Factory Functions Page.....	58
Figure 46: SIP Account Settings Page.....	59
Figure 47: Phone Settings Page	62
Figure 48: White List Page.....	63
Figure 49: Audio Settings Page	64
Figure 50: Events Page.....	65
Figure 51: Input Digit.....	65
Figure 52: Alarm Schedule.....	68
Figure 53: Edit Schedule	69
Figure 54: Alarm Action	70
Figure 55: Edit Alarm Action.....	70
Figure 56: Alarm Phone List.....	71
Figure 57: Email Settings - SMTP Page	72
Figure 58: Upgrade Page.....	73
Figure 59: Reset & Reboot Page	75
Figure 60: Debug Log Page	76
Figure 61: Data Maintenance Page	77
Figure 62: Event Notification.....	78
Figure 63: Event Log.....	79
Figure 64: Upload Trusted CA files	80
Figure 65: Account Status Page	81
Figure 66: System Info Page.....	81
Figure 67: Network Info Page	83
Figure 68: Reset via Web GUI	84
Figure 69: Wiegand Interface Cable	85
Figure 70: Wiegand Cable Connection	86



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 1.0.0.35

- 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 “Test” button for Alarm Action. [Alarm Action Settings]
- 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]

Firmware Version 1.0.0.26

- Added displaying logs at device Web UI. [Event Log]
- Added ability to upload Trusted CA certificate files. [Validate Server Certificate]
- Added option to enable/disable certificate validation. [Trusted CA Certificates]
- 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 <http://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"> • 4 SIP accounts and 4 lines. • Broad interoperability with most 3rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms. • 2 Channels Input/Output alarm. • RS485, Wiegand (26 bits) Input and Output. • RFID card reader. • Weather proof, vandal resistant.
---	---

Technical Specifications

The following table resumes all the technical specifications including the protocols / standards supported, voice codecs, telephony features and upgrade/provisioning settings for GDS3705.

Table 2: GDS3705 Technical Specifications

Network Protocols	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS local upload and mass provisioning using TR-069 (pending), ARP/RARP, ICMP, DNS, DHCP, SSH, SMTP, NTP, STUN, TLS, SRTP.
SIP/VoIP Support	Broad interoperability with most 3 rd party SIP/VoIP devices and leading SIP/NGN/IMS platforms.
Voice Codecs	G.711 μ /a-law, G.722, DTMF (in audio, RFC2833, SIP INFO), AEC.
QoS	Layer 2 QoS (802.1Q, 802.1P).
Security	User and administrator level access control (pending), MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1Q.
Upgrade / Provisioning	Firmware upgrade via HTTP/HTTPS, mass provisioning using TR-069 (Pending) or AES encrypted XML configuration file.
Audio Input	Integrated dual microphones.
Audio Output	Built-in HD Loudspeaker (2 Watt), sound quality suitable for up to 3 m.
Keypad / Buttons	12-Metal Keys plus a Metal doorbell button.
RFID	125KHz: EM4100 (1 RFID card and 1 RFID key fob included).



Alarm Input	Yes, 2 channels, $V_{in} < 15V$, for door sensor or other devices.
Alarm Output	Yes, 2 channels, 125VAC/0.5A, 30VDC/2A, Normal Open or Normal Close, for electric lock, light switch or other devices.
Network Interface	10M/100M auto-sensing.
Expansion Interface	RS485, Wiegand (26 bits) input and output.
Dimensions and Weight	173mm(H) x 80mm(W) x 36mm(D). 0.6 Kg.
Power Supply	PoE (Power over Ethernet) IEEE 802.3af Class 3, or 12VDC/1A connection (AC power adapter not included).
Ingress Protection	Weather proof, vandal resistant, with support for extra back reinforcing metal plate
Temperature and Humidity	Operation: $-30^{\circ}C$ to $60^{\circ}C$ ($-22^{\circ}F$ to $140^{\circ}F$) Storage: $-35^{\circ}C$ to $60^{\circ}C$ ($-31^{\circ}F$ to $140^{\circ}F$) Humidity: 10% to 90% Non-condensing
Protection Class	IP66 (EN60529), IK09 (IEC62262).
Compliance	 FCC: Part 15; Subpart B; Subpart C; MPE CE: 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 RCM: AS/NZS CISPR 22/24; AS/NZS 4268; AS/NZS 60950.1 IC: ICES-003; RSS310

GETTING STARTED

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

Equipment Packaging

Table 3: Equipment Packaging

<ul style="list-style-type: none"> • 1 x GDS3705 • 1 x Installation Bracket • 1 x Drilling Template • 3 x Rubber Gaskets (for sealing the back cable) • 6 x Back Panel Screws • 6 x Bracket Screws and Anchors • 4 x Anti-tamper screws • 1 x Anti-Tamper Hex Key 	<ul style="list-style-type: none"> • 1 x Wiegand Cable • 1 x RFID Card (more can be purchased from Partner/reseller) • 1 x Key Fob (more can be purchased from Partner/reseller) • 1 x Frame Back Cover • 1 x Quick Installation Guide • 1 x GPL License
---	--



Figure 1: 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:

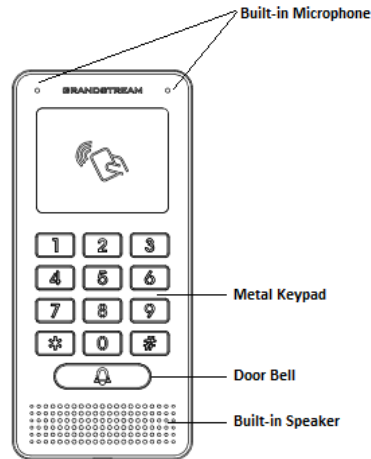


Figure 2: GDS3705 Front View

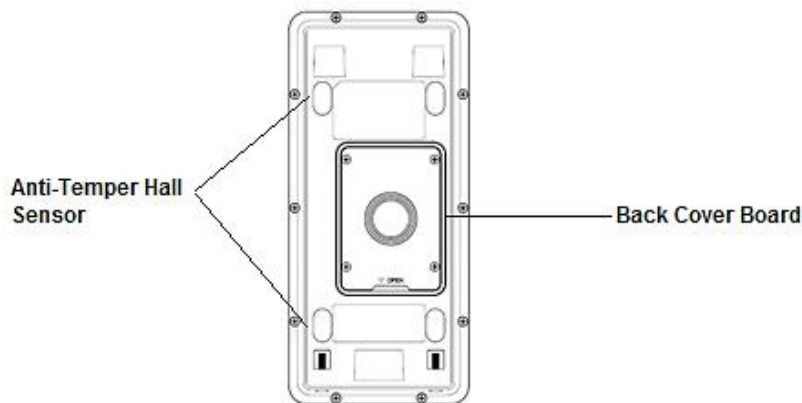


Figure 3: GDS3705 Back View

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 COM2 & NO2 . For " Fail Safe " (Open when No Power) Magnetic Lock, connect COM2 & NC2 . Relay: 30VDC/2A; 125VAC/0.5A	
	COM2			
	NC2			
J4 (Special) 2.0mm	GND	Wiegand Power GND	Black	Both Input and Output MUST be connected
	WG_D1_OUT	Wiegand Output Signal	Orange	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

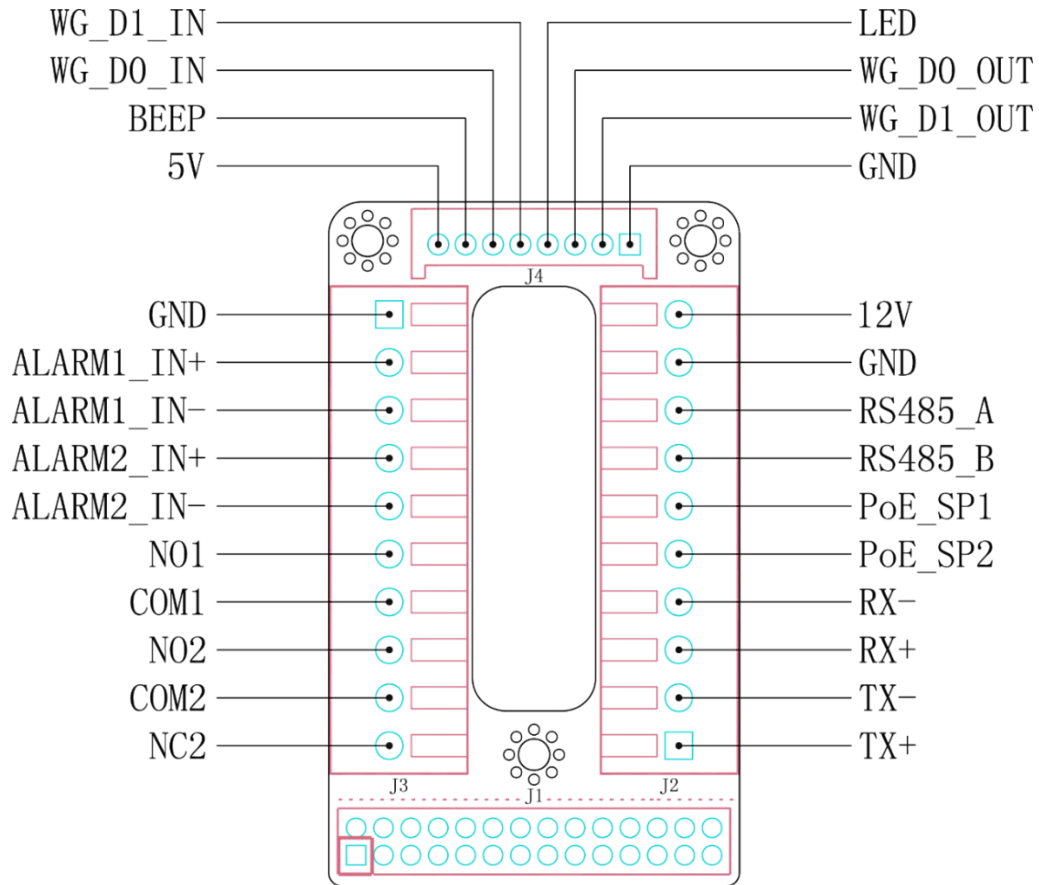


Figure 4: GDS3705 Back Cover Connections

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.

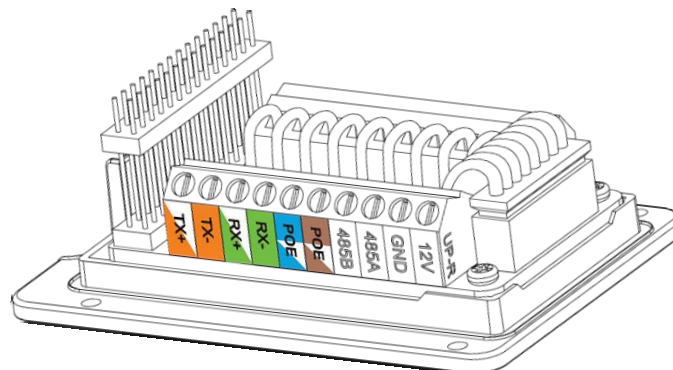


Figure 5: GDS3705 Back Cover

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.

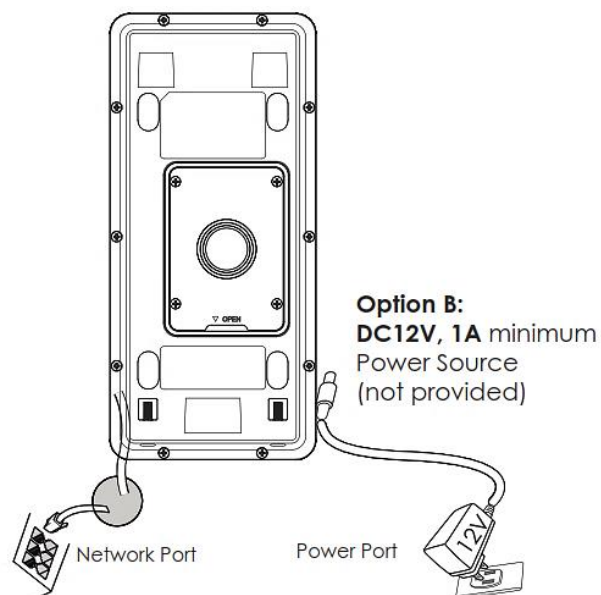


Figure 7: Powering the GDS3705

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

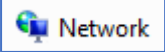
The GDS3705 by default has a DHCP client enabled, it will automatically get IP address from DHCP server.

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.

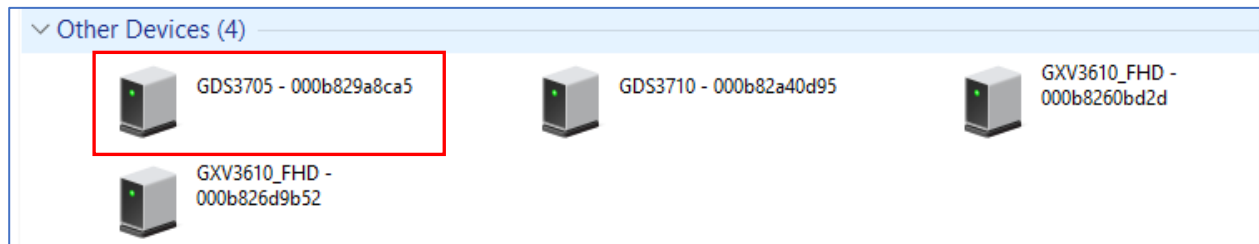


Figure 8: Detecting GDS3705 via UPnP

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.

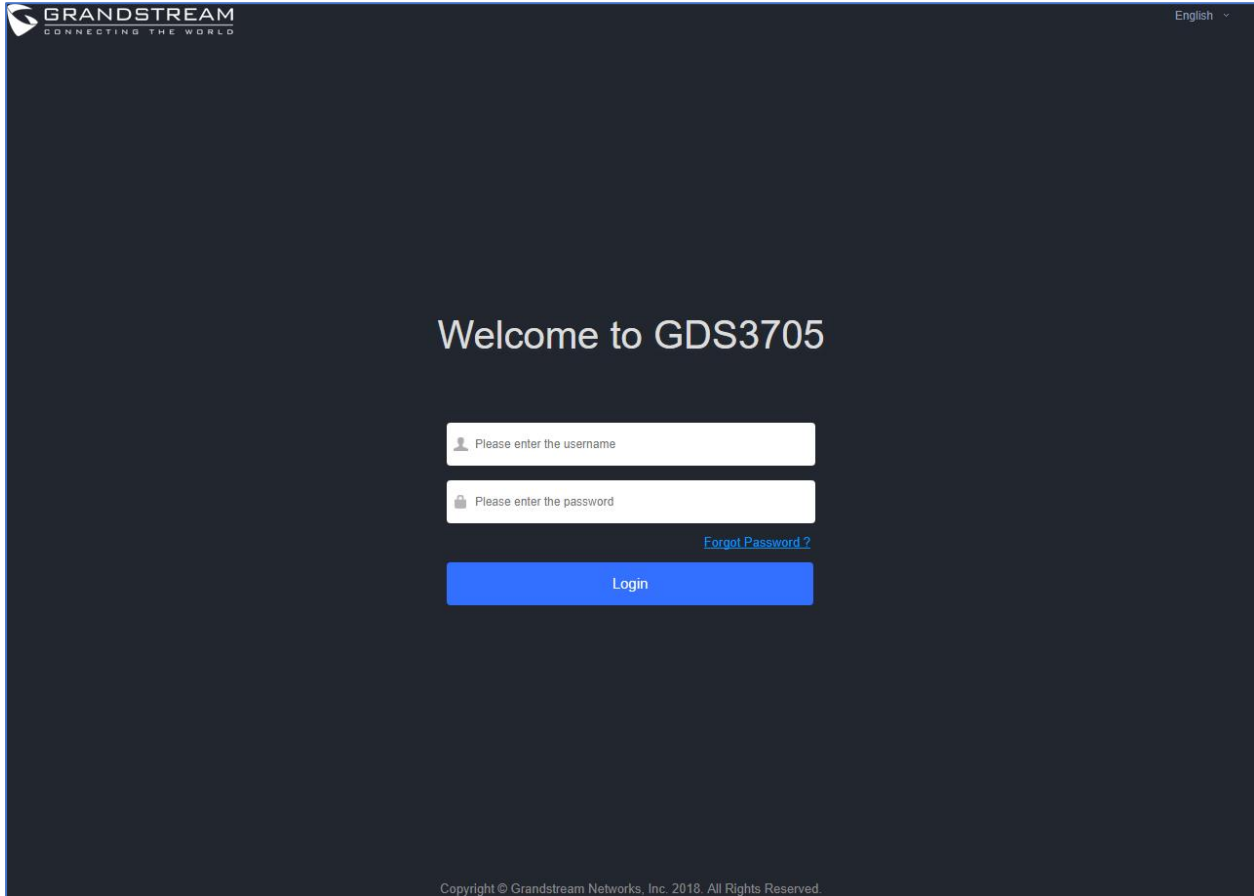

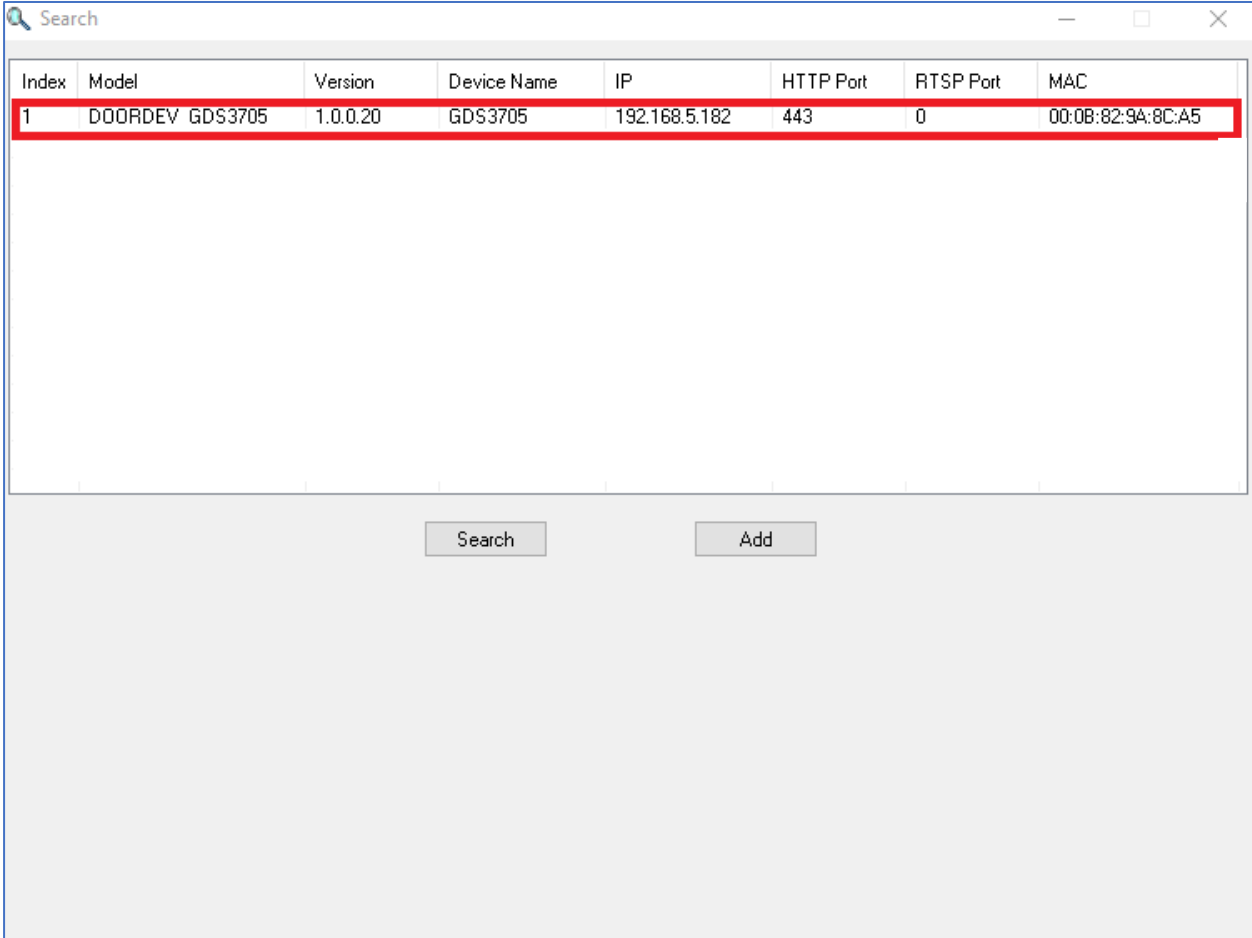


Figure 9: GDS3705 Login Page

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:
http://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

Figure 10: GS Search Discovery


- Double click on a device to access its webGUI.

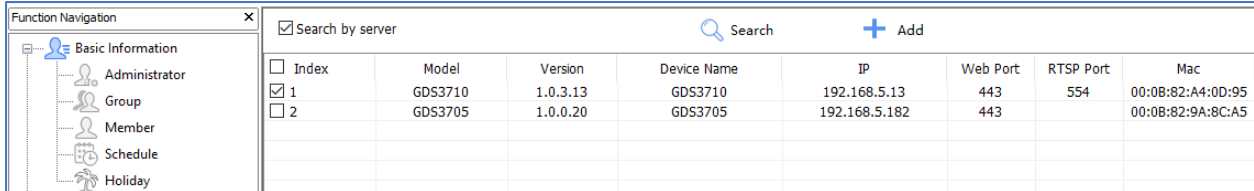
GDS Manager Utility Tool

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



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



Index	Model	Version	Device Name	IP	Web Port	RTSP Port	Mac
<input checked="" type="checkbox"/> 1	GDS3710	1.0.3.13	GDS3710	192.168.5.13	443	554	00:08:82:A4:0D:95
<input type="checkbox"/> 2	GDS3705	1.0.0.20	GDS3705	192.168.5.182	443		00:08:82:9A: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:



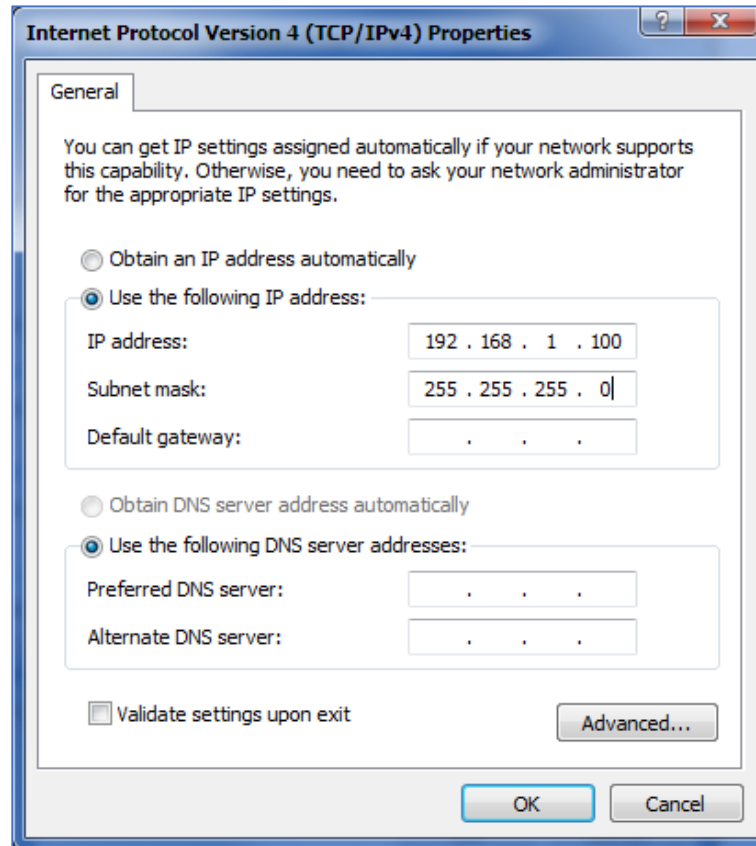


Figure 12: Static IP on Windows

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



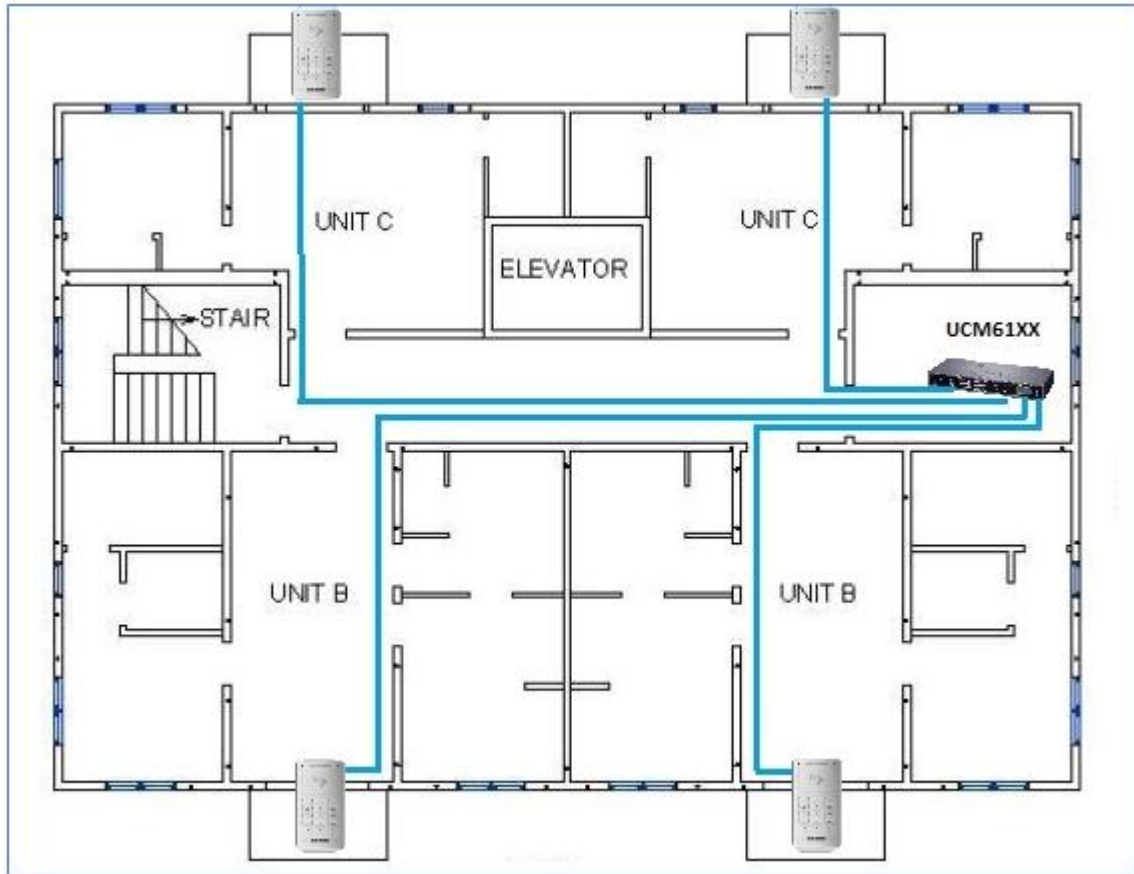


Figure 13: Peering GDS3705 with UCM6XXX

GDS3705 PERIPHERAL CONNECTIONS

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

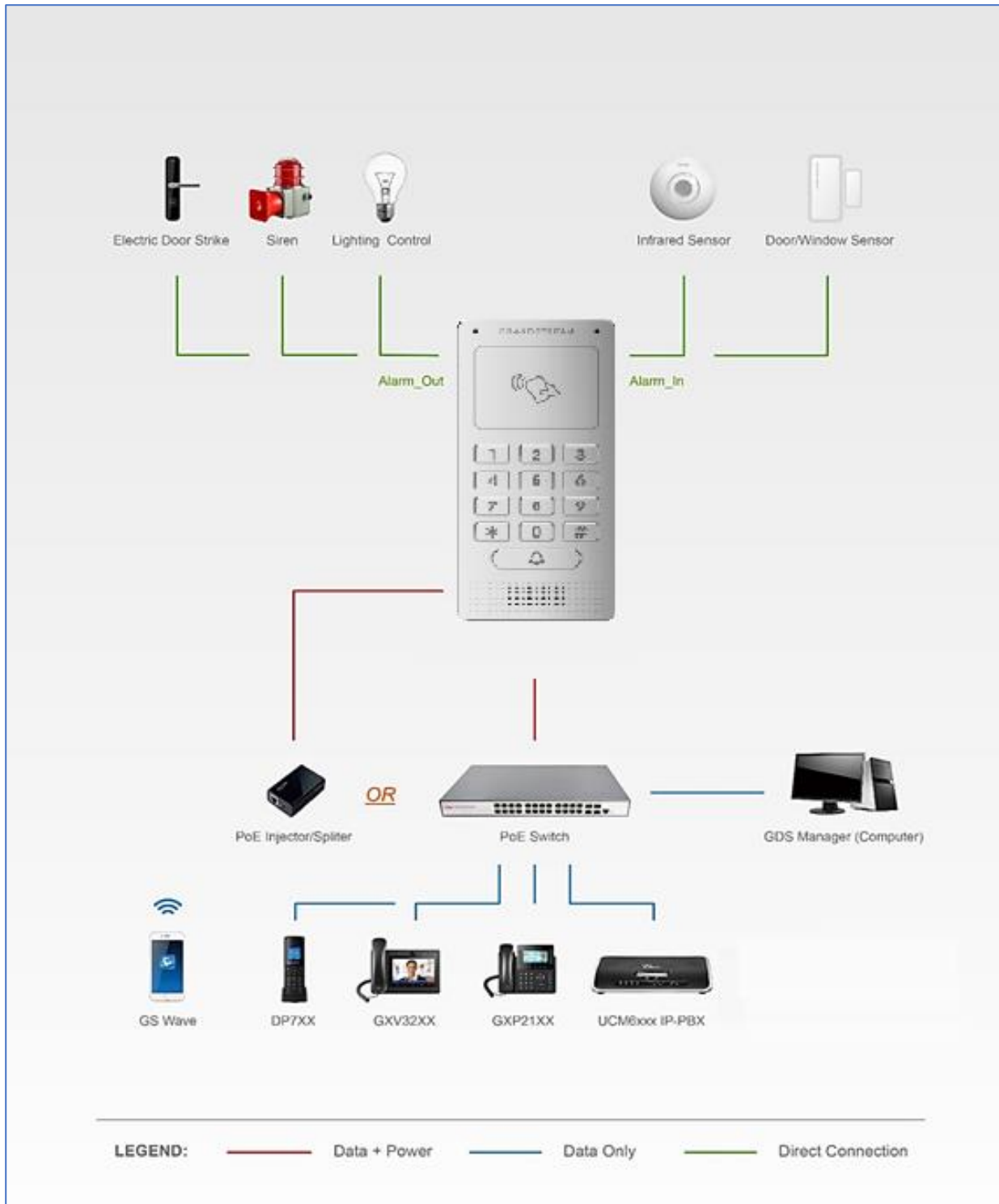


Figure 14: Peripheral Connections for GDS3705

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.

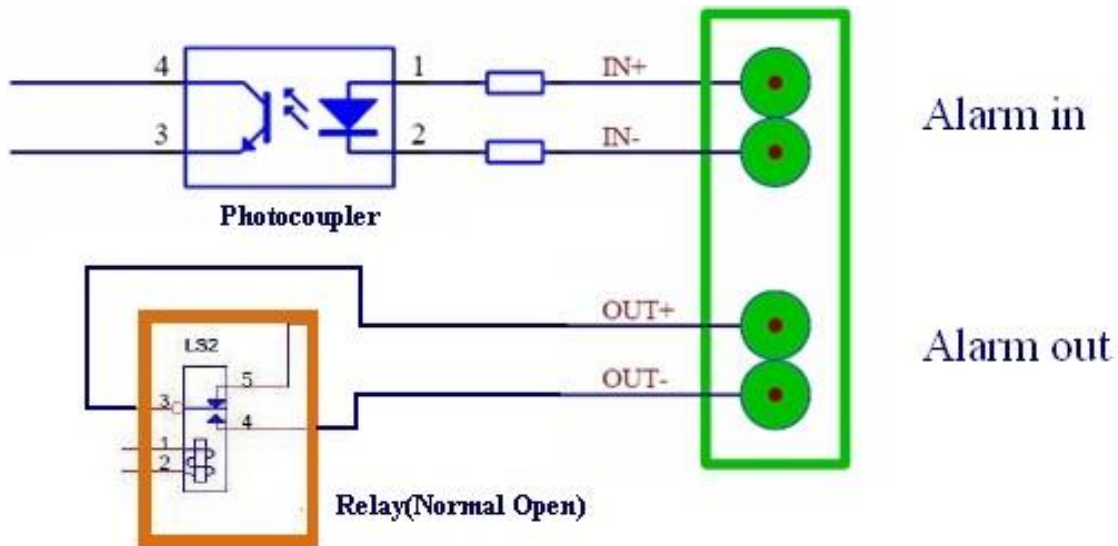


Figure 15: Alarm_In/Out Circuit for GDS3705

Notes:

- The Alarm_In and Alarm_Out circuit for the GDS3705 should meet the following requirement:

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

- The Alarm_In circuit, if there is any voltage change between 3V and 15V, as specified in the table above, the 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.

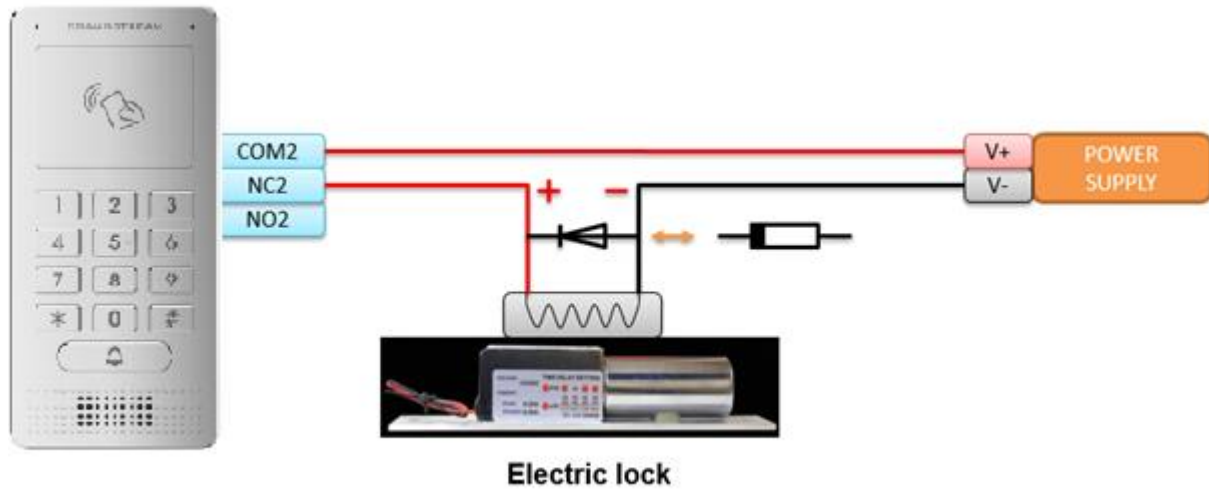


Figure 16: Protection Diode - Example 1

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

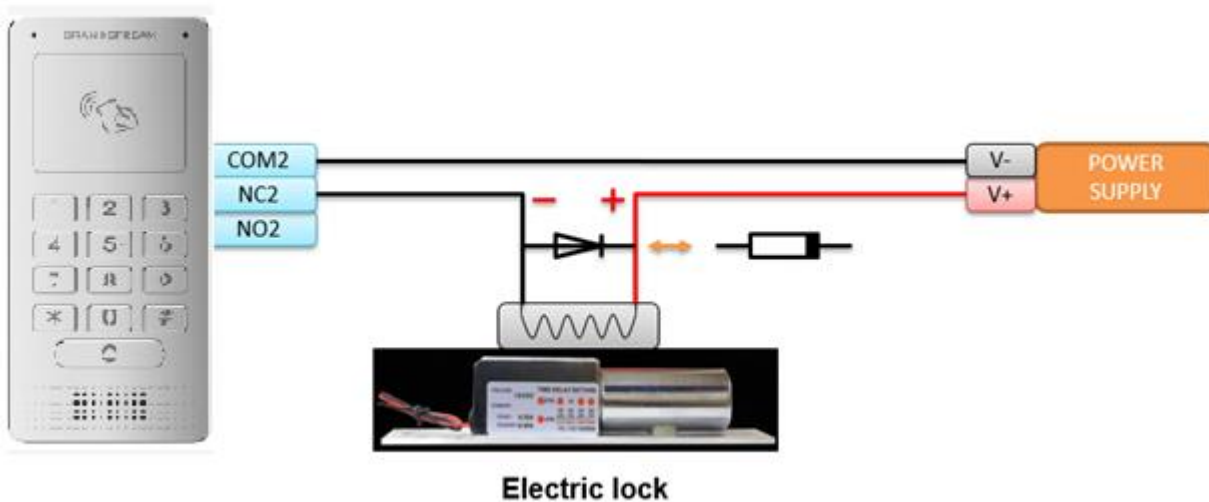


Figure 17: Protection Diode - Example 2

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 3rd Party Power Supply

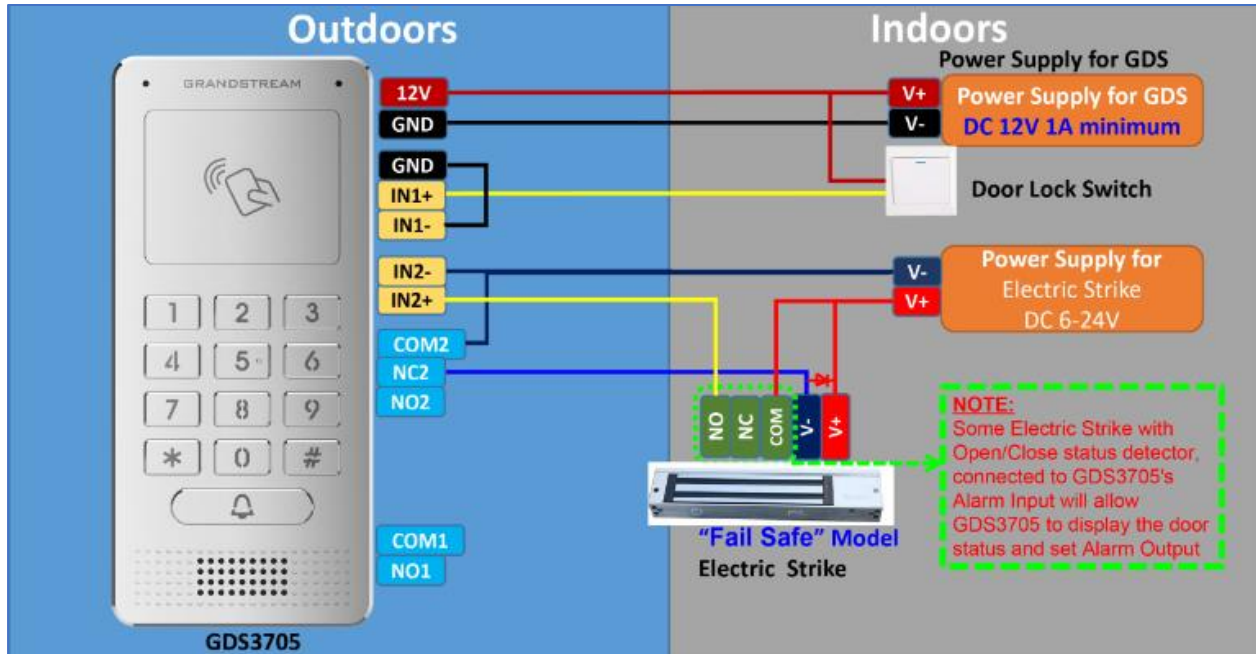


Figure 18: 3rd party Power Supply Wiring Sample

Wiring Sample using Power Supply for both GDS3705 and Electric Strike

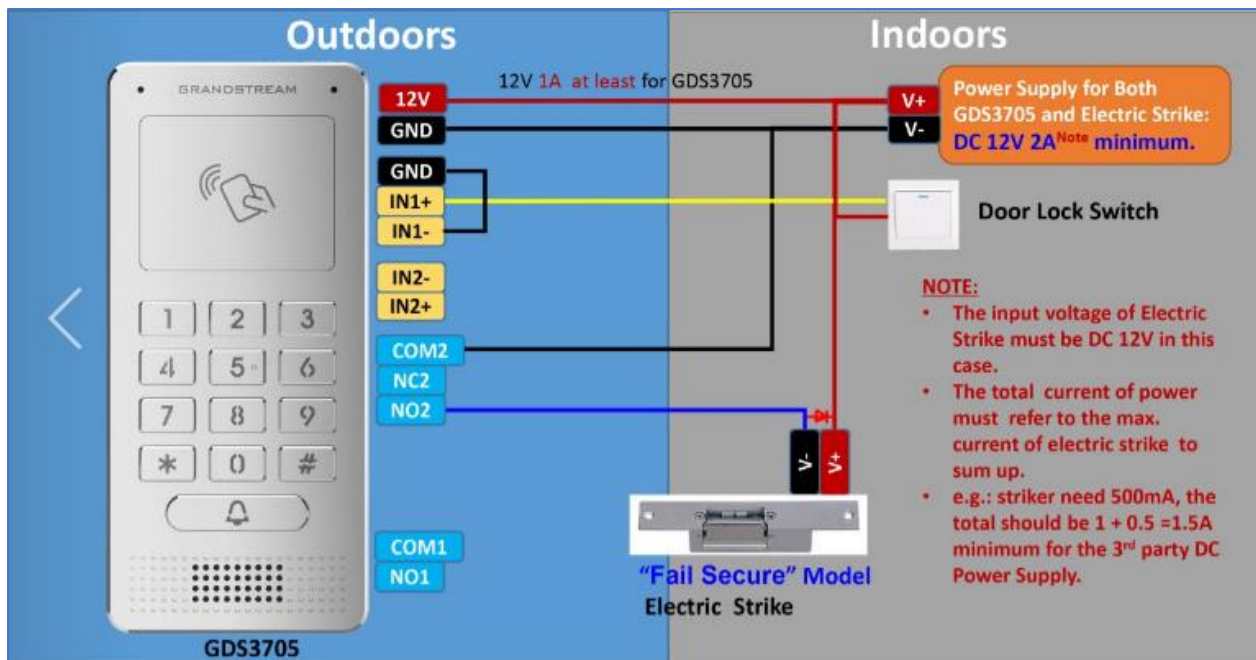


Figure 19: Power Supply used for both GDS3705 and Electric Strike

Wiring Sample using PoE to power GDS3705 and 3rd Party Power Supply for Electric Strike

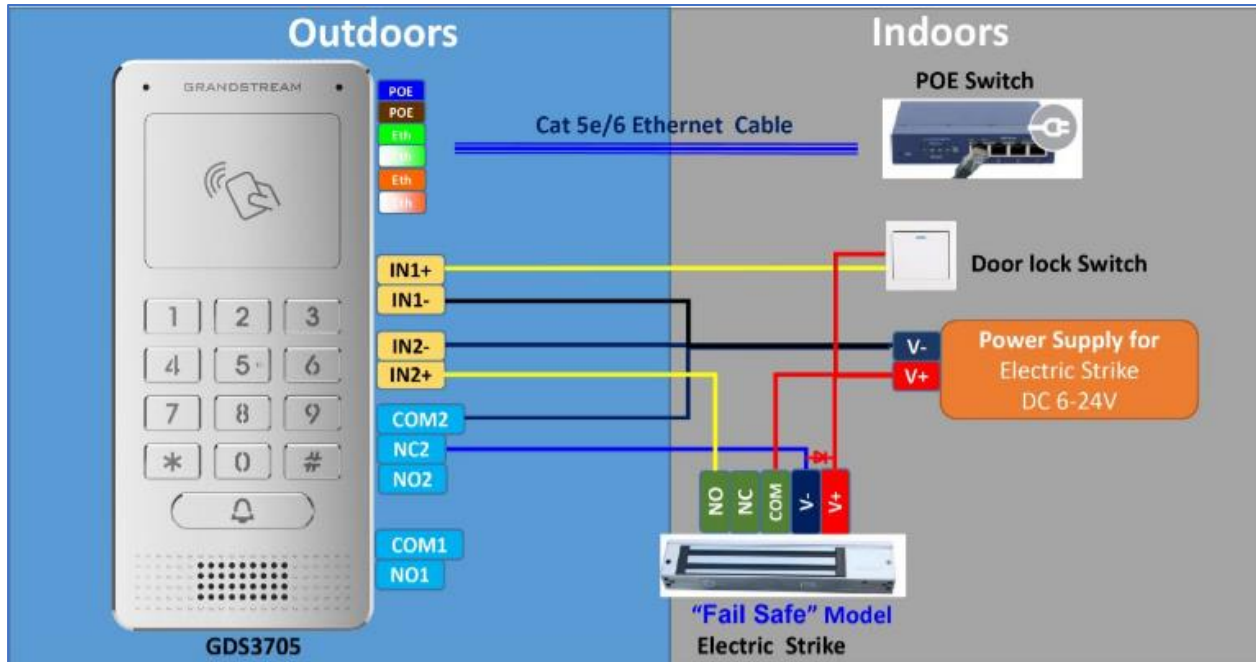


Figure 20: Wiring Sample using PoE to power GDS3705 and 3rd party Power Supply for Electric Strike

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

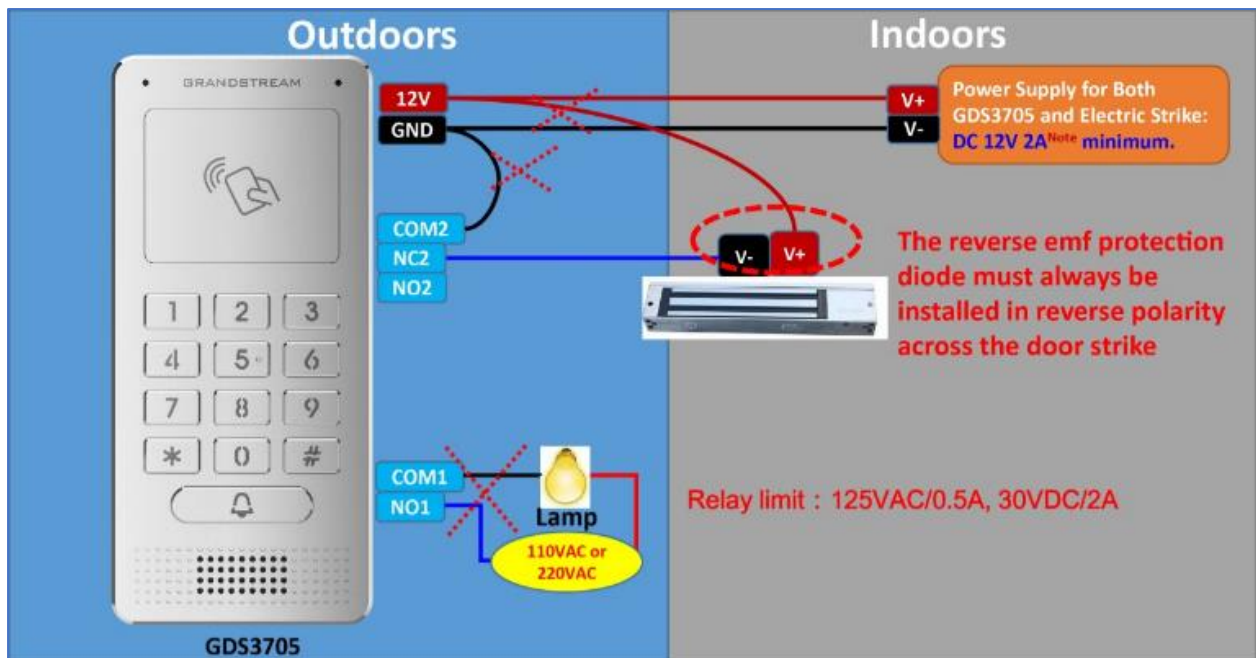


Figure 21: Example to Avoid when Powering the Electric Strike

Good Wiring Sample for Electric Strike and High-Power Device

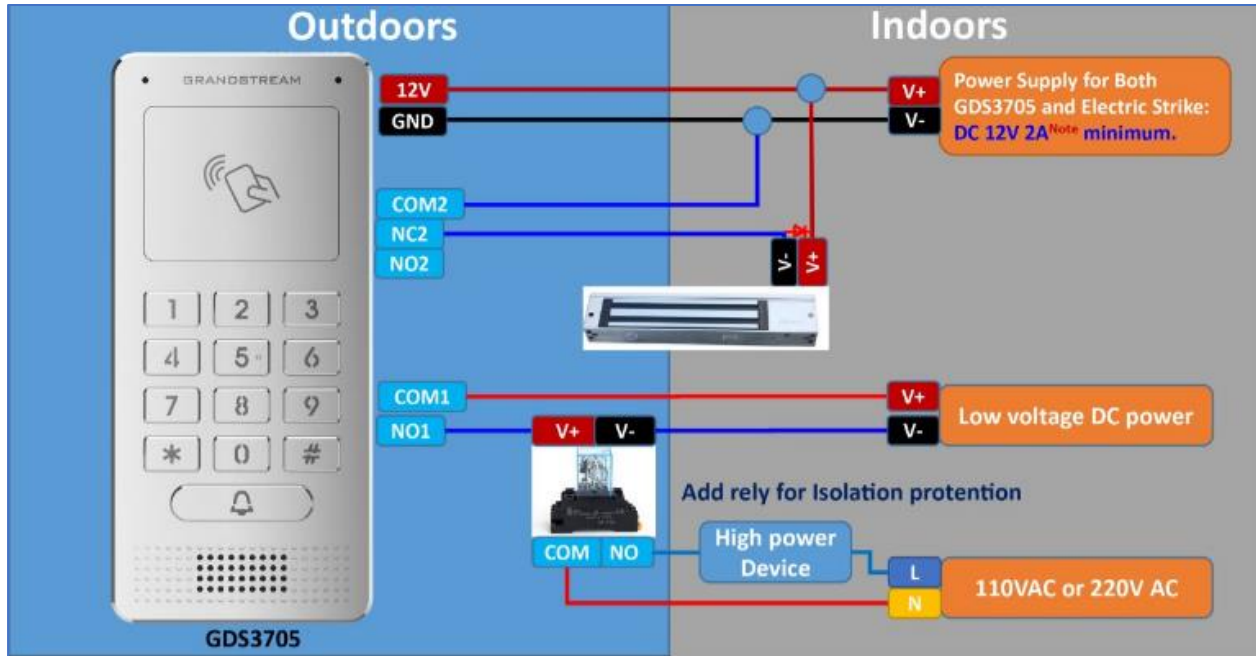


Figure 22: Electric Strike and High-Power Device Example

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 3rd party power supply for Wiegand device

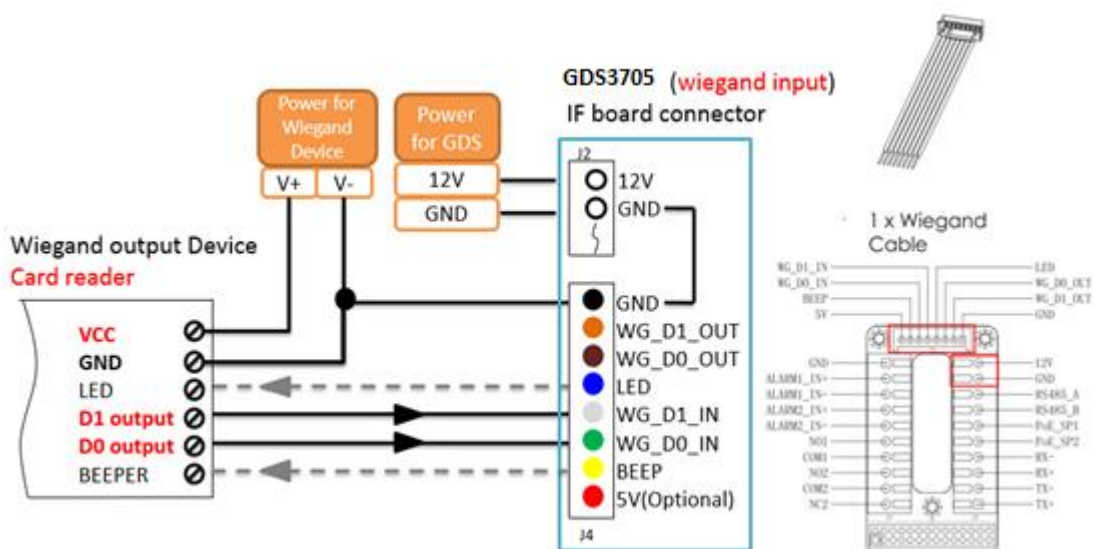


Figure 23: Wiegand Input Example with 3rd party Power Supply

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

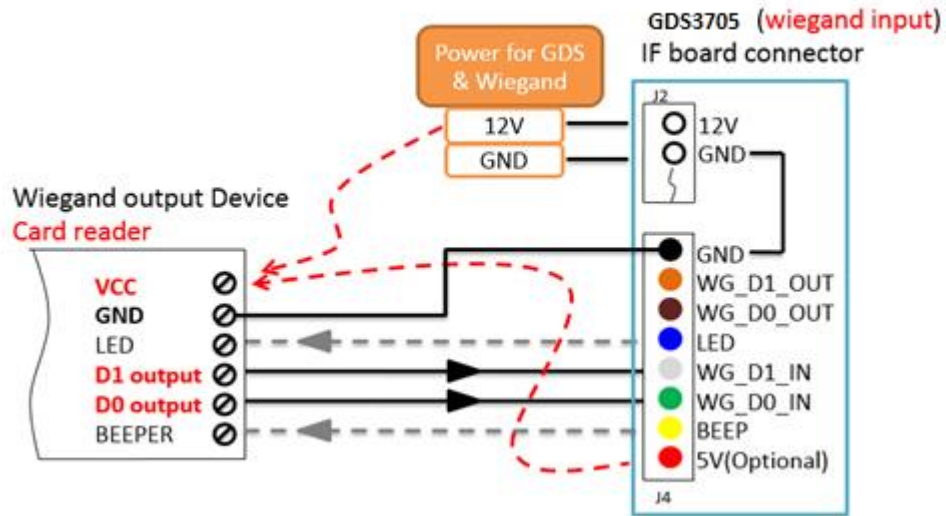


Figure 24: Wiegand Input Example with Power Supply for GDS3705 and Wiegand Device

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 3rd party power supply for Wiegand device

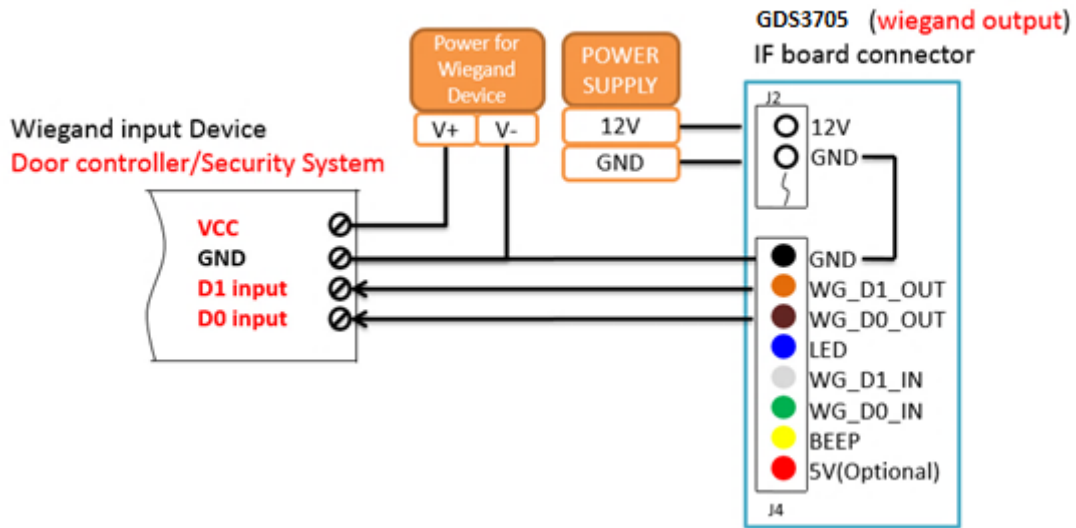


Figure 25: Wiegand Output Wiring Example

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

Wiegand RFID Card Reader Example

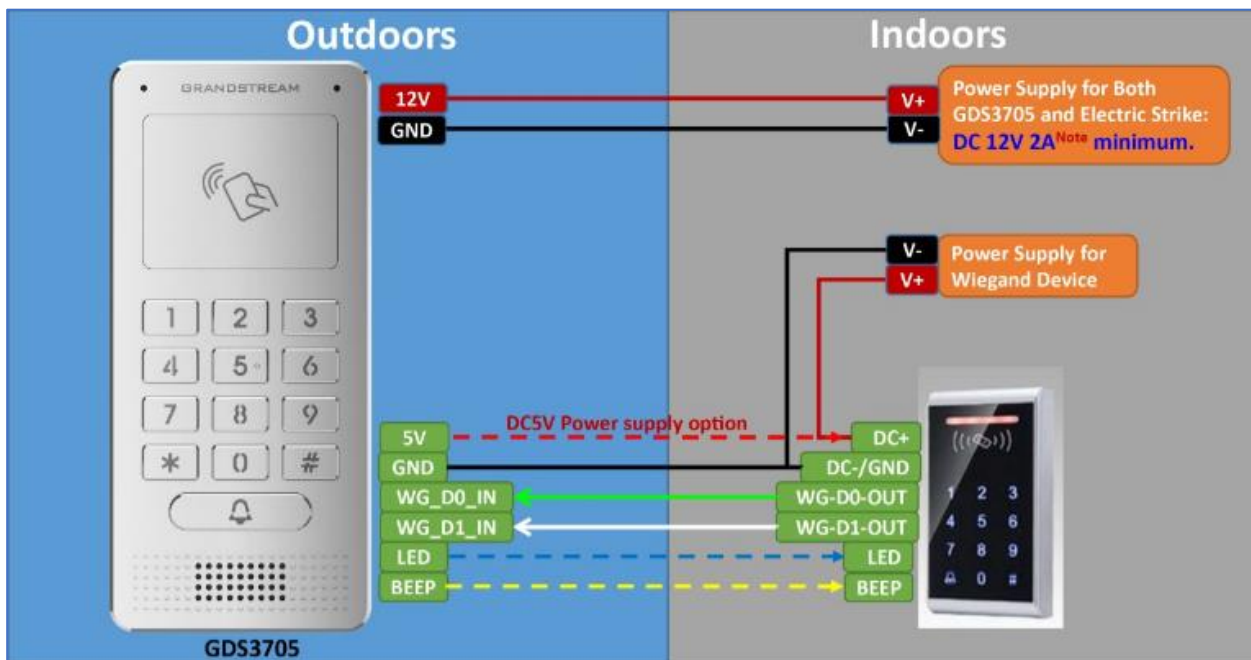


Figure 26: Wiegand RFID Card Reader Example

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.

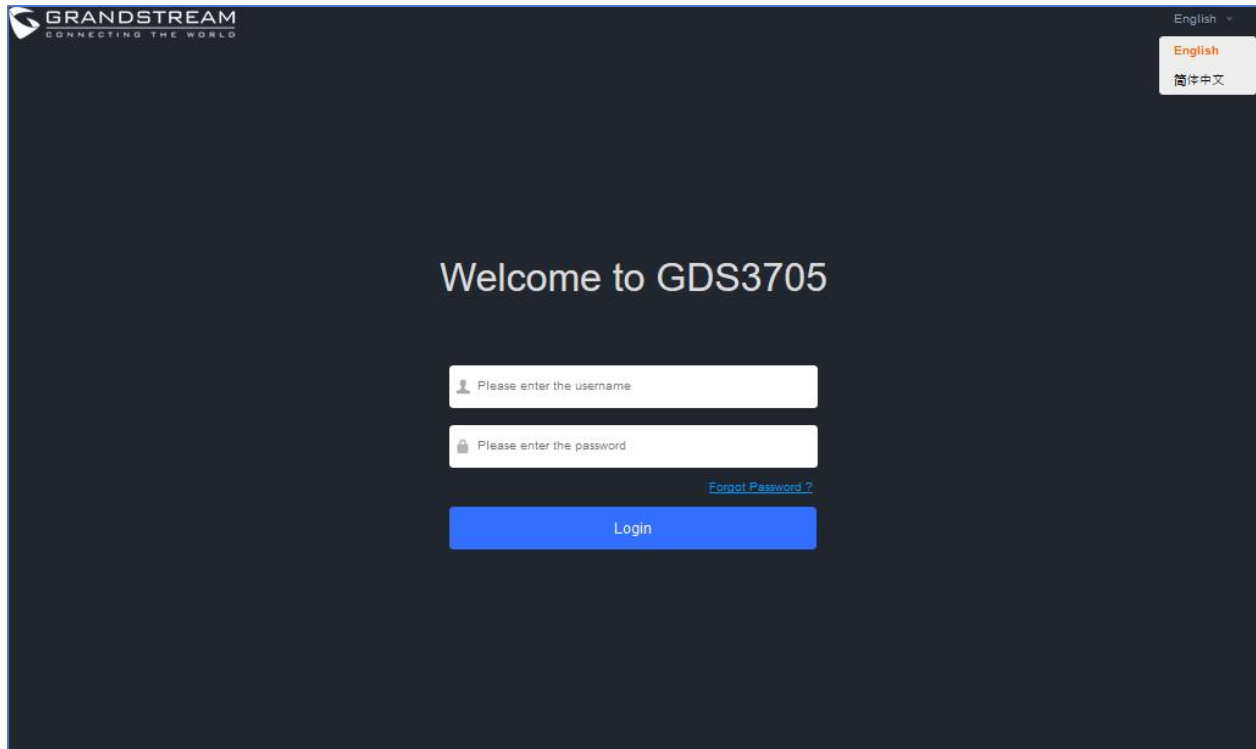


Figure 27: Change Language Page

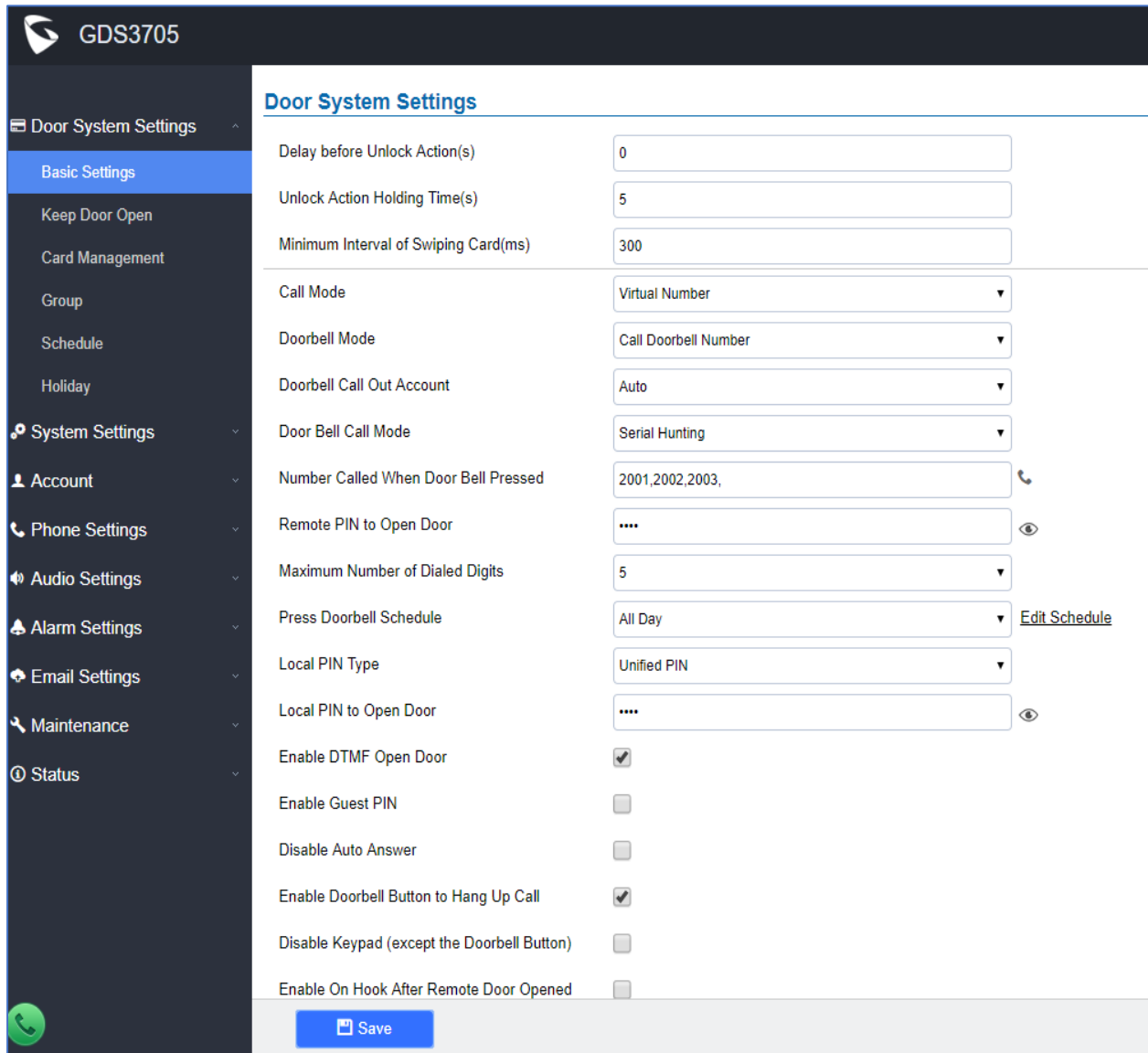
Note: Current firmware supports only English (default) and simplified Chinese.

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	
Delay before Unlock Action(s)	<input type="text" value="0"/>
Unlock Action Holding Time(s)	<input type="text" value="5"/>
Minimum Interval of Swiping Card(ms)	<input type="text" value="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	<input type="text" value="2001,2002,2003,"/> 
Remote PIN to Open Door	<input type="text" value="****"/> 
Maximum Number of Dialed Digits	5 ▼
Press Doorbell Schedule	All Day ▼ Edit Schedule
Local PIN Type	Unified PIN ▼
Local PIN to Open Door	<input type="text" value="****"/> 
Enable DTMF Open Door	<input checked="" type="checkbox"/>
Enable Guest PIN	<input type="checkbox"/>
Disable Auto Answer	<input type="checkbox"/>
Enable Doorbell Button to Hang Up Call	<input checked="" type="checkbox"/>
Disable Keypad (except the Doorbell Button)	<input type="checkbox"/>
Enable On Hook After Remote Door Opened	<input type="checkbox"/>

Figure 28: Door System Settings Page

Table 5: Door System Settings

Delay before Unlock Action(s)	Configures the time delay in second for the electronic lock to be triggered (default value is 0 seconds).
Unlock Action Holding Time(s)	Configures the lock holding time, in seconds (default value is 5 seconds).
Minimum Interval of Swiping Card(ms)	Defines the interval in ms to swipe consecutive RFID cards. The range should be between 0ms and 2000ms.
Call Mode	Chooses whether to make call to the SIP number or Virtual Number when dialing from the GDS3705 keypad.
Doorbell Mode	<p>Configures the action to be taken when the doorbell is pressed, three options are available:</p> <ul style="list-style-type: none"> • Call Doorbell Number: when Doorbell is pressed, a call will be made to the “Number Called When Door Bell Pressed” • Control Doorbell Output (Digital Output 1): when Door Bell is pressed electronic lock for Output 1 is opened. • Both of Above: When selected, both Call Doorbell Number and Control Doorbell Output options are enabled.
Doorbell Call Out Account	This option sets the account that will be used to make the call upon the doorbell trigger. When set to Auto, the GDS will use the first available account.
Door Bell Call Mode	<p>Select the ring strategy for the Numbers Called when pressing the Door Bell button to be either Serial or Parallel:</p> <ul style="list-style-type: none"> • Serial Hunting: the configured extensions and/or IP addresses will ring one after one by order. • Parallel Hunting: The configured extensions and/or IP addresses will ring simultaneously (up to 4 simultaneous SIP calls).

<p>Number Called When Door Bell Pressed</p>	<p>Configures SIP extension number (SIP Server mode), or IP address with port number (peering mode), to be called when the Door Bell is pressed:</p> <ul style="list-style-type: none"> • SIP Server mode: <ul style="list-style-type: none"> - 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 Serial Hunting Mode (GDS will ring each extension by default 30 seconds, this can be changed on the Ring Timeout) or ring them simultaneously in Parallel Hunting Mode. - When using UCM, users can also configure there a Ring Group extension (6400 for example) that will ring multiple extensions simultaneously, or one by one depending on the Ring Group ring strategy. - If early medial is enabled on phone side, user can send the PIN code using the Open-Door button before answering the call (Of course users can open the door also after answering the call). • Peering mode: <ul style="list-style-type: none"> - 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 Serial or Parallel Mode according to Doorbell Call Mode strategy. <p>Note: This field supports a Maximum of 256 characters.</p>
<p>Remote PIN to Open the Door</p>	<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>Maximum Number of Dialed Digits</p>	<p>Configures the maximum digits allowed to be dialed using the keypad.</p> <p>GDS3705 will dial out automatically digits enter after reaching configured maximum numbers without pressing #.</p> <p>Range from 1-20, Default setting is “Disabled”.</p>



Press Doorbell Schedule	<p>Configure a schedule for the Doorbell button during which it will be active. Outside defined schedule, Doorbell button will be inactive. Default setting is “All Day”.</p>
Local PIN Type	<p>Three Options are available: Private Card PIN, Unified PIN or Card and Private PIN.</p> <ul style="list-style-type: none"> • Private Card PIN: Means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3705 to open the door [*Virtual Number*Private PIN#]. Note: When Local PIN type is set to private card PIN, users can also open the door by swiping their cards. • Unified PIN: 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 [*Local PIN to Open Door#]. • Card and Private PIN: Means every member needs to swipe his card and enter his private PIN to open the door using the following sequence [Swipe the card + * Private PIN #]
Local PIN to Open Door	<p>Configures PIN stored in GDS3705, input locally this PIN on the GDS3705 keypad will unlock the door.</p> <p>This feature needs Private Card PIN, means every member has a private PIN, the GDS will record who unlocked the door every time. Users need to enter the following sequence from the GDS3705 to open the door [*Virtual Number*Private Door Password#].</p> <p>Note: When local PIN type is set to private card PIN, users can also open the door by swiping their cards.</p>
Enable DTMF Open Door	<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>
Enable Guest PIN	<p>Enables password entry for guests.</p>
Guest PIN	<p>Configures the password that will be used by guests.</p>
Guest PIN Start Time	<p>Selects the start time when the Guest PIN start to take effect.</p>
Guest PIN End Time	<p>Selects the end time when the Guest PIN will stop working.</p>



Disable Auto Answer	If checked, GDS3705 will not answer incoming calls automatically, users can press any key to answer the call. Default setting in unchecked.
Enable Doorbell Button to Hang Up Call	When checked the door bell will allow users to hang up the ongoing call. Default: Enabled
Disable Keypad (except the Doorbell Button)	When checked the Keypad will be disabled, only Door Bell button can be pressed.
Enable On Hook After Remote Door Opened	When checked calls will be disconnected automatically 5 seconds after the remote open-door event.
Enable HTTP API Remote Open Door	Enabling This option allows to use HTTP API command to open the door remotely. Important note: We will not be responsible for any security problems resulting from opening the HTTP API remote function, this option is disabled by default and the user should enable it while knowing how to mitigate the risk.
Enable Card Issuing Mode	Enables RFID card issuing/program into the GDS3705. When selected sweeping an RFID card into the GDS3705 will add card information into. [Card Management]
Card issuing State Expire Time(m)	Card issuing mode will be automatically disabled when timer reached (The range of value is 1 – 1440, in minutes).
Enable Key Blue Light	When checked, the blue light will be activated when pressing the GDS3705 Keys.
Enable Blue Light	When enabled, Keypad LED will light based on the configured Start/End Time. For instance, this option can be used when GDS is deployed on dark environment, the GDS will be located easily using Keypad LED.
Central Mode	If enabled, Group/Schedule/Holiday can only be synchronized from the Central (GDS Manager), local configuration will not be allowed. If disabled, only local configuration from GDS3705 is allowed. Default setting is “Disabled”.
Key Tone Type	Configures the key tones for the GDS3705. <ul style="list-style-type: none"> • Default: Beeps will be played when pressing the GDS3705 keys. • DTMF: Tones will be played when pressing the GDS3705 keys. • Mute: No sound will be played when pressing keys.
Wiegand Input Enable	Enable Wiegand Input.
Wiegand Output	Enable Wiegand Output.



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

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.

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.

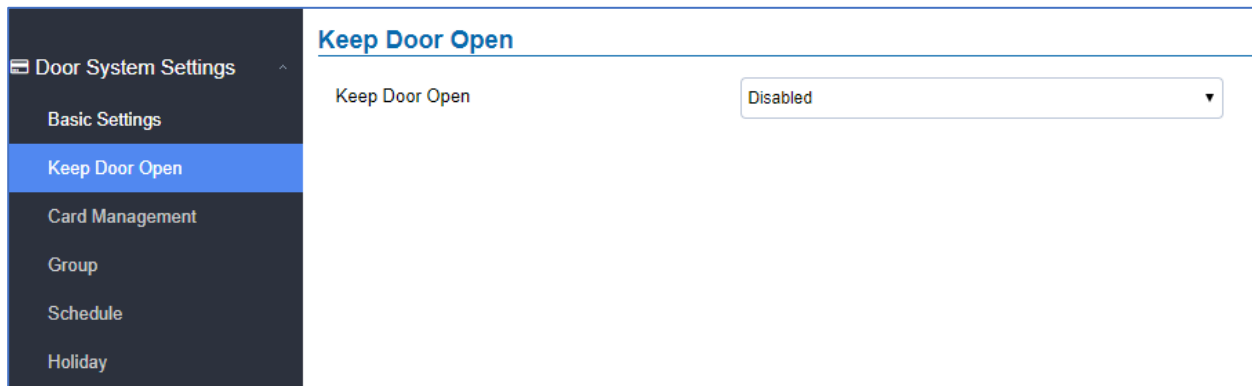


Figure 29: Keep Door Open

There are two modes under this section:

1- Immediate Open Door (One Time Only Action)

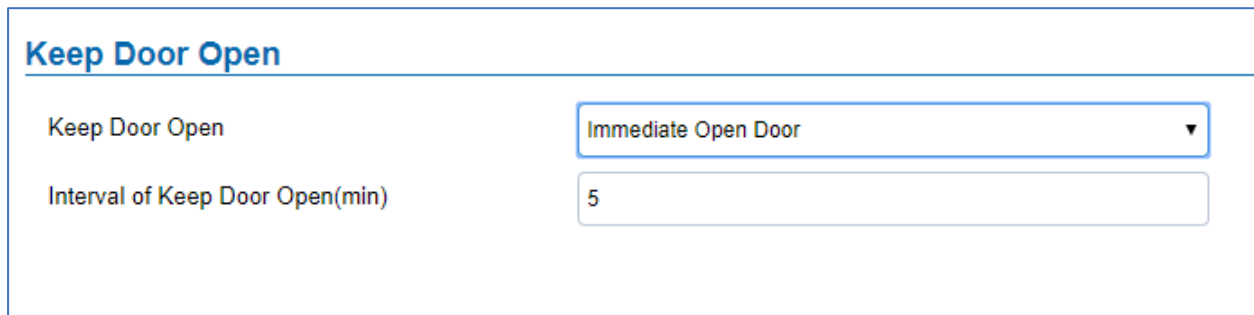
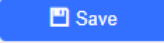


Figure 30: Immediate Door Open




Table 6: Immediate Door-Open Table


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

2- Schedule Open Door (Repeated Action)

Keep Door Open

Keep Door Open Schedule Open Door ▼

Valid Schedule Start Time 2018-06-19 00:00:00 

Valid Schedule End Time 2018-06-19 00:33:00 

Schedule

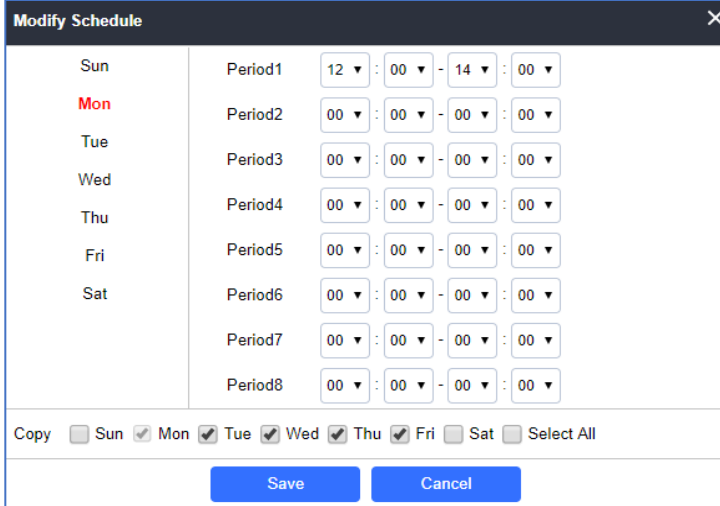
Edit

	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																									

Figure 31: Schedule Door Open
Table 7: Schedule Keep Door Open

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

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



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

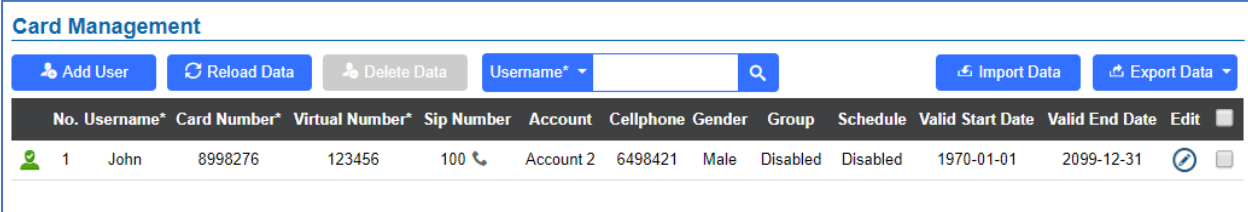
Copy Sun Mon Tue Wed Thu Fri Sat Select All

Save Cancel

Figure 32: Modify Schedule

Card Management

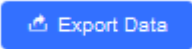


This page allows users to add information about RFID cards, two options are possible either add RFID cards manually or automatically.




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 33: 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.
- 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"/>
Private PIN	<input type="password" value="*****"/>
Gender	<input style="border-bottom: 1px solid #ccc;" type="text" value="Male"/>
ID Number	<input type="text" value="10"/>
Card Number*	<input type="text" value="8998276"/>
Valid Start Date	<input style="border-bottom: 1px solid #ccc;" type="text" value="1970-01-01"/> 
Valid End Date	<input style="border-bottom: 1px solid #ccc;" type="text" value="2099-12-31"/> 
Virtual Number*	<input type="text" value="123456"/>
Sip Number	<input type="text" value="100"/>
Call Out Account	<input style="border-bottom: 1px solid #ccc;" type="text" value="2"/>
Cellphone	<input type="text" value="6498421"/>
Group	<input style="border-bottom: 1px solid #ccc;" type="text" value="Disabled"/>
Schedule	<input style="border-bottom: 1px solid #ccc;" type="text" value="Disabled"/>
Enable	<input checked="" type="checkbox"/>

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

Figure 34: Card Info

Table 8: Card Info

Username	Configures the username to identify the user.
Private PIN	Specifies a specific password to unlock the door.
Gender	Selects a gender, either Male or Female.
ID Number	Enters an ID number (This number is set by the admin to identify each user uniquely).
Card Number	Enters the RFID Card number (this is the number written on the RFID card. When “card issuing mode” is enabled, this filed will be added automatically).
Valid Start Date	Configures the start date of validity of the RFID card.
Valid End Date	Configures the End date of validity of the RFID card.

Virtual Number	When dialing directly from the keypad, the GDS accept only Virtual number to identify a user, once the Virtual number is typed followed by # key, the SIP Number will be dialed.
SIP Number	Configures the SIP Number which is mapped with virtual number. Once the virtual number is dialed the GDS3705 will send an INVITE to the SIP Number. Note: The SIP Number can be configured with an extension/phone number or IP address. Example: 192.168.5.124
Call Out Account	Select the SIP account that will be used to call the SIP Number extension, when choosing Auto, the unit will use the first available SIP account.
Cellphone	Configures cellphone of the user.
Group	Specifies to which group the user will be added.
Schedule	Specifies the schedule that will be assigned to the user.
Enable	Enable/Disable the RFID card.


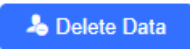






Notes:

- 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.



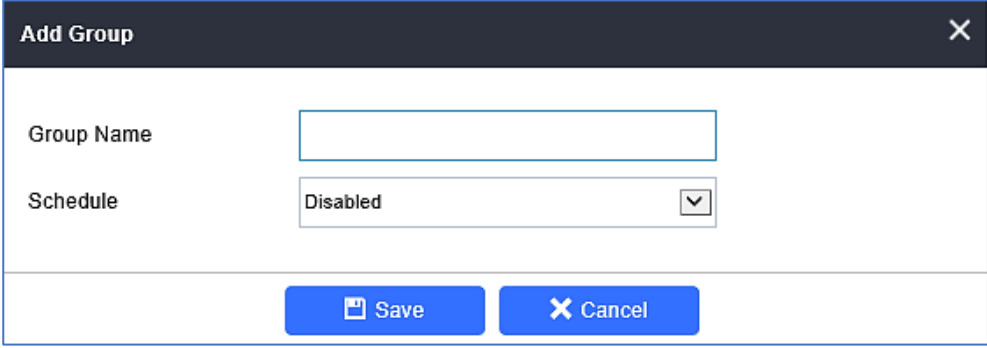
Group

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.



The 'Add Group' dialog box contains the following fields and buttons:

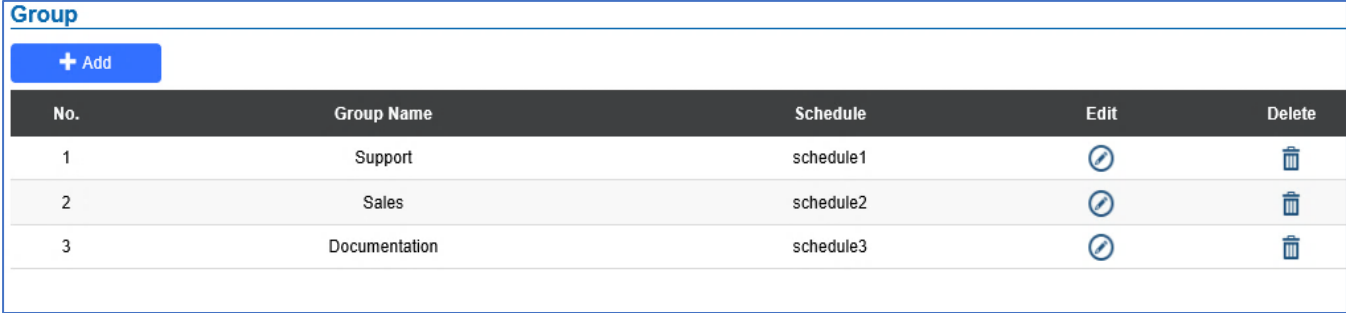
- Group Name:** A text input field.
- Schedule:** A dropdown menu currently showing 'Disabled'.
- Buttons:** 'Save' (with a floppy disk icon) and 'Cancel' (with an 'X' icon).

Figure 35: Add Group

Table 9: Add Group

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

The following screenshots display the list of the created groups.



The 'Groups List' screenshot shows a table with the following data:









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

Figure 36: 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.

Figure 37: Edit Schedule Time

Holiday

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



Click on  to edit the holidays or  for holiday details.

Figure 38: 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.

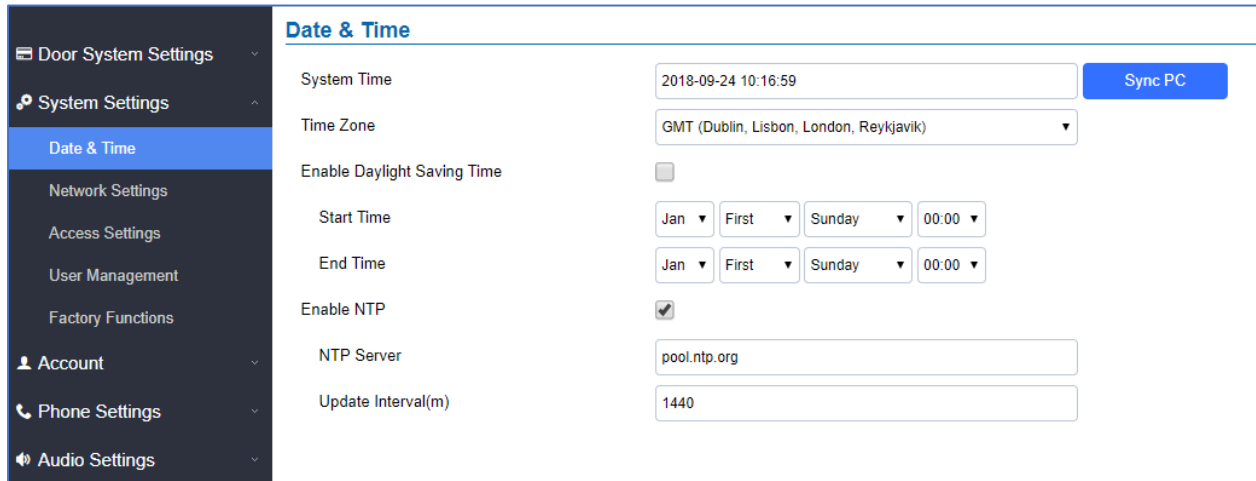


Figure 39: Date & Time Page

Table 10: Date & Time

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

Network Settings

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

- Door System Settings
- System Settings
- Date & Time
- Network Settings
- Access Settings
- User Management
- Factory Functions
- Account
- Phone Settings
- Audio Settings
- Alarm Settings
- Email Settings
- Maintenance
- Status

Basic Settings

IP Address Config

IP Address Mode DHCP Static IP

IP Address

Subnet Mask

Gateway

DNS Config

DNS Address Type Dynamic DNS Static DNS

DNS Server 1

DNS Server 2

Enable LLDP

Enable LLDP Disable Enable

Layer 2 QoS Settings

Enable VLAN Disable Enable

Layer 2 QoS 802.1Q/VLAN Tag

Layer 2 QoS 802.1p Priority Value

Layer 2 QoS 802.1p Priority Value for RTP media

Figure 40: Basic Settings Page

Table 11: Basic Settings

IP Address Mode	Selects DHCP or Static IP. Default DHCP. (Static recommended)
IP Address	Configures the Static IP of the GDS3705.
Subnet Mask	Configures the Associated Subnet Mask.
Gateway	Configures the Gateway IP address.
DNS Address Type	Specifies the DNS type used: Dynamic DNS or Static DNS.
DNS Server 1	Configures DNS Server 1 IP address.
DNS Server 2	Configures DNS Server 2 IP address.
Enable LLDP	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is “Enabled”.



Enable VLAN	Controls the VLAN. Default setting is “Disabled”
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets. Default value is 0.
Layer 2 QoS 802.1p Priority Value for SIP signaling	Assigns the priority value of the Layer2 QoS packets for SIP signaling. Default value is 0.
Layer 2 QoS 802.1p Priority Value for RTP media	Assigns the priority value of the Layer2 QoS packets for RTP media. 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.

Access Settings

This page configures the GDS3705 access control parameters.



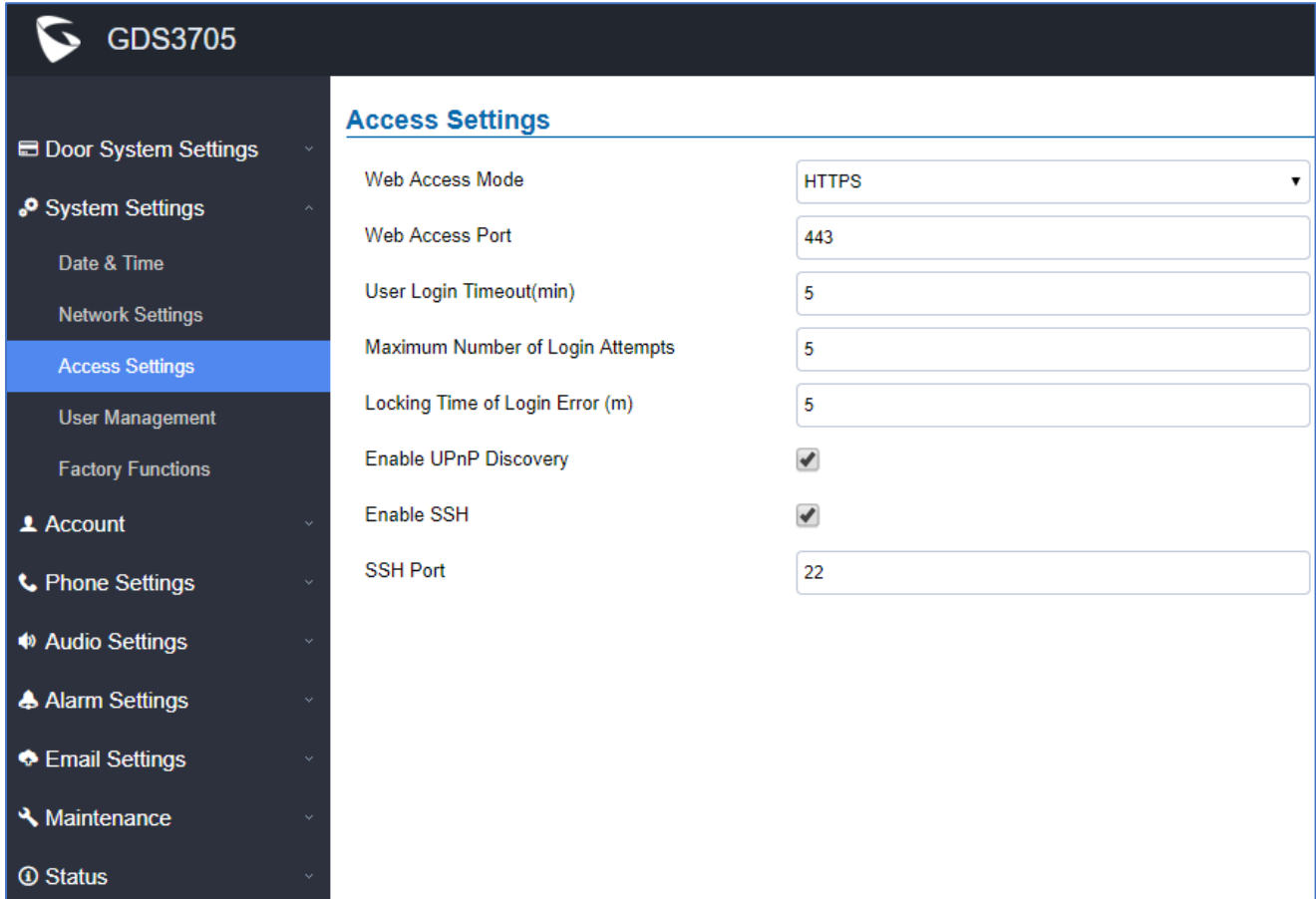


Figure 41: Access Settings Page

Table 12: Access Settings

Web Access Mode	Selects the access mode to the webGUI either HTTP or HTTPS.
Web Access Port	Specifies the TCP port for Web Access, default 443.
User Login Timeout(min)	If no action is made within this time the GDS3705 will logout from the Web GUI, range is between 3 and 60.
Maximum Number of Login Attempts	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 Locking Time of Login Error .
Locking Time of Login Error (m)	Specifies how long the GDS3705 is locked before a new login attempt is allowed.
Enable UPnP Discovery	UPnP (or mDNS) function for local discovery. Default setting is enabled.
Enable SSH	Selects to Enable/Disable SSH access. Default setting is enabled.
SSH Port	Specifies the SSH port. Default setting is 22.

User Management

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

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	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>

Change Recover Email

Password Recover Email Address	<input type="text"/>	Email Settings
--------------------------------	----------------------	--------------------------------

Figure 42: User Management Page

Table 13: User Management

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

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

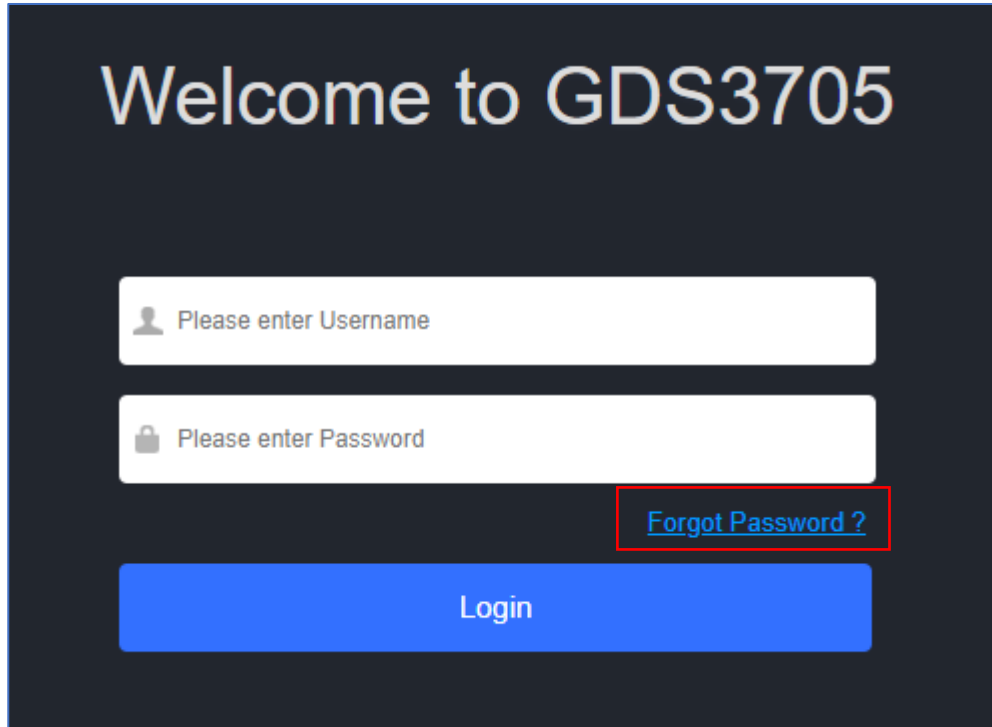


Figure 43: Recover Password

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

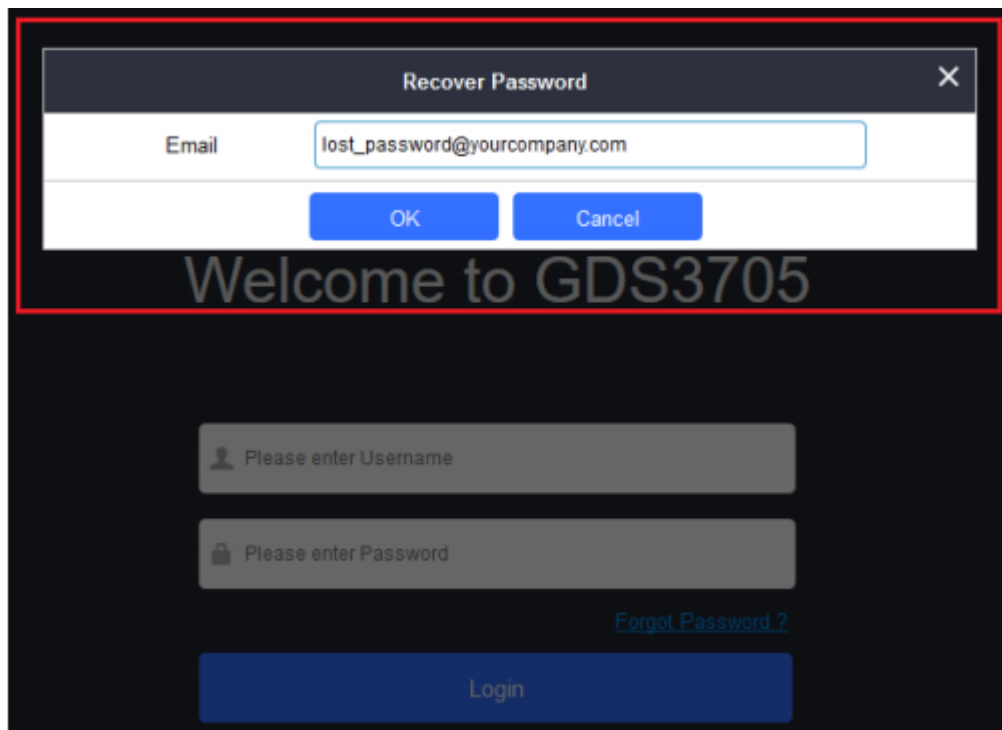
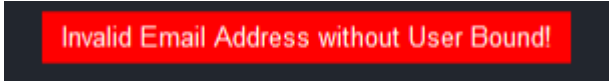


Figure 44: Recover Password - Email Address

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.



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.

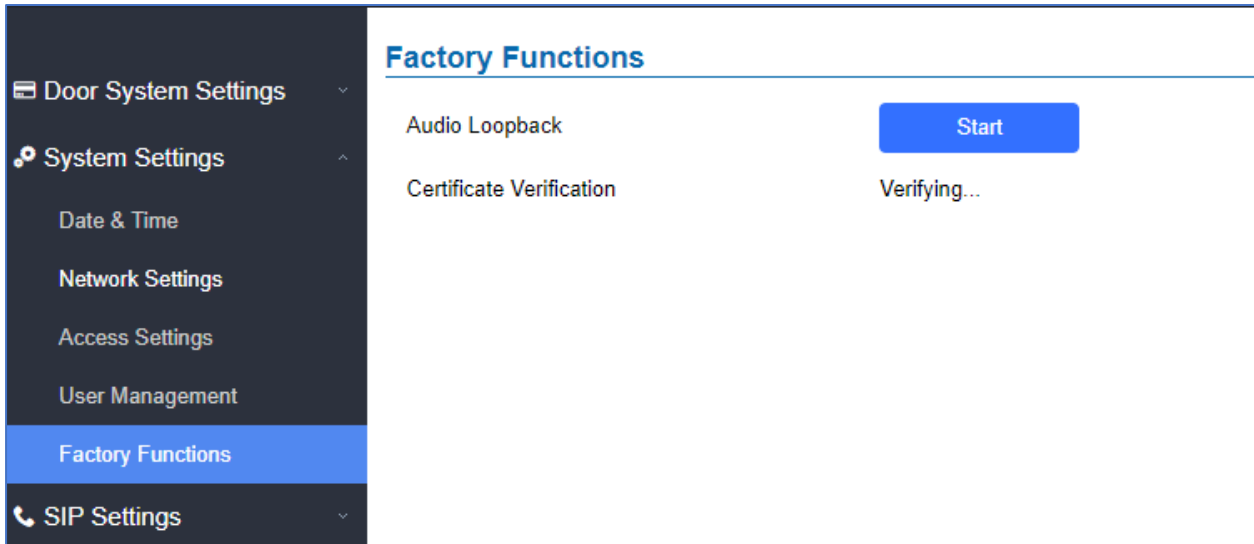


Figure 45 : Factory Functions Page

Table 14: User Management

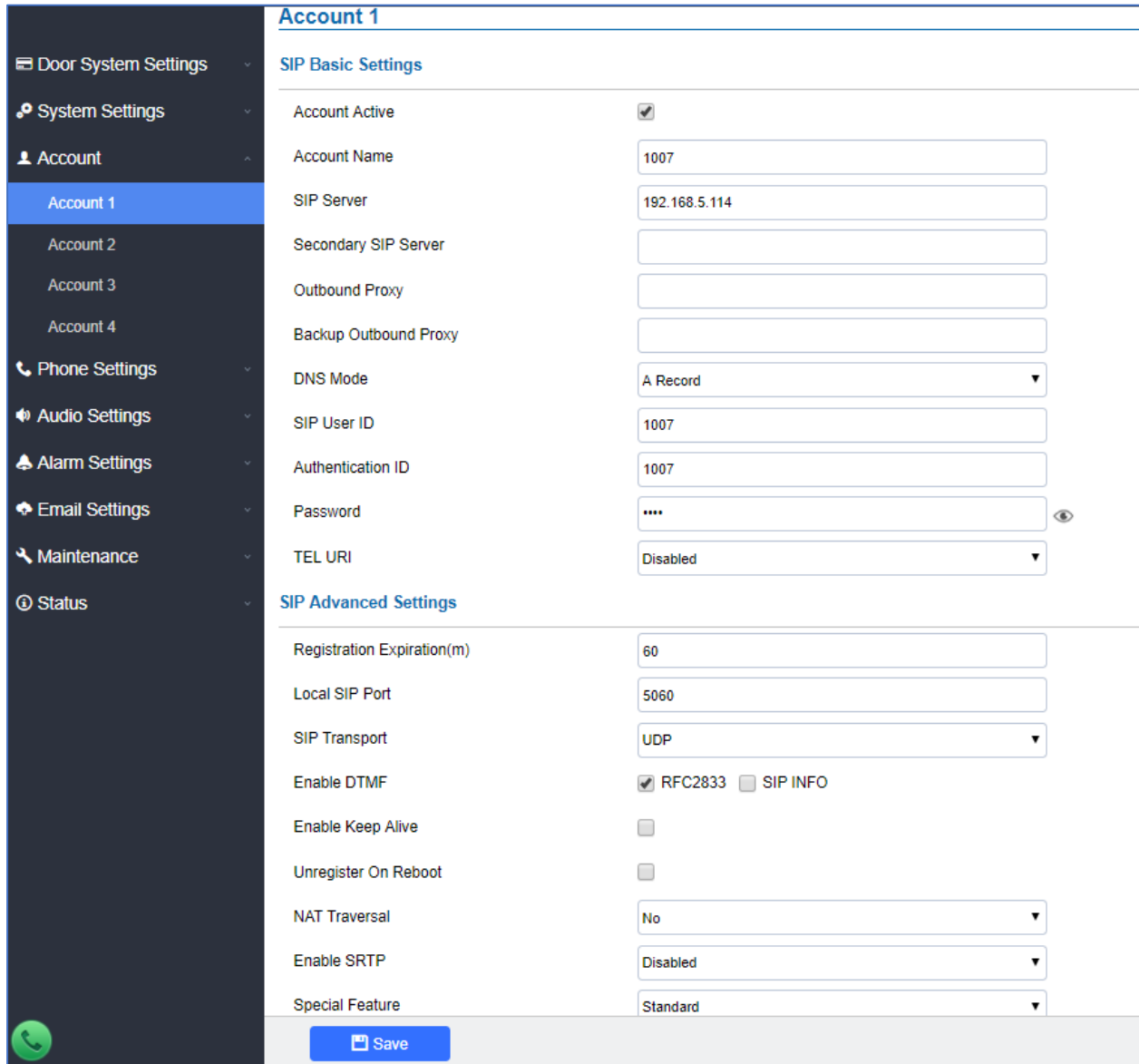
Audio Loopback	Press Start button and speak to the GDS3705. If you can hear your voice, your audio is working fine. Press Stop to exit audio loopback mode.
Certificate Verification	This is used to validate certificate chain for the server’s certificate.

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:




Account 1	
SIP Basic Settings	
Account Active	<input checked="" type="checkbox"/>
Account Name	<input type="text" value="1007"/>
SIP Server	<input type="text" value="192.168.5.114"/>
Secondary SIP Server	<input type="text"/>
Outbound Proxy	<input type="text"/>
Backup Outbound Proxy	<input type="text"/>
DNS Mode	<input type="text" value="A Record"/>
SIP User ID	<input type="text" value="1007"/>
Authentication ID	<input type="text" value="1007"/>
Password	<input type="password" value="****"/> 
TEL URI	<input type="text" value="Disabled"/>
SIP Advanced Settings	
Registration Expiration(m)	<input type="text" value="60"/>
Local SIP Port	<input type="text" value="5060"/>
SIP Transport	<input type="text" value="UDP"/>
Enable DTMF	<input checked="" type="checkbox"/> RFC2833 <input type="checkbox"/> SIP INFO
Enable Keep Alive	<input type="checkbox"/>
Unregister On Reboot	<input type="checkbox"/>
NAT Traversal	<input type="text" value="No"/>
Enable SRTP	<input type="text" value="Disabled"/>
Special Feature	<input type="text" value="Standard"/>
<input type="button" value="Save"/>	

Figure 46: SIP Account Settings Page

Table 15: SIP Account Basic & Advanced Settings

SIP Basic Settings	
Account Active	This field indicates whether the account is active. Default setting is "Yes".
Account Name	Configures the SIP account name used for identification.
SIP Server	Configures the FQDN or IP of the SIP server from VoIP service provider or local IPPBX.
Secondary SIP Server	Configures the FQDN or IP of the Secondary SIP server from VoIP service provider or local IPPBX.
Outbound Proxy	Configures the IP or FQDN of Outbound proxy server.
Backup Outbound Proxy	Configure the IP or FQDN of Backup Outbound Proxy Server.
DNS Mode	Configure which DNS mode will be used to translate the SIP Server FQDN (Default value is A Record): <ul style="list-style-type: none"> • A Record. • SRV. • NAPTR/SRV.
SIP User ID	Configures the SIP username or telephone number from ITSP.
Authenticate ID	Configures the Authenticate ID used by SIP proxy.
Password	Sets the Authenticate password used by SIP proxy.
TEL URI	Select "User=Phone" or "Enabled" from the dropdown list. If the SIP account has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable".
SIP Advanced Settings	
Registration Expiration(m)	Sets the registration expiration time. Default setting is 60 minutes.
Local SIP Port	Sets the local SIP port. Default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4.
SIP Transport	Chooses the SIP transport protocol. Default settings is UDP.
Enable DTMF	Specifies the mechanism to transmit DTMF digits. There are 2 supported modes: <ul style="list-style-type: none"> • RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. • SIP INFO uses SIP INFO to carry DTMF. Default setting is "RFC2833"



Enable Keep Alive	Checks to help NAT resolution, sending alive packets.
Unregister On Reboot	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
NAT Traversal	<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.</p> <p>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&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>
Enable SRTP	<p>Enable SRTP mode based on your selection from the drop-down menu.</p> <p>The default setting is "Disabled", the two other modes are "Enabled but Not Forced" and "Enabled and Forced"</p>
Special Feature	<p>Configures GDS settings to meet different vendors' server requirements.</p> <p>Users can choose from Standard and Broadsoft.</p> <p>The default setting is "Standard".</p>

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.



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

Phone Settings

STUN Server	<input type="text"/>
Local RTP Port	<input type="text" value="5004"/>
Local RTP Port Range	<input type="text" value="200"/>
Use Random Port	<input type="checkbox"/>
Auto On-Hook Timer(s)	<input type="text" value="300"/>
Ringing Timeout(s)	<input type="text" value="30"/>
SIP TLS Certificate	<div style="border: 1px solid #ccc; height: 40px;"></div>
SIP TLS Private Key	<div style="border: 1px solid #ccc; height: 40px;"></div>
SIP TLS Private Key Password	<input type="password"/> 👁
Enable Direct IP Call	<input checked="" type="checkbox"/>
Enable two-way SIP Calling	<input type="checkbox"/>
SIP Proxy Compatibility Mode	<input checked="" type="checkbox"/>

Figure 47: Phone Settings Page

Table 16: Phone Settings

STUN Server	Configures the STUN server FQDN or IP. If the device is behind a non-symmetric router, STUN server can help to penetrate & resolve NAT issues.
Local RTP Port	Sets the local RTP port for media. Default setting is 5004.
Local RTP Port Range	Define the range of local RTP port from 48 to 10000
Use Random Port	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” Note: This parameter must be set to “Disabled” for Direct IP Calling to work.
Auto On-Hook Timer	Configures the auto on-hook timer (in seconds) for automatic disconnecting the SIP call. Default setting is 300.
Ring Timeout(s)	Specifies the Ring timeout, when no reply is returned from the called party after exceeding this field, the GDS3705 will hang up the call. The value is in the range of 0s – 90s. By default; it is “30” seconds.
SIP TLS Certificate	Copy/Paste the TLS certificate here for encryption.

SIP TLS Private Key	Input private key here for TLS security protection.
SIP TLS Private Key Password	Specifies the password for SIP TLS private Key.
Enable Direct IP Call	Accepts peer-to-peer IP call (over UDP only) without SIP server. Default is "Enabled".
Enable two-way SIP Calling	Allows the user to enable/disable the alarm sound during a SIP call triggered by doorbell pressing.
SIP Proxy Compatibility Mode	Enables more proxy compatibility with cost of bandwidth, the SIP call will send audio no matter what.

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), the user can configure up to 30 white phone numbers per SIP account.

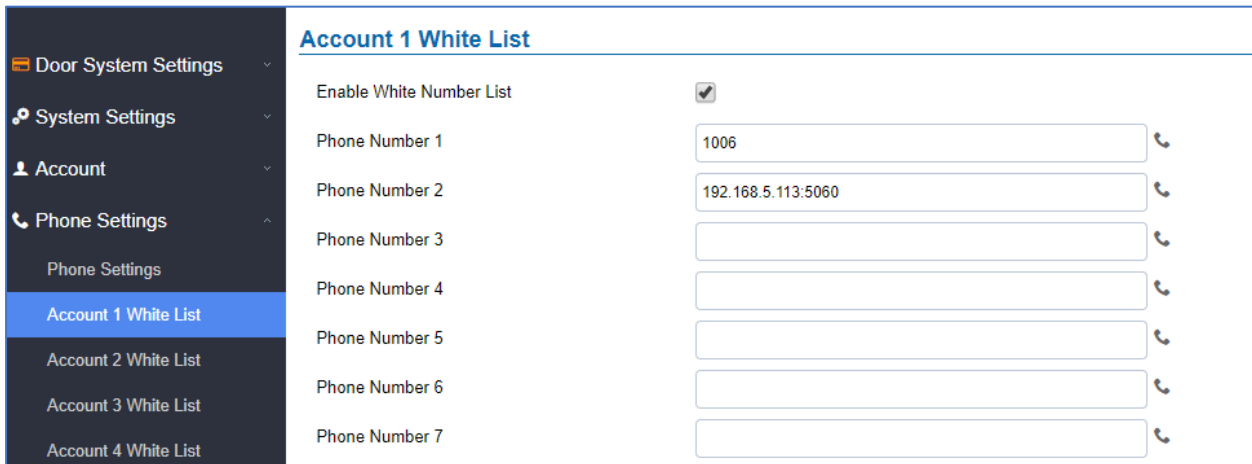


Figure 48: White List Page

The table below gives a brief overview of the options:

Table 17: White List

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

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

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.

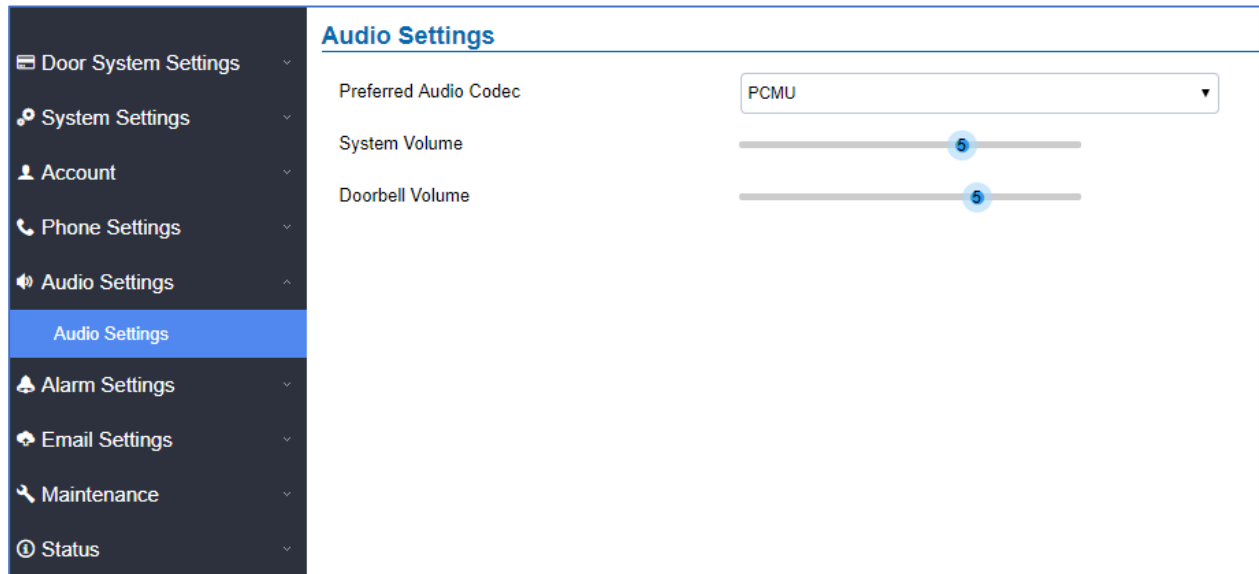


Figure 49: Audio Settings Page

Table 18: Audio Settings

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

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.



Alarm Events Config	
Input Digit	
Input Digit 1	Disable ▼
Input Digit 2	Disable ▼
Digit Output	
Alarm Output Duration(s)	5 ▼
Alarm Config	
Enable Silent Alarm Mode	<input type="checkbox"/>
Enable Hostage Code	<input type="checkbox"/>
Enable Tamper Alarm	<input type="checkbox"/>
Enable Alarm for PIN Input Error	<input checked="" type="checkbox"/>
Select Alarm Action Profile	profile1 ▼ Edit Profile
Enable Non-scheduled Access Alarm	<input type="checkbox"/>

Figure 50: Events Page

Alarm can be triggered by GDS3705 input.

Input Digit

Input Digit	
Input Digit 1	Alarm Input ▼
Input Digit 1 State	Normal Open ▼ Current state is CLOSE
Select Schedule 1	All Day ▼ Edit Schedule
Select Alarm Action Profile 1	profile1 ▼ Edit Profile
Input Digit 2	Alarm Input 2 ▼
Input Digit 2 State	Normal Open ▼ Current state is CLOSE
Select Schedule 2	All Day ▼ Edit Schedule
Select Alarm Action Profile 2	profile1 ▼ Edit Profile

Figure 51: Input Digit



Table 19: Input Digit

Input Digit 1	Selects the Input method for Alarm-IN 1 (Alarm Input or Door Open). <ul style="list-style-type: none"> • Alarm Input: Connect different sensor to trigger alarm • Open Door: Connect a switch button to open door from inside Note: If Digital Input port is connected to a switch button, it will not work during power outage, device booting or firmware upgrading.
Input Digit 1 State	Choose the Input Digit 1 to be either “Normal Close” or “Normal Open”, <i>This field does only appear when select Alarm Input.</i>
Select Schedule 1	Selects the predefined Alarm Schedule.
Select Alarm Action Profile 1	Selects the predefined Alarm Action for Profile 1. <i>This field does only appear when select Alarm Input.</i>
Input Digit 2	Selects the Input method for Alarm-IN 2 (Alarm Input or Door Open). <ul style="list-style-type: none"> • Alarm Input: Connect different sensor to trigger alarm • Open Door: Connect a switch button to open door from inside Note: If Digital Input port is connected to a switch button, it will not work during power outage, device booting or firmware upgrading.
Input Digit 2 State	Choose the Input Digit 2 to be either “Normal Close” or “Normal Open”, <i>This field does only appear when select Alarm Input.</i>
Select Schedule 2	Selects the predefined Alarm Schedule.
Select Alarm Action Profile 2	Selects the predefined Alarm Action for Profile 2. <i>This field does only appear when select Alarm Input.</i>

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

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



Hostage Code

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

Table 21: Hostage Code Alarm

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

Tamper Alarm

Tamper alarm is anti-hack from Hardware level. When this option is checked, if the 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

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

Keypad Input Error Alarm

Table 23: Keypad Input Error Alarm

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

Non-Scheduled Access Alarm

Table 24: Non-Scheduled Access Alarm

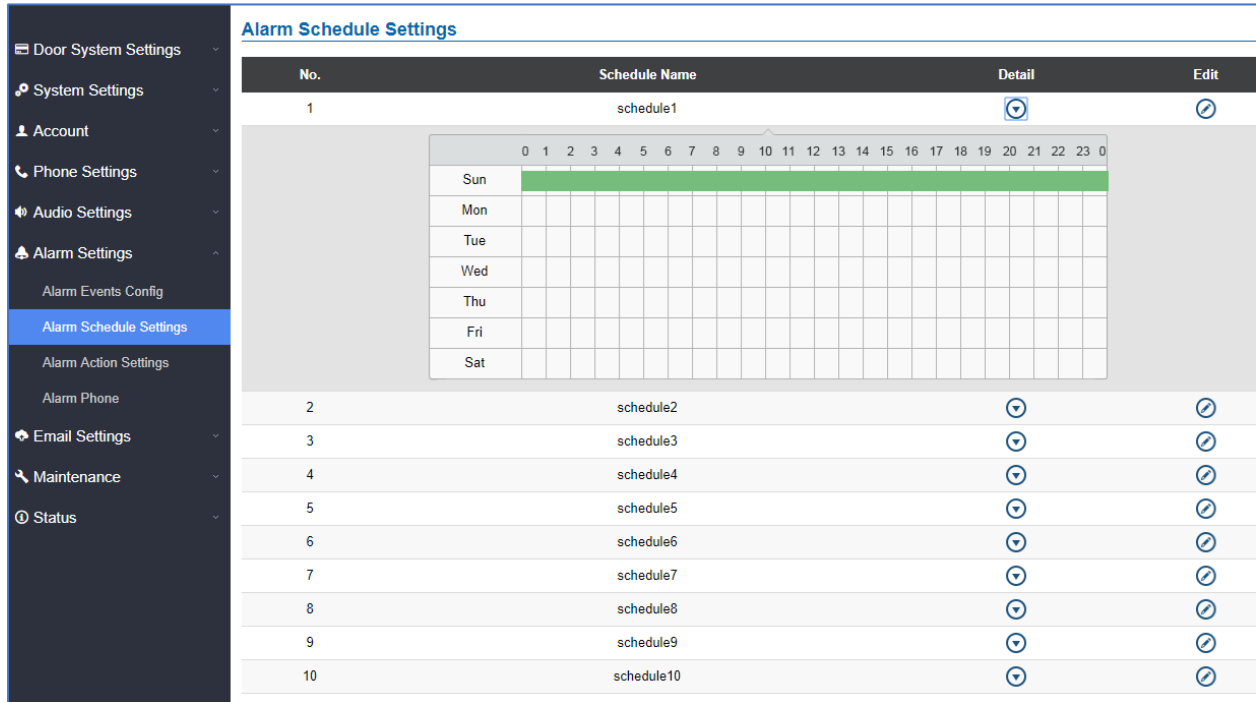
Enable Non-scheduled Access Alarm	When enabling this feature, GDS3705 will trigger alarm to related administrator to be aware when legitimated users access the door out of the allowed configured schedule.
Select Alarm Action Profile	Select the type of alarms actions to be triggered.



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 52: 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

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

Copy Sun Mon Tue Wed Thu Fri Sat Select All

Save
Cancel

Figure 53: Edit Schedule

Alarm Action Settings

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

Alarm Action Settings				
No.	Alarm Action Profile Name	Detail	Edit	Test
1	profile1	<div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p><input type="checkbox"/> Upload to Alarm Center</p> <p><input type="checkbox"/> Audio Alarm to SIP Phone</p> <p><input type="checkbox"/> Send Email</p> </div> <div style="width: 45%;"> <p><input checked="" type="checkbox"/> Audio Alarm</p> <p><input type="checkbox"/> Alarm Output</p> <p><input type="checkbox"/> Upload Snapshot</p> </div> </div>		
2	profile2			
3	profile3			
4	profile4			
5	profile5			
6	profile6			
7	profile7			
8	profile8			
9	profile9			
10	profile10			

Figure 54: Alarm Action

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

Modify Alarm Action Profile ✕

Alarm Action Profile Name

Upload to Alarm Center

Audio Alarm to SIP Phone

Send Email

Audio Alarm

Alarm Output

Save
Cancel

Figure 55: 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

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



Audio Alarm to SIP Phone	If selected, GDS3705 will call pre-configured phone and will play sound alarm.
Send Email	If selected, an email with snapshot will be sent to the pre-configured email destination.
Audio Alarm	If selected, GDS3705 will play alarm audio using built-in speaker.
Alarm Output	If selected, the alarm will be sent to the equipment (for example: Siren) connected to Alarm Output interface.

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.

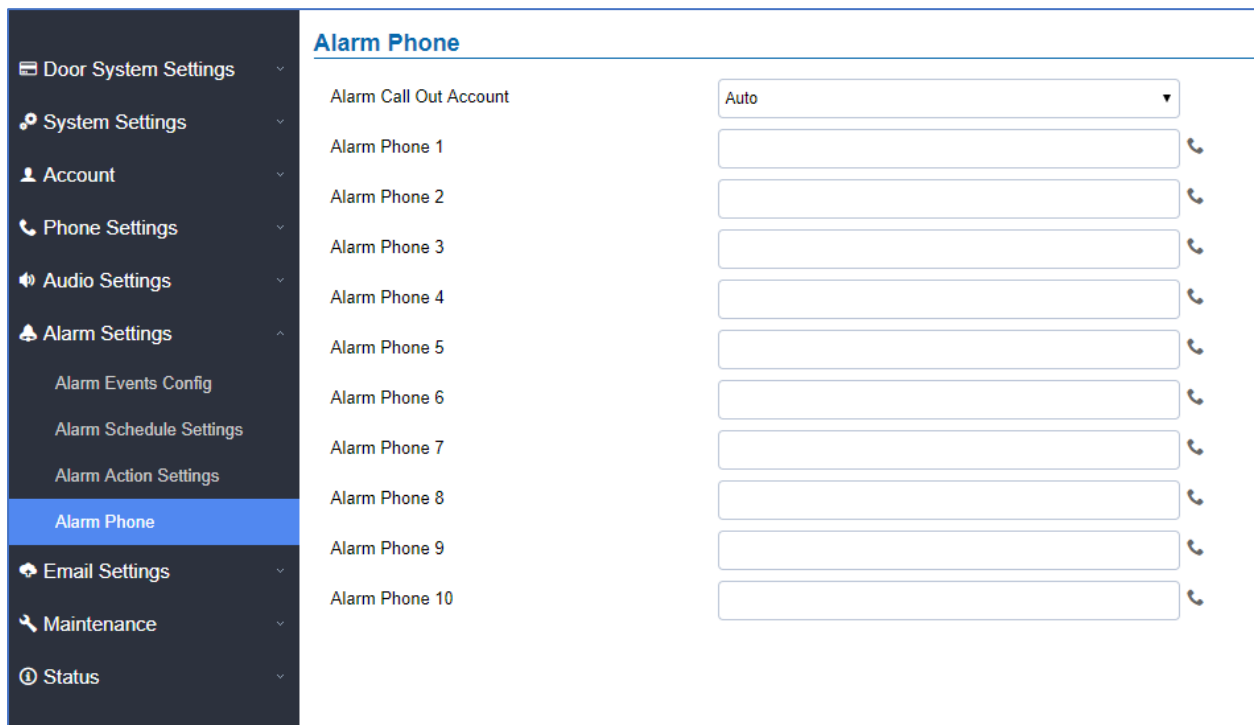


Figure 56: Alarm Phone List

Table 26: Alarm Phone List

Alarm Call Out Account	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.
Alarm Phone 1-10	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.

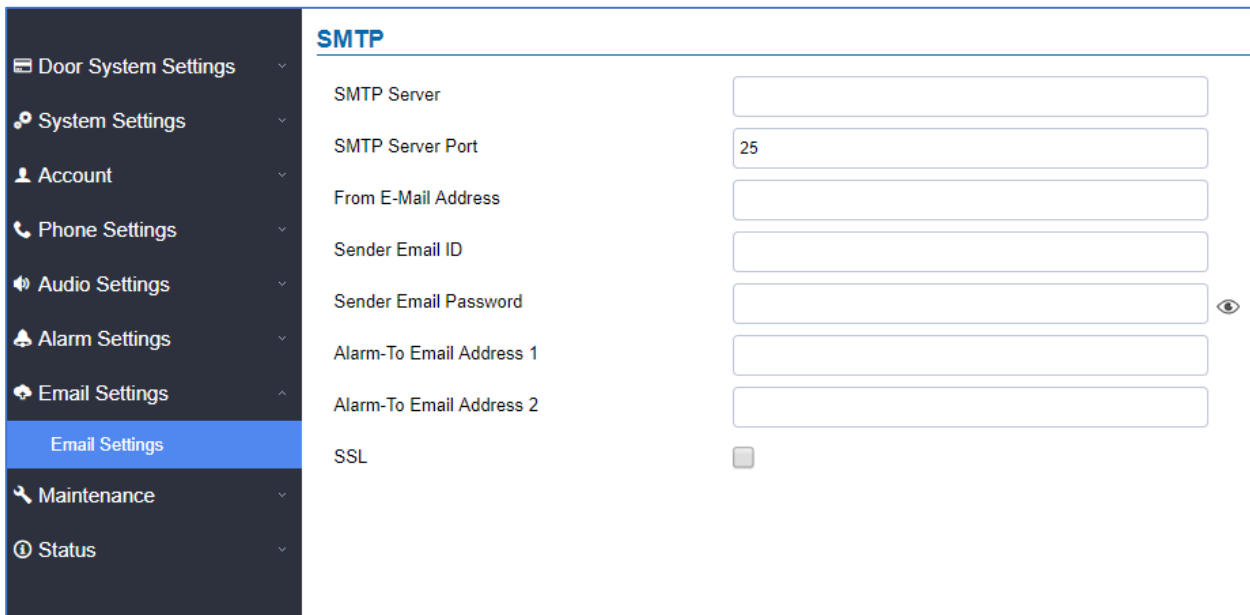


Figure 57: Email Settings - SMTP Page

Table 27: Email Settings - SMTP

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

Notes:

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

Maintenance Settings

This page shows the GDS3705 Maintenance parameters.

Upgrade

This page contains the upgrade parameters of the GDS3705.

<ul style="list-style-type: none"> Door System Settings System Settings Account Phone Settings Audio Settings Alarm Settings Email Settings Maintenance <ul style="list-style-type: none"> <li style="background-color: #007bff; color: white;">Upgrade Reboot & Reset Debug Log Data Maintenance Event Notification Event Log Trusted CA Certificates Status 	Upgrade
	Firmware
	Upgrade Via: HTTP
	Firmware Server Path: fm.grandstream.com/gs
	HTTP/HTTPS User Name: <input type="text"/>
	HTTP/HTTPS Password: <input type="password"/>
	Firmware File Prefix: <input type="text"/>
	Firmware File Postfix: <input type="text"/>
	Config
	Upgrade Via: HTTP
Config Server Path: fm.grandstream.com/gs	
HTTP/HTTPS User Name: <input type="text"/>	
HTTP/HTTPS Password: <input type="password"/>	
Config File Prefix: <input type="text"/>	
Config File Postfix: <input type="text"/>	
XML Config File Password: <input type="password"/>	
Validate Server Certificates: <input type="checkbox"/>	
Automatic Upgrade Interval(m): 10080	
Enable DHCP Option 66 Override Server: <input checked="" type="checkbox"/>	
Save	

Figure 58: Upgrade Page

Table 28: Upgrade

Upgrade Via	Selects the upgrade method (HTTP, HTTPS).
Firmware Server Path	Configures the IP address or the FQDN of the upgrade server.
Config Server Path	Configures the IP address or the FQDN of the configuration server.
HTTP/HTTPS User Name	User name if needed by remote provisioning HTTP/HTTPS server.
HTTP/HTTPS Password	Password to authenticate with remote provisioning HTTP/HTTPS server.
Firmware File Prefix	Prefix that will be added when requesting firmware file.
Firmware File Postfix	Postfix that will be added when requesting firmware file.
Config File Prefix	Prefix that will be added when requesting config file.
Config File Postfix	Postfix that will be added when requesting config file.
XML Config File Password	Specifies the password for the configuration file.
Validate Server Certificate	Enable this option to validate certificate with trusted ones during TLS connection.
Automatic Upgrade Interval(m)	Specifies the upgrade interval in minutes.
DHCP Option 66 Override Server	Activates DHCP option 66 to override upgrade/config servers.
Zero Config	Enables Zero Config feature for auto provisioning.
Automatic Upgrade	Enables automatic upgrade and provisioning.

Reboot & Reset

This page allows user to reboot and reset the GDS3705.



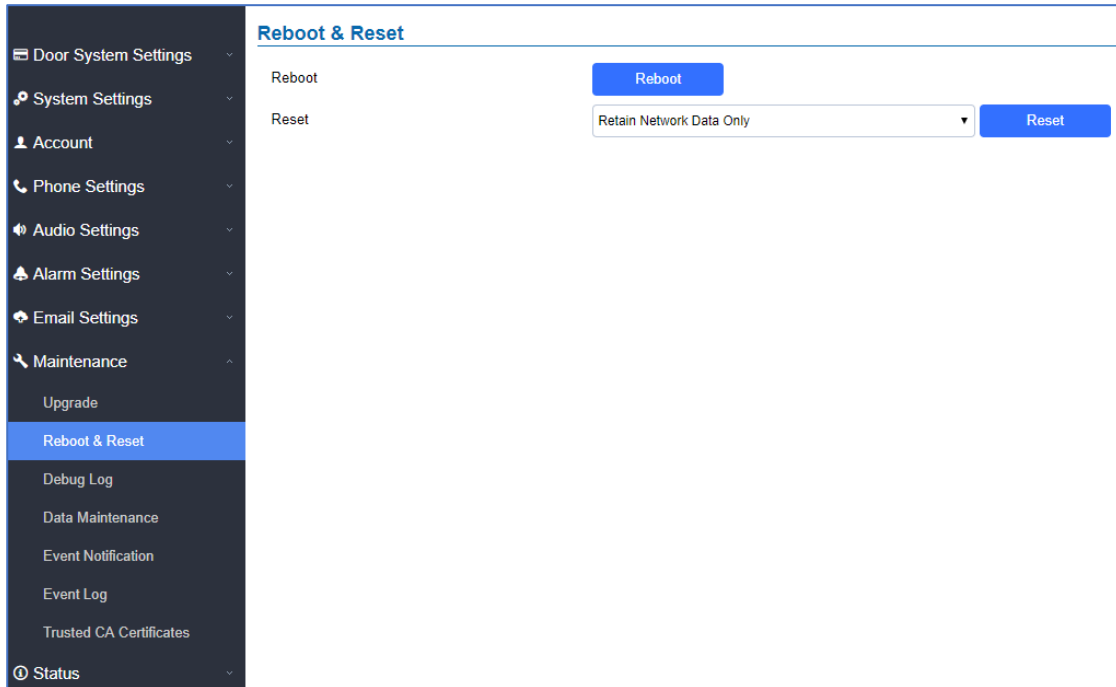


Figure 59: Reset & Reboot Page

Table 29: Reset & Reboot

Reboot	When clicked, the GDS3705 will restart (soft reboot).
Reset	There are two options for the reset function.
Clear All Data	All data will be reset, GDS3705 will be set to factory default.
Retain Network Data Only	All data will be erased except for Network data like IP address...
Retain Only Card Information	All data will be erased except for cards information.
Retain Network Data and Card Information	All data will be erased except for Network Data and Card Information.

Debug Log

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

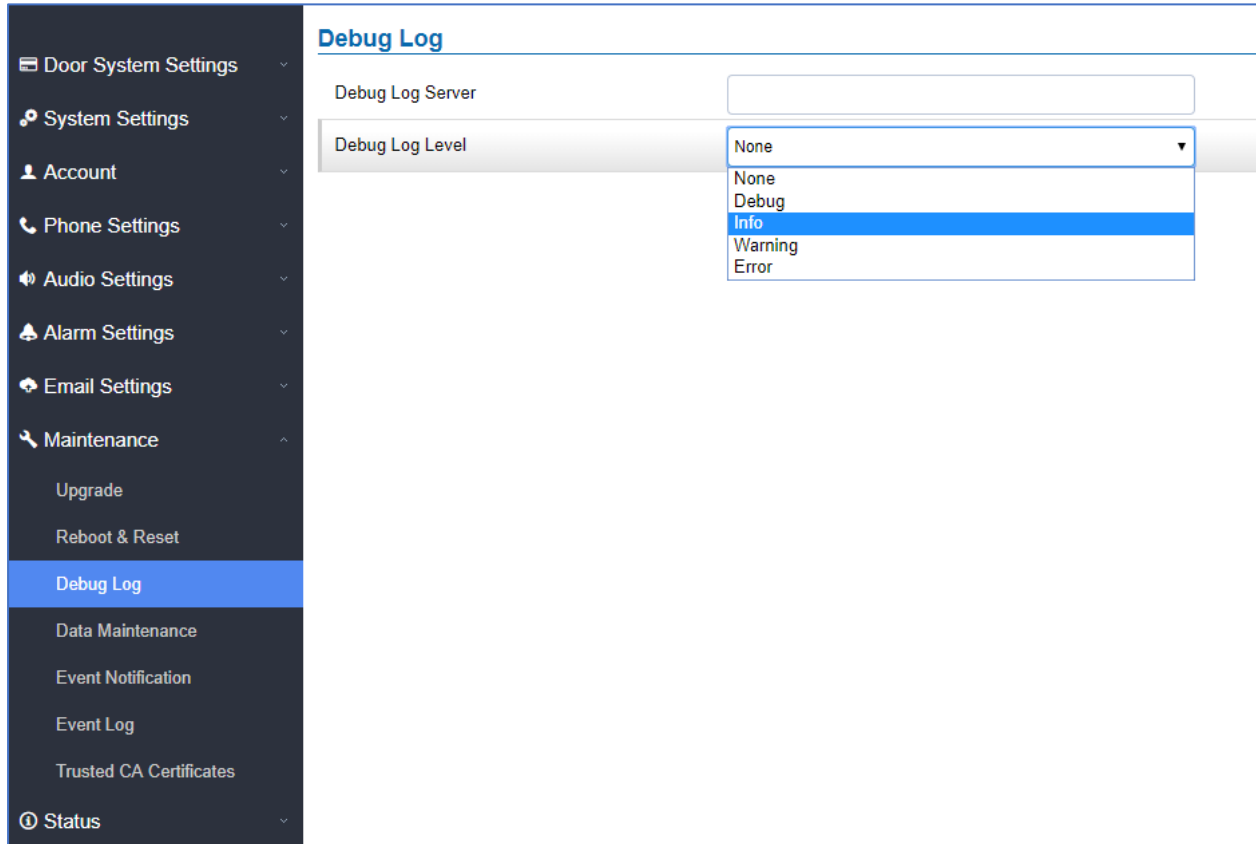


Figure 60: Debug Log Page

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.

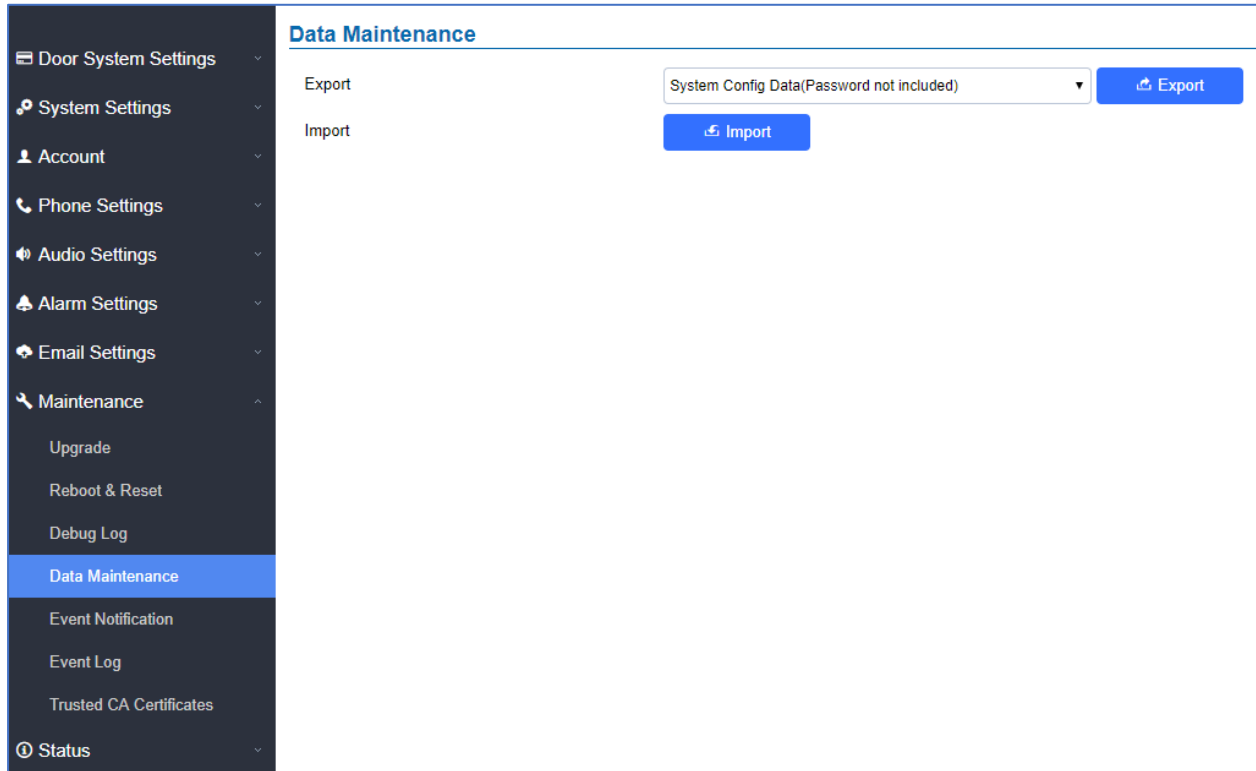



Figure 61: Data Maintenance Page

Click on  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.

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 3rd party software to integrate the GDS3705.

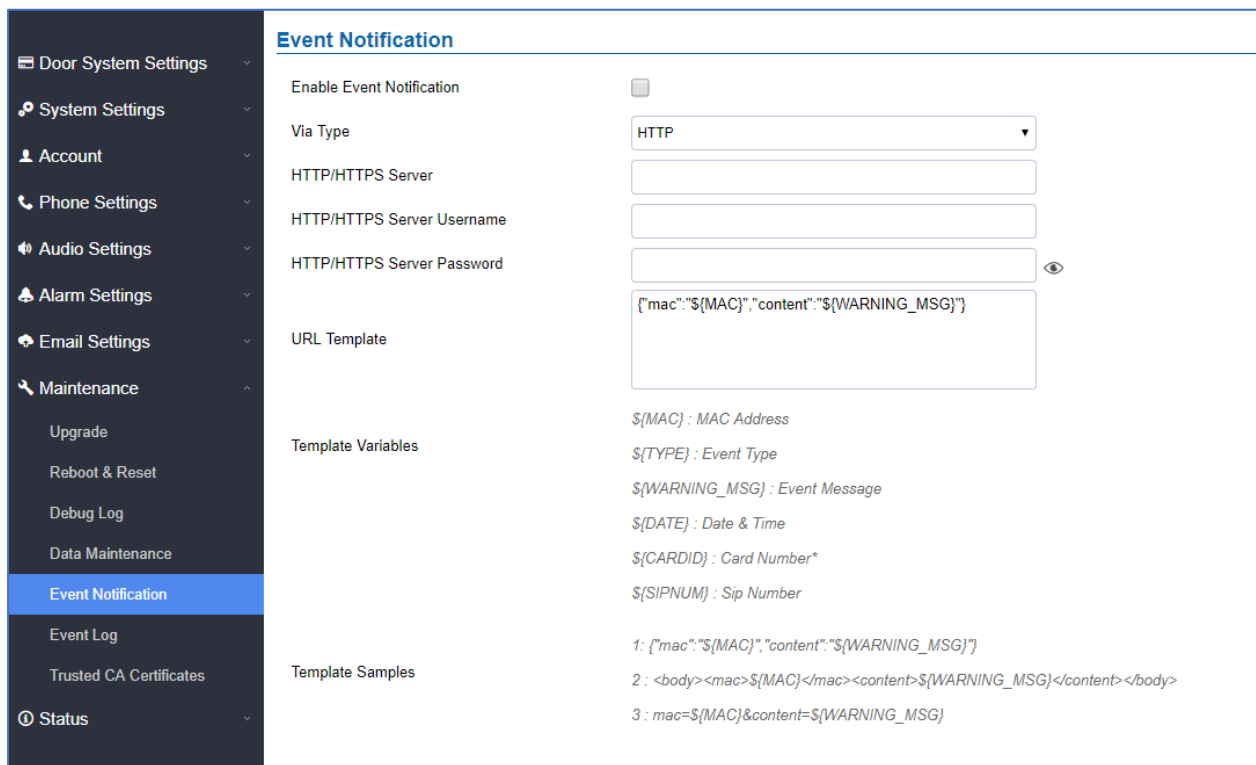
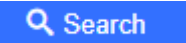


Figure 62: Event Notification

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

Event Log				
Start Time	2018-09-24 00:00:00	End Time	2018-09-24 12:32:55	All
<input type="button" value="Search"/>				
No.	Date & Time	Event Type	Card Number	(Account)Sip Number
1	2018-09-24 09:15:47	System Up		
2	2018-09-24 10:10:53	Reboot		

Figure 63: Event Log

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

Trusted CA Certificates

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

Trusted CA Certificates		
No.	Issued By	Expiration
1		
2		
3		
4		
5		
6		

Figure 64: Upload Trusted CA files

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

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

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

Status

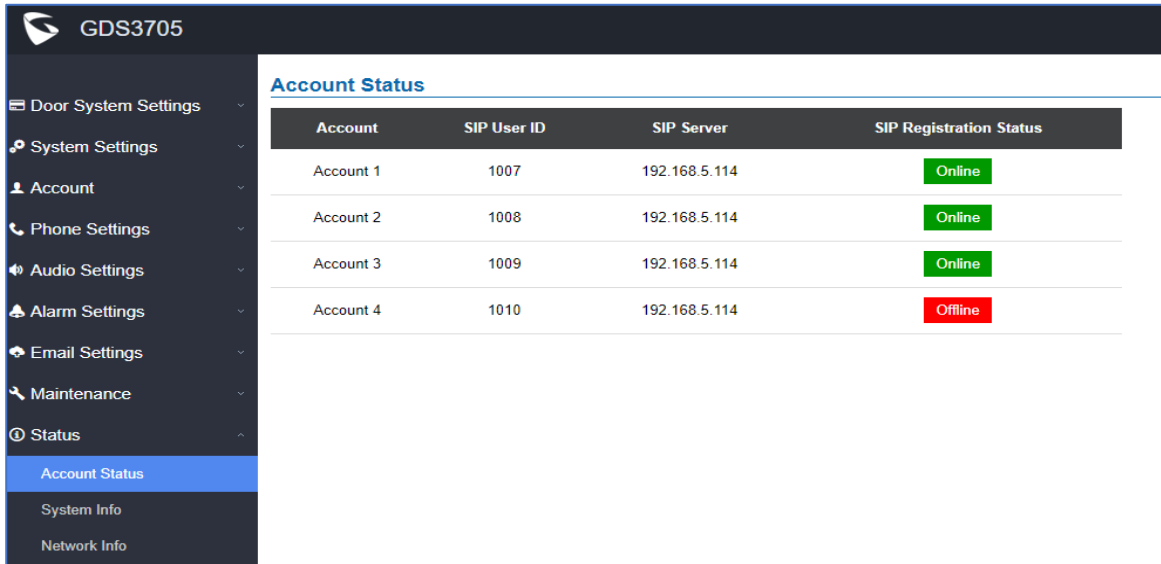
This page displays GDS3705 accounts, system and network information.

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**



GDS3705

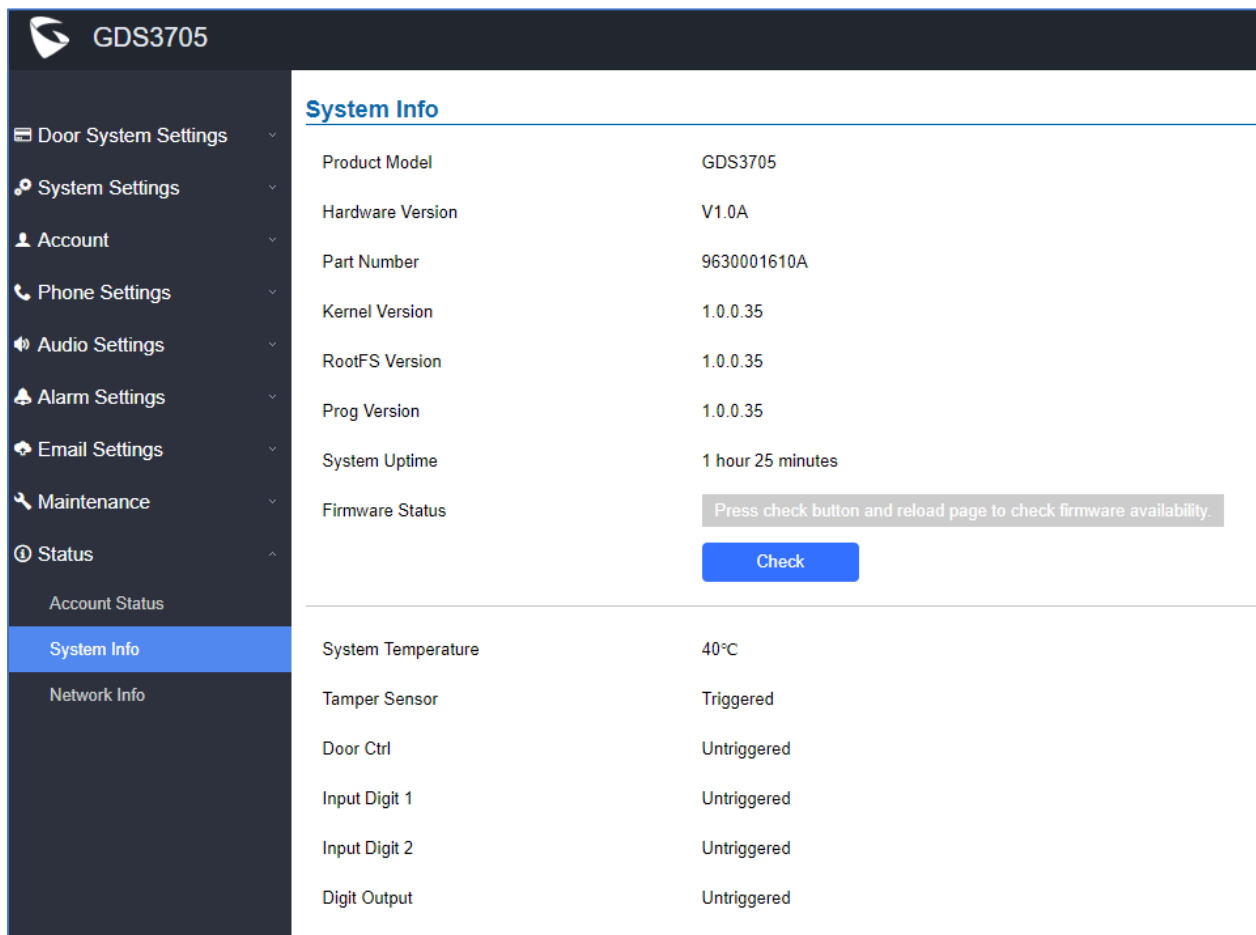
Account Status

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 65: Account Status Page

System Info

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



GDS3705


System Info

Product Model	GDS3705
Hardware Version	V1.0A
Part Number	9630001610A
Kernel Version	1.0.0.35
RootFS Version	1.0.0.35
Prog Version	1.0.0.35
System Uptime	1 hour 25 minutes
Firmware Status	<div style="border: 1px solid gray; padding: 2px;">Press check button and reload page to check firmware availability.</div> <div style="text-align: center; margin-top: 5px;"> <input type="button" value="Check"/> </div>
System Temperature	40°C
Tamper Sensor	Triggered
Door Ctrl	Untriggered
Input Digit 1	Untriggered
Input Digit 2	Untriggered
Digit Output	Untriggered

Figure 66: System Info Page



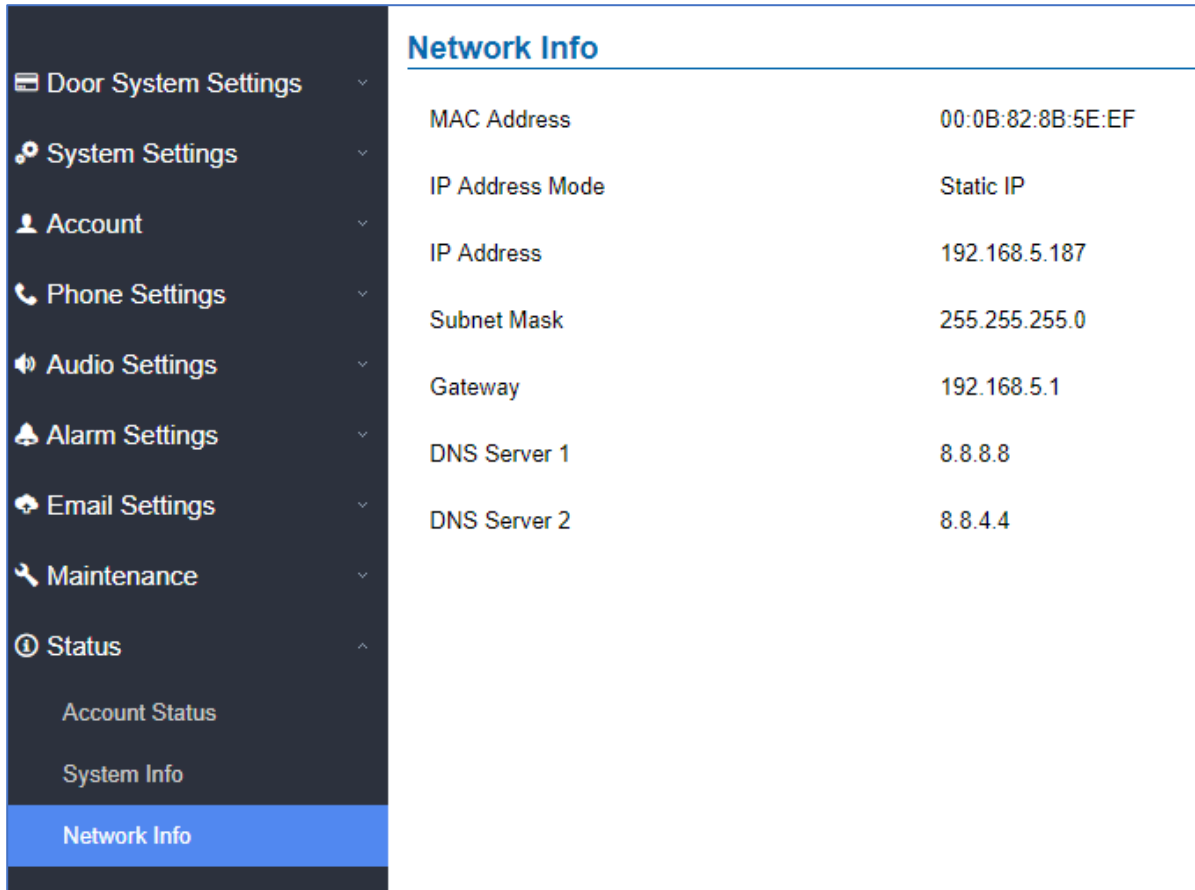
Table 30: System Info

Product Model	Displays the Product Model.
Hardware Version	Displays the Hardware Version.
Part Number	Displays the Part Number.
Kernel Version	Displays the Kernel Version.
RootFS Version	Displays the RootFS Version.
Prog Version	Displays the Prog Version.
System Up Time Since	Displays the time since the first boot of the GDS3705.
Firmware Status	Click the  button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
System Temperature	Shows the current system temperature.
Tamper Sensor	Shows if the Tamper Sensor is triggered or not.
Door Control	Shows if the door control is triggered or not (in case door is opened for example it will show triggered).
Input Digit 1	Shows if Alarm-IN 1 is triggered.
Input Digit 2	Shows if Alarm-IN 2 is triggered.
Digit Output	Shows if digital output is triggered.

Network Info

This page displays the network system information of GDS3705.





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 67: Network Info Page

Table 31: Network Info

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

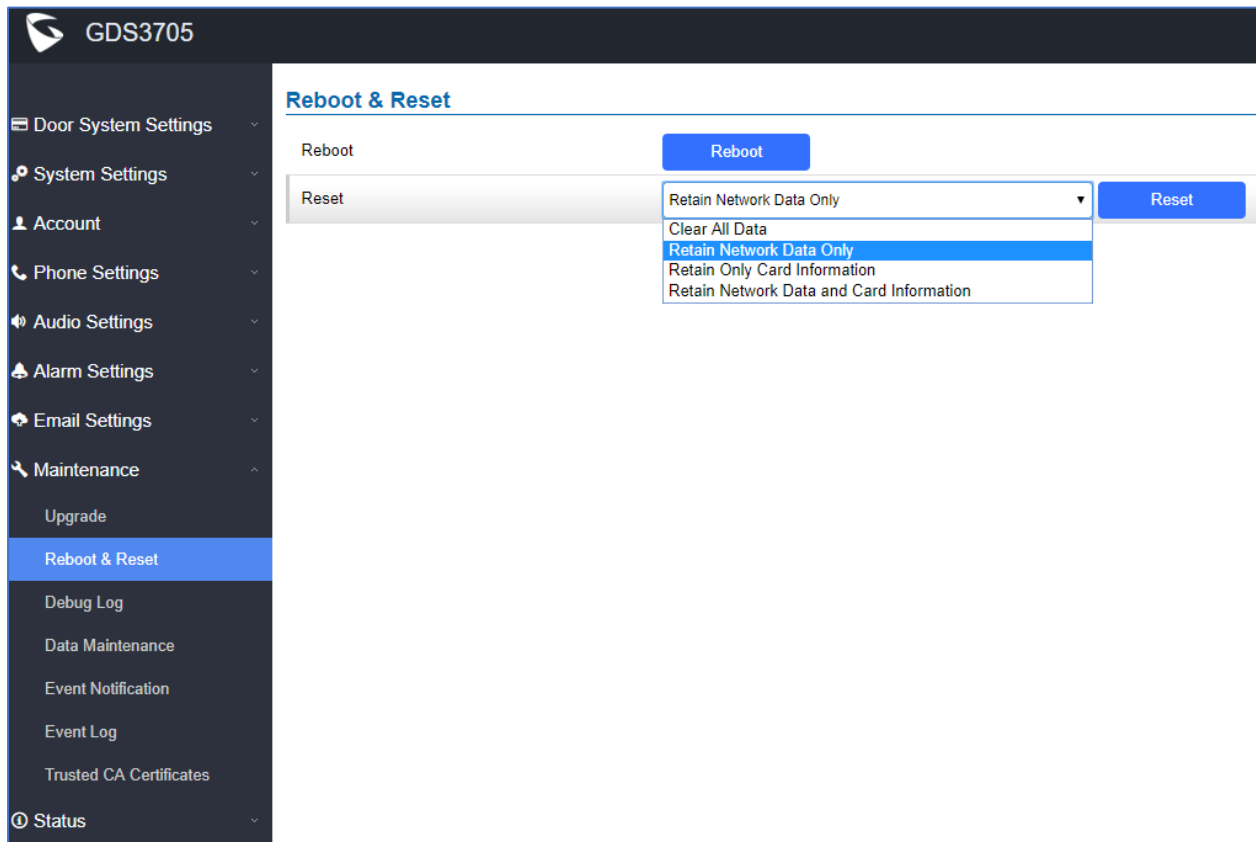


Figure 68: Reset via Web GUI

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 69: 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.

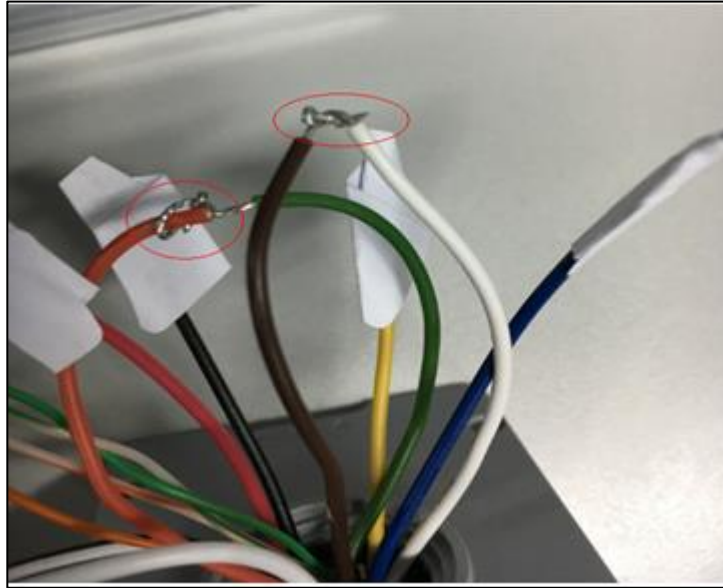


Figure 70: Wiegand Cable Connection

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.

EXPERIENCING THE GDS3705

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

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

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

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

