

GSC3570 – User Manual

WELCOME

Thank you for purchasing the Grandstream GSC3570 Integrated SIP Intercom Phone. The GSC3570 is a powerful Intercom phone for door control and a 2-way intercom. It features a 7” 1024×600 touch screen LCD, integrated dual-band 802.11ac Wi-Fi, 100M network port with PoE, full-duplex 2-way HD audio with advanced AEC, and innovative telephony functionalities. The GSC3570 is fully interoperable with nearly all major SIP platforms on the market and can be seamlessly integrated with Grandstream’s entire range of UC product lines, including SIP-based door systems, security cameras, IP PBXs, and video conferencing systems and services. This Intercom phone is the perfect choice for users looking for an integrated video control and a two-way voice communication solution for their wall mount.

PRODUCT OVERVIEW

Feature Highlights

The following tables contain the major features of GSC3570.

	• 4 lines. • 7” 1024×600 touch screen LCD TFT LCD with Home Key. • 2-way HD audio with advanced AEC. • Integrated dual-band 802.11ac Wi-Fi. • 100M network port with PoE, full-duplex.
---	--

GSC3570 Features at a Glance

GSC3570 Technical Specifications

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

Protocol/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTSP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP-MED, LDAP, TR-069, 802.1x, TLS, SRTP, IPv6, OpenVPN
Network Interface	Dual switched 10/100Mbps ports with integrated PoE
Graphic Display	7” 1024×600 capacitive touch screen TFT LCD with Home Key
Wi-Fi	Yes, dual-band 802.11b/g/n/ac (2.4GHz & 5GHz)
Auxiliary Ports	4 x Alarm Input 1 x Alarm Output Micro SD card slot Micro USB
Voice Codecs and Capabilities	G.711μ/a, G.722 (wide-band), G.726-32, iLBC, Opus, G.729A/B, DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Decoders and Capabilities	H.264 BP/MP/HP, video resolution up to 720p, frame rate up to 30 fps, bit rate up to 2Mbps

Telephony Features	4 SIP accounts, hold, call waiting, call log, auto answer, etc.
Sample Applications	Local apps: Contacts, Call History, Settings, Voicemail, Clock
Operating System	Linux 4.4
HD Audio	Yes, Dual speakers with support for wideband audio and media play in stereo, built-in microphone for improved voice quality, acoustic echo cancellation.
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	Double images for high reliability, random administrator password, user, and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES based secure configuration file, SRTP, TLS, 802.1x media access control
Multi-language	English, German, French, Spanish, and Chinese.
Upgrade/ Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file, manual upload
Power & Green Energy Efficiency	2-pin DC input: 12VDC/1A Integrated PoE: IEEE 802.3af Class 3, power consumption <10W Micro USB input: 5VDC/2A
Temperature and Humidity	Operation: -10°C to 50°C, Storage: -20°C to 60°C, Humidity: 10% to 90% Non-condensing
Package Contents	GSC3570 Intercom Phone, quick installation guide, wall mount bracket.
Compliance	FCC, CE, RCM, IC

GSC3570 Technical Specifications

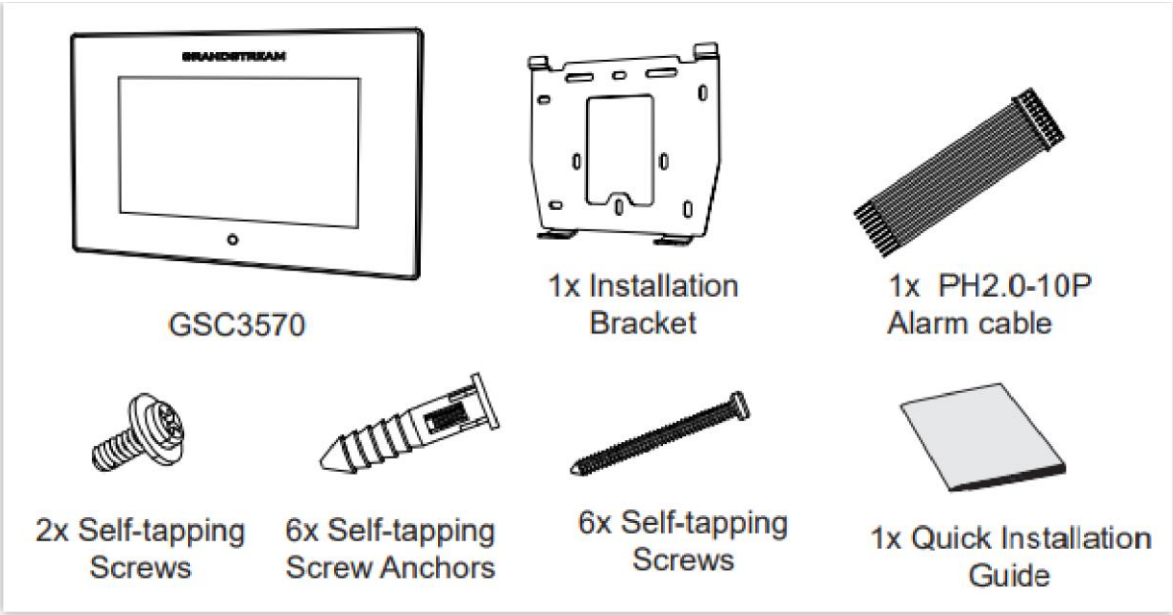
GETTING STARTED

This chapter provides basic installation instructions, including a list of the packaging contents and information for obtaining the best performance with the GSC3570.

Equipment Packaging

GSC3570
1x GSC3570. 1x Installation Bracket 1x PH2.0-10P Alarm cable 2x Self-tapping Screws 6x Self-tapping Screw Anchors 6x Self-tapping Screws 1x Quick Installation Guide

Equipment Packaging



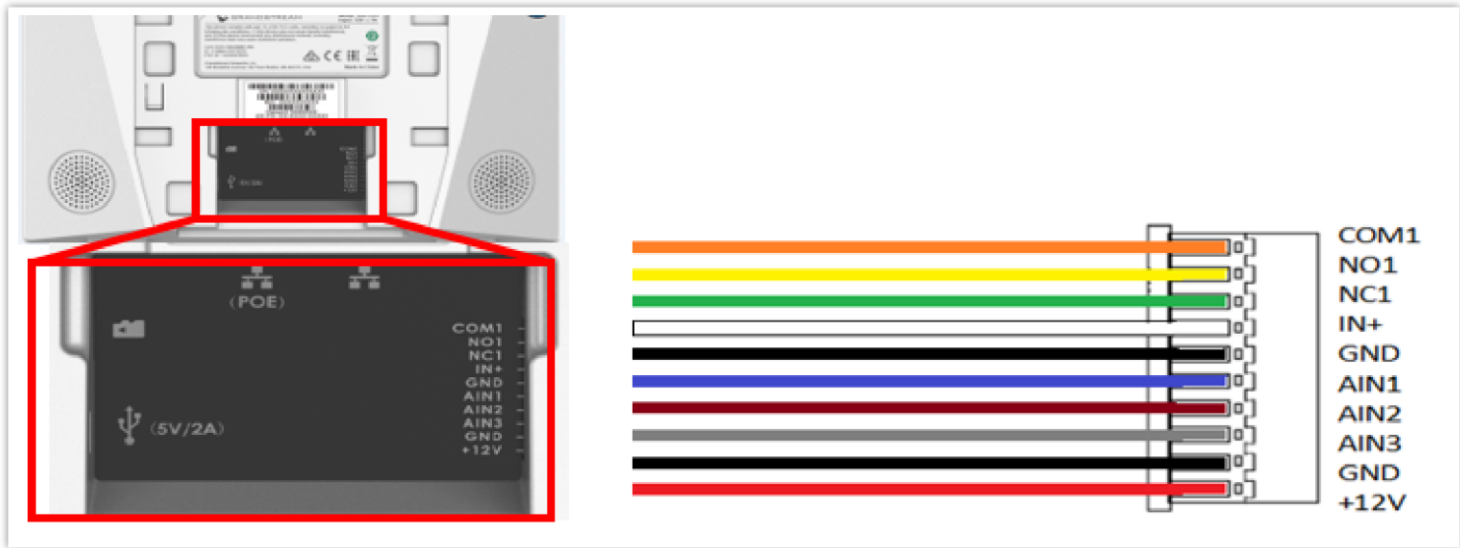
GSC3570 Package Content

Note

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

GSC3570 Wiring Connection

The following figure and table show the Connection PINs available on the GSC3570:



GSC3570 Wiring Connection

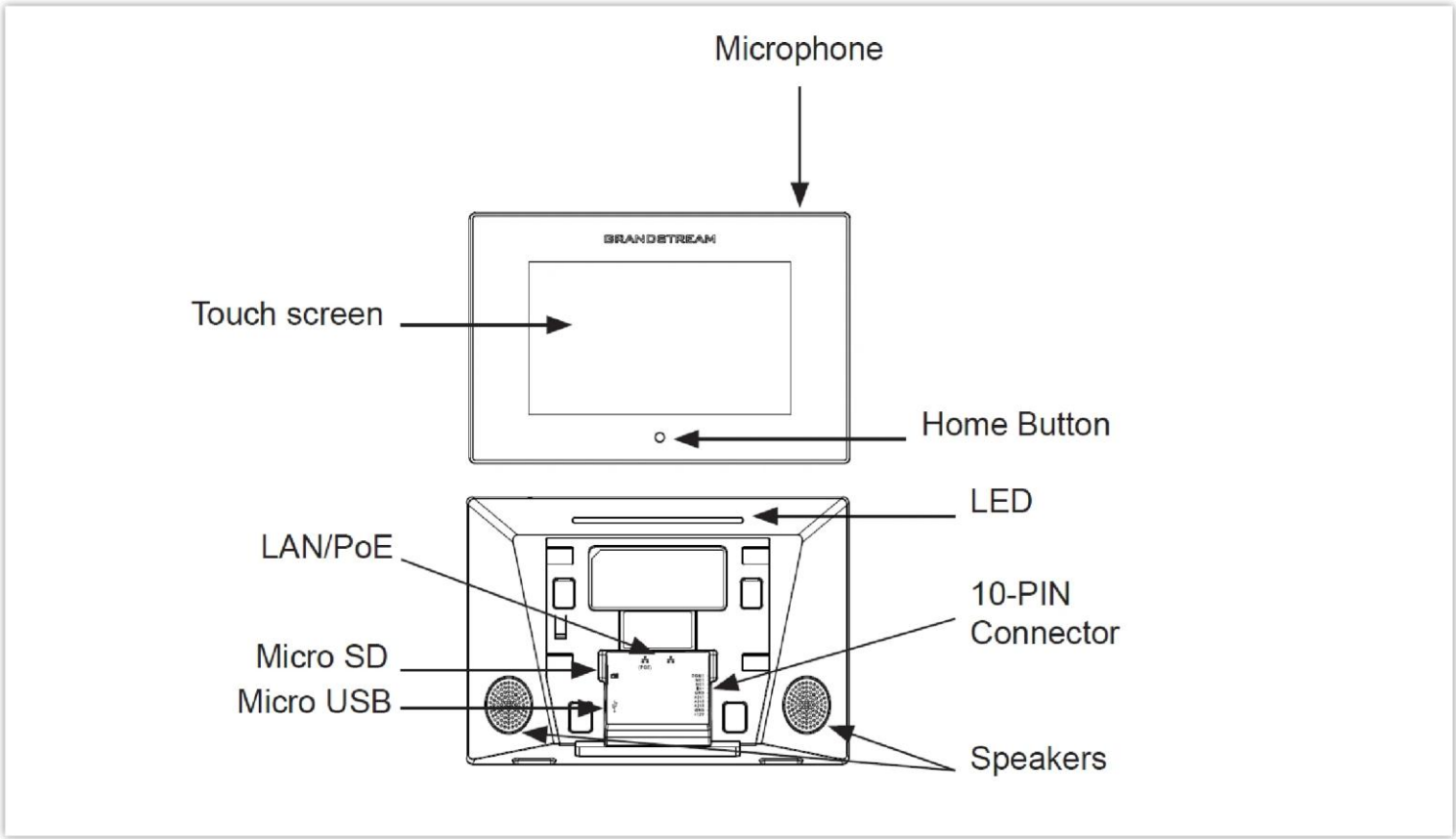
Jack	Port			Function	Remark
	Pin	Signal	Color		
J1	1	COM1	Orange	Alarm OUT	1 Relay output, normal open or close, max 125VAC/0.5A or max DC 30V/2A.
	2	NC01	Yellow		
	3	NC1	Green		
	4	IN+	White	Alarm IN (Active)	Alarm isolated input, for voltage signal detection, IN+ connect the sensor's signal output, please connect the GND to Alarm device's GND or Negative of power. Active voltage range 9-15V.
	5	GND	Black	Alarm GND	Voltage reference for IN+, Switch signal reference for AIN (1/2/3).

	6	AIN1	Blue	Alarm IN (Passive)	Alarm input, for button/door contacts switch signal detection. Please connect the Switch/button to AIN (1/2/3) and GND.
	7	AIN2	Brown		
	8	AIN3	Gray		
	9	GND	Black	Power Supply	DC12V recommend, input voltage rang 9-15V Current at least 1A at 12V.
	10	+12V	Red		
J2	Network Port			POE Supply LAN Port	Dual 10/100 Mbps Network ports: One is POE port with class AF mode. The other one is a LAN port.
J3	Micro SD Port			Data storage	Support microSD/SDHC/SDXC, up to 256G.
J4	Micro USB Port			Data exchange	Data exchange port, Not recommended to use this port to power supply. If needed, please use 5V/2A adapter.

GSC3570 Wiring Connection

GSC3570 Setup

The following illustration shows the different ports and interfaces of the GSC3570 device.



GSC3570 Description

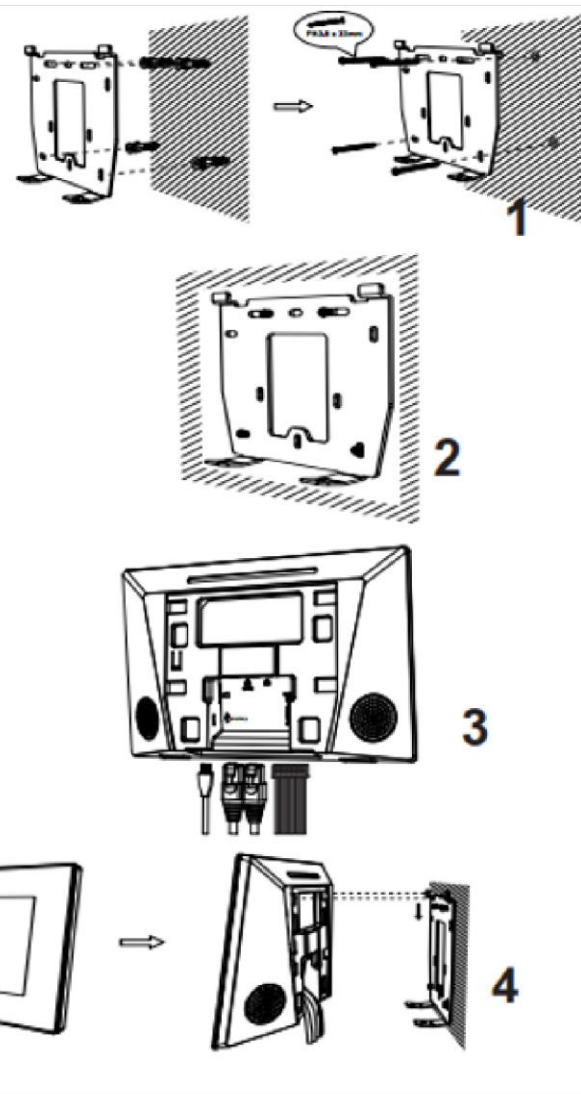
Device Installation

The GSC3570 supports both in-wall and on-wall mounting options to suit various installation environments. Please follow the appropriate steps below for secure and proper installation:

On-Wall Mounting

The GSC3570 can be mounted on the wall. Please refer to the following steps for the Wall installation:

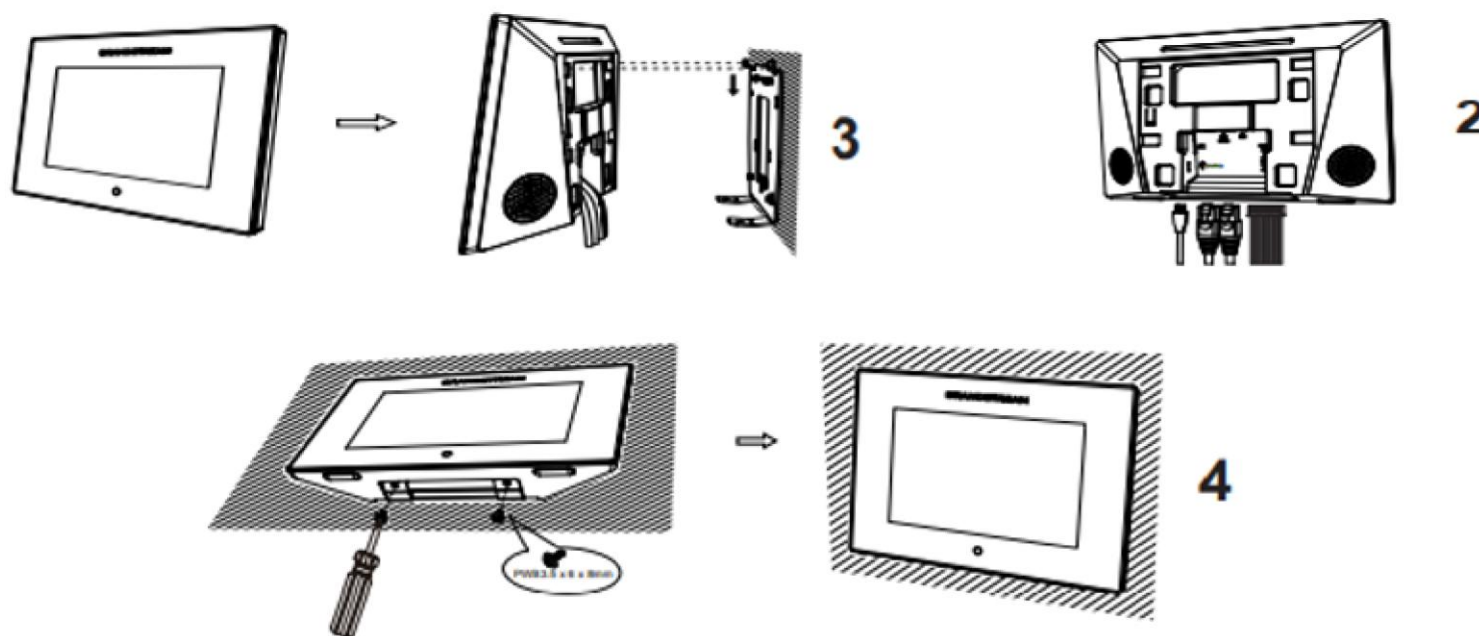
1. Locate the equipment holder on the desired position. Drill four holes on the wall referring to the positions of the ones on the metal bracket. Then, fix a Screw Anchor in each hole.
2. Fix the metal bracket on the wall by Self-tapping Screws.
3. Plug in the cables to the proper GSC3570 ports on the back.
4. Align the position slots on device's back with their correct placement on the Metal Bracket, then fix it by pushing Down.
5. Plug in the Self-tapping Screws at bottom to attach the device to the metal bracket.



On wall Mounting

In-Wall Mounting

1. Locate the box screw holes and align them with the metal bracket holes. Then, fix a Self-tapping Screw on each hole. Below are the supported Box dimensions:
 - 80mm x 80mm
 - 71mm x 115mm
 - 115mm x 115mm
2. Plug in the cables to the proper GSC3570 ports on the back.
3. Align the position slots on device's back with their correct placement on the Metal Bracket, then fix it by pushing Down.
4. Plug in the Self-tapping Screws at bottom to attach the device to the metal bracket.



In Wall Mounting

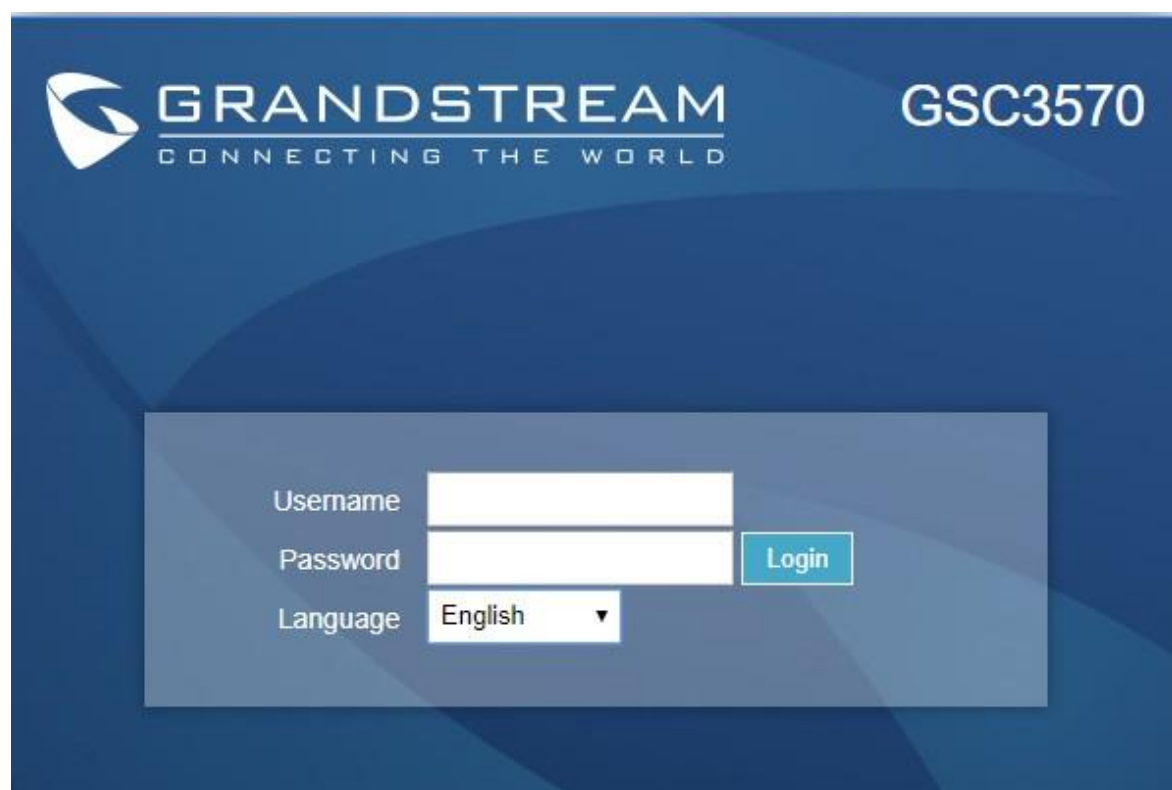
Connecting the GSC3570

To set up your GSC3570 from the web interface, please follow the steps below:

1. Ensure your device is powered up and connected to the Internet.
2. Slide to the second home page and press "Settings".
3. Select "Network Status" to check the IP address.
4. Type the unit's IP address in your PC browser. (See figure below).
5. Enter the admin's username and password to access the configuration menu.

Note

The factory default username is "admin" while the default random password can be found on the sticker at the back of the unit



GSC3570 web interface

To set up your GSC3570 from the LCD, please follow the steps below:

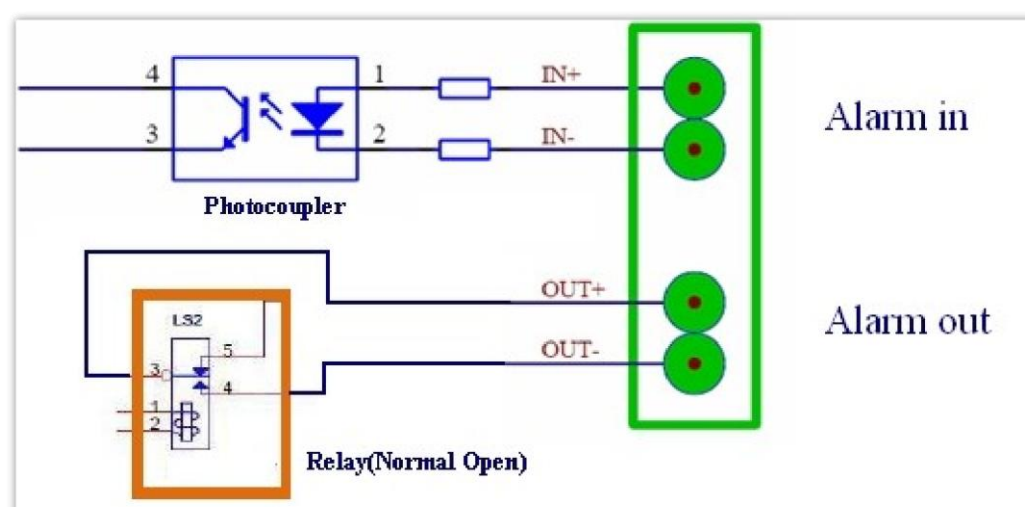
1. Make sure the device is idle.
2. Slide to the second home page and press "Settings". Browse the GSC3570 MENU for Status, Network information, Features, and Basic/Advanced Settings...
3. Press the "Home" Button to go back to the idle screen.

Alarm IN/OUT

Alarm_In could use any 3rd party Sensors (like an IR Motion Sensor).

Alarm_Out device could use a 3rd party Siren and Strobe Light, or an Electric Door Striker, etc.

The figure below shows an illustration of the Circuit for Alarm_In and Alarm_Out.



Alarm InOut Circuit for GSC3570

Notes:

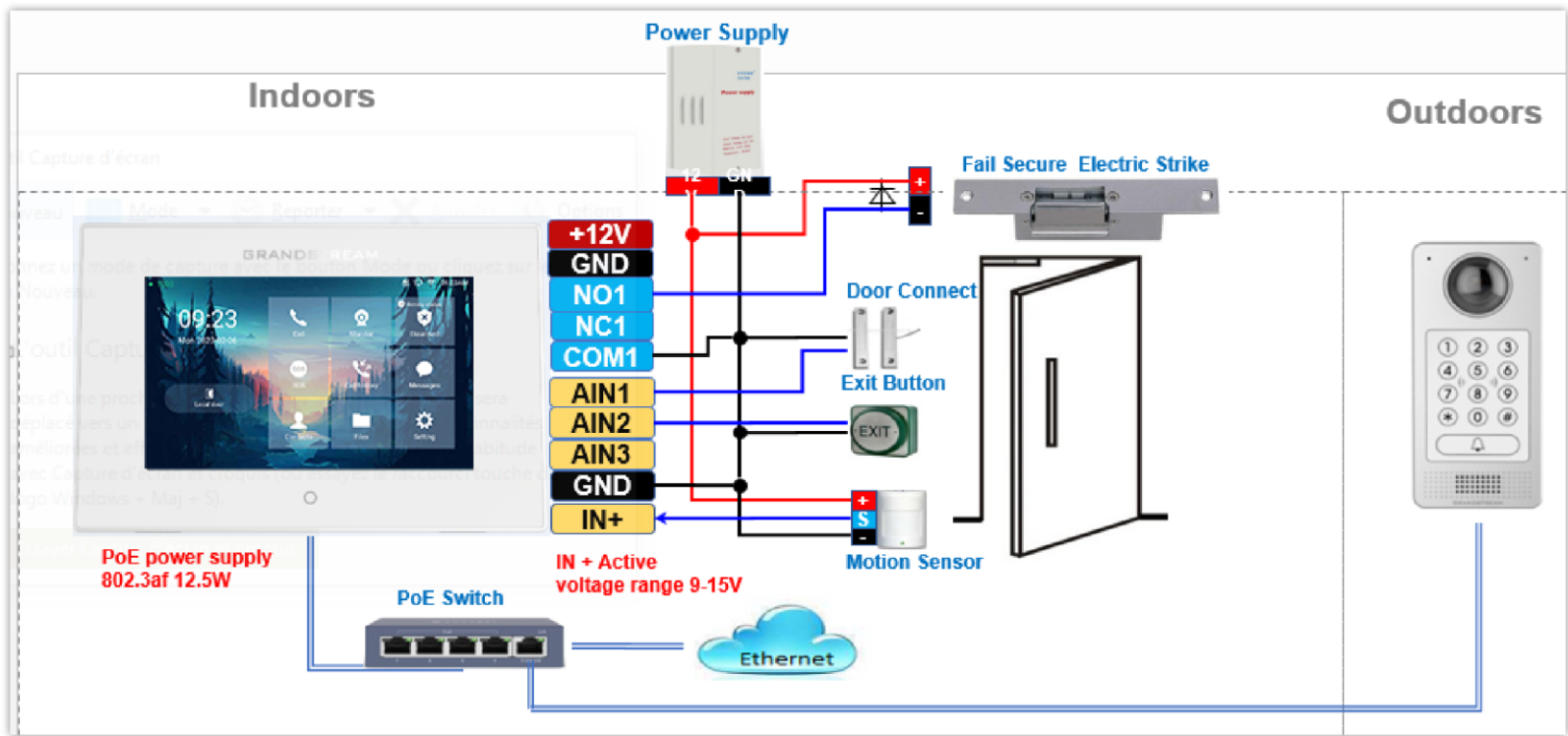
- The Alarm_In and Alarm_Out circuit for the GSC3570 should meet the following requirements:

Alarm Input	9V<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 9V and 15V, as specified in the table above, will detect it and trigger the corresponding action and event at the GSC3570 Alarm_In port.
- Higher voltage and incorrect polarity connections are prohibited because they can damage the devices.

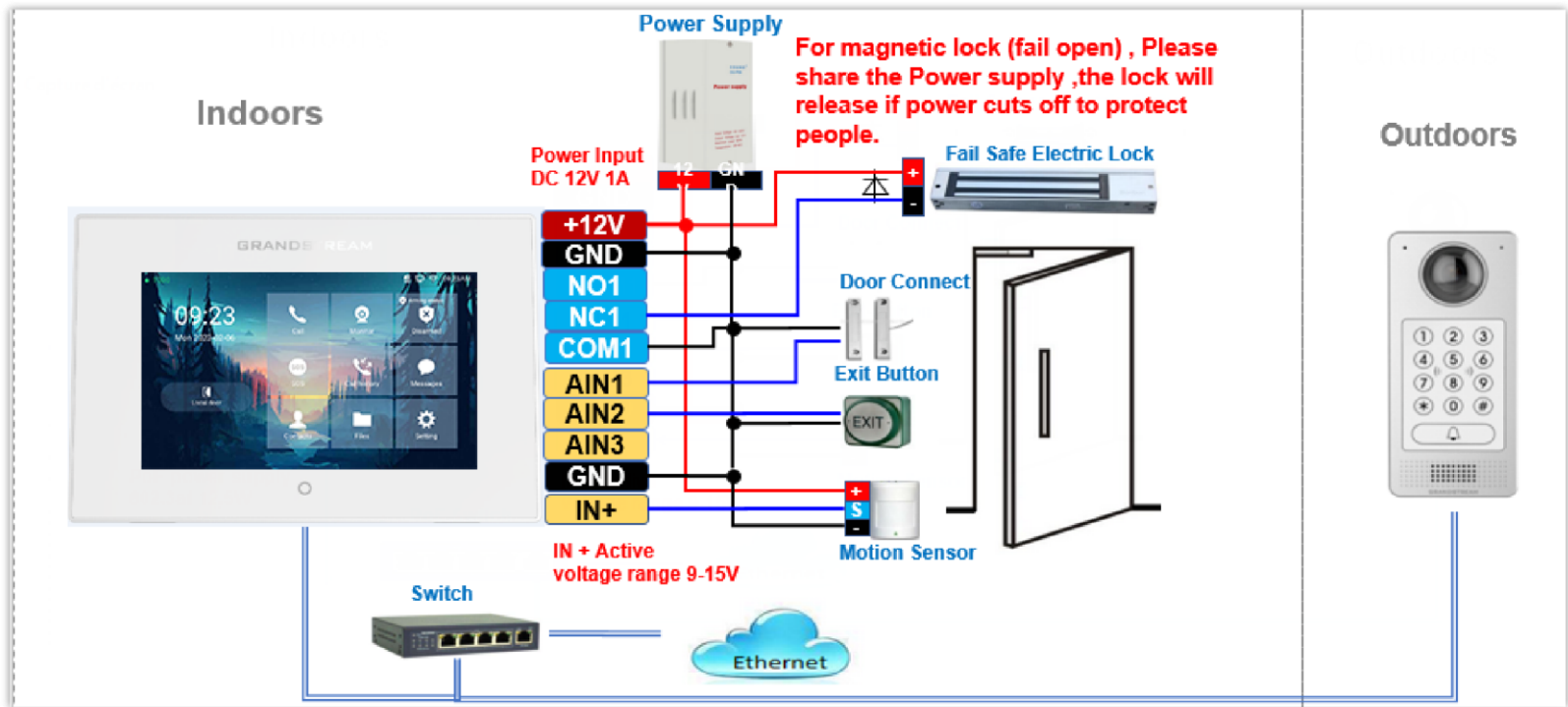
Connection Examples

GSC3570 Connection & Wiring Diagrams – “Fail Secure” Electric Strike, POE Power Supply



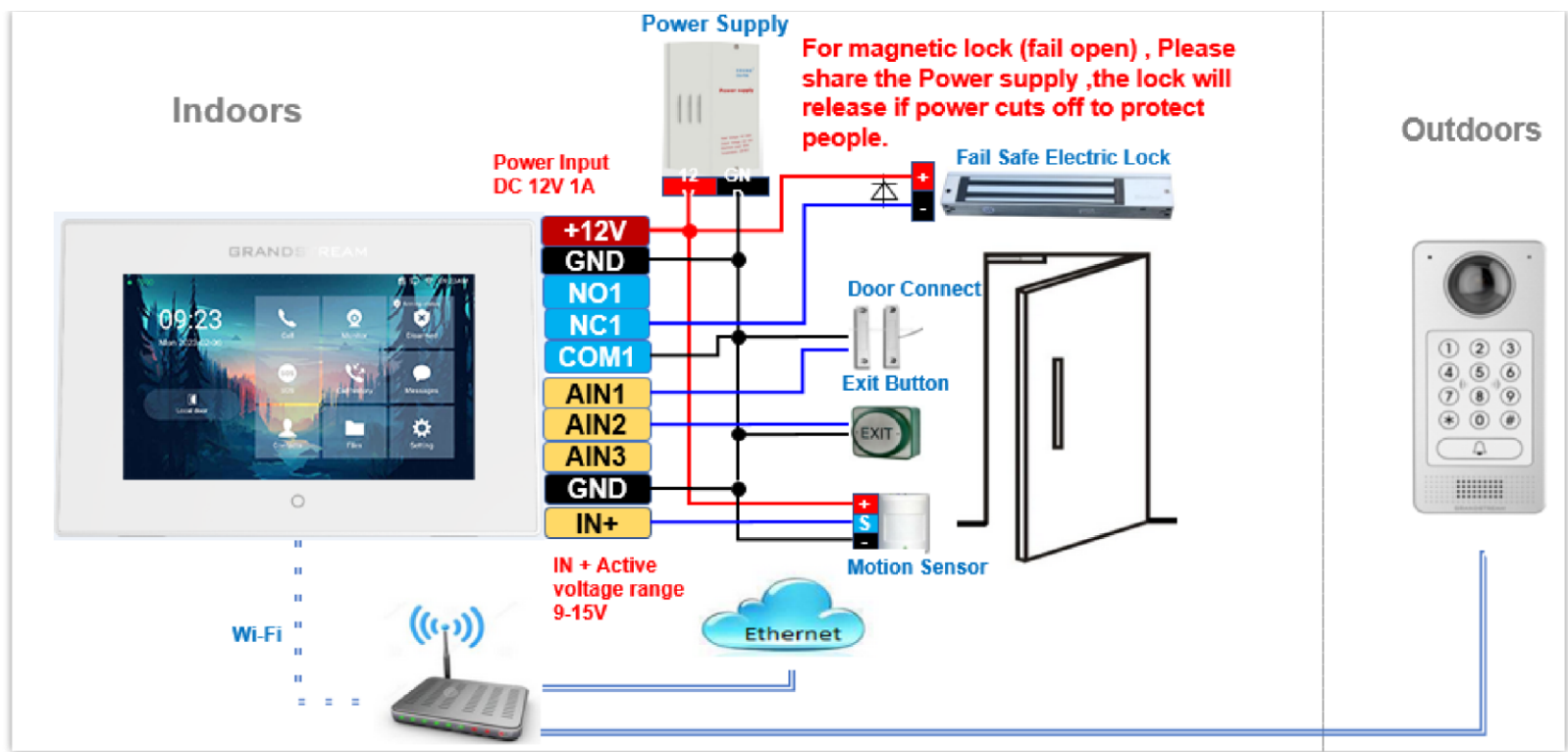
Fail Secure Electric Strike POE Power Supply

GSC3570 Connection & Wiring Diagrams – “Fail Safe” Electric lock, 3rd Party Power Supply



Fail Safe Electric lock 3rd Party Power Supply

GSC3570 Connection & Wiring Diagrams – “Fail Safe” Electric lock, Power Supply, and Wi-Fi



Fail Safe Electric lock 3rd Party Power Supply Wi Fi

Connecting GSC3570 with GDS37xx

The GSC3570 can be configured with up to 20 GDS37xx devices, allowing two doors of remote control per GDS. The configuration is done as follows:

Web interface configuration:

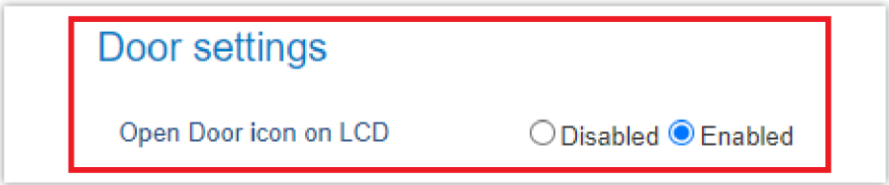
1. Access **Settings**→ **External Service**.
2. Select the **Service Type**, which could be **GDS**, **Others**, or **HTTP**, in case you want to integrate GSC3570 with a third-party Door Access Control system
3. Select the **Account** on which the remote door opening with the softkey will be applied.
4. Enter the name of the GDS unit in **System Identification**. (not a mandatory field)
5. Set GDS SIP Number (or IP address in case of the peering scenario) on **System Number**.
6. Enter the **Door 1 name**. (not a mandatory field)
7. Enter the **Door 1 Access Password**.
8. Enter the **Door 2 name**. (not a mandatory field)
9. Enter the **Door 2 Access Password**.
10. Enter the **HTTP URL** in case the service type chosen is HTTP.
11. Click on Save and Apply.

Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password	HTTP URL
1	HTTP	Account 1	GDS3710_Door1	192.168.5.207	192.168.5.207					
2	HTTP	Account 1	GDS3710_Door2	192.168.5.207	192.168.5.207					
3	GDS	Account 1	GDS3712	1012	192.168.5.59					
4	GDS	Account 1								
5	GDS	Account 1								
6	GDS	Account 1								
7	GDS	Account 1								
8	GDS	Account 1								
9	GDS	Account 1								
10	GDS	Account 1								
11	GDS	Account 1								
12	GDS	Account 1								
13	GDS	Account 1								
14	GDS	Account 1								
15	GDS	Account 1								
16	GDS	Account 1								
17	GDS	Account 1								
18	GDS	Account 1								
19	GDS	Account 1								
20	GDS	Account 1								

External Service Web Configuration

10. Access **Maintenance** → **LCD Access** → **Door settings**

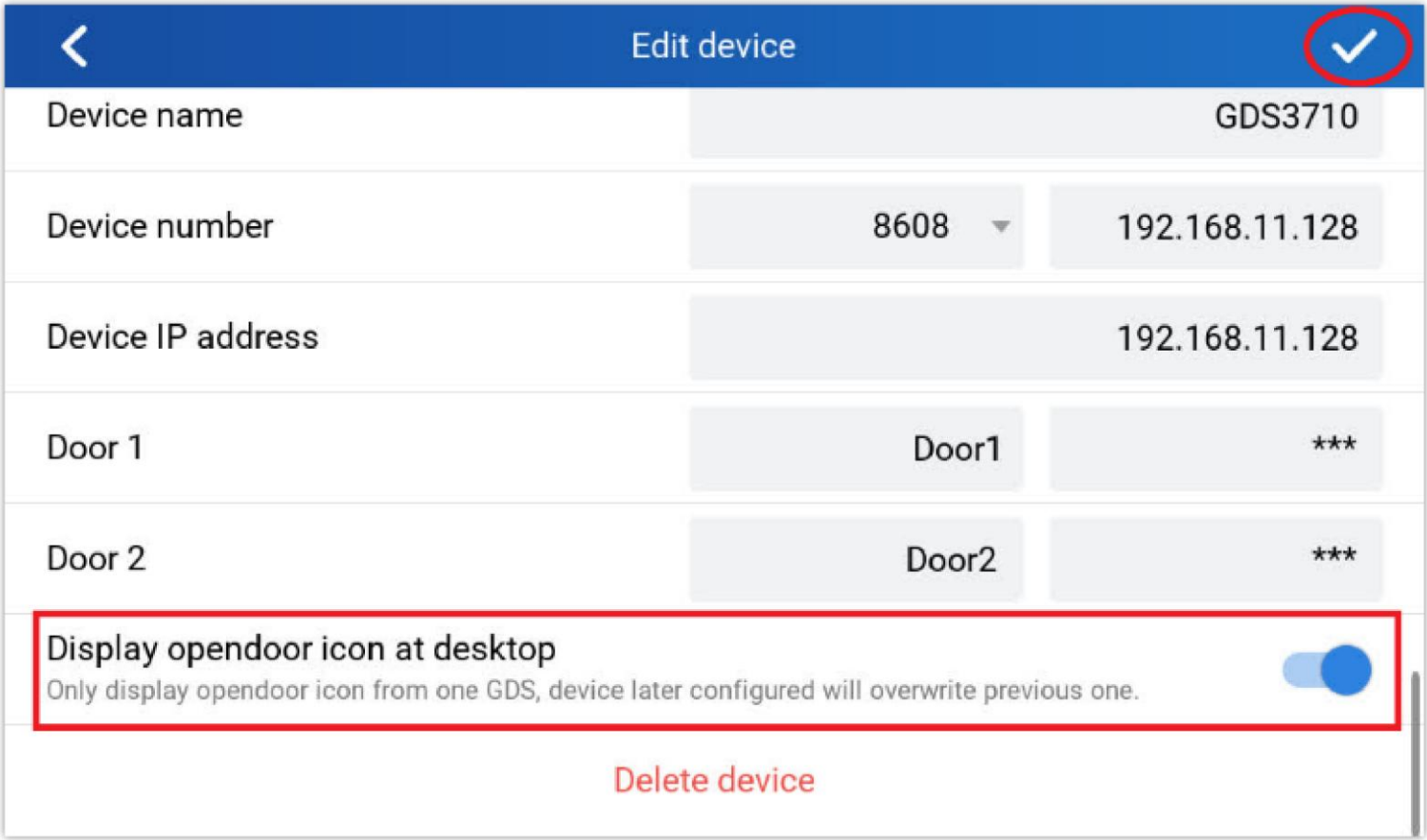
11. Enable “**Open Door icon on LCD**”.



LCD Access Door settings

LCD configuration:

- 1. Tap the menu button if GSC3570 is in the idle state.
- 2. On the first screen menu, tap **Monitor**→ **Door System**.
- 3. Press the **ADD** or **+** button to add a new GDS.
- 4. Enter the GDS Name in the **Device Name** field.
- 5. Select the Account that will have the remote door opening feature and enter the GDS SIP extension (or IP address in case of peering scenario) in the **Device Number** field.
- 6. Enter the **Door Name** for Door 1 and the **Remote PIN to Open Door 1** configured in the GDS in the **Password** Field.
- 7. Enter the **Door Name** for Door 2 and the **Remote PIN to Open Door 2** configured in the GDS in the **Password** Field.
- 8. Enable the “**Display Open door**” icon on the desktop.



External Service LCD Configuration

9. At the GSC3570 idle screen, once configured correctly, there will be one or two virtual buttons displayed at the lower left corner of the screen. If one door is configured, one button will be displayed; if two doors are configured, two buttons will be displayed.



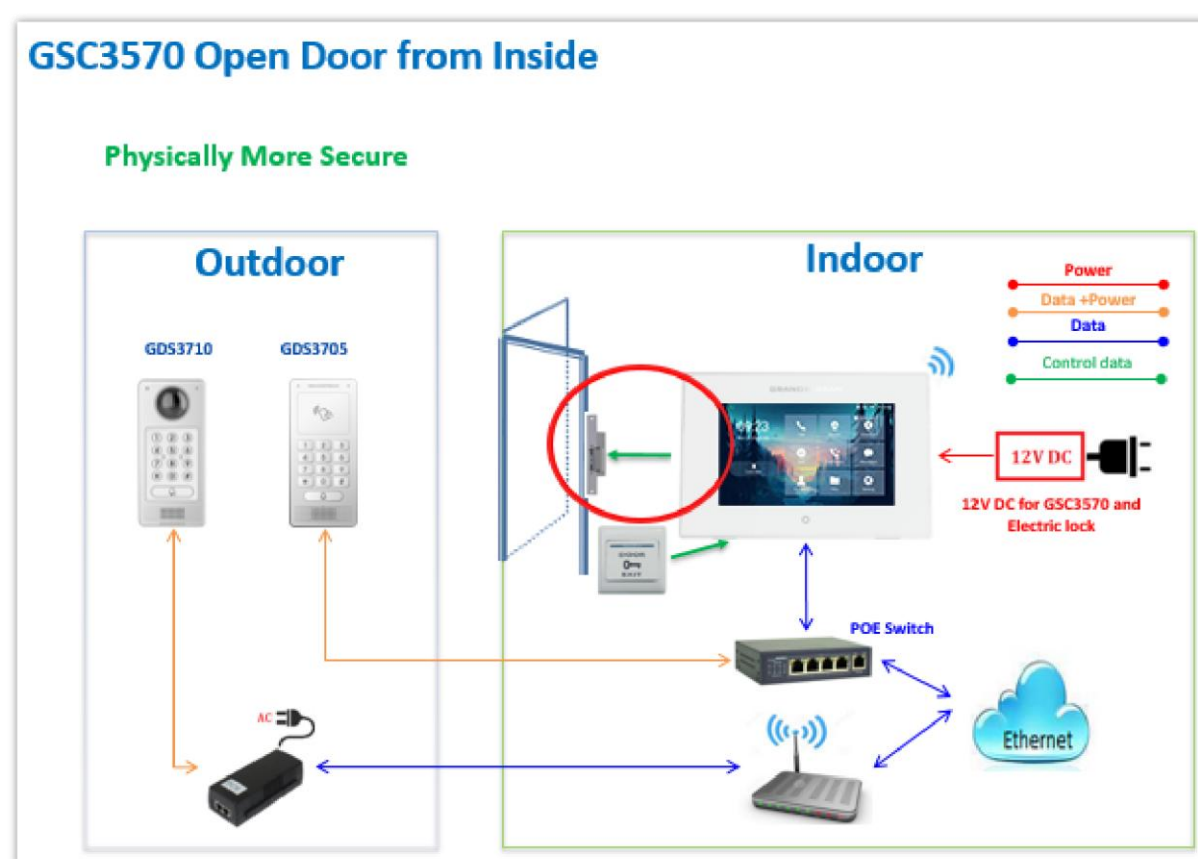
Open door on the GSC3570 idle screen

Notes

- Only ONE GDS37xx can be paired with GSC3570 for such a Virtual Button Open Door
- If the user configures multiple GDS37xx for such a Virtual Button Open Door, the device would NOT prompt the error, but the new input will overwrite the old input, and only the LAST input GDS37xx will work with the corresponding Virtual Button in GSC3570.

Secure Open Door Peering with GDS37xx

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



Secure Open Door Peering with GDS37xx

Notes

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

- GDS371x firmware 1.0.7.19 or above / GDS370x firmware 1.0.1.13 or above are required to work with GSC3570.
- Only one door can be controlled by the GSC3570 since it has only one Relay Control circuit.

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

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

Connecting GSC3570 with 3rd Party Door Access Systems

By selecting and configuring the supported related 3rd party door access system here, when GSC3570 is in a SIP call with DTMF open door operation, the “Soft Button” preprogrammed will appear on the GSC3570 touch screen. The user will be able to press the soft key to send the Open Door PIN to a related 3rd party door access control system to open the door.

This is an enhancement to help system integrators and customers integrate GSC3570 with a third-party Door Access Control system to operate the open door remotely.

Settings

Grandstream Door System

General Settings	Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password
External Service	1	GDS	Account 1	Front_Door	873		Front_Door	
	2	GDS	Account 1	Back_Door	877		Back_Door	
Digital Output	3	GDS	Account 1	GDS3710	8606	192.168.11.125	SIP	
	4	Other	Account 1	3rd Party Door Access	8608		Side_Door	*****
Alarm	5	GDS	Account 1					

External Service 3rd Party Door Control Systems Web Configuration

Note

Starting from firmware version 1.0.5.21, the number of external service operations supported has been increased from 10 to 20.

Using GSC3570 as a Doorbell and a Door opener

The GSC3570 can behave like a doorbell and an open door if the door strike is wired directly to the relay control port of the GSC3570. For licensed electricians, this is a perfect digital upgrade solution for users with a broken traditional analog doorbell system. The existing wiring and switch can be connected to GSC3570, so when visitors press the door switch, the GSC3570 will play a DING-DONG doorbell tone. If connecting the electrical strike directly to the GSC3570 relay control port, a 3d party audio/light strike device can be configured to be triggered when the GSC3570 receives an incoming call, then the user can press the Open-door Icon from the GSC3570 to open the door directly. It can combine with the GSC36xx IP camera to form an absolution package.

GSC3570 as a Digital Doorbell

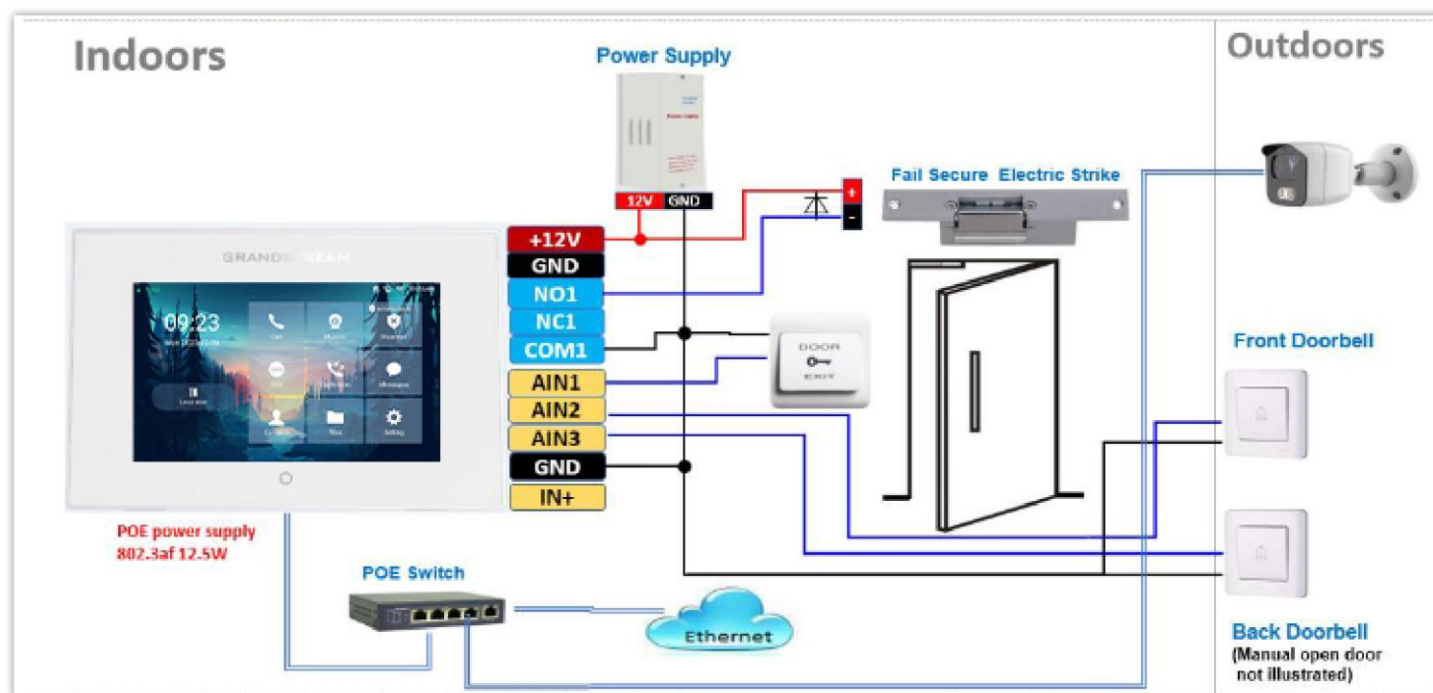


- ❖ DI set as Doorbell in Arming Mode, Wired to Outside Doorbell.
- ❖ GSC3570 plays a DING-DONG tone when Doorbell pressed, also it can trigger an audio/light strike when connected to a 3d party device, The touch screen will pop-up open-door window, pressing the "Open" button to open door from inside.

GSC3570 as a Digital Doorbell and door opener example

This feature is designed to allow GSC3570 to function like a traditional doorbell and open the door if wired to an electric lock, a simple digital upgrade to a traditional (broken) doorbell. If combined with an IP camera, it can help to monitor and update the home security without paying the subscription fee usually involved for such a service.

The wiring example of GSC3570 as a doorbell and open door:



GSC3570 as a Digital Doorbell and door opener wiring example

Wiring:

1. A switch (doorbell button) needs to be wired to AIN1 (Blue), AIN2 (Brown), or AIN3 (Grey) and Ground (Black).
2. The label is printed on the back of GSC3570, and a cable with a color code is provided with the package. Maximum 3 switches/buttons can be connected (example: Front Door, Back Door, Garage Door), but ONLY 1 electrical lock or strike can be controlled (because GSC3570 only has 1 relay control port (COM1, NO1/NC1)).

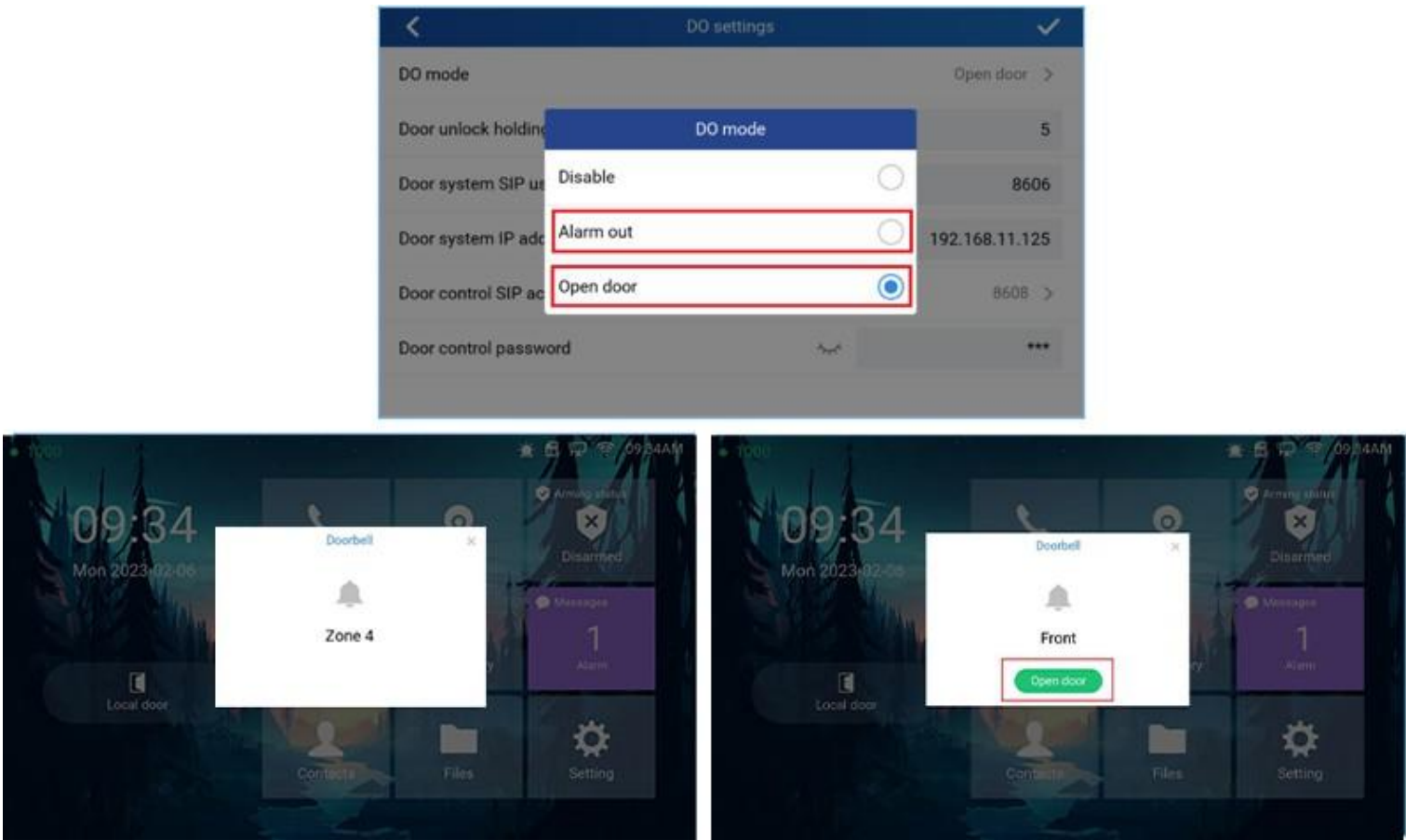
Configuration from Touch UI Screen:

Below are the screenshots of how to configure and enable this feature. This feature is revised from the Zone/Alarming feature; therefore, THREE steps are required:

I. DO mode set to "Alarm out" or "Open door":

1. From touch UI, press "Settings", select "DO settings"

- 2. Choose "DO mode", select "Alarm out" if no door strike is connected, and only want to use the Ding-Dong doorbell tone. No virtual open door button will be displayed in the Alarm Message.
- 3. Choose "Open door" if COM1, NO1/NC1 is connected to the strike to control the door opening. A green virtual open door button will be displayed in Alarm Message when the doorbell switch is pressed.
- 4. Press "<" to exit and select "✓" sign to save the change just made.



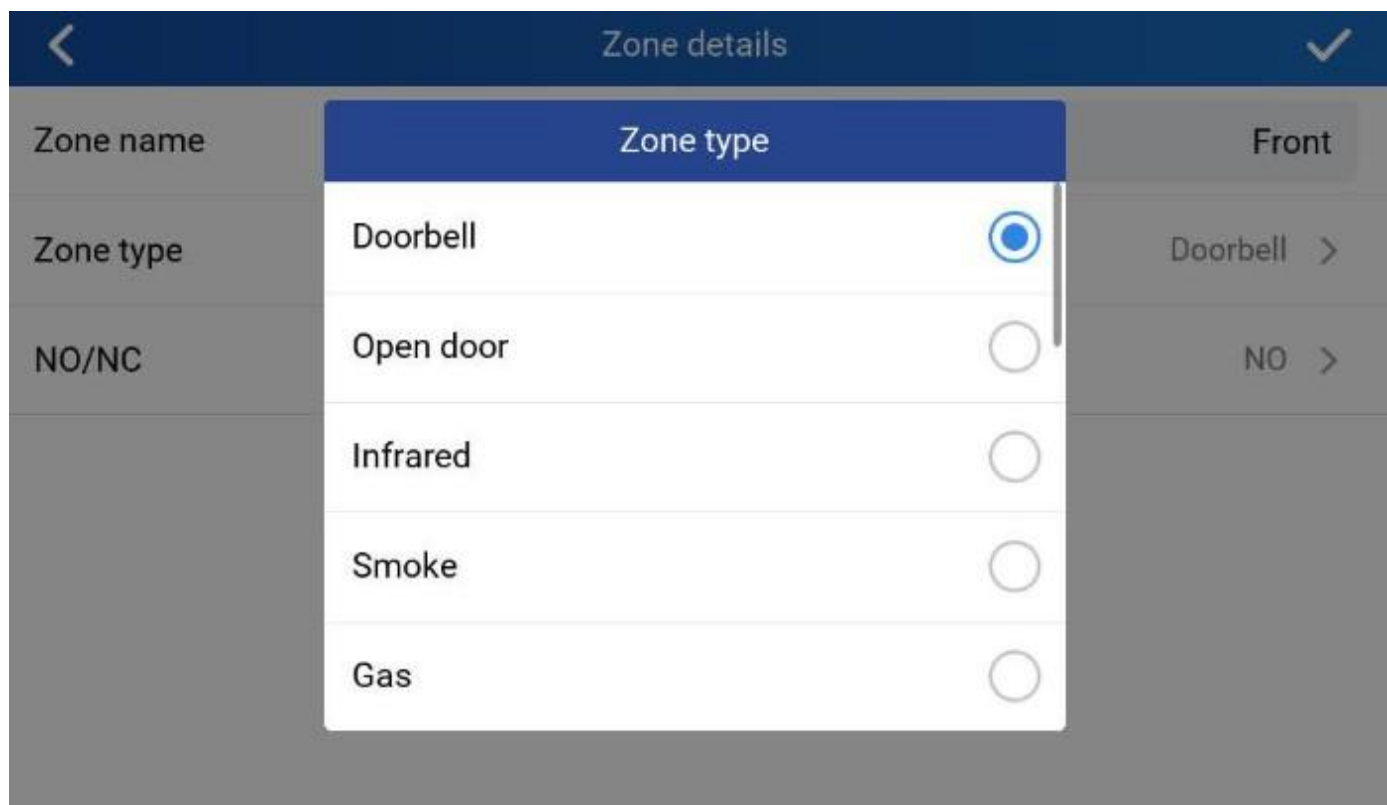
DO mode set to Alarm out or Open door

II. Edit Zone setting for Doorbell:

- 1. From touch UI, press "Settings", select "Zone settings"
- 2. Press "Zone settings"; by default, there are 4 zones. Only Zones 2, 3, and 4 can be used for the Doorbell switch (Zone 1 is an input requiring power). Press the related Zone (2 to 4) to edit. In the screenshot below, as an example, Zone 2 is renamed to "Front" as Front Door, and the "Zone type" has been changed to "Doorbell". Press the "✓" sign at the upper-right corner to save the changes. Then, exit to the "Settings" UI page.

Zone settings			
Zone name	Zone type	NO/NC	Alarm type
Zone 1	Infrared	NO	Delay alarm 30s / 0s
Front	Doorbell	NO	-----
Zone3	Doorbell	NO	-----
Zone 4	Doorbell	NO	-----

Zone setting for Doorbell



Zone Type for Doorbell

III. Enable the Arming mode to enable the doorbell:

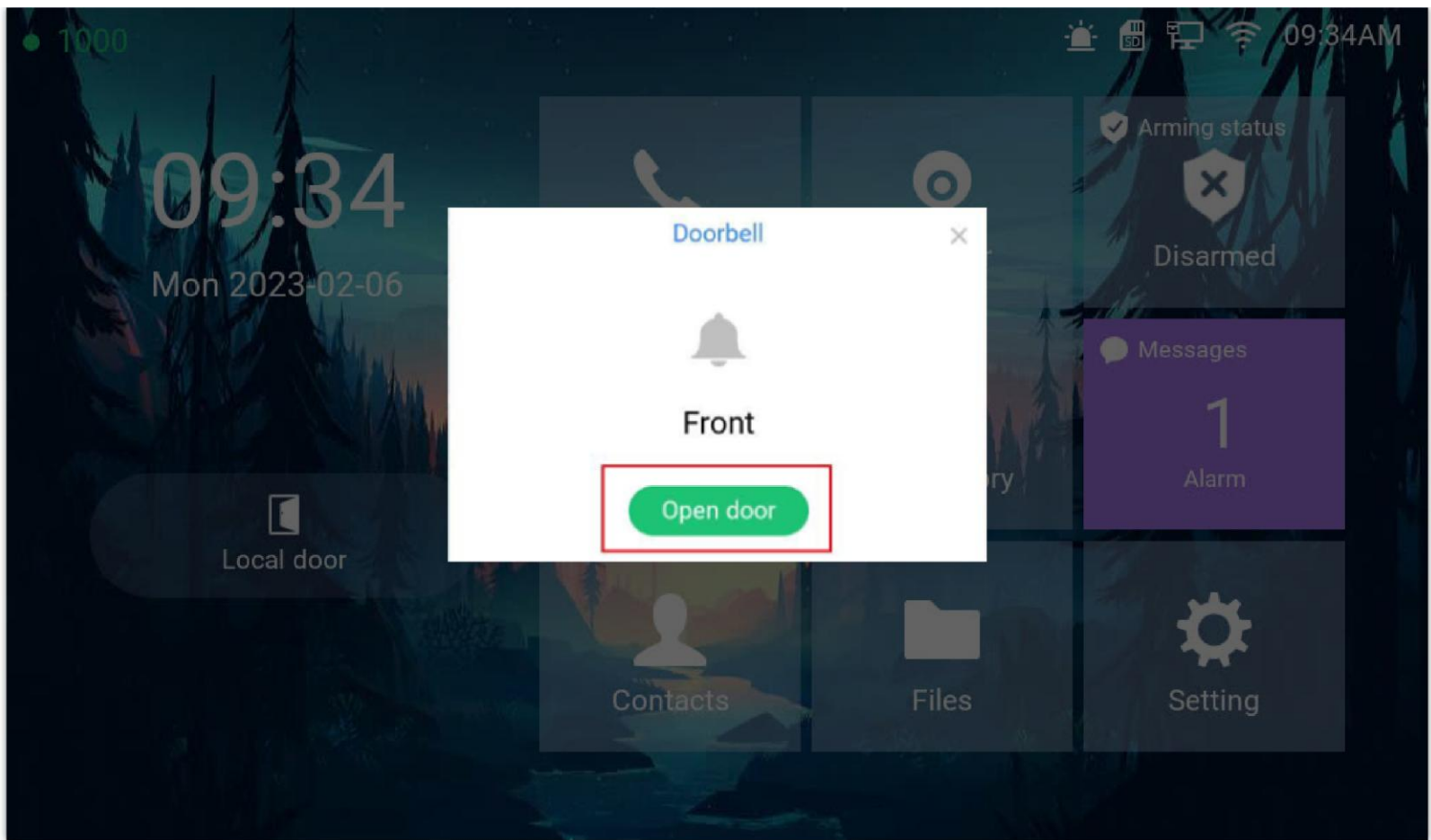
1. Press "Arming mode" to enable the change in Step I above.
2. Select the Arming mode used. For example, "Outdoor" is selected because the doorbell is located outside. Swipe the grey button to enable the feature; the button will become blue when enabled.
3. Press the "<" icon to exit the configuration to the idle screen.

The "Arming status" icon will change color (green). To show the device is "Armed", or the feature is enabled.



Arming mode

Now press the doorbell or switch (AIN1 and GND short-circuit), "DING DONG" doorbell tone will be played at GSC3570, a green open door virtual button will be displayed on the screen (if configured and wired for the strike). Press the green "Open door" virtual button, and the relay will take action to open the door. The GSC3570 top right corner will also display a door opened icon and an "alarm" icon, and "Message" will be displayed with front and back red LED flashing, reminding there is an open door (arming) event has happened. Press the "Messages" icon to check what the message is, then exit the UI, the alarm message and the flashing LEDs will disappear.



Alarm flashing icon and open door button

Messages			
Voice mail	Zone	Type	Time
Alarm	• Touch button	Open door	2023-02-06 09:34:40
	Touch button	Open door	2023-02-06 09:33:03
	Touch button	Open door	2023-02-06 09:27:36
	Touch button	Open door	2023-02-06 09:27:26
	Touch button	Open door	2023-02-06 09:21:42
	Touch button	Open door	2023-02-06 09:21:40
	Touch button	Open door	2023-02-06 09:21:40

Alarm Messages

Open Door via GDS37xx with or without a SIP Call

This feature is requested by customers and implemented to meet customers’ application requirements, where GDS37XX is paired with GSC3570 to open door while no SIP call is required.

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

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

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

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

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

Door System Settings

Basic Settings

Keep Door Open

Card Management

Group

Schedule

Holiday

System Settings

Account

Phone Settings

Audio Settings

Alarm Settings

Email Settings

Maintenance

Status

Door System Settings

Door Relay Options

ALMOUT1 Feature

ALMOUT1 Status

Control Options

Wiegand Control

Door 1 Delay before Unlock(s)

Door 2 Delay before Unlock(s)

Door 1 Unlock Holding Time(s)

Door 2 Unlock Holding Time(s)

Minimum Interval of Swiping Card(ms)

Call Mode

Doorbell Mode

Doorbell Call Out Account

Door Bell Call Mode

Number Called When Door Bell Pressed

Remote PIN to Open Door 1

Remote PIN to Open Door 2

Local Relay

Local Relay

Webrelay

GSC3570 Relay

Normal Open

Door 1

Door 2

Door 1

Door 2

0

0

5

5

300

SIP Number

Call Doorbell Number

Auto

Serial Hunting

192.168.11.138:5060,

.....

.....

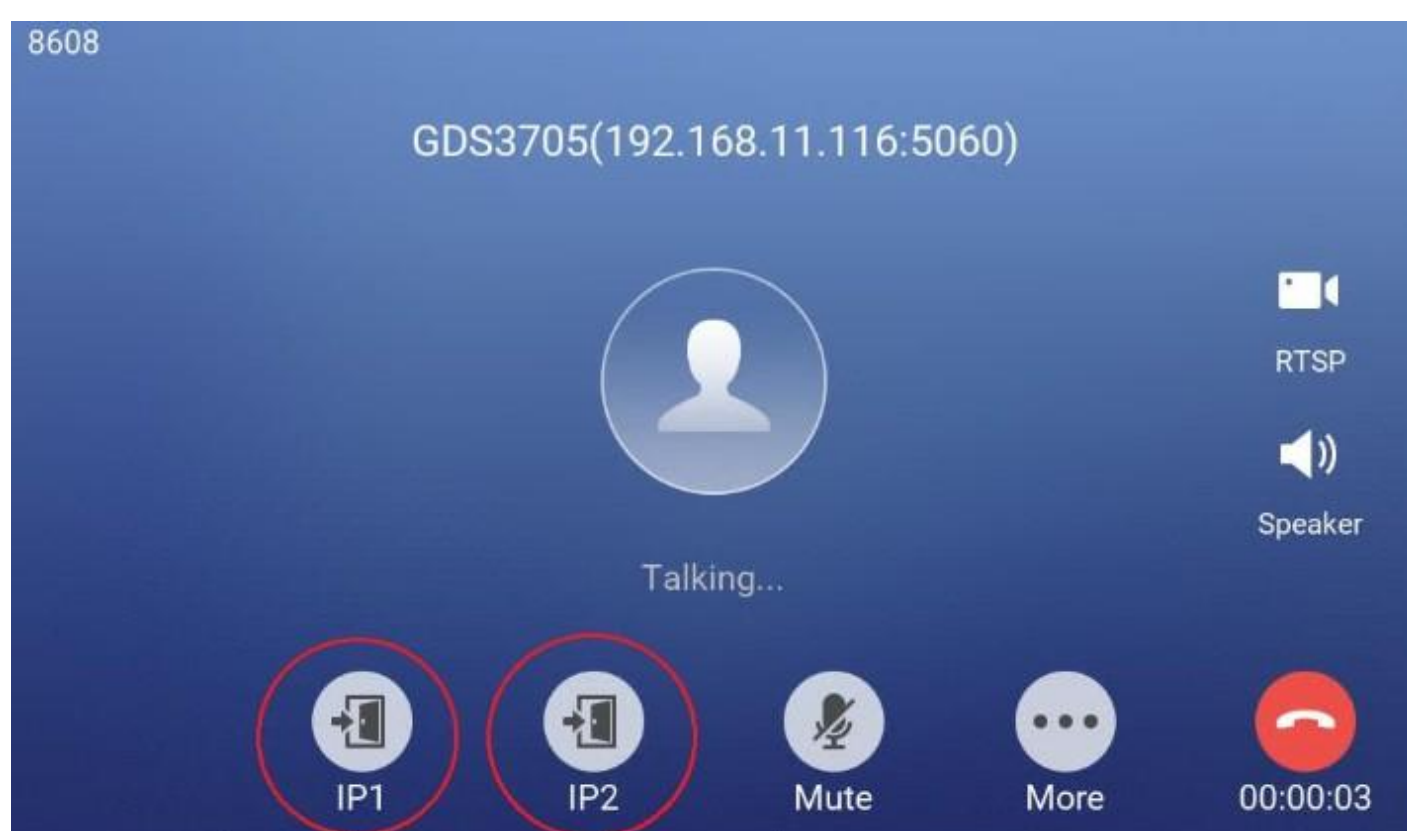
GDS37XX Configuration Example

Settings	Grandstream Door System									
General Settings	Order	Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
External Service	1	GDS	Account 1	Front_Door	873		Front_Door			
	2	GDS	Account 1	Back_Door	877		Back_Door			
Digital Output	3	GDS	Account 1	GDS3710	192.168.11.125	192.168.11.125	JP			
	4	GDS	Account 1	GDS3710	8006		SIP			
Alarm	5	GDS	Account 1	GDS3705	192.168.11.116	192.168.11.116	IP1		IP2	...
SOS	6	GDS	Account 1							

GSC3570 Configuration Example

Door opening with SIP Call:

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

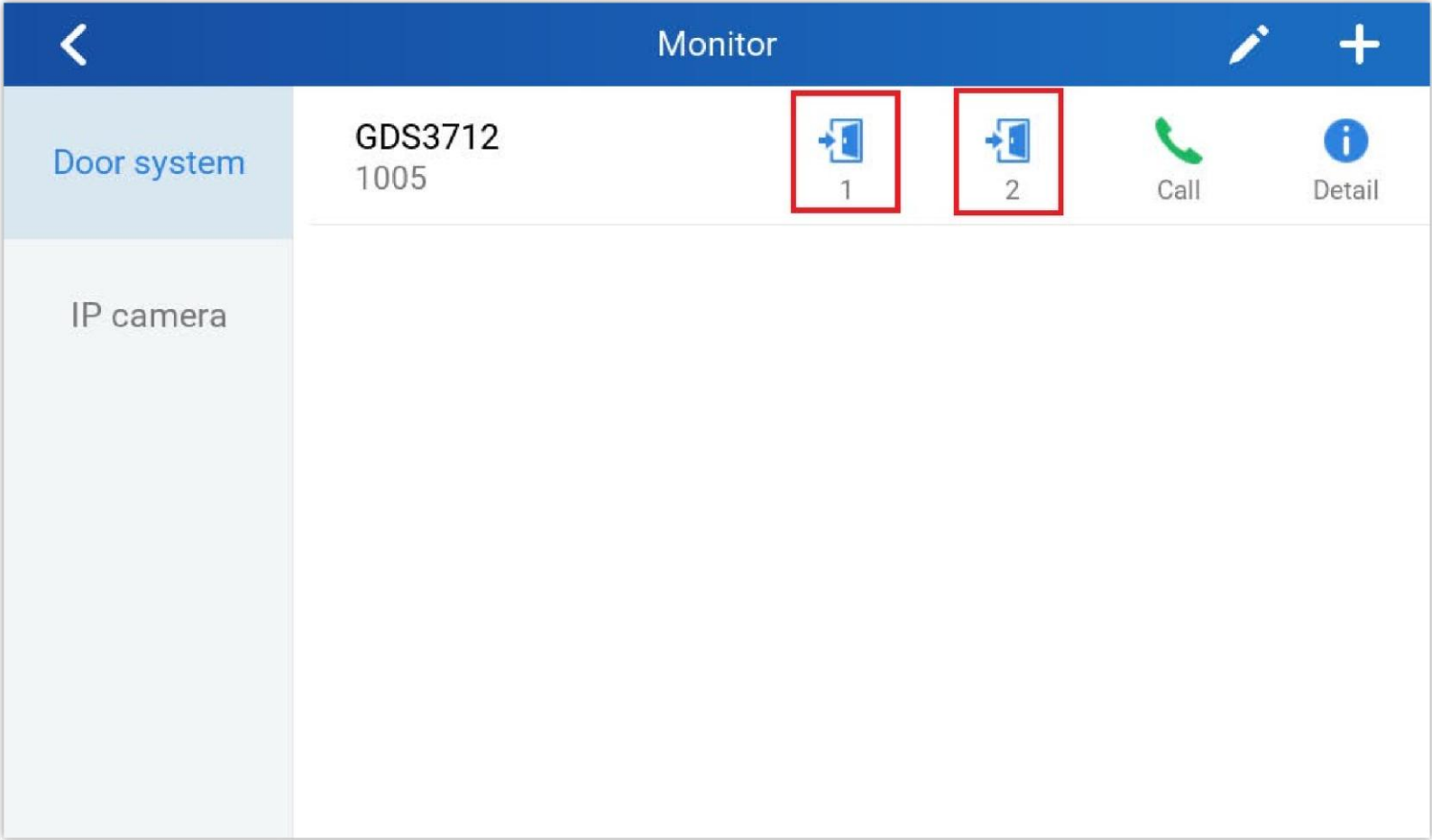


Open Door with SIP Call

GSC3570 Open Door NO SIP Call:

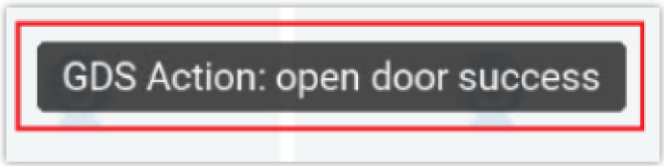
At the GSC3570 idle screen, press "Monitor →Door system", the related GDS37XX will be displayed. In the blue bar, left is a "Phone" icon, and right is the "Open door" icon. The "Phone" icon will establish a SIP call.

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



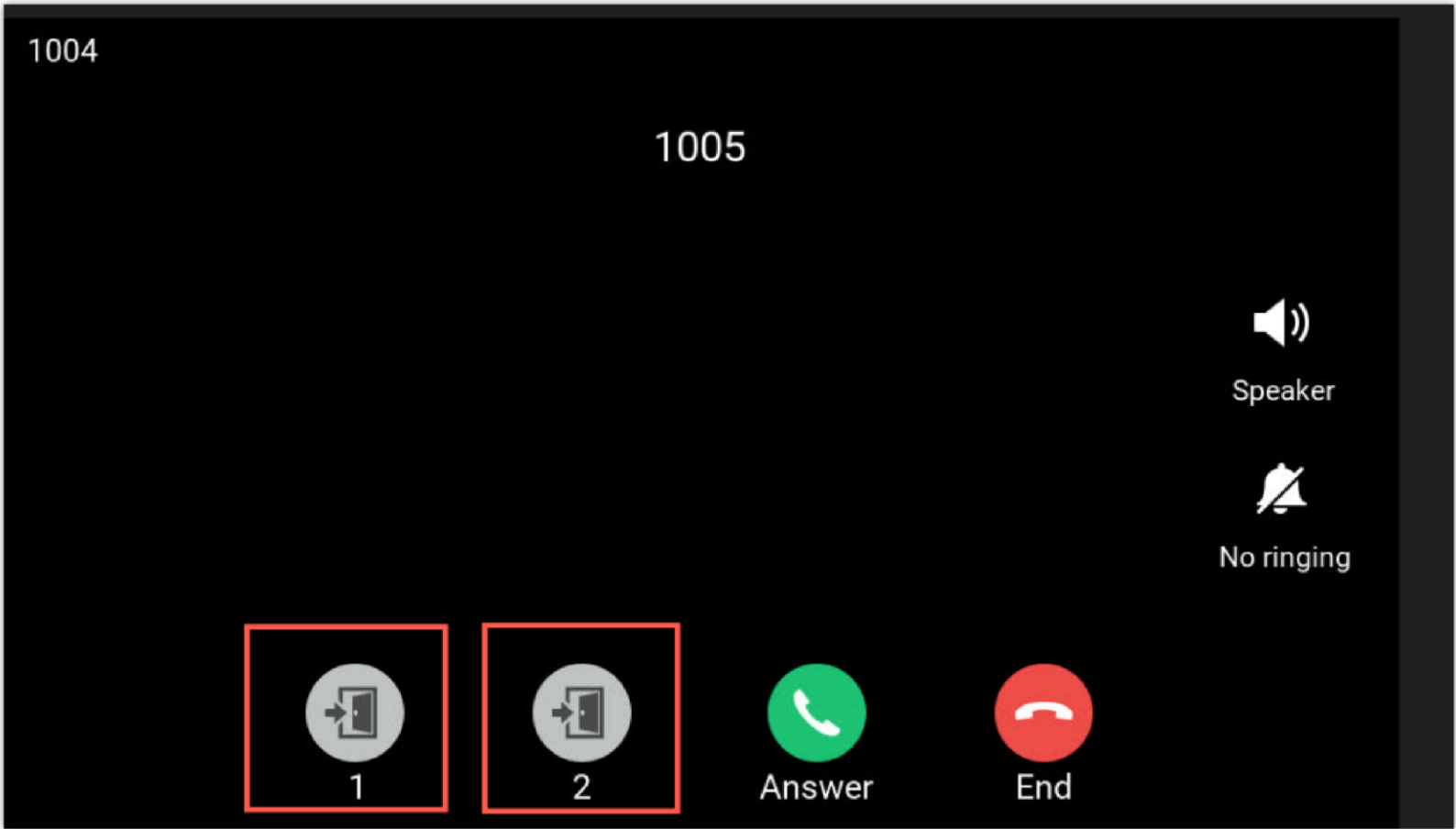
Open Door without SIP Call

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



Open Door without SIP Call

When you receive an incoming call, the call preview will show both doors and allow you to open them, as shown in the illustration below:



Door Preview

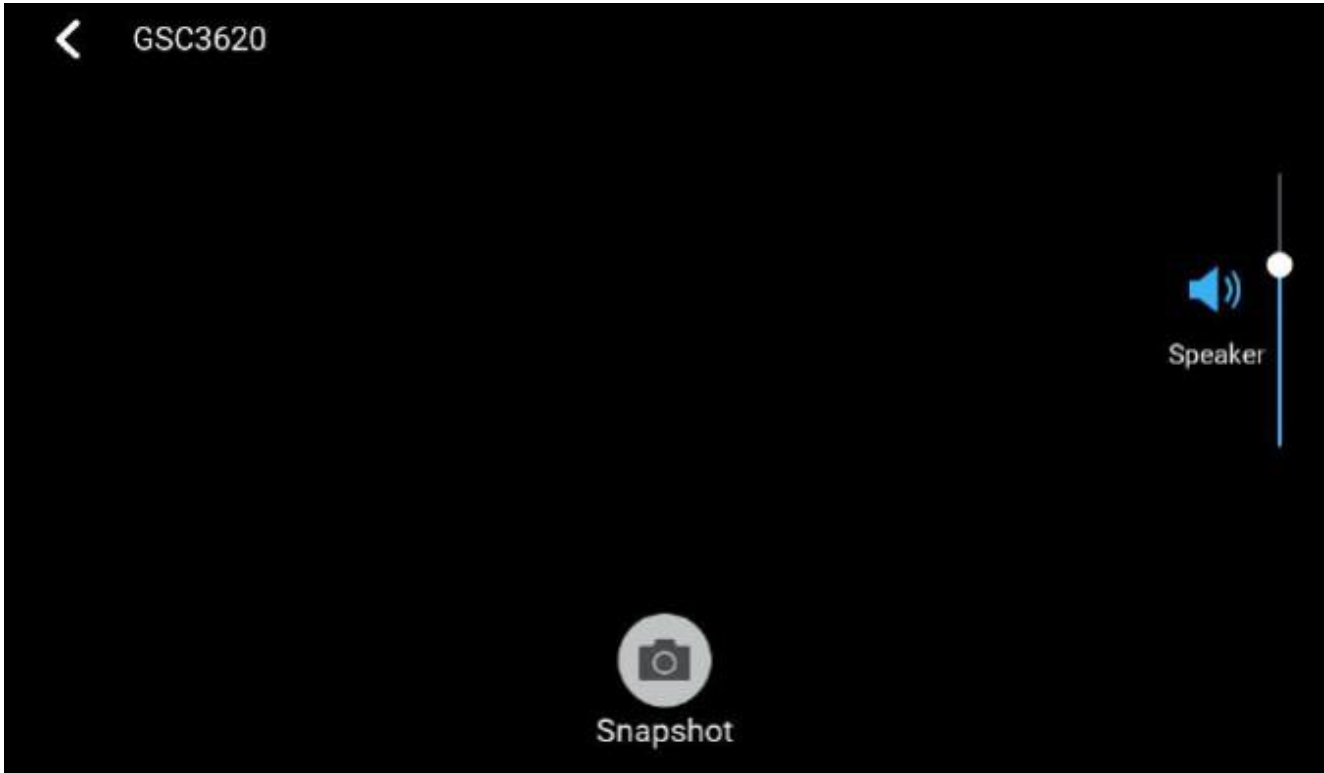
Note

If using a 3th party Door system instead of GDS37xx , then the GSC3570 will send DTMF message to opendoor.

RTSP Audio Volume Control

The touch LCD screen is improved by adding a “Speaker” icon when the RTSP stream is displayed. This feature allows the user to adjust the volume of the speaker to increase or decrease the audio of the RTSP media stream.

Touching the white “Speaker” icon will make it blue, and a vertical bar will appear at the right side of the blue speaker icon. Touch any part of the screen will exit the operation.

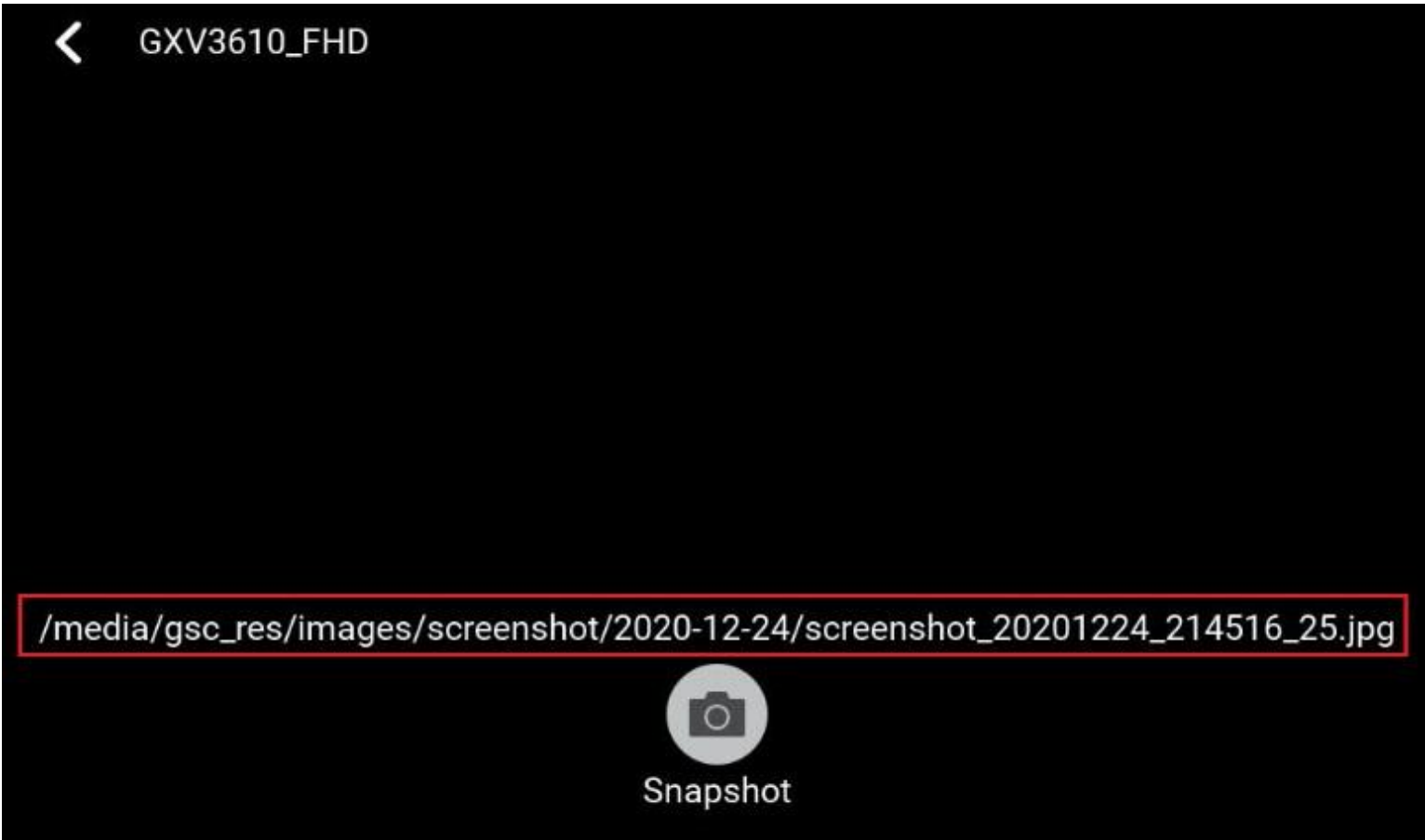


RTSP Audio volume control

Screen Snapshot During RTSP Streaming or SIP Video Call

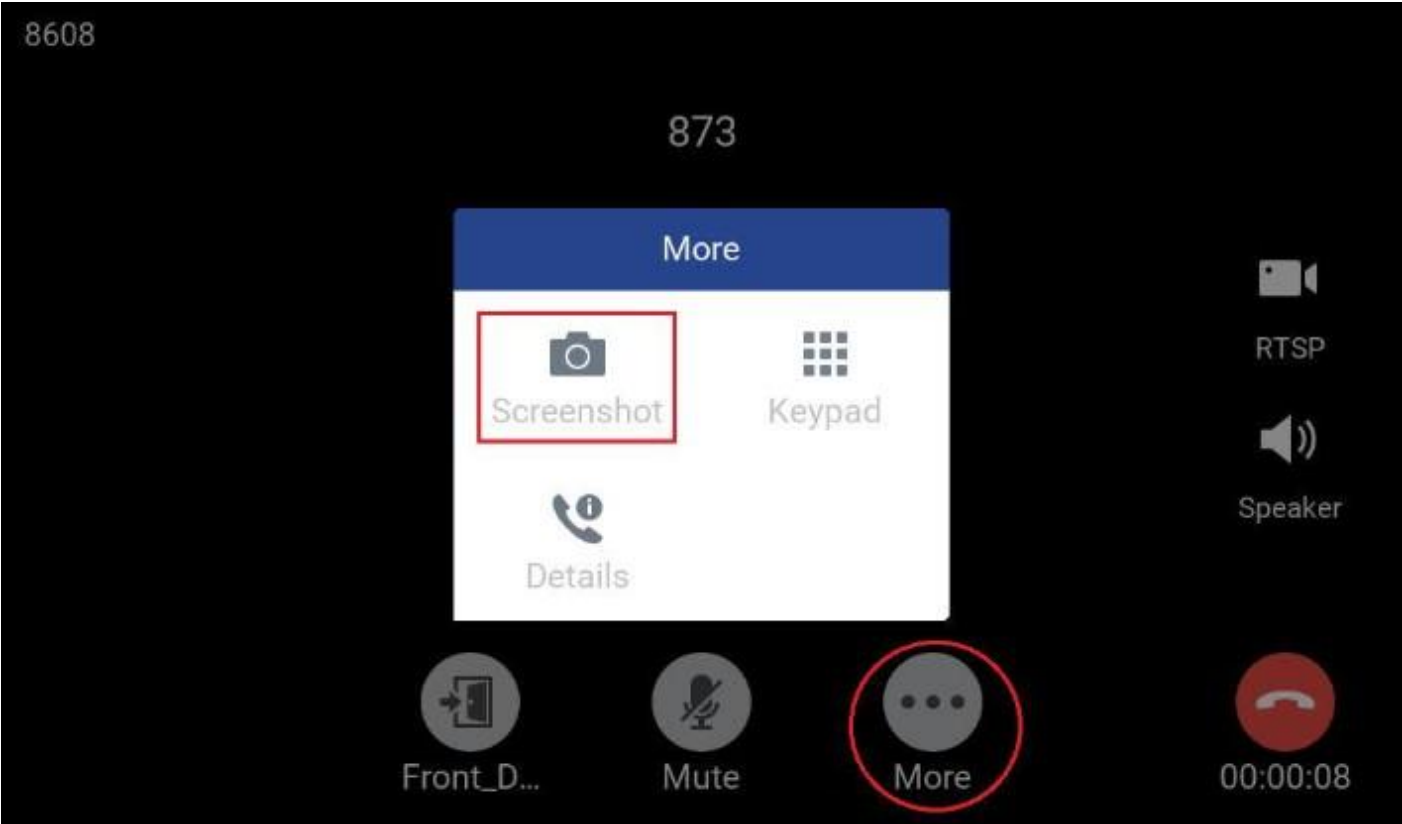
This feature does not need any configuration and is enabled by default, but an SD card is required for this feature to work correctly.

RTSP Streaming: During RTSP streaming, in the middle of the screen, a virtual “Snapshot” button will appear. Pressing that button will capture the current screen, and the snapshot will be saved in the SD. The file path will display on the screen, then disappear.



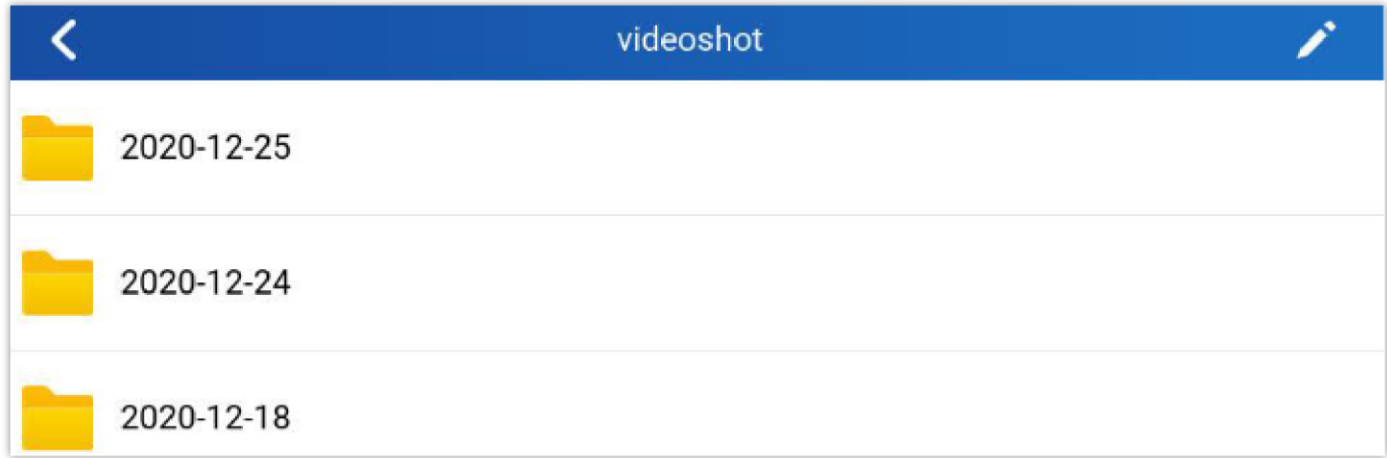
RTSP Snapshot

SIP Video Call: During a SIP video call, pressing the “More” icon will pop up another screen, and the “Screenshot” icon will be displayed. Pressing the “Screenshot” button will capture the current snapshot and store it in the SD card.



SIP Video Call Snapshot

The file path will display on the screen and then disappear after a while. Press the “File” icon from the GSC3570 idle screen, select the “videoshot” file folder, and the snapshots will be stored based on the folder using the date when the snapshots were taken. Select the folder to list the stored snapshots.



Video shot folder

HTTP GET Request

By selecting HTTP as the service type, the user can use a button from the touch screen to generate an HTTP GET request to open the door. When the device in the door system lists calls, an open door button appears corresponding to the URL specified under the field HTTP URL.

Service Type	Account	System Identification	System Number	System IP Address	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password	HTTP URL
HTTP	Account 1								
GDS	Account 1								
GDS	Account 1								
GDS	Account 1								

HTTP GET request

Connecting an IP Camera with GSC3570

The GSC3570 can be configured with up to 32 IP Cameras. The configuration is done as follows:

Web interface configuration:

- 1. Access **Settings**→ **IPC**.
- 2. Enter the name of the IP Camera unit in **System Identification**. (not a mandatory field)
- 3. Select SIP or RTSP on **Connection Type**.
- 4. Enter the IP Camera’s SIP extension (or IP address in case of peering mode) in **System Number**.
- 5. Select the Account to make an outgoing call to the IP Camera under **Account**.
- 6. Click on Save and Apply.

GRANDSTREAM

CONNECTING THE WORLD

STATUS

ACCOUNTS

SETTINGS

NETWORK

MAINTENANCE

Settings

General Settings

Broadsoft

External Service

Alarm

SOS

IPC

Call Features

Multicast Paging

Outbound Notification

Preferences

Web Service

XML Applications

Voice Monitoring

IPC

Order	System Identification	Connection Type	System Number	Account
1	GXV3610	sip	1003	Account 1
2		sip		Account 1
3		sip		Account 1
4		sip		Account 1
5		sip		Account 1
6		sip		Account 1
7		sip		Account 1
8		sip		Account 1
9		sip		Account 1

IPC Web Configuration

LCD configuration:

1. Tap the menu button if GSC is idle state.
2. On the first screen menu, tap **Monitor→ IP Camera**.
3. Press the **Add** or **+** button to add a new IP Camera.
4. Enter the IP Camera Name in the **Device Name** field.
5. Select which Account to make an outgoing call to the IP Camera and enter the IP Camera’s SIP extension (or IP address in case of peering scenario) in the **Device Number** field.

<

Edit Device

✓

Device Type

IP Camera >

Device Name

GXV3610

Device Number

1002

1003

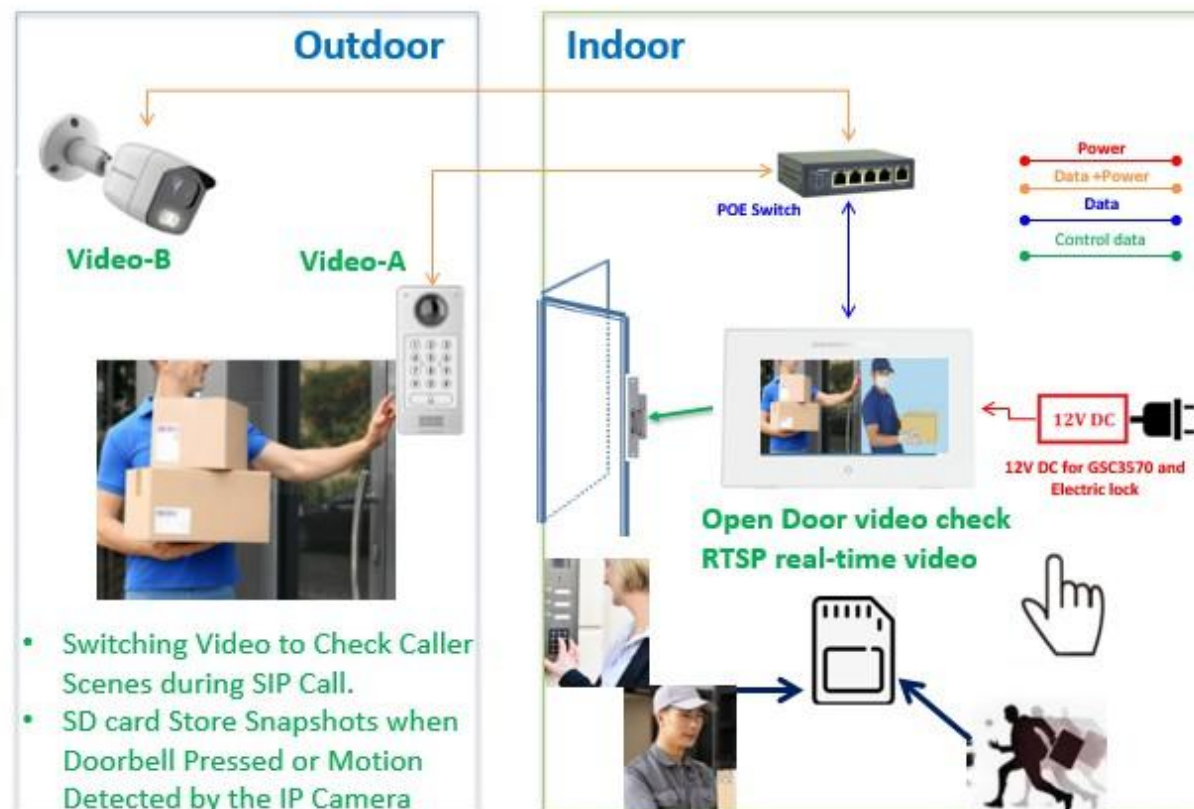
Delete Device

IPC LCD Configuration

Switching to RTSP Monitor during an active SIP call

This feature needs a working SIP call and RTSP stream preconfigured. This feature will work with GDS37xx or any Grandstream SIP phones and Grandstream IP cameras, or even some 3rd party IP cameras. Below is an example usage scene diagram:

GSC3570 RTSP Video Monitor Switching During SIP Calls



Video Monitor Switching During an Active SIP Call

This feature can help to increase safety while keeping convenience, used in public scenes like School/Campus, Dorm/Hallway, Hospital, Library, Gym, Theater, Club, etc.

Basically, in an open/public space where there is a GSC3510 Audio Intercom or IP phone (or GDS3705), a User (e.g., student) pressing the emergency button or making a call to GSC3570 (e.g., security guard).

If the same location has installed an IP camera or a door system, once the call is established and in session, the GSC3570 will display RTSP icon on the right side of touch screen UI, pressing RTSP icon and selecting the related IP Camera as shown in below screenshot, then the call will automatically be put ON HOLD, the person at GSC3570 side can see the RTSP live stream, he can either continue monitoring the RTSP stream or switch back to continue talking to the caller.

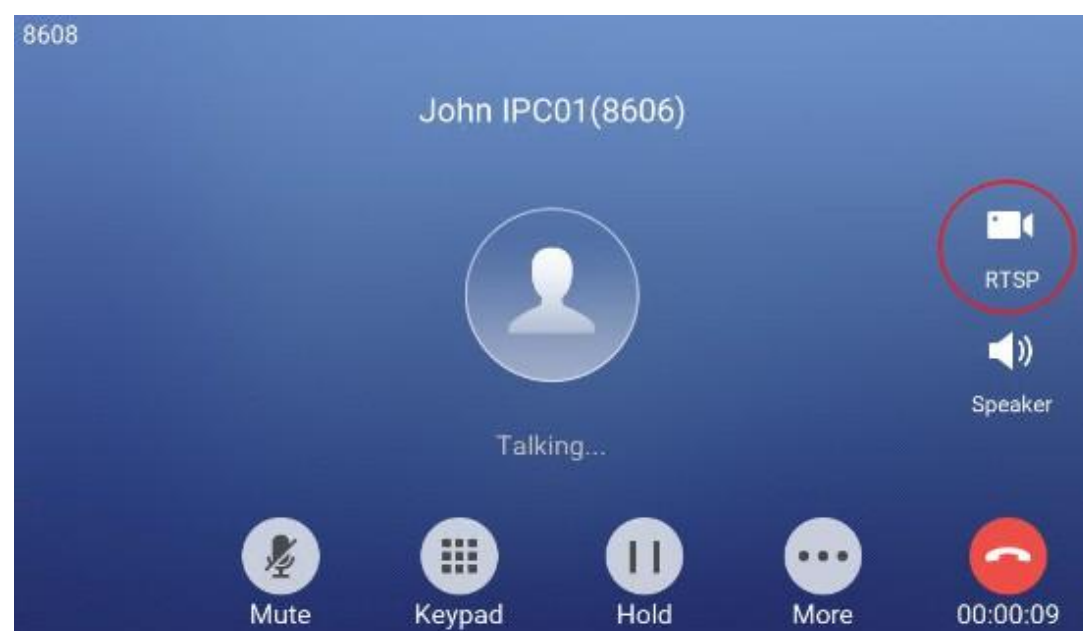
Considering the following scenario as an example :

- Bob Calls Carl on the GSC3570.
- While Bob and Carl are on Call, Carl can press the RTSP icon shown in the screenshot below to monitor the video camera.
- Once Carl starts the monitoring, the call is automatically put on hold with Bob until Carl decides to return to the call by clicking the Back button.

Note

The call can only be hung up from the other party (Caller party) and not from the GSC3570 side. When the call is hung up from the other party, the RTSP stream is resumed on the GSC3570.

The user can also open the door if connected to an access control device without a built-in camera (e.g., GDS3705).



GSC3570 Switching to RTSP stream during an active SIP call

Then users can select the IP Camera to view the live RTSP video stream as shown in the screenshot below:



GSC3570 Selecting RTSP video stream for IP camera

Arming Mode

The GSC3570 can be connected to 1 Active Alarm IN and up to 3 Passive Alarm IN inputs. Each detector input is linked to a Zone that can be set with a different Alarm Action (instant, delayed, 24h alarm).

An arming profile (Outdoor, Indoor, Sleeping, or customer) is a set of zones.

The user can arm the alarm profile via the LCD Menu from the Arming Mode by simply scrolling through the options.

The first step is to configure the zone, so proceed from the **Settings** Menu → **Features** → **Zone Settings**

- 1. Tap the first Zone to Edit
- 2. You may set a new **Zone Name** (Not mandatory).
- 3. Set **Zone Type** depending on the alarm input device used (Infrared, Smoke, Gas, etc.)
- 4. Depending on the alarm input type, you can set it to either NO or NC on **NO/NC**.
- 5. Set the **Alarm Type** to either choices: Instant Alarm, Delayed Alarm, or a 24-hour Alarm:
 - **Instant Alarm:** The zone will alarm when triggered immediately.
 - **Delayed Alarm:** The Enter Delay and Exit Delay will be applied.
 - **24h Alarm:** The zone will be armed for 24h.

Zone Details	
Zone Name	Zone 1
Zone Type	Infrared >
NO/NC	NO >
Alarm Type	Delay Alarm >
Enter Delay(s)	30
Exit Delay(s)	0

Features Zone Settings

Notes:

- Both the Entering/Exiting Delay durations have a range from 0s to 60s.
- The GSC3570 supports up to 4 zones.
- Once the Zone(s) are configured, proceed to **Features → Arming Mode:**

On each **Profile** (Outdoor, Indoor, Sleeping, and Custom) User can enable the zones.

Arming Mode					
Outdoor	Zone Name	Zone Type	NO/NC	Alarm Type	
	Zone 1	Infrared	NO	Delay Alarm 30s / 0s	☐
	Zone 2	Infrared	NO	Delay Alarm 30s / 0s	☐
	Zone 3	Infrared	NO	Delay Alarm 30s / 0s	☐
	Zone 4	Infrared	NO	Delay Alarm 30s / 0s	☐

Features Arming Mode

- Users can activate the arming profile from the LCD Menu as follows, as a quick arming procedure by tapping Arming Status and scrolling through the current Arming profiles:



Features Arming Status

Alarm & SOS Calling

The GSC3570 can be configured with an SOS key that, when this key is held, will trigger the GSC3570 to ring the extension(s) configured under the SOS panel from either the web GUI or LCD Menu.

Web interface configuration:

- 1. Access **Settings**→ **SOS**.
- 2. Set **Call Mode** to either Serial Hunting, where each number will be called one after one based on the order from 1-4 after the first call times out, or Parallel Hunting, where all configured numbers receive the call simultaneously.
- 3. Select the **Account** from which the call will be made and enter the SIP extension or IP address to be called. (Default is Dynamic, so the GSC will use the first available line).
- 4. Click on Save and Apply.

Settings

General Settings

Broadsoft +

External Service

Alarm

SOS

IPC

Call Features

Multicast Paging

Outbound Notification +

Preferences +

Web Service

XML Applications

Voice Monitoring

SOS

Call Mode

Serial Hunting ▼

Order	Account	SIP Number
1	Dynamic ▼	1005
2	Dynamic ▼	1008
3	Dynamic ▼	1006
4	Dynamic ▼	1009

Save

Save and Apply

Reset

SOS Web Configuration

LCD configuration:

- 1. Tap the menu button if GSC is idle state.
- 2. On the first screen menu, tap **SOS**.
- 3. Set **Call Mode** to either Serial Hunting, where each number will be called one after one based on the order from 1-4 after the first call times out, or Parallel Hunting, where all configured numbers receive the call simultaneously.
- 4. Select the **Account** from which the call will be made and enter the SIP extension or IP address to be called. (Default is Dynamic, so the GSC will use the first available line).
- 5. Click on the Save button.

The GSC3570 can be set with a trigger button to execute the Alarm output action, and the numbers configured on the Alarm panel on the web interface will be ringing as well.

09:45
Mon 2023-02-06

Call

Monitor

Arming status

Disarmed

Call history

Messages

Contacts

Files

Setting

SOS

SOS

SOS settings

Call mode

Serial hunting >

Number 1	1000 ▼	1001
Number 2	1000 ▼	1002
Number 3	1000 ▼	Number 3
Number 4	1000 ▼	Number 4

SOS LCD Configuration

Web interface configuration:

- 1. Access **Settings**→ **Alarm**.
- 2. Set **Call Mode** to either Serial Hunting, where each number will be called one after one based on the order from 1-4 after the first call times out, or Parallel Hunting, where all configured numbers receive the call simultaneously.
- 3. Select the **Account** from which the call will be made and enter the SIP extension or IP address to be called. (Default is Dynamic, so the GSC will use the first available line).
- 4. Click on Save and Apply.

Settings

General Settings

Broadsoft

External Service

Alarm

SOS

IPC

Call Features

Multicast Paging

Outbound Notification

Preferences

Web Service

XML Applications

Voice Monitoring

Alarm

Call ModeParallel Hunting

Order	Account	SIP Number
1	1	1008
2	1	1005
3	Dynamic	
4	Dynamic	

SaveSave and ApplyReset

Alarm Web Configuration

LCD configuration:

1. Tap the menu button if GSC3570 is in the idle state.
2. On the first screen menu, tap **Settings app → Advanced → Alarm Settings**.
3. Set **Call Mode** to either Serial Hunting, where each number will be called one after one based on the order from 1-4 after the first call times out, or Parallel Hunting, where all configured numbers receive the call simultaneously.
4. Select the **Account** from which the call will be made and enter the SIP extension or IP address to be called. (Default is Dynamic, so the GSC will use the first available line).
5. Click on the Save icon.

<Alarm Settings✓

Call ModeParallel Hunting >

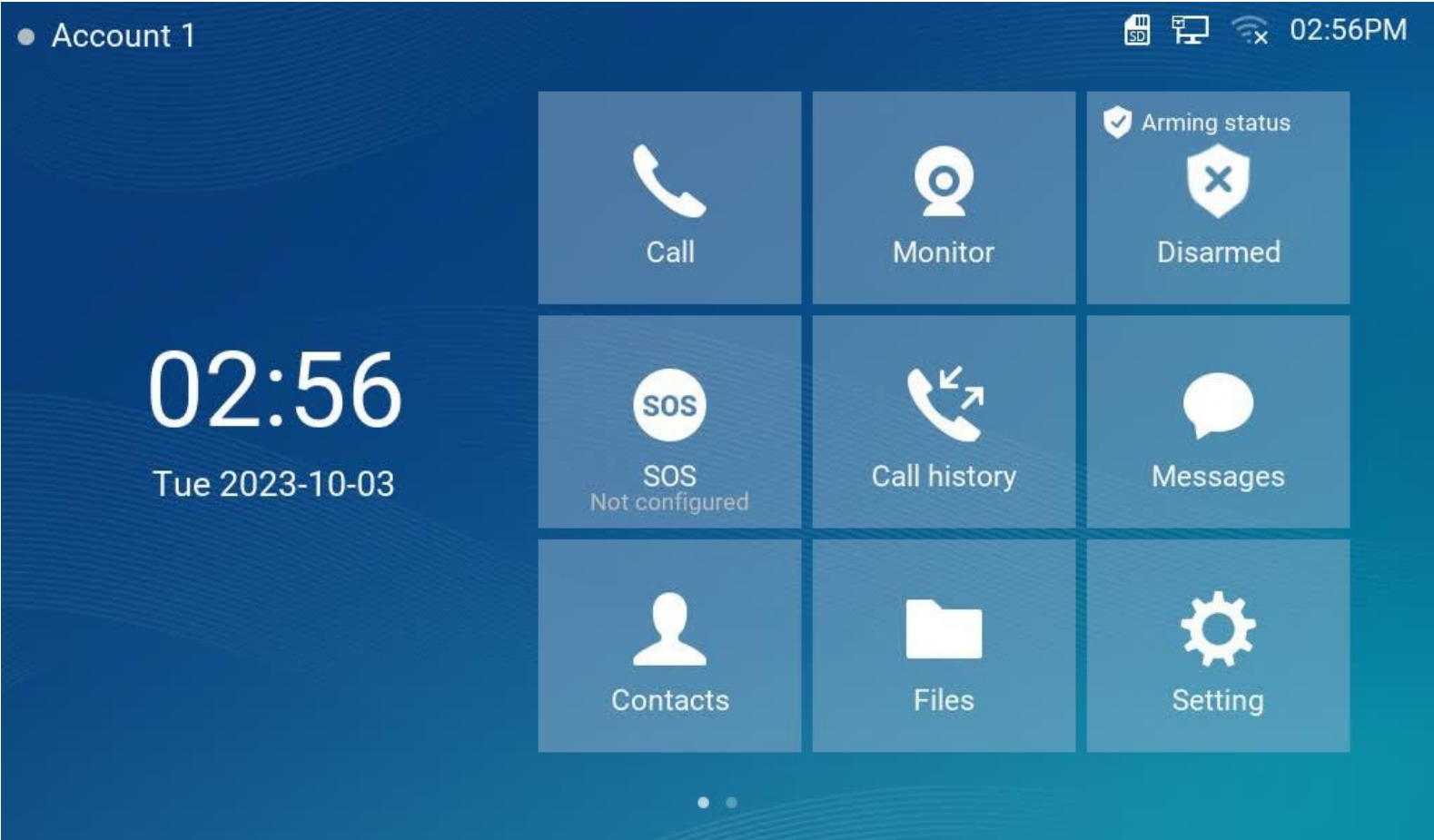
Number 1	1002	1008
Number 2	1002	1005
Number 3	Dynamic Acco...	Number 3
Number 4	Dynamic Acco...	Number 4

Alarm LCD Configuration

GSC3570 Meeting Room Panel Mode

GSC3570 has the option to alter the device mode based on the required functions. The user can choose between the following two options:

- **Control Station Mode (Default):** In this mode, the GSC3570 functions as a normal control station of the on premise security control, where it is usually deployed with other IP surveillance cameras such as the GSC36xx devices, and Door systems, such as the GDS37xx device models, in this mode the main functionalities deployed are the open door features, the "Monitor" feature, used to display the video feed of the cameras, in addition to some functionalities related to alarm out/in settings, this mode is the default mode of the GSC3570.

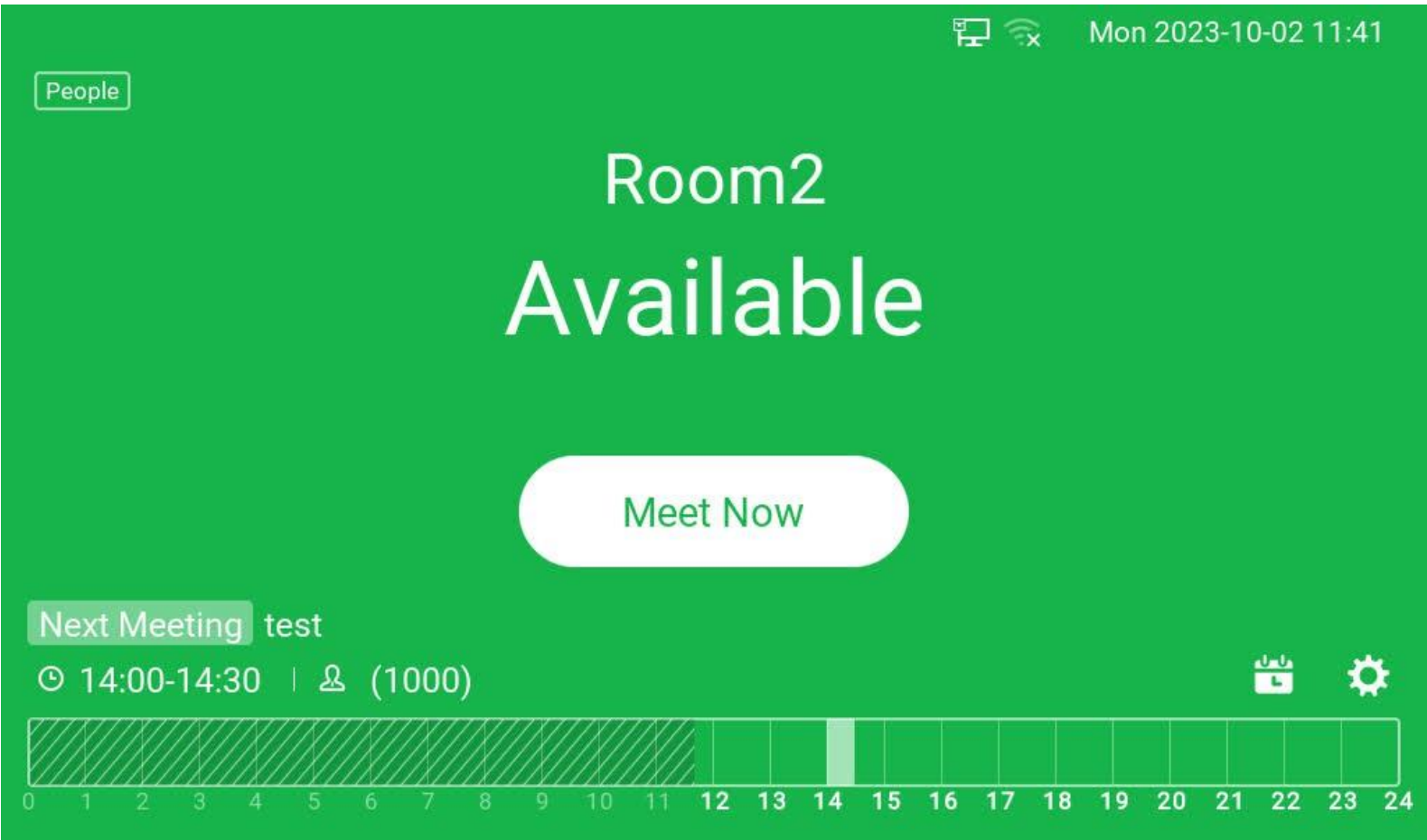


Control Station Mode view

- **Meeting Room Panel Mode:** In this mode, the GSC3570 can function as an extension of the UCM63xx model for in-person meetings or as a standalone device for hosting local meetings independently, eliminating the necessity of connecting to a UCM, if used as a UCM63xx extension, it will display the organized onsite meetings from the UCM platform, through the control interface, users can monitor room occupancy status, reserve meeting times by choosing slots from the displayed timeline, adjust meeting duration, and receive a 10 minutes countdown notification as scheduled meetings approach.

Note

For more information on the configuration and setup of the Meeting Room Panel Mode, please refer to the guide: [GSC3570: Meeting Room Panel Mode User Guide](#).



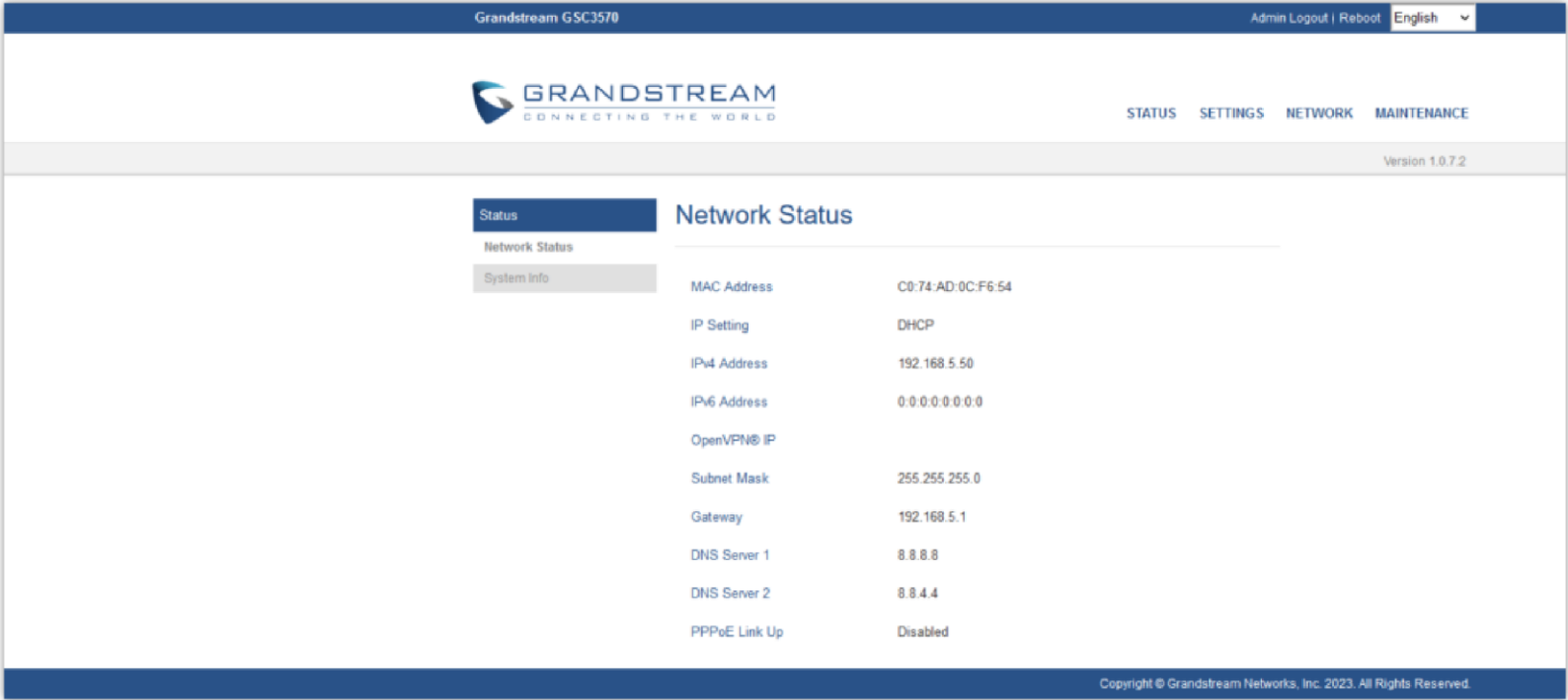
Meeting Room Panel Mode view

Note

Please note that a reboot is required for the above modes to take effect.

Meeting Room Panel Mode Web UI view

The settings available on the GSC3570 Meeting Room Panel Mode are limited and different from the control station mode. Here is a view of the available settings:

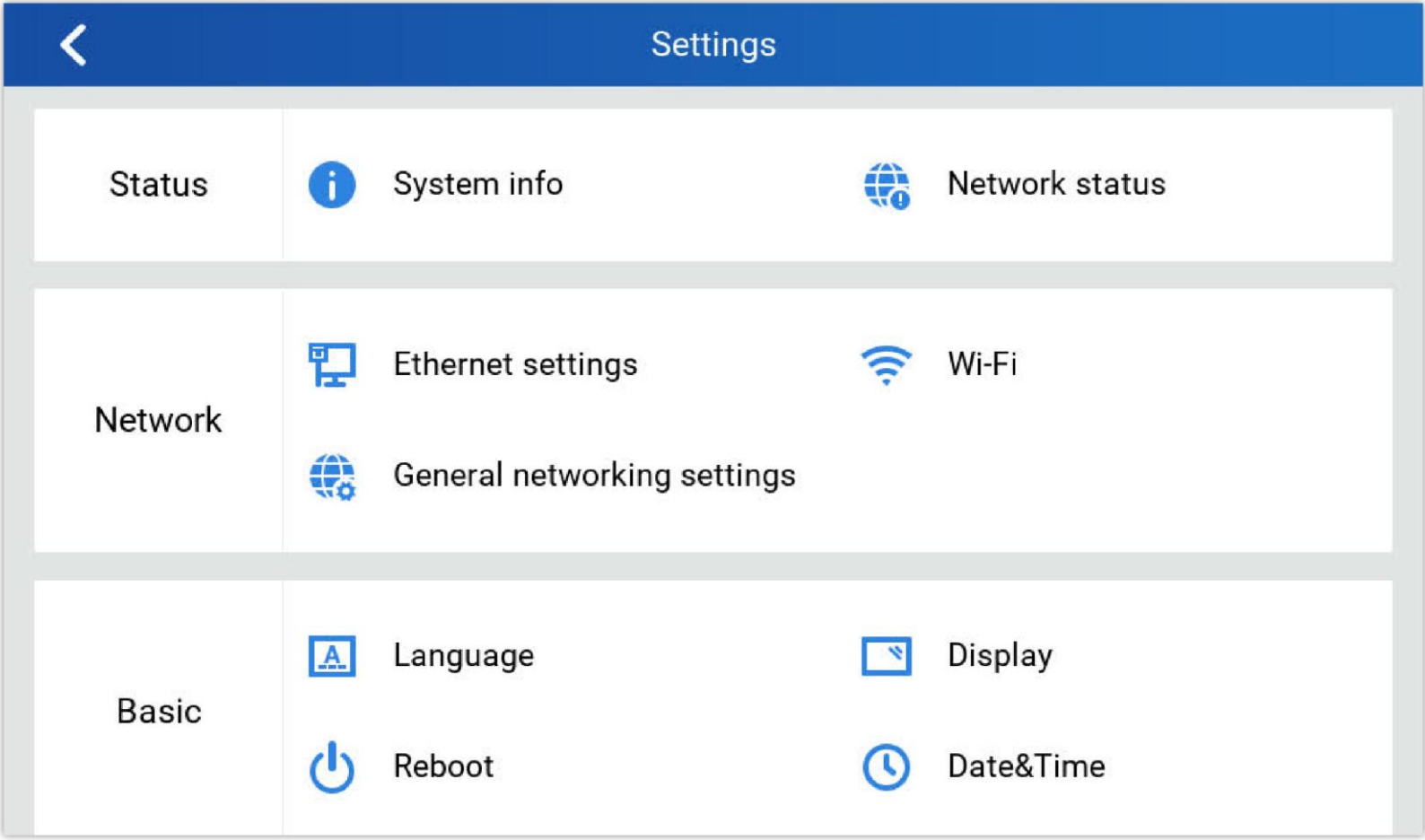


Web UI Settings

When Control Station Mode is enabled, it triggers an override in the settings, leading to notable variations, such as the exclusion of SIP account configuration options... Please refer to the [Configuration via Browser](#) section to learn more about the settings exclusive to the Meeting Room Panel Mode.

Meeting Room Panel Mode LCD settings view

Some functionalities are not available in the LCD settings. The available settings are :



GSC3570 LCD SETTINGS

The GSC3570 LCD MENU provides easy access to the settings on the GSC3570. Some of the settings from Web GUI could be configured via the LCD as well. The following table shows the LCD menu options.

- **Control Station Mode**

Status	1. Account status 2. Network status 3. System info 4. Storage info
Network	1. Ethernet settings 2. WI-FI 3. General networking settings
Features	1. Auto answer 2. DND 3. Arming mode 4. DO settings 5. Zone settings 6. FTP server settings
Basic	1. Sound 2. Display 3. Date&Time 4. Screen lock 5. Desktop shortcut settings 6. Desktop icon displayed 7. Reboot
Advanced	1. Accounts 2. SD card 3. SOS settings 4. System updates 5. Monitor 6. Alarm settings 7. Syslog 8. Reset

GSC3570 Control Station Mode LCD SETTINGS

○ Meeting Room Panel Mode

Status	1. Account status 2. Network status
Network	1. Ethernet settings 2. WI-FI 3. General networking settings
Basic	1. Language. 2. Display 3. Reboot 4. Date&Time
Advanced	1. Meeting Room Setting 2. Syslog

	3. System updates 4. Reset
--	-------------------------------

GSC3570 Meeting Room Panel Mode LCD SETTINGS

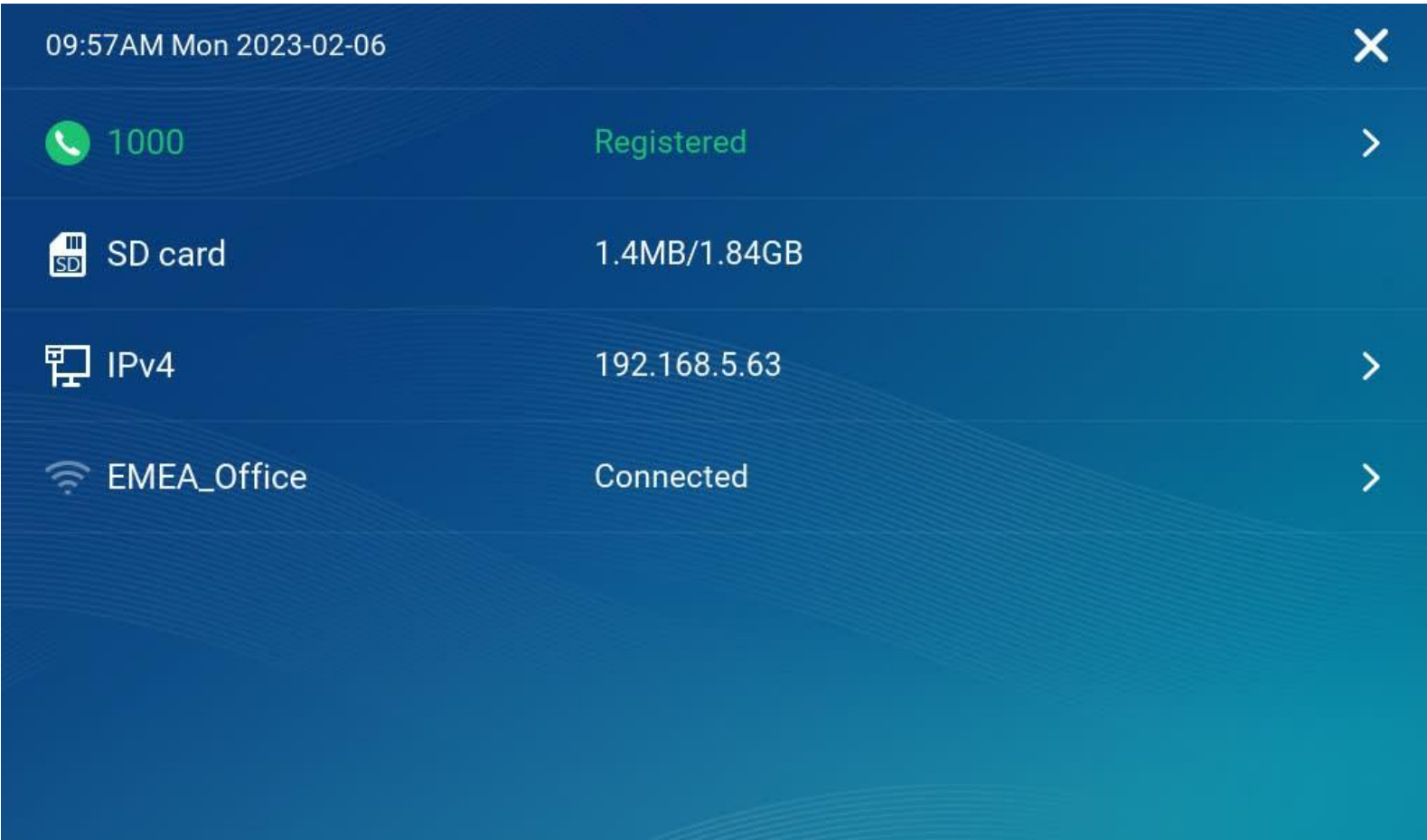
Access LCD Settings

Idle Screen

The Idle home screen offers direct access to the options selected by the user enabled from **Settings** → **Desktop Settings**, such as Call, Monitor APP, and Settings, etc. In addition to the improved Panel in the idle screen (at the top right corner), to displays detailed information about the GSC3570. For example, from the screenshot below, the user will know that the GSC3570 is using PoE power on, with an SD card inserted for storage, and the FTP server is turned on to receive the alarm snapshot of IP cameras, along with an indication of the registration status of the SIP Account.



Idle Home Screen



Idle Home Screen Toolbar

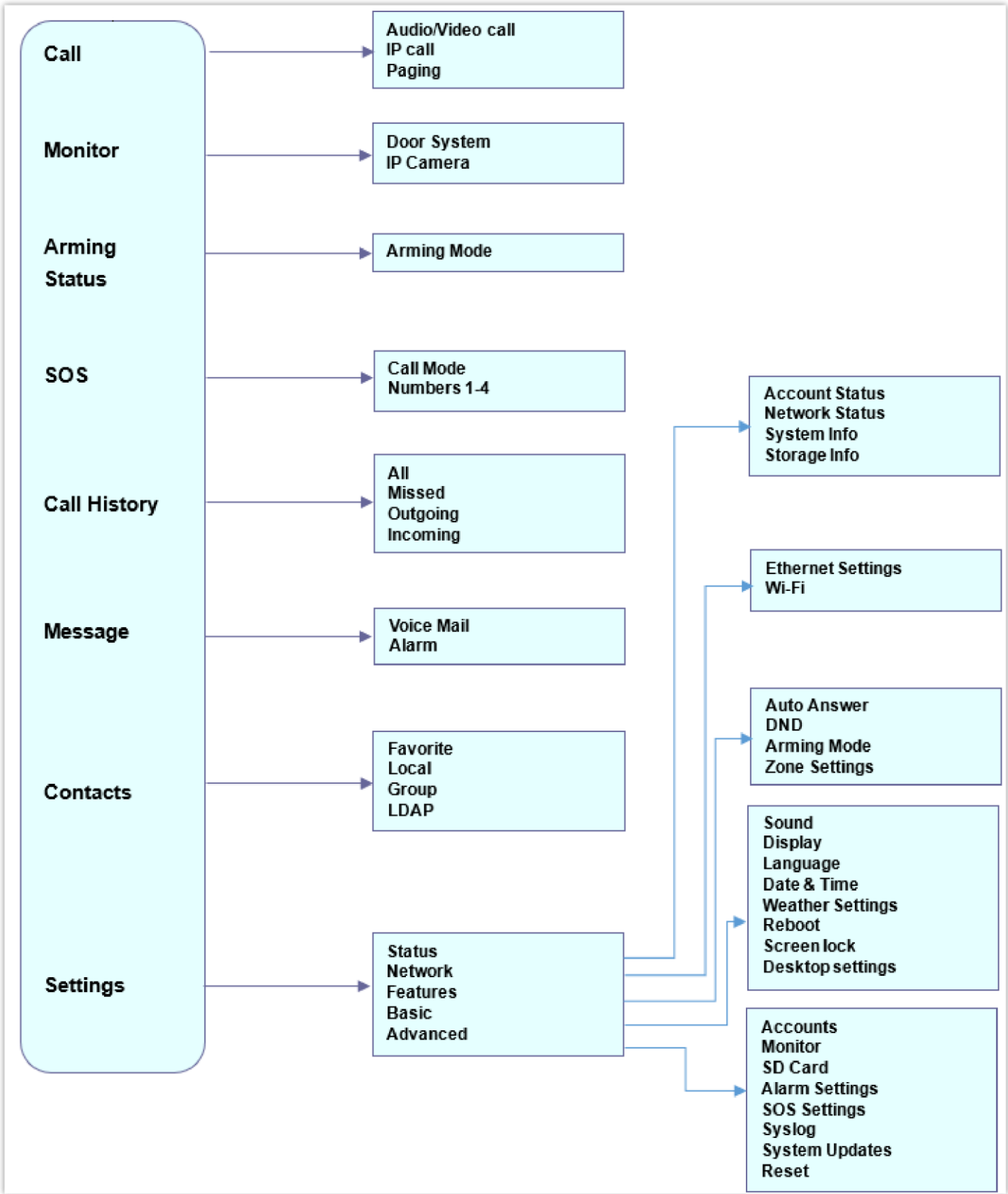
- GSC3570 is registered to a SIP server with extension number 1000.
- SD card available 1.4 MB with usage 1.84GB.
- Device IP is 192.168.5.63

- The device is connected to Wi-Fi with the SSID "EMEA_Office".

Note

- Touching the related field with ">" can jump directly to the related configuration UI.
- When the LCD is turned OFF and in energy saving mode, but a secure open door event happens, the LCD will be turned ON to light up and display the open door icon with a long "beep" to notify the user that an open door event happened.

The following diagram describes the LCD Menu and sub-menus:



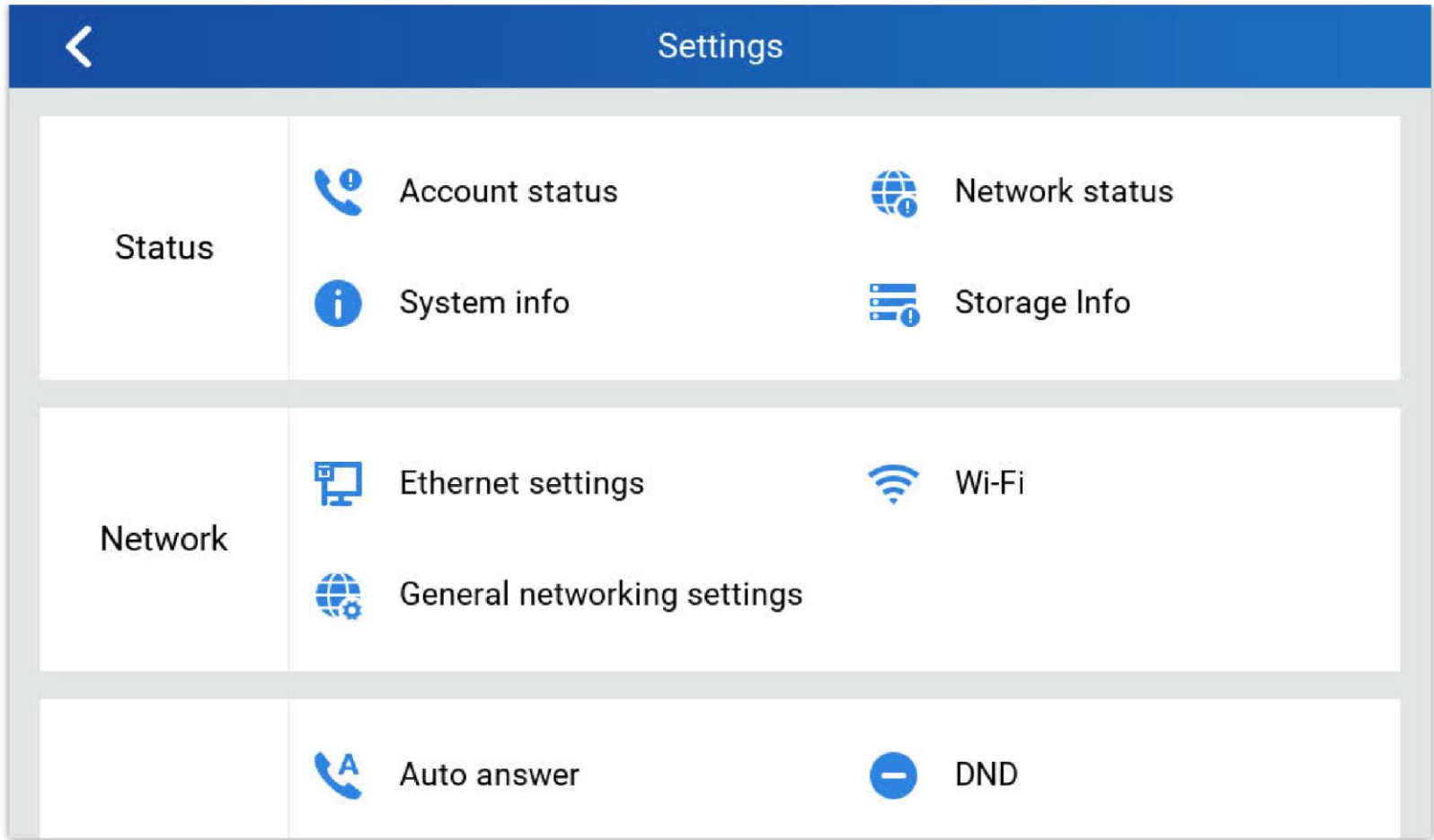
MENU Configuration

To open the settings menu, you should:

- Tap on



Settings app on the screen.



GSC3570 System Settings

Status

Account Status

This page displays all available accounts on the phone with their respective status (Configured/Not Configured and Registered/Unregistered).

Network Status

This page displays Network status including Ipv4/v6 address, subnet mask, gateway, DNS server...

System Info

This page shows system info, including Hardware version, P/N, U-boot version, Kernel version, System version, Certificate version, and System uptime.

Parameter	Description
Product Model	Product model of the phone.
Part Number	Product part number.
Certificate Type	This field indicates the type of the certificate used. It shows the used protocols for encryption and hashing.
Serial Number	This field shows the serial number of the device.
Security Version	This field shows the version of the security tools of the IP phone.
Software Version	
Boot	Bootling code version.
Core	Specifies Core version.
Prog	This indicates the software version of the device.
CPE	This field indicates the version of the remote management software.
IP Geographic Information	

City	Indicates the city where the device is located.
Language	Indicates the language of the region.
Time Zone	Time Zone information
Country Code	The code of the country where the device is located.
Special Feature	
OpenVPN® Support	This field indicates OpenVPN® feature support.
System Time	
System Up Time	System up time since last reboot.
System Time	Shows actual time and date according to your configuration
Service Status	
GUI	Reveals status of GUI
Phone	Reveals status of phone
CPE	Shows the status of the remote device management software.
System Information	
Download System Information	Click to “download” the user’s configuration file.
User Space	
User Space Used	Reveals status of user space
Database Status	Reveals status of database
Core Dump	
Generate core dump	Generate core dump by killing program.
Core Dump	Core Dump status
Clear Core Dumps	Clear the core dump files
Screenshot	
Screenshot	Click on "Start" to take the screenshot of the screen of the device.

Storage Info

This page shows the SD Card storage info.

Network

Users can configure Ethernet settings and Wi-Fi settings here.

Ethernet Settings

- **IPv4 Settings:** Here user can configure the IPv4 address type for both data and VoIP calls. For network configuration of data, if **DHCP** is selected, the phone will get an IP address automatically from the DHCP server in the network. This is the default mode. If **Static IP** is selected, manually enter the information for IP Address, Subnet Mask, Default Gateway, DNS Server, and Alternative DNS Server.

- **802.1x mode:** This option allows the user to enable/disable 802.1x mode on the phone. The default setting is disabled. To enable 802.1x mode, select the 802.1x mode and enter the required configuration depending on the 802.1x mode chosen. The available modes are **EAP-MD5**, **EAP-TLS**, and **EAP-PEAP**

Wi-Fi

- Tap on “**Wi-Fi**” to turn on/off the Wi-Fi connection. By default, it is turned off.
- **Add Network.** If the Wi-Fi network SSID doesn’t show up in the list, or users would like to set up advanced options for the Wi-Fi network, scroll to the end of the Wi-Fi list and select “Add Network”. Then enter the SSID, Security type, password, and set up address type (DHCP/Static IP) in the prompt dialog. The phone will reboot with the Wi-Fi network connected.

General Networking Settings

This feature helps system administrators or customers to configure and adjust the VLAN parameters conveniently from the touch screen.

Features

In this menu, users can configure different features related to each account of the active accounts:

Auto-Answer

- If enabled and set to “Always”, the phone will automatically turn on the speaker phone to answer all incoming calls.
- If enabled and set to “Enable Intercom/Paging”, the phone will answer the call based on the SIP info header sent from the server/proxy.
- By default, it is turned off.

DND

Enable/Disable the DND mode. When enabled, all incoming calls are rejected.

Arming mode

Enable/Disable the Arming mode on configured zones (Zone 1- 4) per profile (Outdoor, Indoor, Sleeping, or Custom).

The zones are configured under **Settings→ Zone Settings**.

Zone Settings

Tap the zone to be edited and set Zone Name, Zone Type, along with the alarm type...Etc.

- **Zone Name:** Enter the name of the zone.
- **Zone Type:** Select the **Type** of the Zone:
 - Infrared
 - Smoke
 - Gas
 - Dragnets (door lock)
 - Urgency
 - Others
- **NO/NC:** Match the alarm type:
- **NO:** Normally Open device
- **NC:** Normally Close device
- **Alarm Type:** Select the **Type** of Alarm **arming:**

- **Delay Alarm:** Enter the **Delay/Exit Delay** (Duration between 0-60 seconds)
- **Instant Alarm:** Alarm is armed instantly when triggered.
- **24h Alarm:** Alarm is always armed when triggered.

DO Settings

Configures the Door Open settings on the GSC3570. You can choose to put the DO mode to :

- Disable
- Alarm Out
- Open Door
- Incoming Call Ringing

In the Open Door Mode, the following Parameters are defined :

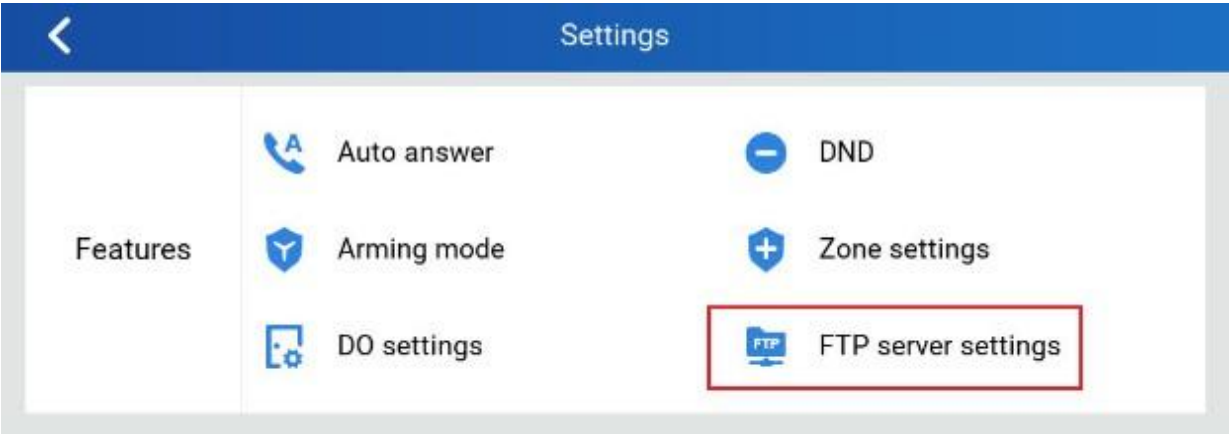
- **Door unlock holding time (S):** Duration of time in seconds that the door remains open.
- **Door system SIP user ID:** Defines the SIP extension of the Door system used.
- **Door system IP Address:** Defines the IP Address of the Door system used.
- **Door Control SIP account:** Defines the Account used on the door system side for the GSC3570 Relay Mode
- **Door Control Password:** Defines the Account used on the door system side for the GSC3570 Relay Mode
- **Display open door** icon at desktop: Enables the option to display the open door icon on the homescreen. This Open Door Button has a higher priority than the GDS device in Monitor => Door System.

The Door Open feature is disabled by Default.

FTP Server Settings

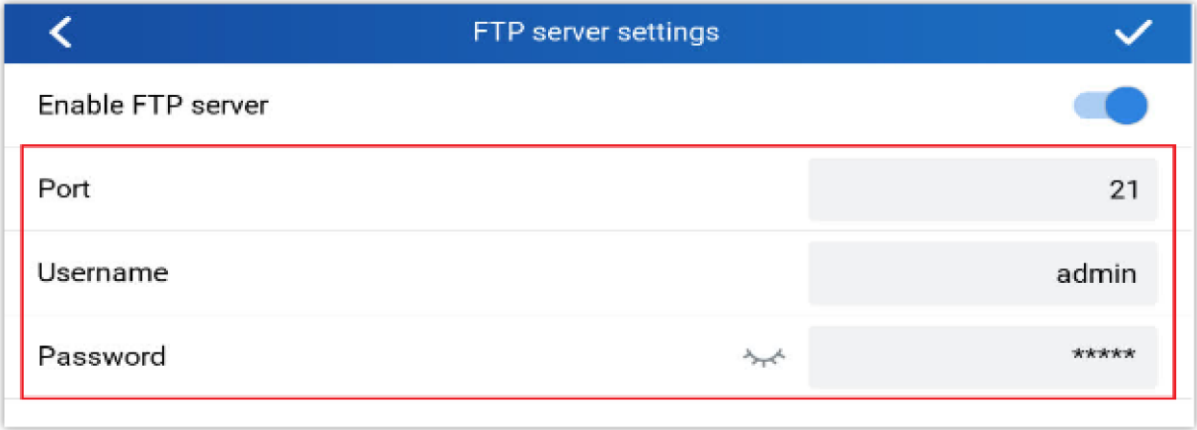
The GSC3570 has a built-in FTP server.

Press “Settings” on the touch screen, get into the “Settings” screen, then touch the “FTP server settings” to configure the FTP server parameters, as shown in the screenshot below:



FTP Server Settings

By default, the FTP Server is disabled. Touch to “Enable” the FTP, then configure the Port used, create a username, and a password. The default port is TCP 21, but customers can configure it to a different port based on network conditions.



Enable FTP Server Settings

Note

If Username and Password are left blank as default (not configured), then this means they are not required, and “anonymous FTP” is used. This is not secure, but convenient for some LAN integration.

Basic

Sound

Use the Voice settings to configure the phone’s sound mode, volume, ring tone, and notification tone.

- **Media Volume:** Adjust the sound volume for media audio.
- **Ring Volume:** Adjust the phone’s ringing volume.
- **Doorbell volume:** Adjust the Doorbell volume.
- **Ringtone:** Select the phone’s ringtone for an incoming call.
- **Door Ringtone:** Select the Door ringtone when a call arrives from GDS37XX.
- **Button tone:** Enable/disable Button tone.

Display

- **Brightness:** Tap on **Brightness** and scroll left/right to adjust the LCD brightness.
- **Screen timeout:** Tap to open the dialog to set the screen timeout interval.
- **Screensaver timeout:** Tap to set the screensaver timeout interval.
- **Call screen icon size:** Tap to set the icon size to Normal-sized or Big-sized icons.
- **Enable back LED indicator:** Enable/disable the back LED indicator.
- **Enable home key LED indicator:** Enable/disable the home key LED indicator for missed calls.

Language

- **Language:** Tap to open the list of available languages. The selected language will be used on GSC3570. By default, it is set to “Auto” to automatically select the best-matching language from available languages based on the GSC3570 location.

Date & Time

- **NTP server:** Assign the URL or IP Address of the NTP Server. The default NTP Server used is pool.ntp.org
- **Set date:** Set the current date for the GSC3570.
- **Set time:** Set the time on the GSC3570 manually.
- **Select time zone:** Select the time zone for the GSC3570.
- **Date format.** Select the format of year, month, and day for the date to be displayed. The default is “yyyy-mm-dd”. Available options are:
 - *yyyy-mm-dd*
 - *mm-dd-yyyy*
 - *dd-mm-yyyy*
- **Use 12-hour format.** Check/uncheck to display the time using 24-hour time format or not. For example, in 24-hour format, 13:00 will be displayed instead of 1:00 p.m.

Screen lock

For enhanced security, the following configuration sets a PIN code containing a minimum of 6 digits.

The following two configurations are defined :

- **Screen lock enable:** Enables the PIN Screen lock. Disabled by Default
- **Screen lock Password:** Defines the PIN code that should consist of a minimum of 6 digits.

Desktop Shortcut Settings

This option allows users to customize the Home screen by Adding Desktop shortcuts.

- Press the “Add shortcut” button and then select the shortcut type :
 1. **Speed dial**
 2. **RTSP (TCP)**
 3. **Send HTTP URL**
 4. **RTSP (UDP)**
 5. **RTSP (Multicast)**

Speed dial

This feature configures a speed dial icon on the Home screen, Desktop by setting the following two attributes :

- Shortcut name
- Number: the phone number to be dialed

RTSP

This option sets the RTSP streaming configuration by defining the following attributes :

- Shortcut name: the name of the streaming.
- RTSP URL: the RTSP URL for the source input (e.g, rtsp://@GDS3712_IP Address).
- RTSP username: Username of the Door System.
- RSTP Password: Password of the Door System.

Send HTTP URL

This option sets the HTTP URL configuration by defining the following attributes :

- Shortcut name: The name of the HTTP Link
- HTTP URL: The HTTP URL for the source input (e.g,: HTTP://@GDS3712_IPAddress/View.html).
- HTTP username: Username of the Door System.
- HTTP Password: Password of the Door System.

Desktop icon displayed

This section configures the icons to be displayed on the main homepage. The user can add up to nine Icons with different purposes or remove undesired icons. The icons available to be added are :

- Call
- SOS
- Messages
- Contacts
- Files
- Call History
- Settings (Added by Default and can not be removed)
- Arming

- Monitor

Note

The icons on the home page are auto-arranged to fit a 3*3 grid and are restricted to that format; they can not be moved around everywhere on the screen

Reboot

- Reboot the GSC3570.

Advanced

Accounts

Set up to 4 SIP accounts. The Account Settings page allows you to configure SIP settings for each account. Tap on Account# to access the settings. When configured, press the ✓ sign (on the top right corner) to confirm the changes or press the back button to cancel them. Users can press Empty configuration at the bottom of the page to clear all the settings. The following settings can be configured for each account. Refer to [Account/General Settings] for a description of each option.

- **Account Activation:** activate/deactivate the current SIP account.
- **SIP Server:** Enter the SIP server FQDN or IP.
- **SIP User ID:** Set the SIP Account User ID.
- **SIP Authentication ID:** Set the SIP Account Authentication ID.
- **SIP Authentication Password:** Set the SIP Account Authentication Password.
- **Account Name:** Enter the Account Name.
- **Display Name:** Enter the extension name to be displayed on the LCD.
- **Outbound Proxy:** Enter the Outbound Proxy URL.
- **Voicemail Access Number:** Configure the Voicemail access number.

Monitor

- **Door System:** Add/Edit or delete the GDS37xx's configuration. Make a Call to GDS37xx.
- **Device Type:** Select either **Door System** or **IP Camera**.
- **Device Name:** Set the device name.
- **Connection type:** Select the signaling protocol to be used, SIP, RTSP(TCP), RTSP(UDP), RTSP(Multicast). The default is SIP.
- **Device Number:** Set the SIP extension or the IP address of the Door System.
- **Door 1/2:** Enter the DTMF PIN to open the door remotely.
- **IP Camera:** Add/Edit or delete the IP Camera's configuration. Make a Call to an IP Camera.
- **Device Type:** Select either **Door System** or **IP Camera**.
- **Device Name:** Set the device name.
- **Device Number:** Set the SIP extension or the IP address of the IP Camera.

Alarm Settings

- Select the Call Mode and configure from which account to make calls when an alarm is triggered, as well as the receiving numbers.
- **Call Mode:** Select between Serial or Parallel Hunting.
- **Number 1-4:** Set the Account from which the outgoing call will be made and towards which Number.

SD Card

An SD card inserted into the SD card slot can be used to store snapshots triggered by the motion detection alarm of IP cameras, or snapshots of doorbell calls or open-door events.

- **Format:** Touch “Format” to perform SD card initialization and mount.
- **Uninstall:** Uninstall the SD card.

Notes

- The maximum SD/TF card supported is 256G.
- The SD card must be formatted by GSC3570 before usage.

SOS Settings

- Select the Call Mode and configure from which account to make calls when the SOS key is pressed, as well as the receiving numbers.
- **Call Mode:** Select between Serial or Parallel Hunting.
- **Number 1-4:** Set the Account from which the outgoing call will be made and towards which Number.

Syslog



This page allows to initiation upgrade process by checking if a new firmware is available in the configured firmware server path, and then upgrading if available. Users can press **Settings** to configure Firmware/Provisioning settings directly from the phone’s LCD. The following settings can be configured from this screen:

- **Syslog level:** Select the level of logging for syslog. The default setting is “None”. There are 4 levels: DEBUG, INFO, WARNING, and ERROR.
- **System log protocol:** Select the protocol of syslog (UDP or SSL/TLS).
- **Syslog server address:** The URL/IP address for the syslog server. If the GSC3570 has a network connection, the phone will send the syslog packets to this server address.
- **System log keyword filtering:** Only send the syslog with keywords; multiple keywords are separated by a comma. Example: set the filter keyword to “SIP” to filter the SIP log.

System Update

- Configure the Firmware server path and protocol. Click on the “Update Now” button to start the immediate upgrade.
- Click on



to access the Upgrade and Provisioning configuration:

- **Firmware Upgrade and Provisioning:**
- Always Check for New Firmware:
- Always check at bootup when F/W pre/suffix changes
- Skip the Firmware Check.
- **Firmware Upgrade via:** Set the protocol to either HTTP/HTTPS or TFTP for the Firmware server.
- **Firmware Server Username:** Configures the username for the Firmware HTTP/HTTPS server.
- **Firmware Server Password:** Configures the password for the Firmware HTTP/HTTPS server.
- **Firmware Server Path:** Configure the Firmware server path.
- **Config Upgrade via:** Set the protocol to either HTTP/HTTPS or TFTP for the Config server.

- **Config Server Username:** Configures the username for the Config HTTP/HTTPS server.
- **Config Server Password:** Configures the password for the Config HTTP/HTTPS server.
- **Config Server Path:** Configure the Config server path.

Reset

- Factory reset the device to default settings.

CONFIGURATION VIA WEB BROWSER

The GSC3570 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the GSC3570 through a Web browser such as Google Chrome, Mozilla Firefox, and Microsoft Edge.

To access the Web GUI:

1. Connect the computer to the same network as the GSC3570.
2. Make sure the GSC3570 is turned on and shows its IP address. You may check the IP from the LCD **Menu →Settings →Status →Network Status**.
3. Open a Web browser on your computer.
4. Enter the GSC3570’s IP address in the address bar of the browser.
5. Enter the administrator’s login and password available on the MAC sticker to access the Web Configuration Menu.

Notes:

- The computer must be connected to the same sub-network as the GSC3570. This can be easily done by connecting the computer to the same hub or switch as the GSC3570 is connected to. In the absence of a hub/switch (or free ports on the hub/switch), please connect the computer directly to the PC port on the back of the GSC3570.
- If the GSC3570 is properly connected to a working Internet connection, the IP address of the GSC3570 will display in the **MENU→Status→Network Status**. This address has the format: xxx.xxx.xxx.xxx, where xxx stands for a number from 0-255. Users will need this number to access the Web GUI. For example, if the GSC3570 has an IP address of 192.168.40.154, please enter “http://192.168.40.154” in the address bar of the browser.
- There are two access levels for the Web UI page:

User Level	User	Password	Web Pages Allowed
End User Level	user	Set by admin	Only Status and Basic Settings
Administrator Level	admin	Random Password (on the back of the unit)	Browse all pages

Note:

User account login is disabled by default. In order to enable user web access for the first time (or after a factory reset), the administrator needs to set a new user password under **Maintenance→Web Access→User Password**.

- When accessing the GSC3570, the user can then change the default administrator password when proceeding from the web interface→Maintenance→Web Access.
- The new password field is case sensitive with a maximum length of 25 characters. Using a strong password including letters, digits, and special characters is recommended for better security.

Maintenance

Web Access

Web Access

LCD Access

Upgrade and Provisioning

Syslog

Security Settings

Security

Trusted CA Certificates

Automatic Reboot

Packet Capture

Tools

Web Access

User Password

New Password

Confirm Password

Admin Password

Current Password

New Password

Confirm Password

Save

Change Password

- When changing any settings, always SUBMIT them by pressing the “Save” or “Save and Apply” button at the bottom of the page. If the change is saved but not applied, after making all the changes, click on the “APPLY” button at the top of the page to submit. After submitting the changes in all the Web GUI pages, reboot the GSC3570 to have the changes take effect if necessary (All the options under the “Accounts” page and “Phonebook” page do not require reboot. Most of the options under the “Settings” page do not require reboot).

Definitions

This section describes the options in the GSC3570’s Web GUI. As mentioned, you can log in as an administrator or an end user.

- **Status:** Displays the Account status, Network status, and System Info of the GSC3570.
- **Accounts:** To configure the SIP account settings and swap account settings.
- **Settings:** To configure Alarm, IP cameras, call features, ringtones, audio control, LCD display, date, and time, etc.
- **Network:** To configure network settings.
- **Maintenance:** To configure web access, upgrading and provisioning, syslog, security settings, etc.
- **Directory:** To manage contacts, LDAP directory, and call history...

Status Page Definitions

Status → Account Status	
Account	Account index. For GSC3570: up to 4 SIP accounts
SIP User ID	Displays the configured SIP User ID for the account.
SIP Server	Displays the configured SIP Server address, URL or IP address, and port of the SIP server.
SIP Registration	Displays SIP registration status for the SIP account, it will display Yes/No with Green/Red background.
Status → Network Status	
MAC Address	Global unique ID of device, in HEX format. The MAC address will be used for provisioning and can be found on the label coming with original box and on the label located on the back of the device.
IP Setting	The configured address type: DHCP, Static IP.

Ipv4 Address	The Ipv4 address obtained on the GSC3570.
Ipv6 Address	The Ipv6 address obtained on the GSC3570.
OpenVPN IP	The OpenVPN IP obtained on the GSC3570.
Subnet Mask	The subnet mask obtained on the GSC3570.
Gateway	The gateway address obtained on the GSC3570.
DNS Server 1	The DNS server address 1 obtained on the GSC3570.
DNS Server 2	The DNS server address 2 obtained on the GSC3570.
PPPoE Link Up	PPPoE Link status
NAT Type	Displays the configured NAT type
NAT Traversal	Display the status of NAT connection for each account on the GSC3570.
Status  System Info	
Product Model	Product model of the GSC3570.
Part Number	Product part number.
Software Version	Boot: boot version number. Core: core version number. Base: base version number. Prog: program version number. This is the main firmware release number, which is always used for identifying the software system of the GSC3570. CPE: shows CPE version.
IP Geographic Information	City: displaying GSC3570 location. Language: displaying language. Time Zone: displaying time zone. Country Code: displaying the country code;
Special Feature	
OpenVPN® Support	Displys wether OpenVPN® is supported or not.
System Time	System Up Time: System up time since the last reboot. System Time: Current system time on the GSC3570 system.
Service Status	GUI and Phone service status.
System Information	Download system information
User Space	Shows the percentage of the user space used and the status of the Database
Core Dump	Shows the status of the core dump and the core dump files generated if any. It also gives the ability to generate GUI/Phone core dump files manually.

Accounts Page Definitions

Account x  General Settings	
Account Active	This field indicates whether the account is active. Account number 1 is disabled by default, the other accounts are enabled by default.
Account Name	The name associated with each account to be displayed on the LCD.
SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (ITSP).
Secondary SIP Server	The URL or IP address, and port of the SIP server. When configured, GSC3570 will register to both Primary and Secondary SIP Server. If Primary SIP Server is not reachable then the GSC3570 will use Secondary SIP Server for GSC3570 services (including making/receiving calls).
Outbound Proxy	IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller. It is used by the GSC3570 for Firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and ONLY an Outbound Proxy can provide a solution.
Backup Outbound Proxy	IP address or Domain name of the Secondary Outbound Proxy which will be used when the primary proxy cannot be connected.
SIP User ID	User account information provided by your VoIP service provider (ITSP). It is usually in the form of digits like phone number or a phone number. Notes: Users can register an account with a SIP user ID that carries “@”. (For example: “111@test.com”, so the GSC3570 will register the account as “111@test.com” instead of 111) The server domain will not be included in the SIP from header.
Authenticate ID	SIP service subscriber’s Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
Authenticate Password	The account password required for the GSC3570 to authenticate with the ITSP (SIP) server before the account can be registered. After it is saved, this will appear as hidden for security purpose.
Name	The SIP server subscriber’s name (optional) that will be used for Caller ID display.
Voice Mail Access Number	This parameter allows you to access voice messages by pressing the MESSAGE button on the GSC3570. This ID is usually the VM portal access number. For example, in UCM6xxx IPPBX, *97 could be used.
Account x  Dial Plan	
Name	Enter the name for the configured rules.
Rule	Enter the rule settings (number pattern, prefix to add ...etc.).
Type	Choose the type of the rule: Pattern Block Dial now Prefix Second tone

Account x  Network Settings	
DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. There are four modes: A Record, SRV, NATPTR/SRV, Use Configured IP. The default setting is “A Record”. If the user wishes to locate the server by DNS SRV, the user may select “SRV” or “NATPTR/SRV”. If “Use Configured IP” is selected, please fill in the three fields below: Primary IP: Backup IP 1. Backup IP 2. If SIP server is configured as domain name, GSC3570 will not send DNS query, but use “Primary IP” or “Backup IP x” to send SIP message if at least one of them are not empty. GSC3570 will try to use “Primary IP” first. After 3 tries without any response, it will switch to “Backup IP x”, and then it will switch back to “Primary IP” after 3 re-tries. If SIP server is already an IP address, GSC3570 will use it directly even “User Configured IP” is selected.
Primary IP	Configures the primary IP address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
Backup IP1	Configures the backup IP1 address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
Backup IP2	Configures the backup IP2 address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
NAT Traversal	This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No (Default), STUN, Keep-alive, UPnP, Auto or VPN. If set to “STUN” and STUN server is configured, the GSC3570 will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the GSC3570 will try to use public IP addresses and port number in all the SIP&SDP messages. The GSC3570 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.
Proxy-Require	A SIP Extension to notify the SIP server that the Intercom is behind a NAT/Firewall. Do not configure this parameter unless this feature is supported on the SIP server.
Account x  SIP Settings  Basic Settings	
TEL URI	If the GSC3570 has an assigned PSTN phone 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 “Enabled”, “Tel:” will be used instead of “SIP:” in the SIP request. The default setting is “Disable”.
SIP Registration	Selects whether the GSC3570 will send SIP Register messages to the proxy/server. The default setting is “Yes”.
Unregister on Reboot	Allows the SIP user’s registration information to be cleared when the GSC3570 reboots. The SIP REGISTER message will contain “Expires: 0” to unbind the connection. Three options are available: The default setting is “No”. If set to “All”, the SIP user’s registration information will be cleared when the GSC3570 reboots. The SIP Contact header will contain “*” to notify the server to unbind the connection. If set to “Instance”, the SIP user will be unregistered on current GSC3570 only. If set to “No”, the GSC3570 will not unregister the SIP account when rebooting.

Register Expiration	Specifies the frequency (in minutes) in which the GSC3570 refreshes its registration with the specified registrar. The default value is 60 minutes. The maximum value is 64800 minutes (about 45 days).
Subscribe Expiration	Specifies the frequency (in minutes) in which the GSC3570 refreshes its subscription with the specified registrar. The maximum value is 64800 (about 45 days). The default value is 60 minutes.
Reregister Before Expiration	Specifies the time frequency (in seconds) that the GSC3570 sends re-registration request before the Register Expiration. The default value is 0.
Enable OPTIONS Keep Alive	Enable OPTIONS Keep Alive to check SIP Server.
OPTIONS Keep Alive Interval	Time interval for OPTIONS Keep Alive feature in Second.
OPTIONS Keep Alive Max Lost	Number of max lost packets for OPTIONS Keep Alive feature before the GSC3570 re-registration.
Local SIP Port	Defines the local SIP port used to listen and transmit. The default value is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4, 5068 for Account 5, 5070 for Account 6. The valid range is from 1 to 65535.
SIP Registration Failure Retry Wait Time	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
SIP Transport	Determines the network protocol used for the SIP transport. Users can choose from TCP, UDP and TLS. The default setting is “UDP”.
SIP URI Scheme when using TLS	Specifies if “sip” or “sips” will be used when TLS/TCP is selected for SIP Transport. The default setting is “sips”.
Use Actual Ephemeral Port in Contact with TCP/TLS	This option is used to control the port information in the Via header and Contact header. If set to No, these port numbers will use the permanent listening port on the GSC3570. Otherwise, they will use the ephemeral port for the connection. The default setting is “No”.
Outbound Proxy Mode	The Outbound proxy mode is placed in the route header when sending SIP messages, or they can be always sent to outbound proxy.
Support SIP Instance ID	Defines whether SIP Instance ID is supported or not. Default setting is “Yes”.
SUBSCRIBE for MWI	When set to “Yes”, a SUBSCRIBE for Message Waiting Indication will be sent periodically. The GSC3570 supports synchronized and non-synchronized MWI. The default setting is “No”.
SUBSCRIBE for Registration	When set to “Yes”, a SUBSCRIBE for Registration will be sent out periodically. The default setting is “No”.
Enable 100rel	The use of the PRACK (Provisional Acknowledgment) method enables reliability to SIP provisional responses (1xx series). This is particularly important to support PSTN internetworking. To invoke a reliable provisional response, the 100rel tag is appended to the value of the required header of the initial signaling messages. The default setting is “No”.

Callee ID Display	When set to “Auto”, the GSC3570 will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in the 180 Ringing. If “Disabled”, callee ID will be displayed as “Unavailable”. When set to “To Header”, caller ID will not be updated and displayed as To Header.
Caller ID Display	When set to “Auto”, the GSC3570 will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. When set to “Disabled”, all incoming calls are displayed with “Unavailable”. When set to “From Header”, the GSC3570 will display the caller ID based on the From Header in the incoming SIP INVITE. The default setting is “Auto”.
Add Auth Header on Initial REGISTER	To define whether authorization Header will be added on initial REGISTER from the first REGISTER. The default setting is “No”.
Allow SIP Reset	This is used to perform a factory reset through SIP NOTIFY. When the GSC3570 receives the NOTIFY with event:reset, the GSC3570 should perform a factory reset after the authentication. The default setting is “No”.
Ignore Alert-Info header	This option is used to configure default ringtone. If set to “Yes”, configured default ringtone will be played. The default setting is “No”.
Account x  SIP Settings  Custom SIP Headers	
Use Privacy Header	Controls whether the Privacy header will present in the SIP INVITE message or not, whether the header contains the caller info. If set to “Yes”, the Privacy Header will always show in INVITE. If set to “No”, the Privacy Header will not show in INVITE. Default setting is “Default”.
Use P-Preferred- Identity Header	Controls whether the P-Preferred-Identity Header will present in the SIP INVITE message. The default setting is “default” If set to “Yes”, the P-Preferred-Identity Header will always show in INVITE. If set to “No”, the P-Preferred-Identity Header will not show in INVITE.
Use X-Grandstream-PBX Header	Enables / disables the use of X-Grandstream-PBX header in SIP request. When disabled, the SIP message sent from the GSC3570 will not include the selected header. Default setting is “Yes”.
Use P-Access-Network-Info Header	Enables / disables the use of P-Access-Network-Info header in SIP request. When disabled, the SIP message sent from the GSC3570 will not include the selected header. Default setting is “Yes”.
Use P-Emergency-Info Header	Enables / disables the use of P-Emergency-Info header in SIP request. When disabled, the SIP message sent from the GSC3570 will not include the selected header. Default setting is “Yes”.
Use MAC Header	If Yes except REGISTER, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header; If Yes to all SIP, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP message including REGISTER will attach the MAC address to the User-Agent header; If No, neither will the MAC header be included in the register or unregister message nor the MAC address be attached to the User-Agent header for any outgoing SIP message. The default setting is “No”.
Account x  SIP Settings  Advanced Features	
Music on Hold URI	Configures Music on Hold URI to call when a call is on hold. This feature must be supported on the server side.
Omit charset=UTF-8 in MESSAGE	Omit charset=UTF-8 in MESSAGE content-type
Allow Unsolicited REFER	Allow Unsolicited REFER to accomplish an outgoing call.
Special Feature	Different soft switch vendors have special requirements. Therefore, users may need select special features to meet these requirements. Users can choose from Standard, Nortel MCS, BroadSoft, CBCOM, RNK, Sylantrio, PhonePower and UCM Call center depending on the server type. The default setting is “Standard”.

Session Timer	
Enable Session Timer	This option is used to enable or disable session timer on the GSC3570 side when server side can provide both session timer UPDATE or session audit UPDATE. The default setting is “Yes”.
Session Expiration	The SIP Session Timer extension (in seconds) that enables SIP sessions to be periodically “refreshed” via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180. The valid range is from 90 to 64800.
Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
Caller Request Timer	If set to “Yes” and the remote party supports session timers, the GSC3570 will use a session timer when it makes outbound calls. The default setting is “No”.
Callee Request Timer	If set to “Yes” and the remote party supports session timers, the GSC3570 will use a session timer when it receives inbound calls. Default setting is “No”.
Force Timer	If Force Timer is set to “Yes”, the GSC3570 will use the session timer even if the remote party does not support this feature. If Force Timer is set to “No”, the GSC3570 will enable the session timer only when the remote party supports this feature. To turn off the session timer, select “No”. The default setting is “No”.
UAC Specify Refresher	As a Caller, select UAC to use the GSC3570 as the refresher; or select UAS to use the Callee or proxy server as the refresher. The default setting is “Omit”.
UAS Specify Refresher	As a Callee, select UAC to use caller or proxy server as the refresher; or select UAS to use the GSC3570 as the refresher. The default setting is “UAC”.
Force INVITE	The Session Timer can be refreshed using the INVITE method or the UPDATE method. Select “Yes” to use the INVITE method to refresh the session timer. The default setting is “No”.
Account x  SIP Settings  Security Settings	
Check Domain Certificates	Choose whether the domain certificates will be checked or not when TLS/TCP is used for SIP Transport. The default setting is “No”.
Validate Certificate Chain	Validate certification chain when TCP/TLS is configured. Default setting is “No”.
Validate Incoming Messages	Choose whether the incoming messages will be validated or not. The default setting is “No”.
Check SIP User ID for Incoming INVITE	If set to “Yes”, SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the GSC3570’s SIP User ID, the call will be rejected. The default setting is “No”.
Accept Incoming SIP from Proxy Only	When set to “Yes”, the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is “No”.
Authenticate Incoming INVITE	If set to “Yes”, the GSC3570 will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. Default setting is “No”.
Account x  Codec Settings	

Audio Settings	
Preferred Vocoder	Multiple vocoder types are supported on the GSC3570, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message.
Use First Matching Vocoder in 2000K SDP	When it is set to “Yes”, the device will use the first matching vocoder in the received 2000K SDP as the codec. The default setting is “No”.
Codec Negotiation Priority	Configures the GSC3570 to use which codec sequence to negotiate as the callee. When set to “Caller”, the GSC3570 negotiates by SDP codec sequence from received SIP Invite. When set to “Callee”, the GSC3570 negotiates by audio codec sequence on the GSC3570. Default is “Callee”.
Disable Multiple m line in SDP	When it is set to “No”, the device will reply with multiple m lines; Otherwise, it will reply 1 m line. The default setting is “No”.
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu. The default setting is “Disabled”.
SRTP Key Length	Allows users to specify the length of the SRTP calls. The available options are AES 128&256 bit, AES 128 bit and AES 256 bit. Default setting is AES 128&256 bit
Crypto Lifetime	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, GSC3570 will not add the crypto lifetime to SRTP header. The default setting is “Yes”.
Symmetric RTP	Defines whether symmetric RTP is supported or not. Default setting is “No”.
Silence Suppression	Controls the silence suppression/VAD feature of the audio codecs except forG.723 (pending) and G.729. If set to “Yes”, a small quantity of RTP packets containing comfort noise will be sent during the periods of silence. If set to “No”, this feature is disabled. Default setting is “No”
Jitter Buffer Type	Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is “Adaptive”.
Jitter Buffer Length	Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is “300ms”.
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the “ptime” value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is 2.
G723 Rate	This option determines the encoding rate for G723 codec. Users can choose from 6.3kbps encoding rate and 5.3kbps encoding rate. The default setting is “5.3kbps encoding rate”.
iLBC Frame Size	This option determines the iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is “30ms”.
iLBC Payload Type	This option is used to specify iLBC payload type. Valid range is 96 to 127. The default setting is “97”.
OPUS Payload Type	Specifies OPUS payload type. Valid range is 96 to 127. Cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Send DTMF	This parameter specifies the mechanism to transmit DTMF digits. There are 3 supported modes:

	• In audio: DTMF is combined in the audio signal (not reliable with low-bit-rate codecs). • 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”.
DTMF Delay	Configures the delay between sending DTMF (in milliseconds). Default is 250 ms.
Video Settings	
H.264 Image Size	Sets the H.264 image size. It can be selected from the dropdown list. 720P 4CIF VGA CIF QVGA QCIF Note: For some network environment, the default setting “720P” might be too high that causes no video or video quality issue during video call. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower. The default setting is 720P.
H.264 Profile Type	Selects the H.264 profile type from the dropdown list. Baseline Profile Main Profile High Profile BP/MP/HP (Default Setting) Note: Lower levels are easier to decode, but higher levels offer better compression. Usually, for the best compression quality, choose “High Profile”; for playback on low-CPU machines or mobile devices, choose “Baseline Profile”. If “BP/MP/HP” is selected, all three profiles “Baseline Profile” “Main Profile” and “High Profile” will be used for negotiation during video decoding to achieve the best result. This is usually used in video conference when there is higher requirement on the video.
Video Bit Rate	Configures the bit rate for video call. It can be selected from the dropdown list. The default setting is 2048 kbps. The valid range is from 32 – 2048 kbps. Note: The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. For some network environment, the default setting “720P” might be too high that causes no video or video quality issue during video call. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower.
H264 Payload Type	Specifies the H.264 codec message payload type format. The default setting is 99. The valid range is from 96 to 127.
Enable Proxy Video Compatibility	This feature enhancement is designed for some ITSP customers that providing video phone call service. Because GSC3570 does not have camera, this enhancement will improve the video call by sending some fake video packets to notify the proxy then displaying black screen on the other side of the video phone. Default is set to No.
Account x  Call Settings	
Send Anonymous	If set to “Yes”, the “From” header in outgoing INVITE messages will be set to anonymous, blocking the Caller ID to be displayed. Default is “No”.
Anonymous Call Rejection	If set to “Yes”, anonymous calls will be rejected. The default setting is “No”.

Auto Answer	If set to “Yes”, the GSC3570 will automatically turn on the speakerphone to answer incoming calls after a short reminding beep. Default setting is “No”.
Disable Call Waiting	Enables / disables the call waiting feature for the current account. When set to “Default”, global call feature setting will be used. Default setting is Default.
Account x  Intercom Settings	
Allow Auto Answer by Call-Info/Alert-Info	Allows the GSC3570 to automatically turn on the speakerphone to answer incoming calls after a short reminding beep when enabled, based on the SIP Call-Info/Alert-Info header sent from the server/proxy. Default setting is “No”.
Mute on answer Intercom call	When enabled, the GSC3570 will mute the incoming intercom call.
Custom Alert-Info for Auto Answer	Allows to customize Alert-Info header for auto answer. The GSC3570 will auto answer only if matching content of the custom Alert-info header.
Accounts  Account Swap	
Swap Account Settings	Allows users to swap the two accounts that they have configured. This will Increase the flexibility of account management. Note: Make sure to press “Start” to complete the process.

Account Page Definitions

Settings Page Definitions

Settings → Device Mode Settings	
Device Mode	Select the device mode of the GSC3570; two options are available: ● Control Station Mode (Default): In this mode, the GSC3570 functions as a normal control station of the on premise security control, where it is usually deployed with other IP surveillance cameras such as the GSC36xx devices, and Door systems, such as the GDS37xx device models, in this mode the main functionalities deployed are the open door features, the “Monitor” feature, used to display the video feed of the cameras, in addition to some functionalities related to alarm out/in settings, this mode is the default mode of the GSC3570. ● Meeting Room Panel Mode: In this mode, the GSC3570 works as an extension of the UCM63xx model, it is used to display the organized onsite meetings from the UCM platform, and it can also create immediate meetings based on the availability of the time slots, this feature is useful when the GSC3570 is deployed in a meeting room scenario where hosts will need to either create immediate meetings or join an already scheduled meeting.
Settings → Meeting Room Settings (Only on Meeting Room Panel Mode)	
Server Connection	Chooses whether the connection will be established to the meeting server. The server’s meeting data will overwrite and clear the local meeting data if set to yes. If set to no, the system will remove the current meeting date. The default value is Yes.
Meeting Room Name	Defines the meeting room name, when not connected to any SIP server, when it’s connected to a SIP server it will display the name defined on the UCM63xx onsite meeting settings.

Meeting Server	Defines the Meeting server address, which can be the IP address of the UCM on which the onsite meetings will be configured, Example: http(s)://192.168.86.199:8089
Server Connection Status	Displays the connection status, whether it has been connected to the meeting server or not.
Settings  General Settings	
Local RTP Port	This parameter defines the local RTP port used to listen and transmit. It is the base RTP port for channel 0. When configured, channel 0 will use this port _value for RTP; channel 1 will use port_value+2 for RTP. Local RTP port ranges from 1024 to 65400 and must be even. Default value is 5004.
Local RTP Port Range	Gives users the ability to define the parameter of the local RTP port used to listen and transmit. This parameter defines the local RTP port from 48 to 10000. This range will be adjusted if local RTP port + local RTP port range is greater than 65486. Default setting is 200.
Use Random Port	When set to “Yes”, this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple GSC3570s are behind the same full cone NAT. The default setting is “Yes” Note: This parameter must be set to “No” for Direct IP Calling to work.
Keep-alive Interval	Specifies how often the GSC3570 sends a blank UDP packet to the SIP server to keep the “ping hole” on the NAT router to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN Server	The IP address or Domain name of the STUN server. STUN resolution results are displayed in the STATUS page of the Web GUI. Only non-symmetric NAT routers work with STUN.
Test Password Strength	Only allow password with these constraints to ensure better security: The password must be more than 9 characters/digits and must fulfill at least 3 options among 4 options below: 1. Numeric (0-9) 2. Capital letters (A-Z) 3. Lower case (a-z) 4. Special characters (!, @, #, \$, %, ^, &, *, (,), etc.) Default setting is “No”.
Settings  External Service	
Order	Displays the order of the service.
Service Type	Specifies the service GDS, other or HTTP.
Account	Specifies the account on which the service will be applied.
System Identification	Specifies the name to identify the service.
System Number	Specifies the system number, in case the service type option is set to GDS, the system number is the SIP user ID configured on GDS37xx, or the IP address of the GDS37xx itself if it’s using IP call.
System IP Address	Specifies the IP Address of the system.
Door 1 Name	Specifies the name of door 1.
Door 1 Access Password	Determines the access password in case the service type option is set to GDS, the access password is the one configured on “Remote PIN to Open the Door 1” field on GDS37xx settings.

Door 2 Name	Specifies the name of door 2.
Door 2 Access Password	Determines the access password in case the service type option is set to GDS, the access password is the one configured on “Remote PIN to Open the Door 2” field on GDS37xx settings.
Digital Output	
Digital Output	Defines the Digital output mode that will be used. • To Alarm • To Door • Ring For Incoming Call • Disabled Default value is “Disabled”
Alarm Output Duration (s)	Configures (in seconds) the alarm output duration.
Door Control SIP Account	Defines the SIP account used by the GSC3570 for digital output action.
Door System SIP User ID	Defines the SIP user ID registered to the door control device, such as the GDS37xx device.
Door System IP Address	Defines the IP Address of the connected Door system.
Door Control Password	Defines the Door Access Password defined in the Door system.
Door Unlock Holding Time	Defines the duration of the door being unlocked. The default value is 5 seconds.
Arming Settings	
Arming Mode	Selects the Arming Mode of the device, depending on the state you want the GSC3570 to be in, the options available are: • Outdoor • Indoor • Sleeping • Custom • Disarm Default value is “Disarm”
Arming Mode Settings	Specifies the Arming Mode Settings for application to one or multiple zones. There are four zones available (Zone1, Zone2, Zone3, and Zone4), and users can activate arming modes according to the specified zone. The available arming modes include Outdoor, Indoor, Sleeping, and Custom.
Zone Settings	Defines the zone settings based on the below parameters: • Zone Name: Specifies the Zone name. • Zone Type: Select the Zone type, this can be: Doorbell, open door, infrared, smoke sensor, Gas, Drmagnet, Urgency, and Others. • NO/NC: Defines the door reaction on the selected zone to be either: Normal Open, or Normal Close. • Alarm Type: Defines the alarm type to either, a delay alarm, instant alarm, or alarm in 24H. • Enter Delay(s): defines the Enter delay in seconds, which is the period of time allowed for a person to enter a secured area after disarming the system. The default value is 30 seconds. • Exit Delay(s): Defines Exit delay in seconds, which is the time provided for a person to leave a secured area after arming the system. The default value is 0 seconds.
Settings ⚡ Alarm	

Call Mode	Allows user to select between “Serial Hunting” so call will be made towards all configured SIP Number by order of priority, and Parallel Hunting where all Configured SIP Numbers will receive the call simultaneously.
Order (1-4)	Displays the order of the service.
Account	When set to “Dynamic”, the GSC3570 will use the first available Account. User can specify from which account the call can be made for each destination. Default is Dynamic.
SIP Number	Enter the Number to receive the call. User can set up to 4 SIP Numbers.
Settings ⚡ SOS	
Call Mode	Allows user to select between “Serial Hunting” so call will be made towards all configured SIP Number by order of priority, and Parallel Hunting where all Configured SIP Numbers will receive the call simultaneously.
Order (1-4)	Displays the order of the service.
Account	When set to “Dynamic”, the GSC3570 will use the first available Account. User can specify from which account the call can be made for each destination. Default is Dynamic.
SIP Number	Enter the Number to receive the call. User can set up to 4 SIP Numbers.
Settings ⚡ IPC	
Order (1 – 32)	Displays the order of the IP camera
System Identification	Specifies the name to identify the IP camera.
Connection Type	Select the signaling protocol to be used SIP, RTSP(TCP), RTSP(UDP), RTSP(Multicast). Default is SIP.
System Number	Specifies the system number, in case the system number is the SIP user ID configured on IP Camera, or the IP address of the IP Camera itself if it is using IP call.
Account	Specifies the account on which this feature will be applied.
Settings ⚡ Call Features	
Bypass Dial Plan Through Call History and Directories	Enable/Disable the dial plan check while dialing through the call history and any Phonebook directories. The default setting is “No”.
Disable Call Waiting	Disables the call waiting feature. The default setting is “No”.
Disable Call Waiting Tone	Disables the call waiting tone when call waiting is on. Default setting is “No”.
Enable Auto Unmute	If the option is enabled, automatically unmute phone when a user resumes the call or establishes a new call. Default is “No”.
Do Not Escape # as %23 in SIP URI	Specifies whether to replace # by %23 or not for some special situations. The default setting is “No”.
Return Code When Refusing Incoming Call	When refusing the incoming call. The GSC3570 will send the selected type of SIP message of the call. Default setting is “Busy 486”.

	Busy (486) Temporarily unavailable (480) Not Found (404) Decline (603)
User-Agent Prefix	Add a new option for input the user agent field with operator configurable value or value that identifies the device. The option should be configurable to give the end point device specific identification. Ex. The value could be Mobile, Fixed, Desktop, etc. The configured “User Agent” should be prepend to vendor’s default User.
Settings ⚡ Preferences ⚡ Date and Time	
NTP Server	Defines the URL or IP address of the NTP server. The GSC3570 may obtain the date and time from the server. The default setting is “pool.ntp.org”.
Secondary NTP Server	Defines the URL or IP address of the NTP server. The GSC3570 may obtain the date and time from the server. Allow user to configure 2 NTP server domain names. GSC will loop through all the IP addresses resolved from them.
NTP Update Interval	Time interval for updating time from the NTP server. Valid time value is in between 5 to 1440 minutes. The default setting is “1440” minutes.
Allow DHCP Option 42 Override NTP Server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is “Yes”.
Time Zone	Configures the date/time used on the GSC3570 according to the specified time zone.
Allow DHCP Option 2 to Override Time Zone Setting	Defines whether DHCP Option 2 should override time zone or not. The default setting is “Yes”.
Self-Defined Time Zone	This parameter allows the users to define their own time zone. The syntax is: std offset dst [offset], start [/time], end [/time] Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0 MTZ+6MDT+5 This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east. M4.1.0,M11.1.0 The 1st number indicates Month: 1,2, 3..., 12 (for Jan, Feb, ..., Dec) The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday...) The 3rd number indicates weekday: 0,1, 2...,6 (for Sun, Mon, Tues, ... ,Sat)
Date Display Format	Configures the date display format on the LCD. The following formats are supported: 1. yyyy-mm-dd: 2012-07-02 2. mm-dd-yyyy: 07-02-2012 3. dd-mm-yyyy: 02-07-2012 4. dddd, MMMM dd: Friday, October 12 5. MMMM dd, dddd: October 12, Friday 6. The default setting is yyyy-mm-dd.
Time Display Format	Configures the time display in 12-hour or 24-hour format on the LCD. The default setting is in 12-hour format.
Settings ⚡ Preferences ⚡ Language	

Display Language	Selects display language on the phone. There are 21 languages can be set as display language, user could also choose “Auto” or “Downloaded Language” as display language. The default setting is “Auto”.
Settings ⚡ Preferences ⚡ LCD Display	
Turn OFF LCD	LCD panel auto-off timer settings are configurable in seconds, with options including 0, 120, 180, 300, 600, 1200, 1800, and 3600 seconds. The maximum allowed duration is 3600 seconds while setting it to 0 means the LCD panel will never turn off (it will remain ON continuously). If the configured auto-off timer is set to a shorter duration than the “Turn ON Screensaver” timer, the screensaver, including “IPC RTSP Streaming,” will not activate as the LCD panel will turn off first. When “IPC RTSP Streaming” is chosen as the source for the screensaver and the screensaver is triggered, the “Turn OFF LCD” feature will be disabled, ensuring that the LCD panel remains ON continuously. The default value is 180.
Active Backlight Timeout	Allows users to set up the backlight time (in minutes) for the extension board. Valid range from 0 to 90. The default value is 1. Note: When Active Backlight Timeout is set to 0, the backlight will be constantly on.
Upload Wallpaper	The file must be JPEG or PNG format, with resolution 1024 x600, and maximum size 500KB.
Screensaver Timeout	Configures the minutes of idle before the screensaver activates. Valid range is 3 to 6. The default time is 3 minutes.
Turn ON Screensaver	Configurable timer (in seconds) for screensaver activation. Options include: 0, 15, 30, 60, 120, 300, 600, and 1800 seconds. The maximum allowable duration is 1800 seconds, and setting it to 0 disables the screensaver.
Screensaver Source	Select the location where the screensaver is loaded from. the options are : 1. Default 2. Upload: Uploads the screensavers to the GSC3570 through the WebUI , up to three screensavers can be uploaded. 3. SD: If pictures are taken from SD, please have a folder named “/gsc_res/screensaver/” containing your pictures name as screensaver_x.jpg, screensaver_x.jpeg or screensaver_x.png(x:1-10), up to 10 pictures. 4. IPC RTSP Stream: the screensaver will display a stream of what is displayed by the connected IP camera devices chosen from the 32 IP camera options, note that more than one camera can be chosen for the display, with a maximum of 32 cameras at once.
Screensaver 1	Uploads the first Screensaver, Must be in JPG or PNG format, resolution 1024 X 600. 200 KB or smaller.
Screensaver 2	Uploads the second Screensaver, Must be in JPG or PNG format, resolution 1024 X 600. 200 KB or smaller.
Screensaver 3	Uploads the third Screensaver, Must be in JPG or PNG format, resolution 1024 X 600. 200 KB or smaller.
IPC RTSP Stream	Displays the RTSP stream from the connected IP Cameras to the control station, Please configure this option in the “Settings->IPC” page and make sure the IPC connection type is RTSP, when more than one IP Camera is selected, enable the patrol mode by configuring the stream patrol interval.
IPC RTSP Stream Patrol Interval(s)	Configure the IPC RTSP stream patrol interval(in seconds).Range is 10-300. Default value is 30.
Icon Position Layout on Screen	Describes comma separated list of icons displayed on screen, it can be any combination of 0,1,2,3,4,5,6,7,8 or empty. Call icon is 0, Monitor is 1, Arming Status is 2, SOS is 3, Call history is 4, Message is 5, Contacts is 6, Files is 7, Settings is 8. Examples are 0,4,6 means only show call, call history, contacts and setting. Empty means show all icons, 8, means only show setting. Setting icon is always displayed.

Allow not Display “Setting” Icon	When enabled, you have the option to configure the screen so that it does not show the “Setting” icon. Disabled by Default.
Settings ⚡ Preferences ⚡ Ring Tone	
Call Progresses Tones Second Dial Tone Message Waiting Speaker Ring Volume	Configures ring or tone frequencies based on parameters from local telecom. The default value is North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing (“On time” in ‘ms’) while OFF is the period of silence. To set a continuous ring, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported. Speaker volume range is 0-7 (default is 5)
Settings ⚡ Preferences ⚡ Desktop Shortcut Settings	
Desktop Shortcut Settings	Allows users to customize the Home screen by Adding Desktop shortcuts from Web UI , up to 9 Shortcuts can be added and the following parameters needs to be defined: 1. Shortcut type: Speed Dial, RTSP(TCP), HTTP (URL), RTSP(UDP), RTSP(Multicast). 2. Name: The name of the shortcut. 3. Account: the account from which the action will be taken. 4. Destination : Defines destination address. 5. Username : Defines the Username. 6. Password : Defines the password.

Settings Page Definitions

Network Page Definitions

Network ⚡ Basic Settings	
IPv4 Address	Allows users to configure the appropriate network settings on the GSC3570 to obtain IPv4 address. Users could select “DHCP”, “Static IP”. By default, it is set to “DHCP”.
Host name (Option 12)	Specifies the name of the client. This field is optional but may be required by some Internet Service Providers.
DHCP Vendor Class ID (Option 60)	Used by clients and servers to exchange vendor class ID. The default setting is “Grandstream GSC3570” for GSC3570.
IPv4 Address	Enter the IP address when static IP is used.
Subnet Mask	Enter the Subnet Mask when static IP is used for IPv4.
Gateway	Enter the Default Gateway when static IP is used for IPv4.
DNS Server 1	Enter the DNS Server 1 when static IP is used for IPv4.
DNS Server 2	Enter the DNS Server 2 when static IP is used for IPv4.
Preferred DNS Server	Enters the Preferred DNS Server for IPv4.
Network ⚡ Advanced Settings	

802.1X mode	Allows the user to enable/disable 802.1X mode on the GSC3570. The default value is disabled. To enable 802.1X mode, this field should be set to EAP-MD5, users may also choose EAP-TLS, or EAP-PEAP/MSCHAPv2.
802.1X Identity	Enter the Identity information for the 802.1x mode. Note: Valid input needs to match [a-zA-Z0-9]*
MD5 Password	Enter the MD5 Password for the 802.1X mode. Note: Valid input needs to match [a-zA-Z0-9]*
802.1X CA Certificate	Uploads / deletes the 802.1X CA certificate to the GSC3570; or delete existed 802.1X CA certificate from the GSC3570.
802.1X Client Certificate	Uploads / deletes 802.1X Client certificate to the GSC3570; or delete existed 802.1X Client certificate from the GSC3570.
HTTP Proxy	Specifies the HTTP proxy URL for the GSC3570 to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the GSC3570 to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Bypass Proxy For	Enter host names that do not require a proxy to reach. Commas should separate those names.
Layer 3 QoS for SIP	Defines the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 26.
Layer 3 QoS for RTP	Defines the Layer 3 QoS parameter for RTP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 46.
Enable DHCP VLAN	Enables auto configure for VLAN settings through DHCP. Disabled by default.
Enable Manual VLAN Configuration	Enables/disables manual VLAN configuration. When this option is set to Disabled, the GSC3570 will bypass VLAN configuration and only use the DHCP VLAN to configure VLAN tag and priority. Default is “Enabled”.
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets. The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assigns the priority value of the Layer2 QoS packets. The default value is 0.
Enable CDP	Enables/Disables CDP “Cisco Discovery Protocol”. The default setting is “Enabled”.
Enable LLDP	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is “Enabled”.
Maximum Transmission Unit (MTU)	Configure custom MTU. Default is 1500.
Network  OpenVPN® Settings	
OpenVPN® Enable	Enable/Disable OpenVPN® feature. Default is No.
OpenVPN® Server Address	Specify the IP address or FQDN for the OpenVPN® Server.
OpenVPN® Port	Specify the listening port of the OpenVPN® server. Default is 1194.

OpenVPN® Transport	Specify the Transport Type of OpenVPN® whether UDP or TCP. Default is UDP.
OpenVPN® CA	Click on “Upload” to upload the Certification Authority of OpenVPN®. For a new upload, users could click on “Delete” to erase the last certificate, and then upload a new one.
OpenVPN® Certificate	Click on “Upload” to upload OpenVPN® certificate. For a new upload, users could click on “Delete” to erase the last certificate, and then upload a new one.
OpenVPN® Client Key	Click on “Upload” to upload OpenVPN® Key. For a new upload, users could click on “Delete” to erase the last certificate, and then upload a new one.
OpenVPN® Cipher Method	Specifies the Cipher method used by the OpenVPN® server. The available options are: Blowfish, AES-128, AES-256 and Triple-DES. Default setting is: Blowfish.
OpenVPN® Username	Configures the optional username for authentication if the OpenVPN server supports it.
OpenVPN® Password	Configures the optional password for authentication if the OpenVPN server supports it.
Additional Options	Additional options to be appended to the OpenVPN® config file, separated by semicolons. For example, comp-lzo no;auth SHA256 Note: Please Make sure that the options are recognizable by OpenVPN® and do not unnecessarily override the other configurations above.
Network ⚡ SNMP Settings	
Enable SNMP	Enables/Disables the SNMP feature. Default settings is No.
Version	SNMP version: ● Version 1 ● Version 2 ● Version 3 (Default)
Port	SNMP port (Default 161).
Community	Enters SNMP Community.
SNMP Trap Version	SNMP Trap Version ● Trap Version 1 ● Trap Version 2 (Default) ● Trap Version 3
SNMP Trap IP	IP address of the SNMP trap receiver.
SNMP Trap Port	Port of the SNMP trap receiver (Default 162)
SNMP Trap Interval	The interval between each trap sent to the trap receiver
SNMP Trap Community	Community string associated to the trap. It must match the community string of the trap receiver.
SNMP Username	Username for SNMPv3
Security Level	● noAuthUser: Users with security level noAuthnoPriv and context name as noAuth.

	● authUser: Users with security level authNoPriv and context name as auth. ● privUser: Users with security level authPriv and context name as priv.	
Authentication Protocol	Select the Authentication Protocol: “None” or “MD5” or “SHA”.	
Privacy Protocol	Select the Privacy Protocol: “None” or “DES” or “AES”.	
Authentication Key	Enter the Authentication Key.	
Privacy Key	Enter the Privacy Key.	
SNMP Trap Username	Username for SNMPv3 Trap.	
Trap Security Level	● noAuthUser: Users with security level noAuthnoPriv and context name as noAuth. ● authUser: Users with security level authNoPriv and context name as auth. ● privUser: Users with security level authPriv and context name as priv.	
Trap Authentication Protocol	Select the Authentication Protocol: “None” or “MD5” or “SHA”.	
Trap Privacy Protocol	Select the Privacy Protocol: “None” or “DES” or “AES”.	
Trap Authentication Key	Enter the Trap Authentication Key	
Trap Privacy Key	Enter the Trap Privacy Key.	
Network  Wi-Fi Settings		
Enable/Disable Wi-Fi	Enables / Disables the Wi-Fi on the phone. Three options are available: ● No: Disables Wi-Fi. User has ability to enable Wi-Fi from LCD Menu. ● Off & Hide Menu from LCD: Disables Wi-Fi and hides “Wi-Fi Settings” menu from phone LCD. ● Yes: Enables Wi-Fi to connect to Wi-Fi network. Default setting is “No”.	
Country	Specifies the Wi-Fi encryption type.	
Access Point (1 – 10)	SSID	Enters Wi-Fi SSID name to connect.
	Password	Configures the authentication password to access Wi-Fi Network.
	Security Type	Specifies the Wi-Fi encryption type from the available: None, WEP, WPA, WPA Enterprise and Auto. And set EAP Method, Identity/Password when required.
	EAP Settings	Set up “ EAP Method ” (Default: None, PEAP, TLS, TTLS, PWD, SIM, AKA or AKA’), “ EAP Identity ” and “ EAP Password ”

Network Page Definitions

Maintenance Page Definitions

User Password	
New Password	Set a new password for web GUI access as User. Note: This field is case sensitive.
Confirm Password	Enter the new User password again to confirm.
Admin Password	
Current Password	The current admin password is required for setting a new admin password.
New Password	Set a new password for web GUI access as Admin. Note: This field is case sensitive.
Confirm Password	Enter the new Admin password again to confirm.
Maintenance 🔑 LCD Access	
LCD Access	This feature allows controlling access to LCD settings or to the LCD Menu globally with LCD Lock using a password. Password Required: When enabled, it will require the user to enter the LCD password in order to access the unit’s LCD screen. The default is disabled. Screen lock password: the password required if LCD Lock is enabled. Note: Password length must be 6 digits. Icon Feature/password: Password for icon/feature. Password must be 6 digits exactly. This is the password required after the screen timeout. LCD configuration timeout: the period of time, which the unit is not used to lock the LCD screen.
LCD Icons	This feature allows users to show or hide icons on the LCD Screen. Note: Only the Settings icon cannot be hidden. Call icon on LCD: enable/disable the call icon on the LCD screen. Arming icon on LCD: enable/disable the arming icon on the LCD screen. Monitor icon on LCD: enable/disable the monitor icon on the LCD screen. SOS icon on LCD: enable/disable the SOS icon on the LCD screen. Call history icon on LCD: enable/disable the call history icon on the LCD screen. Messages icon on LCD: enable/disable the messages icon on the LCD screen. Settings Icon On LCD: enable/disable the settings icon on the LCD screen. Contacts on LCD: enable/disable the contacts icon on the LCD screen. Files on LCD: enable/disable the file’s icon on the LCD screen. Shortcuts On LCD: enable/disable the shortcut’s icon on the LCD screen.
LCD settings	This feature allows users to select which setting to apply the Configuration password to. Ethernet settings on LCD: if enabled, the user will be required to enter the configuration password to manage Ethernet settings from the LCD screen. Wi-Fi settings on LCD: if enabled, the user will be required to enter the configuration password to manage Wi-Fi settings from the LCD screen. Auto answer settings on LCD: if enabled, the user will be required to enter the configuration password to manage Auto answer settings from the LCD screen. DND settings on LCD: if enabled, the user will be required to enter the configuration password to manage DND settings from the LCD screen. Arming mode settings on LCD: if enabled, the user will be required to enter the configuration password to manage arming mode settings from the LCD screen. Alarm zone settings on LCD: if enabled, the user will be required to enter the configuration password to manage alarm zone settings from the LCD screen. Digital output settings on LCD: if enabled, the user will be required to enter the configuration password to manage digital output settings from the LCD screen. Sound settings on LCD: if enabled, the user will be required to enter the configuration password to manage sound settings from the LCD screen. Display settings on LCD: if enabled, the user will be required to enter the configuration password to manage display settings from the LCD screen. Language settings on LCD: if enabled, the user will be required to enter the configuration password to manage language settings from the LCD screen.

	Time and date settings on LCD: if enabled, the user will be required to enter the configuration password to manage time and date settings from the LCD screen. Reboot settings on LCD: if enabled, the user will be required to enter the configuration password to manage reboot settings from the LCD screen. Screen lock settings on LCD: if enabled, the user will be required to enter the configuration password to manage arming mode settings from the LCD screen. Account settings on LCD: if enabled, the user will be required to enter the configuration password to manage account settings from the LCD screen. SD card settings on LCD: if enabled, the user will be required to enter the configuration password to manage SD card settings from the LCD screen. Alarm settings on LCD: if enabled, the user will be required to enter the configuration password to manage alarm settings from the LCD screen. Syslog settings on LCD: if enabled, the user will be required to enter the configuration password to manage syslog settings from the LCD screen. System update settings on LCD: if enabled, the user will be required to enter the configuration password to manage system update settings from the LCD screen. FTP settings on LCD: if enabled, the user will be required to enter the configuration password to manage FTP settings from the LCD screen. Reset settings on LCD: if enabled, the user will be required to enter the configuration password to manage reset settings from the LCD screen.
Open Door Icon On LCD	If enabled, this feature allows the user to add an icon on the LCD screen to open the doors of the paired GDS37xx. The default is disabled.
Hide RTSP Button During the Call	Allows hiding the RTSP button during audio/video call. The default setting is Disabled.
Hide Numpad Button During the Call	Allows hiding the Numpad button during audio/video calls. The default setting is Disabled.
Default Contacts Directory	Chooses the default contacts directory from the following options: Local , Favorite , Group , and LDAP . The default setting is Local.
Maintenance 🔑 Upgrade and Provisioning	
Upgrade Firmware	Allows users to upload the firmware file locally by pressing Start. After selecting the correct firmware file from the local storage, the GSC3570 will start the firmware upgrade automatically.
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning requests are to be sent: Always Check for New Firmware, Check New Firmware only when F/W pre/suffix changes, Always Skip the Firmware Check. The default setting is “Always Check for New Firmware”.
Always Authenticate Before Challenge	Only applies to HTTP/HTTPS. If enabled, the GSC3570 will send credentials before being challenged by the server. The default setting is “No”.
Validate Hostname in Certificate	After enabling this feature, the device validates the hostname in the SSL certificate. The default setting is “No”.
Allow DHCP Option 43 and Option 66 to Override the Server	The default setting is “Yes”. DHCP option 66 was originally designed only for the TFTP servers. Later, it was extended to support an HTTP URL. GSC3570 supports both TFTP and HTTP servers via option 66. Users can also use the DHCP option 43 vendor-specific option to do this. The DHCP option 43 approach has priorities. The GSC3570 will fall back to the original server path configured in case the server from option 66 fails.
Additional Override DHCP Option	When enabled, users could select Option 150 or Option 160 to override the firmware server instead of using the configured firmware server path or the server from Option 43 and Option 66 in the local network. Please note that this option will be effective only when the option “Allow DHCP Option 43 and Option 66 to Override Server” is enabled. The default setting is “None”.
Allow DHCP Option 120 to override SIP Server	Enables DHCP Option 120 from the local server to override the SIP Server on the GSC3570. The default setting is “No”.
3CX Auto Provision	Enables the automatic provision feature (PNP) on the GSC3570. The default setting is “Yes”.

Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options: 1. No: The GSC3570 will only do upgrade once at boot up. 2. Check every X minutes: User needs to specify a period in minutes. 3. Check every day: User needs to specify “Hour of the day (0-23)”. 4. Check every week: The user needs to specify “Hour of the day (0-23)” and “Day of the week (0-6)”. (Day of the week starts from Sunday). The default is No.
Randomized Automatic Upgrade	Randomized Automatic Upgrade within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s).
Hour of the Day (0-23)	Defines the hour of the day to check the HTTP/TFTP/FTP server for firmware upgrades or configuration file changes. The default value is 1.
Day of the Week (0-6)	Defines the day of the week to check the HTTP/TFTP/FTP server for firmware upgrades or configuration file changes. The default value is 1.
Disable SIP NOTIFY Authentication	Device will not challenge NOTIFY with 401 when set to “Yes”. The default setting is “No”.
Firmware Upgrade Confirmation	If set to “Yes” (Default), the GSC3570 will ask the user to upgrade. If there is no response, the GSC3570 will proceed with the upgrade.
Config	
Config Upgrade Via	Allows users to choose the config upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is “HTTPS”.
Config Server Path	Defines the server path for provisioning. Default is “fm.grandstream.com/gs”
Config Server Username	The username for the Config server.
Config Server Password	The password for the Config server.
Config File Prefix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the GSC3570.
Config File Postfix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the GSC3570.
XML Config File Password	The password for encrypting XML configuration file using OpenSSL. This is required for the GSC3570 to decrypt the encrypted XML configuration file.
Authenticate Conf File	Sets the GSC3570 system to authenticate the configuration file before applying it. When set to “Yes”, the configuration file must include value P1 with the GSC3570 system’s administration password. If it is missed or does not match the password, the GSC3570 system will not apply it The default setting is “No”.
Download Device Configuration	Click to download GSC3570’s configuration file in .txt format. Note: The file does not include passwords or CA/Custom certificates.
Download Device Configuration (XML)	Click to download GSC3570’s configuration file in .xml format. Note: The file does not include passwords or CA/Custom certificates.
User protection	When user protection is on, the p-values that the user sets will not be changed by the provision or provider. If “User protection” is OFF, everyone (Provider, user, or admin) has access to most of the P-values.

	If “User protection” is ON, only those (normally user or admin) who have the privilege can modify the configuration.
Download and Process All Available Config Files	By default, the device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, and cfg.xml (corresponding to device-specific, model-specific, and global configs). If this option is enabled, the GSC3570 will invert the downloading process to cfg.xml > cfgGSC3570.xml > cfgMAC.bin > cfgMAC.xml. The following files will override the files that have already been loaded and processed.
Download User Configuration	This allows users to download part of the configuration that does not include any personal settings, like usernames and Passwords. Also, it will include all the changes manually made by the user from the web UI, or config file uploaded from “Upload Device Configuration”, but will not include the changes from the server provision via TFTP/FTP/FTPS/HTTP/HTTPS.
Upload Device Configuration	Uploads configuration file to GSC3570.
Export backup Package	Export backup package, which contains device configuration along with personal data.
Restore from Backup package	Click to upload backup package and restore.
Firmware	
Firmware Upgrade Via	Allows users to choose the firmware upgrade method: TFTP, FTP, FTPS, HTTP, or HTTPS. The default setting is “HTTP”.
Firmware Server Path	Defines the server path for the firmware server. Default is “fm.grandstream.com/gs”
Firmware Server Username	The username for the Firmware server.
Firmware Server Password	The password for the Firmware server.
Firmware File Prefix	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the GSC3570.
Firmware File Postfix	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the GSC3570.
Maintenance  Syslog	
Syslog Protocol	If set to SSL/TLS, the Syslog messages will be sent through secured TLS protocol to the Syslog server. The default setting is UDP. Note: The CA certificate is required to connect with the TLS server.
Syslog Server	URL or IP address of the syslog server for the GSC3570 to send syslog to. Note: By adding a port number to the Syslog server field (i.e., 172.18.1.1:1000), the GSC3570 will send Syslog to the corresponding port of that IP.
Syslog Level	Selects the level of logging for syslog. The default setting is “None”. There are 4 levels: DEBUG, INFO, WARNING and ERROR. Syslog messages are sent based on the following events: ● Product model/version on boot up (INFO level). ● NAT related info (INFO level). ● Sent or received SIP message (DEBUG level). ● SIP message summary (INFO level). ● Inbound and outbound calls (INFO level).

	• registration status change (INFO level). • Negotiated codec (INFO level). • Ethernet link up (INFO level). • SLIC chip exception (WARNING and ERROR levels). • Memory exception (ERROR level).
Syslog Keyword Filtering	Syslog will be filtered based on keywords provided. If you enter multiple keywords, it should be separated by ‘,’. Please note that no spaces are allowed.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages. The default setting is “No”. Note: By setting Send SIP Log to Yes, the GSC3570 will still send SIP log from syslog even when Syslog Level set to NONE.
Maintenance 🔑 TR-069	
ACS URL	URL for TR-069 Auto Configuration Servers (ACS). The default setting is: https://acs.gdms.cloud
TR-069 Username	ACS username for TR-069.
TR-069 Password	ACS password for TR-069.
Periodic Inform Enable	Enables periodic inform. If set to “Yes”, device will send inform packets to the ACS. The default setting is “Yes”.
Periodic Inform Interval	Sets up the periodic inform interval to send the information packets to the ACS. The default is 60sec.
Connection Request Username	The username for the ACS to connect to the phone.
Connection Request Password	The password for the ACS to connect to the phone.
Connection Request Port	The port for the ACS to connect to the phone.Defqult is 7547.
CPE SSL Certificate	The Cert File for the phone to connect to the ACS via SSL.
CPE SSL Private Key	The Cert Key for the phone to connect to the ACS via SSL.
Randomized TR069 Startup	When enabled, TR-069 will send out first INFORM message to server on randomized timing between 1 to 3600 seconds after phone boots up. Disabled by Default
Maintenance 🔑 Security Settings 🔑 Security	
Enable/Disable Weak Ciphers	Select the cipher suites’ policy. • Enable Weak TLS Ciphers Suites • Disable Symmetric Encryption RC4/DES/3DES • Disable Symmetric Encryption SEED • Disable All Weak Symmetric Encryption • Disable Symmetric Authentication MD5 • Disable All Weak TLS Ciphers Suites
Validate Server Certificates	After enabling this feature, GSC3570 will validate the server’s certificate. If the server that our GSC3570 tries to register on is not on our list, it will not allow server to access the GSC3570.

SIP TLS Certificate	SSL Certificate used for SIP Transport in TLS/TCP.
SIP TLS Private Key	SSL Private key used for SIP Transport in TLS/TCP.
SIP TLS Private Key Password	SSL Private key password used for SIP Transport in TLS/TCP.
Custom Certificate	The uploaded custom certificate will be used for SSL/TLS communication instead of the GSC3570 default certificate. Note: 2nd Generation Certifications are supported too.
Web Access Mode	Sets the protocol for web interface. • HTTPS • HTTP • Disabled • Both HTTP and HTTPS The default setting is “HTTP”.
HTTP Web Port	Configures the HTTP port under the HTTP web access mode. Default is 80.
HTTPS Web Port	Configures the HTTPS port under the HTTPS web access mode. Default setting is “443”.
Enable User Web Access	Allows to enable/disable user web access. Default setting is disabled.
Disable SSH	Disables SSH access. The default setting is “No”. (The SSH default port is 22)
SSH Public Key	This option allows you to use authentication keys for SSH access. The public key should be loaded to GSC3570’s web UI while the private key should be used in the SSH tool side. Note: This will allow upcoming SSH access without password.
Web Session Timeout	Configures timer to logout web session during idle. Default is 10 min. Range is 2-60 min.
Web Access Attempt Limit	Configures attempt limit before lockout. Default is 5. Range is 1-10.
Maintenance 🔧 Security Settings🔧 Trusted CA Certificates	
Trusted CA Certificates	Allows to upload and delete the CA Certificate file to GSC3570. Note: Users can either upload the file directly from the web or they can choose to provision it from their cfg.xml file.
Load CA Certificates	Users can specify which certificate they are going to use: • Default Certificates: (Default) Built-in Certificates. • Custom Certificates: Uploaded Certificates. • All Certificates: Both built-in and uploaded Certificates. Note: 2nd Generation Certifications are supported too.
Maintenance 🔧 Automatic Reboot	
Automatic Reboot	Users can configure the GSC3570 to automatically reboot daily, weekly, or monthly. The default is disabled. Note: The GSC3570 needs to be rebooted for this option to take effect.
Reboot Time	Configure the GSC3570 to automatically reboot at the selected time.
Maintenance → Packet Capture	

Status	Displays packet capture status. When the user starts to capture a trace file, it will show “RUNNING” status; otherwise, it will show “STOPPED”.
With RTP Packets	Defines whether the packet capture file contains RTP or not. Default is No
Maintenance → Tools	
Provision	Launch provision process.
Factory Reset	Reset device.
Ping	Start ping on a destination.
Traceroute	Start Traceroute on a destination.

Maintenance Page Definitions

Directory Page Definitions

Phonebook → Contacts	
Search Bar	Allows users searching for Phonebook entries.
Add Contact	Specifies Contact’s First Name, Last Name, Phone Number, Accounts and Groups Blacklist, Whitelist, Work, Friends and Family) to add one new contact in Phonebook. Note: If the contact number belongs to Blacklist group, the call from this number will be blocked. If the contact number belongs to Whitelist group, when the GSC3570 is on DND mode, the call from whitelist number will be allowed.
Edit Contact	Edits selected contact.
Delete All Contacts	Deletes all contacts from Phonebook. NOTE: A message prompt will be displayed so that users will confirm to delete or cancel the operation, to prevent users from losing contacts when deleting them accidentally.
Phonebook → Group Management	
Add Group	Specifies Group’s name to add new group and select a default ringtone for this group. Up to 30 Groups can be added.
Edit Group	Edits selected group.
Phonebook → Phonebook Management	
Enable Phonebook XML Download	Configures to enable Phonebook XML download. Users could select HTTP/HTTPS/TFTP to download the Phonebook file. The default setting is “Disabled”.
HTTP/HTTPS Username	The username for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.

Phonebook XML Server Path	Configures the server path to download the Phonebook XML. This field could be IP address or URL, with up to 256 characters.
Phonebook Download Interval	Configures the Phonebook download interval (in minutes). If it is set to 0, the automatic download will be disabled. The default value is 0. The valid range is 5 to 720 minutes.
Remove Manually edited Entries on Download	If set to “Yes”, when XML Phonebook is downloaded, the entries added manually will be automatically removed. The default setting is “Yes”.
Import Group Method	When set to “Replace”, existing groups will be completely replaced by imported one; When set to “Append”, the imported groups will be attended with the current one.
Download XML	Click on “Download” to download the XML Phonebook file to local PC
Phonebook	
Upload XML Phonebook	Click on “Upload” to upload local XML Phonebook file to the GSC3570.
Default search mode	Configures default phonebook search mode. Quick Match: The quick search feature allows users to search parts and strings of the entries. For instance, if users only remember the first name, last name, or parts of the name / phone number, they can use the string in the search bar. Exact Match: Users can search their contacts using alphabets in the exact mode which allows them to find their contacts even if they forget the numbers. To perform this type of search, make sure that search type is set to “Exact Match” then you can enter the exact name of the contact for lookup. The default setting is “Quick Match”.
Phonebook ⚡ Call History	
Delete	Users can select an entry, then click “Delete” to remove it from the list.
Delete All	Click on Delete All to remove all Call History stored in the phone. Note: Users could use the drop-down list to show only selected call history type (All, Answered, Dialed, Missed, Transferred) and use navigation keys to browse pages when many entries exist.
Phonebook ⚡ LDAP	
LDAP Protocol	Configures the LDAP protocol to LDAP or LDAPS. The default setting is “LDAP”. LDAPS is a feature to support LDAP over TLS.
Server Address	Configures the IP address or DNS name of the LDAP server.
Port	Configures the LDAP server port. The default port number is “389”.
Base	Configures the LDAP search base. This is the location in the directory where the search is requested to begin. Example: dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com

Username	Configures the bind “Username” for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	Configures the bind “Password” for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
LDAP Number Filter	Configures the filter used for number lookups. Examples: (!(telephoneNumber=%)(Mobile=*)) returns all records which has the “telephoneNumber” or “Mobile” field starting with the entered prefix; (&(telephoneNumber=*) (cn=*)) returns all the records with the “telephoneNumber” field starting with the entered prefix and “cn” field set.
LDAP Name Filter	Configures the filter used for name lookups. Examples: (!(cn=*)(sn=*)) returns all records which has the “cn” or “sn” field starting with the entered prefix; (!(sn=*)) returns all the records which do not have the “sn” field starting with the entered prefix; (&(cn=*) (telephoneNumber=*)) returns all the records with the “cn” field starting with the entered prefix and “telephoneNumber” field set.
LDAP Version	Selects the protocol version for the GSC3570 to send the bind requests. The default setting is “Version 3”.
LDAP Name Attributes	Specifies the “name” attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes. Example: gn cn sn description
LDAP Number Attributes	Specifies the “number” attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated number attributes. Example: telephoneNumber telephoneNumber Mobile
LDAP Display Name	Configures the entry information to be shown on Intercom’s LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber
Max. Hits	Specifies the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. The default setting is 50.
Search Timeout	Specifies the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 30 seconds.
Sort Results	Specifies whether the searching result is sorted or not. Default setting is “No”.

Directory Page Definitions

NAT Settings

If the devices are kept within a private network behind a Firewall, we recommend using a STUN Server. The following settings are useful in the STUN Server scenario:

- **STUN Server**

Under **Settings→General Settings**, enter a STUN Server IP (or FQDN) that you may have, or look up a free public STUN Server on the internet and enter it in this field. If using a Public IP, keep this field blank.

○ **Use Random Ports**

It is under **Settings → General Settings**. This setting depends on your network settings. When set to “Yes”, it will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple GSCs are behind the same NAT. If using a Public IP address, set this parameter to “No”.

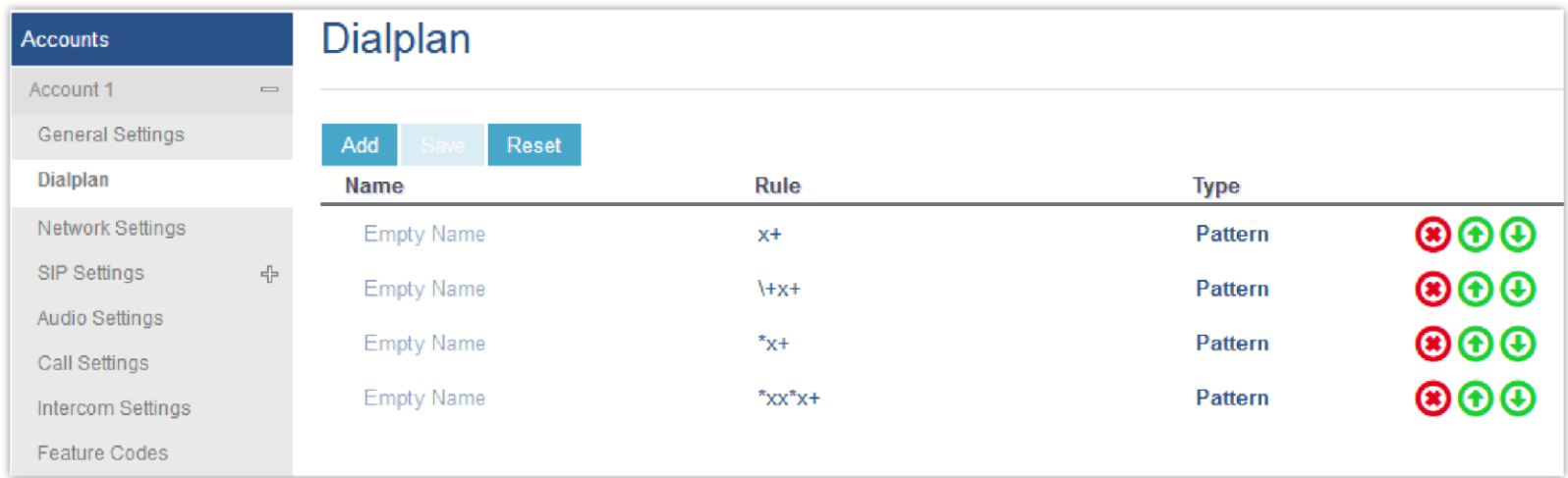
○ **NAT Traversal**

It is under **Accounts X→Network Settings**. The default setting is “No”. Enable the device to use NAT traversal when it is behind a firewall on a private network. Select Keep-Alive, Auto, STUN (with STUN server path configured too), or other option according to the network setting.

Dial Plan Configuration

Dial plan sets the rules to manage outgoing calls, to allow or block some types of calls, or change the number format before dialing out. Users can configure dial plan rules through a simple and well-designed interface under the menu “**Account X → Dial Plan**”.

For explanation purposes, we will be using the dial plan user interface.



Dial Plan Configuration

The current interface features are as follows:

- 1. **Name:** Users can name their dial plans for identification.
- 2. **Rule:** The rules can be typed out separately or in combination with “Type”.
- 3. **Type:** We now support the following types.
 - 1. **Pattern:** The general rule. It will not change the dial plan you configured.
 - 2. **Block:** The rules you set in combination with this type will be blocked.
 - 3. **Dial Now:** The rules you set in combination with this type will be dialed out once the DTMF matches the Dial Plan.
 - 4. **Prefix:** The rules you set in combination with this type will include a configured prefix automatically. If Replaced was set, your used prefix will replace the “Replaced” value.

Replaced:

1,2,3,4,5,6,7,8,9,0

Used:

1,2,3,4,5,6,7,8,9,0

Prefix

Rule:

1,2,3,4,5,6,7,8,9,0 , * , #, A,a,B,b,C,c,D,d

For example: If Dialed 3456, the DTMF will send 123456. See configuration below.

Replaced:

3

Used:

123

Prefix

Rule:

xxx|

- 5. Second tone: The rules you set in combination with this type will play second tone if matching the Trigger.

Trigger:

1,2,3,4,5,6,7,8,9,0

Second tone

Rule:

1,2,3,4,5,6,7,8,9,0 , * , #, A,a,B,b,C,c,D,d

- 4. Automatically update the configured data to the Dial Plan in Call Settings.
- 5. Dial Plan Verification.

Notes

- This feature is not supported by config files (both .xml and .txt).
- Users can increase or decrease the priority of each Pattern by pressing  to move it up and  to move it down.

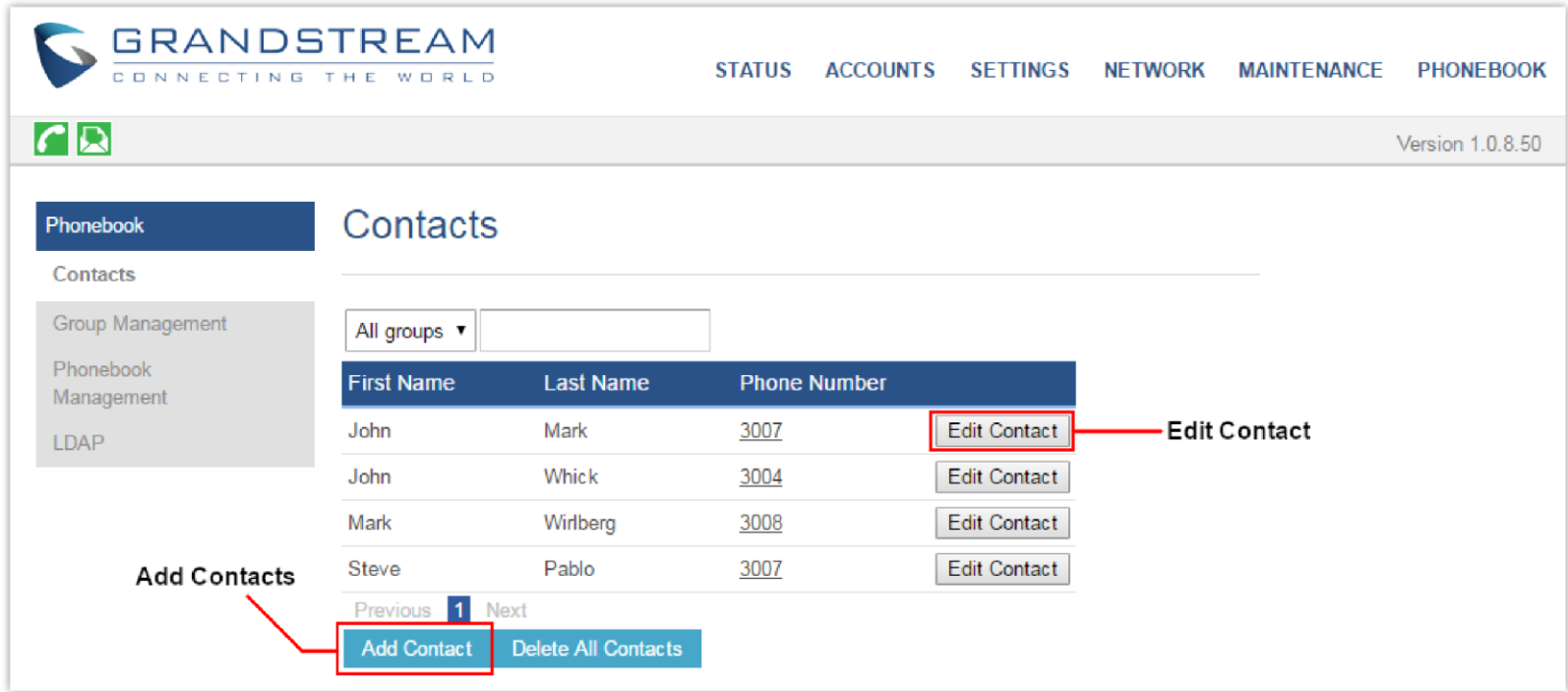
Edit contacts

Users can navigate under the web GUI menu « **Directory →Contacts** » and edit all the related settings to each contact. The following fields are available for configuration:

- **First Name.**
- **Last Name.**
- **Favorite.**
- **Company**
- **Department.**
- **Job.**
- **Job Title.**
- **Work.**
- **Home.**
- **Mobile.**
- **Account.**
- **Groups**
- **Ring Tone** (Set a specific ring tone for the contact).
- **Picture.**

Note

For the ring tone, currently only .wav file is supported. Users can upload their customized .wav files as custom ringtones. (File size and format are restricted to 500KB or less.)



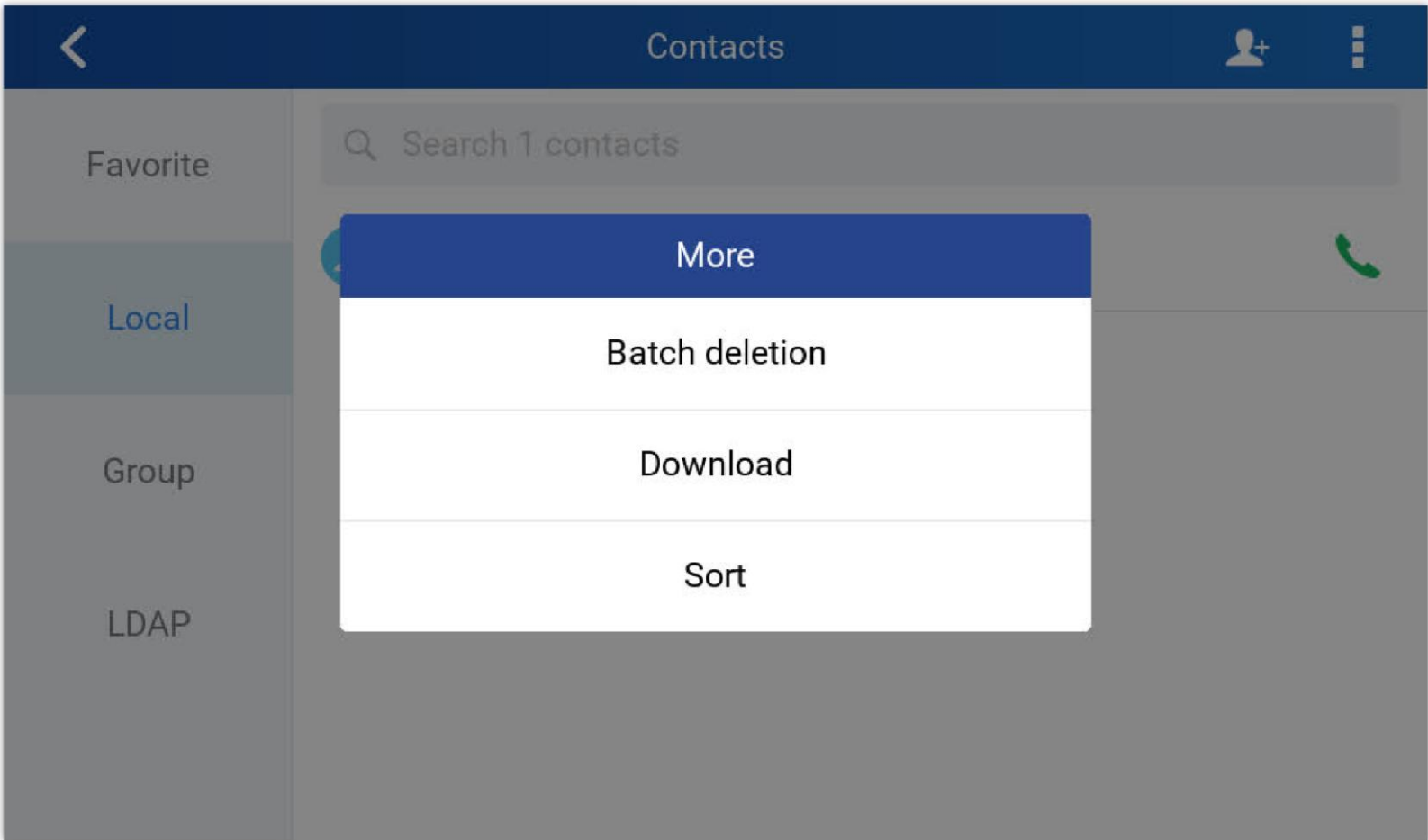
Edit contacts

Phonebook – Immediate Download

Once the Phonebook download is enabled, three ways would make the Intercom trigger the download:

○ **The download Button:**

Go to the Intercom’s Contact and tap  then tap on Download on LCD.



Download XML phonebook

○ **Phonebook Download Interval:**

After each time the interval set for “Phonebook Download Interval” passes, the Intercoms will download the Phonebook.

Saving Configuration Changes

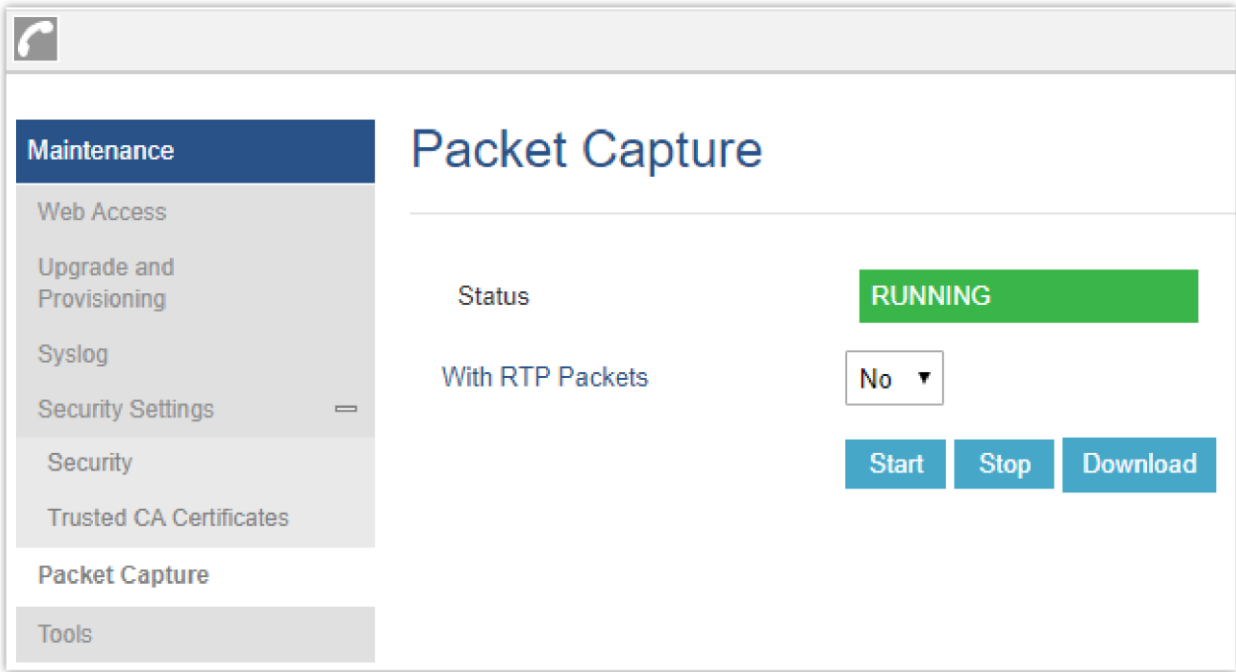
After users make changes to the configuration, pressing the “Save” button will save but not apply the changes until the “Apply” button at the top of the web GUI page is clicked. Or users could directly press the “Save and Apply” button. We recommend rebooting or power cycling the GSC3570 after applying all the changes.

Rebooting from Remote Locations

Press the “Reboot” button on the top right corner of the web GUI page to reboot the GSC3570 remotely. The web browser will then display a reboot message. Wait for about 1 minute to log in again.

Packet Capture

GSC3570 is embedded with a packet capture function. The related options are under **Maintenance→Packet Capture**.



Packet Capture

The user can also define whether RTP packets will be captured or not from the **With RTP Packets** option.

When the capture configuration is set, press the Start button to start packet capture. The Status will become RUNNING while capturing. Press the **Stop** button to end capture.

Press the Download button to download the capture file to the local PC. The capture file is in .pcap format.

UPGRADING AND PROVISIONING

The GSC3570 can be upgraded via TFTP / FTP / FTPS / HTTP / HTTPS by configuring the URL/IP Address for the TFTP / HTTP / HTTPS / FTP / FTPS server and selecting a download method. Configure a valid URL for TFTP, FTP/FTPS, or HTTP/HTTPS; the server’s name can be an FQDN or IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

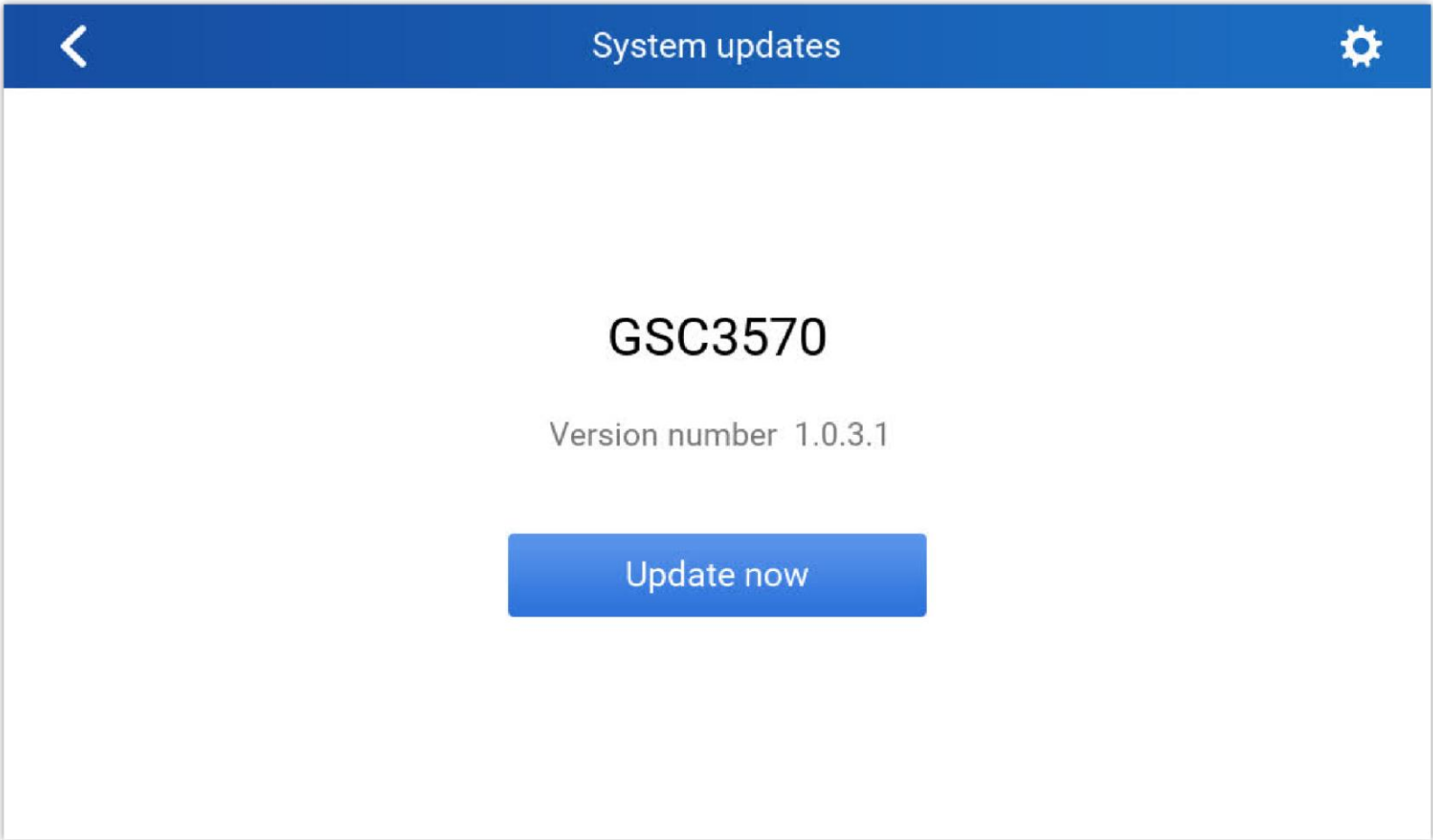
fw.mycompany.com

There are two ways to set up a software upgrade server: The LCD Menu or the Web Configuration Interface.

Upgrade via LCD Menu

Follow the steps below to configure the upgrade server path via the LCD menu:

- Press the MENU button and navigate to **System**.
- In the System options, tap **System Updates**.
- Click Update now.



LCD upgrade

Upgrade via Web GUI

Open a web browser on a PC and enter the IP address of the GSC3570. Then, log in with the administrator username and password. Go to the **Maintenance → Upgrade and Provisioning** page, enter the IP address or the FQDN for the upgrade server in the “Firmware Server Path” field, and choose to upgrade via TFTP or HTTP/HTTPS, or FTP/FTPS. Update the change by clicking the “Save and Apply” button. Then, “Reboot” or power cycle the GSC3570 to update the new firmware.

When upgrading starts, the screen will show the upgrading progress. When done, you will see the GSC3570 restart again. Please do not interrupt or power cycle the GSC3570 when the upgrading process is on.

Firmware upgrading takes around 60 seconds in a controlled LAN or 5-10 minutes over the Internet. We recommend completing firmware upgrades in a controlled LAN environment whenever possible.

No Local TFTP/FTP/HTTP Servers

For users who would like to use remote upgrading without a local TFTP/FTP/HTTP server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for their GSC3570 via this server. Please refer to the webpage:

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

Alternatively, users can download a free TFTP, FTP, or HTTP server and conduct a local firmware upgrade. A free Windows version of the TFTP server is available for download from:

http://www.solarwinds.com/products/freetools/free_tftp_server.aspx

<http://tftpd32.jounin.net/>.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the GSC3570 to the same LAN segment.
3. Launch the TFTP server and go to the **File menu → Configure → Security** to change the TFTP server’s default setting from “Receive Only” to “Transmit Only” for the firmware upgrade.
4. Start the TFTP server and configure the TFTP server in the GSC3570’s web configuration interface.
5. Configure the Firmware Server Path to the IP address of the PC.
6. Update the changes and reboot the GSC3570.

End users can also choose to download a free HTTP server from <http://httpd.apache.org/> or use

Microsoft IIS web server.

Configuration File Download

Grandstream SIP Devices can be configured via the Web Interface as well as via a Configuration File (binary or XML) through TFTP, FTP/FTPS, or HTTP/HTTPS. The “Config Server Path” is the TFTP, FTP/FTPS or HTTP/HTTPS server path for the configuration file. It needs to be set to a valid URL, either in FQDN or IP address format. The “Config Server Path” can be the same or different from the “Firmware Server Path”.

A configuration parameter is associated with each field in the web configuration page. A parameter consists of a Capital letter P and 2 to 5-digit numbers. i.e., P2 is associated with the “New Password” in the Web GUI→**Maintenance→Web Access page→Admin Password**. For a detailed parameter list, please refer to the corresponding configuration template.

When the GSC3570 boots up or reboots, it will issue a request to download a configuration file named “cfgxxxxxxxxxxx” followed by an XML file named “cfgxxxxxxxxxxx.xml”, where “xxxxxxxxxxx” is the MAC address of the GSC3570, i.e., “cfg000b820102ab” and “cfg000b820102ab.xml”. If the download of the “cfgxxxxxxxxxxx.xml” file is not successful, the GSC3570 will issue a request to download a specific model configuration file “cfg<model>.xml”, where <model> is the GSC3570 model, i.e., “cfgGSC3570.xml” for the GSC3570, “cfgGSC3570” for the GSC3570. If this file is not available, the GSC3570 will issue a request to download the generic “cfg.xml” file. The configuration file name should be in lower-case letters.

For more details on XML provisioning, please refer to:

<https://documentation.grandstream.com/knowledge-base/sip-device-provisioning-guide/>

No Touch Provisioning

After the GSC3570 sends, config file request to the BroadSoft provisioning server via HTTP/HTTPS, if the provisioning server responds “401 Unauthorized” asking for authentication, the GSC3570’s LCD will prompt a window for the user to enter the username and password. Once the correct username and password are entered, the GSC3570 will send a config file request again with authentication. Then the GSC3570 will receive the config file to download and get provisioned automatically.

Besides manually entering the username and password in the LCD prompt, users can save the login credentials for the provisioning process as well. The username and password configuration are under GSC3570’s web UI→**Maintenance→Upgrade and provisioning** page: “HTTP/HTTPS Username” and “HTTP/HTTPS Password”. If the saved username and password are correct, the login window will be skipped. Otherwise, the login window will pop up to prompt users to enter the correct username and password again.

Note

- Firmware can NOT be downgraded to 1.0.5.12 or below due to Wi-Fi security enhancement update.
- Added Support HW1.5A, 1.5B on firmware upgrade 1.0.5.21
- Factory Reset is required if upgraded from firmware 1.0.3.1 or before, to initialize all internal parameters correctly.
- SD Card must be formatted via touch screen UI before using it for storage.

Wallpaper Provisioning

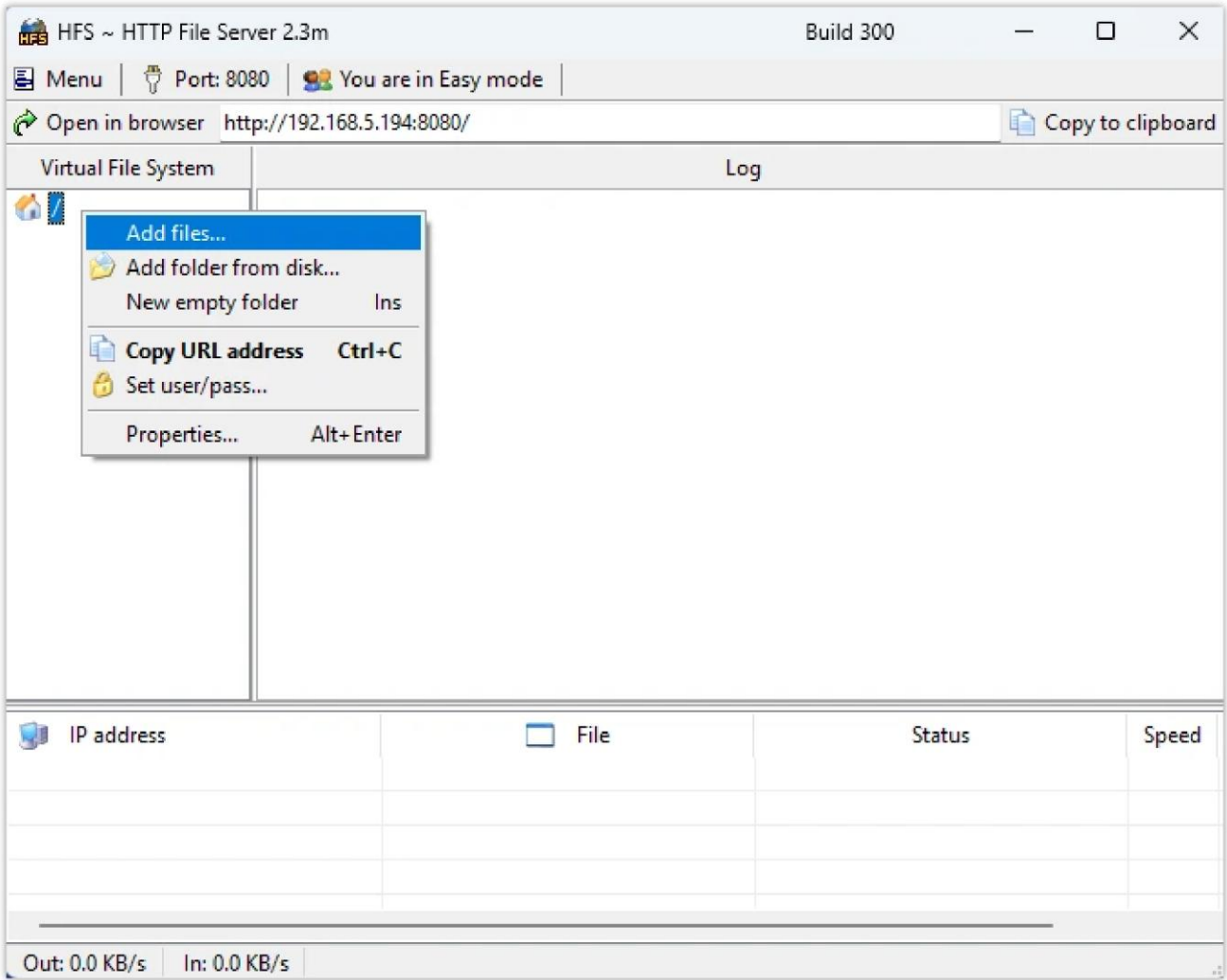
Users can also provision a wallpaper to the GSC3570 control station via the firmware upgrade server path. This can be done by uploading the wallpaper on the firmware server and configuring the GSC3570 to retrieve it through HTTP/HTTPS.

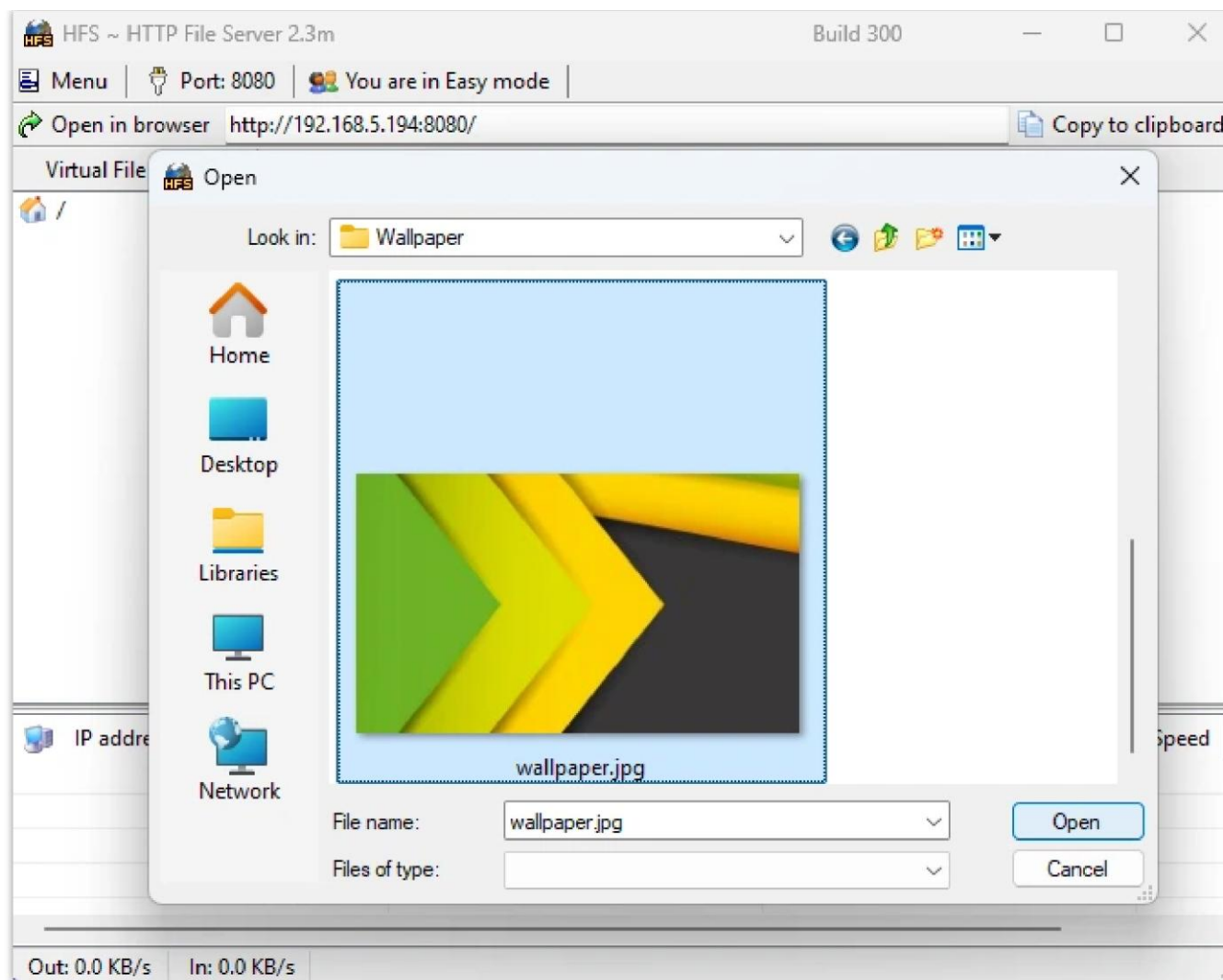
Note:

The wallpaper should not exceed 500KB with a resolution of 1024×600.

The following steps demonstrate how to provision a wallpaper to the GSC3570 control station using a local HTTP server:

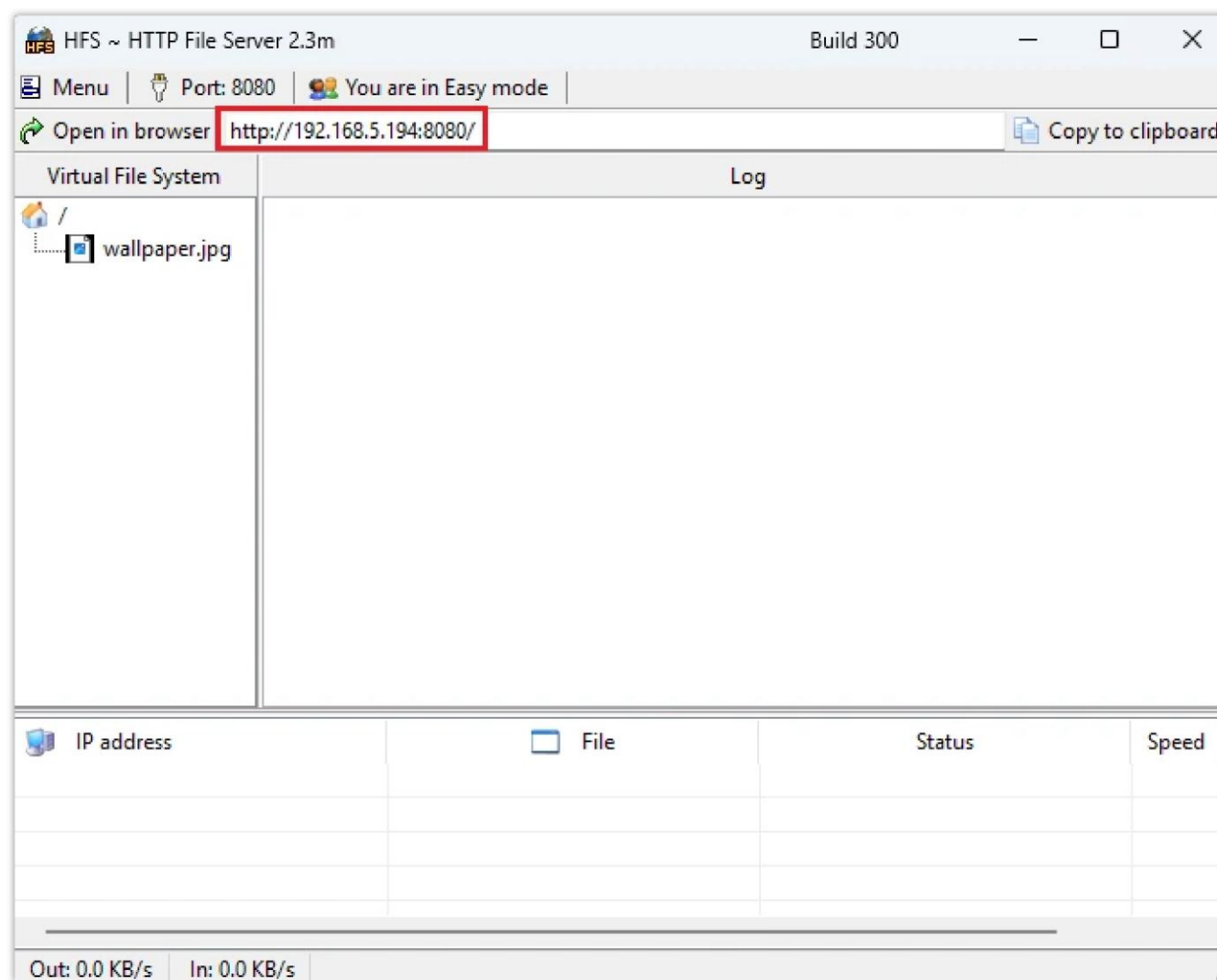
1. Launch the installation of the tool once it’s fully downloaded from the following link: “ <https://www.rejetto.com/hfs/download> ”
2. Click on Run to launch the HTTP server.
3. When HFS starts, browse and add the wallpaper image file from the local directories. Select the file and click Open to upload it to the HTTP server.





Uploading the wallpaper to the HTTP server

4. Once the image is uploaded, copy the path of the HTTP server.



Copying the HTTP server path

5. On the GSC3570 Web UI, go to **Maintenance** → **Upgrade and Provisioning** → **Firmware**, select HTTP for firmware upgrade, and paste the HTTP server path under **Firmware Server Path**.

Firmware

Firmware Upgrade via

☐ TFTP ☒ HTTP ☐ HTTPS ☐ FTP ☐ FTPS

Firmware Server Path

http://192.168.5.194:8080

Firmware Server Username

Firmware Server Password

Firmware File Prefix

Firmware File Postfix

Save

Save and Apply

Reset

Firmware Upgrade configuration

6. Click on **Save and Apply**.
7. On the server log, the HTTP GET request sent by the GSC3570 will appear as shown below:

HFS ~ HTTP File Server 2.3m

Build 300

Menu

Port: 8080

You are in Easy mode

Open in browser

http://192.168.5.194:8080/

Already in clipboard

Virtual File System

/

wallpaper.jpg

Log

1:05:48 PM 192.168.6.251:48084 Requested GET /wallpaper.jpg

1:05:48 PM 192.168.6.251:48084 Fully downloaded - 36.2 K @ 2.4 MB/s - /wallpaper.jpg

IP address

File

Status

Speed

Out: 0.0 KB/s

In: 0.0 KB/s

HTTP Server Log

8. Once the wallpaper is fully downloaded, the GSC3570 idle screen will display the new wallpaper instead of the default one.

Account 1

11:57AM

11:57

Mon 2024-08-26

Call

Monitor

Arming Status

Disarmed

SOS

SOS

Not configured

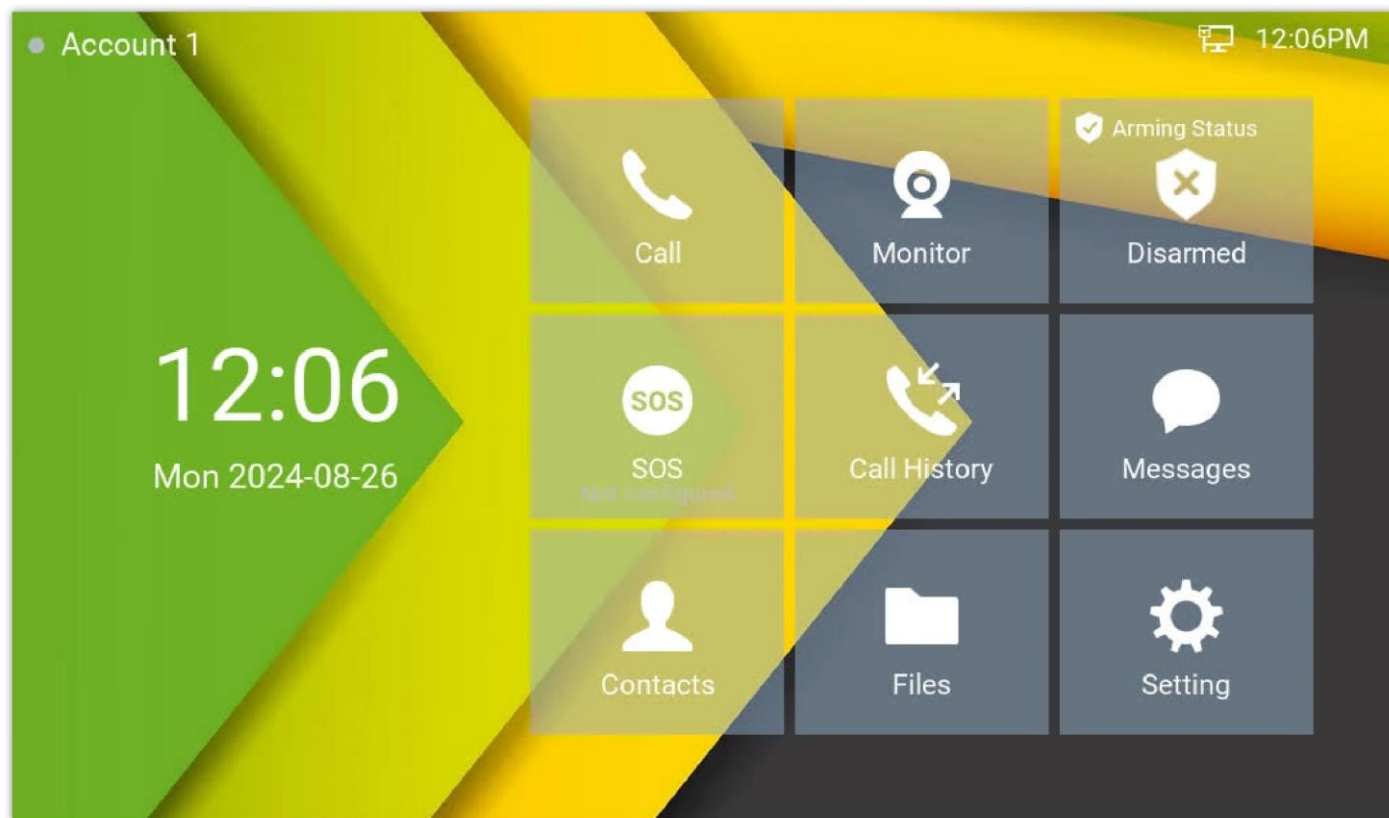
Call History

Messages

Contacts

Files

Setting



GSC3570 Provisioned Wallpaper

RESTORE FACTORY DEFAULT SETTINGS

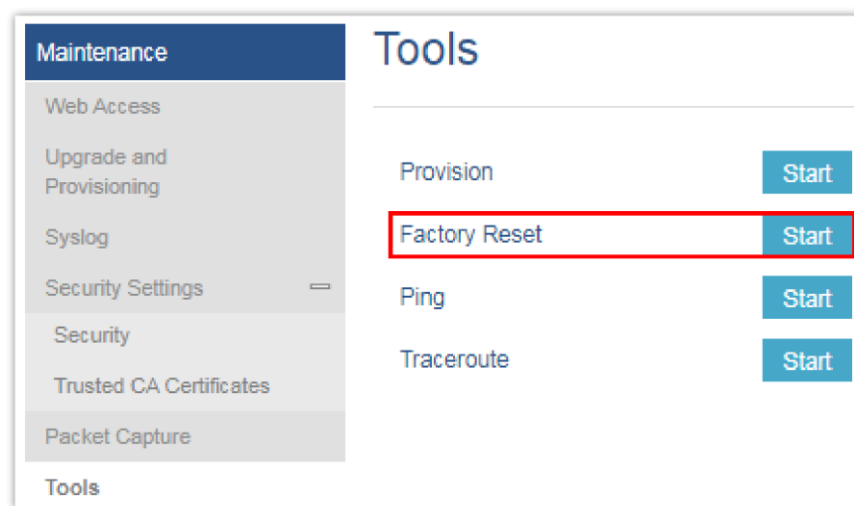
Warning

Restoring the Factory Default Settings will delete all configuration information on the GSC3570. Please back up or print all the settings before you restore to the factory default settings. Grandstream is not responsible for restoring lost parameters and cannot connect your device to your VoIP service provider.

There are two methods to perform a factory reset on the GSC3570 IP Intercom series, which are described below.

Restore to factory using Web GUI

From the web GUI and as shown in the following screenshot, users need to access Maintenance→Tools, then need to click on **Start** to launch the factory reset process.

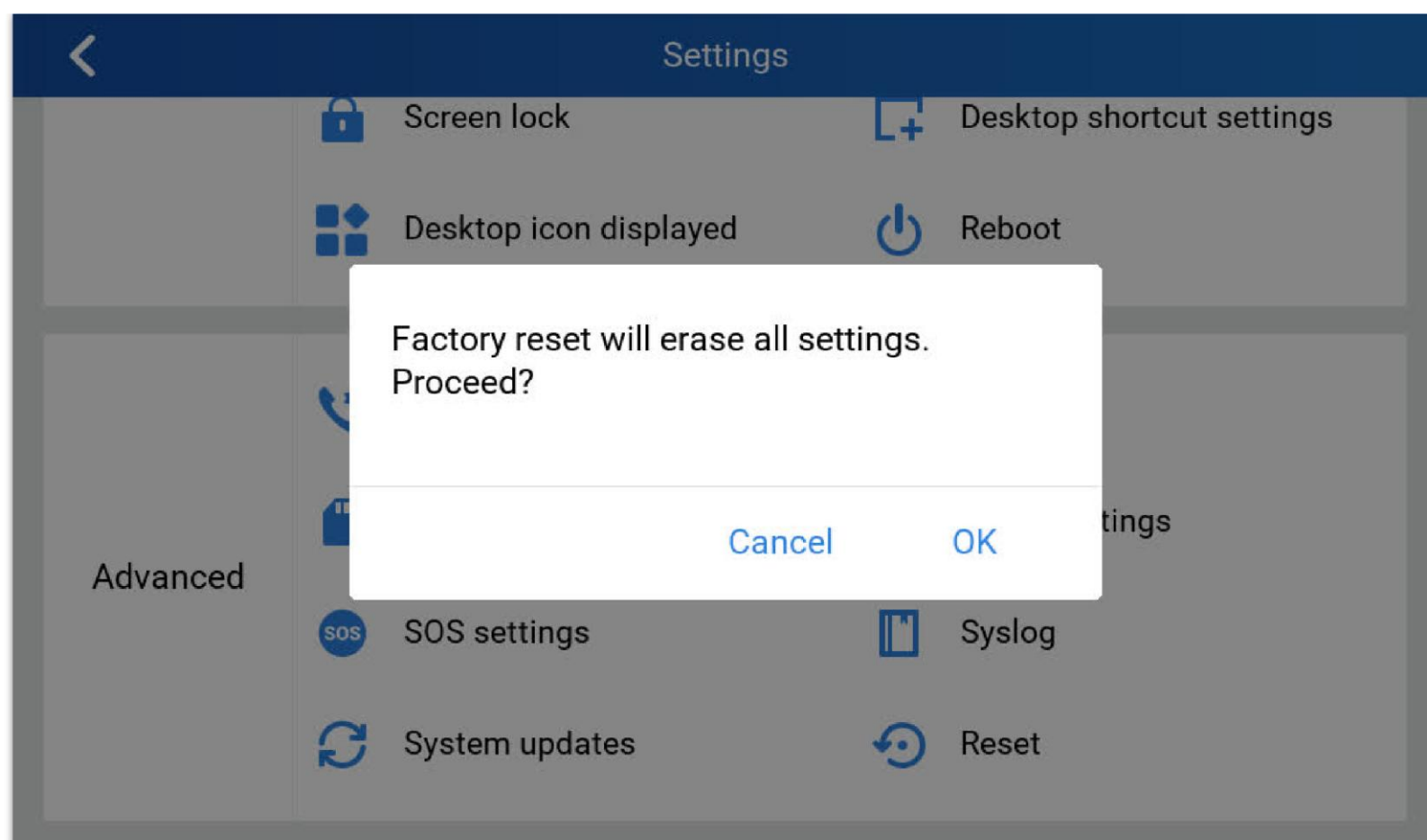


Factory Reset from web GUI

Restore to factory using the LCD menu

Please follow the instructions below to reset the GSC3570:

- Press the MENU button, navigate to Settings Menu, then click Reset.



Factory Reset from LCD

CHANGE LOG

This section documents significant changes from earlier versions of the user manual for GSC3570. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.7.10

- Added support for SSL Medium Strength Cipher Suites. [[Enable/Disable Weak Ciphers](#)]
- Added security version. [[Security Version](#)]
- Account 1 active status is now set to “No” by default. [[Account Active](#)]
- “Use Random Port” for RTP is now enabled by default. [[Use Random Port](#)]

Firmware Version 1.0.7.8

- Added support to configure “Alarm Output Duration”. [[Alarm Output Duration](#)]
- Added CPE display on the Status page. [[CPE](#)]
- Added “Enable User Web Access” in Security Settings. [[Enable User Web Access](#)]
- Added the ability to change the default contacts directory. [[Default Contacts Directory](#)]
- Disabled non-admin account by default. [[Enable User Web Access](#)]
- Added support to hide the buttons displayed during a call. [[Hide RTSP Button During the Call](#)][[Hide Numpad Button During the Call](#)]
- Added support for wallpaper provisioning. [[Wallpaper Provisioning](#)]
- Updated CPE to version 1.0.4.99. [[CPE](#)]

Firmware Version 1.0.7.5

- Disable non-admin accounts by default. [[Configuration via Web browser](#)]

Firmware Version 1.0.7.4

- No Major Changes.

Firmware Version 1.0.7.2

- Added support for Meeting Room Schedule Feature. [[Meeting Room Panel Mode](#)]
- Added displaying RTSP live video when the device is idle. [[IPC RTSP Stream](#)]
- Added support for IPC RTSP Stream Patrol Interval. [[IPC RTSP Stream Patrol Interval](#)]

- Added support to turn off the LCD. [[Turn OFF LCD](#)]
- Added support to turn on the Screensaver. [[Turn ON Screensaver](#)]
- Added support to hide the settings icon. [[Allow not Display “Setting” Icon](#)]
- Added support for the digital output configuration from the web UI. [[Digital Output](#)]
- Added support for configuring Arming settings from the web UI. [[Arming Settings](#)]
- Added support for 2nd Generation Certification. [[Custom Certificate](#)]

Firmware Version 1.0.5.30

- Added Screensaver Customization. [[Screensaver Source](#)]
- Added Icon Position layout. [[Icon Position Layout on Screen](#)]
- Added that both door buttons will be displayed under the preview. If it is not GDS37xx, it will send a DTMF message to opendoor. [[OpenDoor via GDS37xx](#)]

Firmware Version 1.0.5.27

- Added feature: when configured, the missing call(s) will not light up the “HOME” button and blink. [[Enable home key LED indicator](#)]
- Added support for RTSP multicasting. [[Connection type](#)]
- Added TR-069 settings page in the web UI [[TR-069](#)]

Firmware Version 1.0.5.21

- Added ability to switch to “Monitor” during an active call and end call from a 3d party phone to resume Monitor/RTSP. [[Monitor during a SIP call](#)]
- Added restriction in the option “Icon Position Layout on Screen”. [[Desktop settings](#)]
- Added new feature: Dial Shortcut touch UI on Desktop. [[Shortcut touch UI on Desktop](#)]
- Added Door Open port to trigger a 3rd-party audio/light strike device when receiving an incoming call. [[Door open Port Trigger](#)]
- Added the ability to display big icons at the call screen in the active call. [[Big Icons at Call Screen](#)]
- Added option to adjust the “Doorbell volume” in the “Sound” setting of touch UI. [[Doorbell Volume](#)]
- Increased the number of supported GDS37xx operations from 10 to 20. [[GDS37xx Operations](#)]

Firmware Version 1.0.5.17

- Added support to send an HTTP GET request during an answered call. [[HTTP GET Request](#)]
- Added icons on the desktop with password protection. [[LCD Access](#)]
- Added audio volume control in the touch UI for RTSP streaming. [[RTSP](#)]

Firmware Version 1.0.5.12

- Added “System Uptime” under “System info” display at Touch UI. [[System Info](#)]
- Added scheduled auto-reboot to improve device stability. [[Automatic Reboot](#)]
- Added the ability to open the door using Virtual Keys from the Idle Screen. [[Open Door icon on LCD](#)]
- Added language support for Polish and Czech in the Web GUI. [[Language](#)]

Firmware Version 1.0.5.9

- Added support for Proxy Video Compatibility Mode. [[Enable Proxy Video Compatibility](#)]
- Added support to display two open door icons for the door system supporting a two-door configuration. [[Connecting GSC3570 with GDS37xx](#)]
- Added to turn on the LCD when the device is in energy save mode (LCD Off), but the secure open-door event happened. [[Secure Open Door Peering with GDS37xx](#)]
- Added Panel in idle screen (top right corner) to display detailed information. [[Idle Screen](#)]
- Added remote open door via GDS without a SIP call. [[Open Door via GDS37xx with or without a SIP Call](#)]
- Added functioning as a doorbell and direct open door when connected to the strike. [[Using GSC3570 as a Doorbell and a Door opener](#)]

- Added screen snapshot feature during RTSP streaming or SIP Video Call. [[Screen Snapshot During RTSP Streaming or SIP Video Call](#)]

Firmware Version 1.0.5.4

- Added support for RTSP. [[Connection Type](#)]
- Added Secure Open Door by using GSC3570 (Alarm Output Interface), controlling strike/lock from the inside building via peering with GDS37xx. [[Secure Open Door Peering with GDS37xx](#)]
- Added support for switching to RTSP Monitor during an active SIP call. [[Switching to RTSP Monitor during an active SIP call](#)]
- Added support for FTP server settings and SD card. [[FTP Server Settings](#)] [[SD Card](#)]
- Added Tooltip specified file requirement for uploading customized wallpaper. [[Upload Wallpaper](#)]
- Added support to customize the main idle screen. [[Desktop Settings](#)]
- Added Open Door softkey support for 3rd party door systems. [[Connecting GSC3570 with 3rd Party Door Access Systems](#)]
- Added VLAN functions in “General networking settings” at LCD Settings. [[General Networking Settings](#)]
- Added Czech language support in touch UI. [[Language](#)]

Firmware Version 1.0.3.1

- This is the initial version for GSC3570.
-