

# Grandstream Networks, Inc.

---

GSC3570

HD Intercom & Facility Control Station

**User Manual**



## **COPYRIGHT**

©2020 Grandstream Networks, Inc. <http://www.grandstream.com>

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

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

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

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

## **CAUTION**

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

## **WARNING**

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



## GNU GPL INFORMATION

GSC3570 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

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

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



## Regulatory Information

### Common part

This equipment complies with radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Après examen de ce matériel aux conformités ou aux limites d'intensité de champ RF, les utilisateurs peuvent sur l'exposition aux radiofréquences et la conformité and compliance d'acquérir les informations correspondantes. La distance minimale du corps à utiliser le dispositif est de 20cm.

### U.S. FCC Part 15 Regulatory Information

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

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

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

**Note:** This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in an installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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



## Canada Regulatory Information

### Radio equipment

Operation of 5150-5250 MHz is restricted to indoor use only.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s).

Operation is subject to the following two conditions:

- (1) This device may not cause interference.
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

- 1) L'appareil ne doit pas produire de brouillage;
- 2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3(B)

## U.S. FCC Part 15 Regulatory Information

Support Frequency Bands and Power:

WLAN/BT 2.4 GHz < 20 dBm;

WLAN 5.2 GHz < 23 dBm;

WLAN 5.3/ 5.6 GHz < 20 dBm;

The simplified EU declaration of conformity referred to in Article 10(9) shall be provided as follows:

Hereby, **[Grandstream Networks, Inc.]** declares that the radio equipment type **[GSC3570]** is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address:

**[www.grandstream.com](http://www.grandstream.com)**



## Table of Content

<b>DOCUMENT PURPOSE .....</b>	<b>10</b>
<b>CHANGE LOG .....</b>	<b>11</b>
Firmware Version 1.0.3.1 .....	11
<b>WELCOME .....</b>	<b>12</b>
<b>PRODUCT OVERVIEW .....</b>	<b>13</b>
Feature Highlights .....	13
GSC3570 Technical Specifications .....	13
<b>GETTING STARTED .....</b>	<b>15</b>
Equipment Packaging .....	15
GSC3570 Wiring Connection .....	16
GSC3570 Setup .....	17
<i>On-Wall Mounting</i> .....	18
<i>In-Wall Mounting</i> .....	19
Connecting the GSC3570 .....	19
Alarm IN/OUT .....	21
Connection Examples .....	22
<i>GSC3570 Connection &amp; Wiring Diagrams - "Fail Secure" Electric Strike, POE Power Supply ...</i>	22
<i>GSC3570 Connection &amp; Wiring Diagrams - "Fail Safe" Electric lock, 3rd Party Power Supply ...</i>	22
<i>GSC3570 Connection &amp; Wiring Diagrams - "Fail Safe" Electric lock, Power Supply and Wi-Fi ..</i>	23
Connecting GDS37xx with GSC3570 .....	23
Connecting IP Camera with GSC3570 .....	25
Arming Mode .....	27
Alarm & SOS Calling .....	28
<b>GSC3570 LCD SETTINGS .....</b>	<b>32</b>
Access LCD Settings .....	33
Status .....	35
<i>Account Status</i> .....	35
<i>Network Status</i> .....	35
<i>System Info</i> .....	35



<i>Storage Info</i> .....	35
Network .....	36
<i>Ethernet Settings</i> .....	36
<i>Wi-Fi</i> .....	36
Features .....	36
<i>Auto-Answer</i> .....	36
<i>DND</i> .....	36
<i>Arming mode</i> .....	37
<i>Zone Settings</i> .....	37
Basic .....	37
<i>Sound</i> .....	37
<i>Display</i> .....	38
<i>Language</i> .....	38
<i>Date &amp; Time</i> .....	38
<i>Weather Settings</i> .....	38
<i>Reboot</i> .....	39
<i>Screen Lock</i> .....	39
Advanced .....	39
<i>Accounts</i> .....	39
<i>Monitor</i> .....	39
<i>Alarm Settings</i> .....	40
<i>SOS Settings</i> .....	40
<i>Syslog</i> .....	40
<i>System Update</i> .....	41
<i>Reset</i> .....	41
<b>CONFIGURATION VIA WEB BROWSER .....</b>	<b>42</b>
Definitions .....	43
<i>Status Page Definitions</i> .....	44
<i>Accounts Page Definitions</i> .....	45
<i>Settings Page Definitions</i> .....	56
<i>Network Page Definitions</i> .....	61



<i>Maintenance Page Definitions</i> .....	65
<i>Directory Page Definitions</i> .....	71
NAT Settings .....	74
Dial Plan Configuration .....	75
Phonebook - Immediate Download .....	77
Saving Configuration Changes .....	78
Rebooting from Remote Locations .....	78
Packet Capture .....	78
<b>UPGRADING AND PROVISIONING</b> .....	<b>79</b>
Upgrade via LCD Menu .....	79
Upgrade via Web GUI .....	80
No Local TFTP/FTP/HTTP Servers .....	80
Configuration File Download .....	80
No Touch Provisioning .....	81
<b>RESTORE FACTORY DEFAULT SETTINGS</b> .....	<b>82</b>
Restore to factory using Web GUI .....	82
Restore to factory using LCD menu .....	82
<b>EXPERIENCING GSC3570</b> .....	<b>84</b>





## Table of Tables

Table 1: GSC3570 Features in a Glance .....	13
Table 2: GSC3570 Technical Specifications .....	13
Table 3: Equipment Packaging .....	15
Table 4: GSC3570 Wiring Connection .....	16
Table 5: GSC3570 LCD Menu .....	32
Table 6: Status Page Definitions .....	44
Table 7: Account Page Definitions .....	45
Table 8: Settings Page Definitions .....	56
Table 9: Network Page Definitions .....	61
Table 10: Maintenance Page Definitions.....	65
Table 11: Directory Page Definitions .....	71



## Table of Figures

Figure 1: GSC3570 Package Content .....	15
Figure 2: GSC3570 Wiring Connection.....	16
Figure 3: Built in Stand and Mounting Slots on The GSC3570.....	17
Figure 4: On-Wall Mounting .....	18
Figure 5: In-Wall Mounting .....	19
Figure 6: GSC3570 web interface.....	20
Figure 7: Alarm_In/Out Circuit for GDS3710.....	21
Figure 8: Fail Secure” Electric Strike, POE Power Supply .....	22
Figure 9: Fail Safe” Electric lock, 3rd Party Power Supply .....	22
Figure 10: Fail Safe” Electric lock, 3rd Party Power Supply, Wi-Fi.....	23
Figure 11: External Service: Web Configuration .....	24
Figure 12: External Service: LCD Configuration .....	25
Figure 13: IPC: Web Configuration .....	26
Figure 14: IPC: LCD Configuration .....	26
Figure 15: Features: Zone Settings .....	27
Figure 16: Features: Arming Mode .....	28
Figure 17: Features: Arming Status .....	28
Figure 18: SOS: Web Configuration.....	29
Figure 19: SOS: LCD Configuration.....	30
Figure 20: Alarm: Web Configuration.....	30
Figure 21: Alarm: LCD Configuration .....	31
Figure 22: MENU Configuration.....	34
Figure 23: GSC3570 System Settings .....	35
Figure 24: Change Password .....	43
Figure 25: Dial Plan Configuration .....	75
Figure 26: Edit contacts .....	77
Figure 27: Download XML phonebook.....	77
Figure 28: Packet Capture .....	78
Figure 29: LCD upgrade.....	79
Figure 30: Factory Reset from web GUI .....	82
Figure 31: Factory Reset from LCD .....	83



## DOCUMENT PURPOSE

This document describes how to configure the GSC3570 features via LCD menu and Web GUI menu. To learn the basic functions of GSC3570, please visit <http://www.grandstream.com/support> to download the latest User Manual.

This guide covers the following topics:

- [Product Overview](#)
- [Getting Started](#)
- [GSC3570 LCD Settings](#)
- [Configuration via Web interface](#)
- [Upgrading and Provisioning](#)
- [Restore Factory Default Settings](#)
- [Experiencing GSC3570](#)



## CHANGE LOG

This section documents significant changes from earlier versions of 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 1.0.3.1**

- This is the initial version for GSC3570.



## WELCOME

Thank you for purchasing Grandstream GSC3570 Integrated SIP Intercom Phone. The GSC3570 is a powerful Intercom phone for door control and 2-way intercom. It features a 7" 1024x600 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 two-way voice communication solution for their wall-mount and desktop.




# PRODUCT OVERVIEW

## Feature Highlights

The following tables contain the major features of GSC3570.

**Table 1: GSC3570 Features in a Glance**

	<b>GSC3570</b>	<ul style="list-style-type: none"> <li>• 4 lines</li> <li>• 7" 1024x600 touch screen LCD TFT LCD with Home Key</li> <li>• 2-way HD audio with advanced AEC</li> <li>• integrated dual-band 802.11ac Wi-Fi</li> <li>• 100M network port with PoE, full duplex</li> </ul>
---	----------------	---

## GSC3570 Technical Specifications

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

**Table 2: GSC3570 Technical Specifications**

<b>Protocol/Standards</b>	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, 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
<b>Network Interface</b>	Dual switched 10/100Mbps ports with integrated PoE
<b>Graphic Display</b>	7" 1024×600 capacitive touch screen TFT LCD with Home Key
<b>Wi-Fi</b>	Yes, dual-band 802.11b/g/n/ac (2.4GHz & 5GHz)
<b>Auxiliary Ports</b>	4 x Alarm Input 1 x Alarm Output Micro SD card slot Micro USB
<b>Voice Codecs and Capabilities</b>	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
<b>Video Decoders and Capabilities</b>	H.264 BP/MP/HP, video resolution up to 720p, frame rate up to 30 fps, bit rate up to 2Mbps
<b>Telephony Features</b>	4 SIP accounts, hold, call waiting, call log, auto answer, etc.



<b>Sample Applications</b>	Local apps: Contacts, Call History, Settings, Voicemail, Clock API/SDK available to allow integration with 3 <sup>rd</sup> party door system products
<b>Operating System</b>	Linux 4.4
<b>HD Audio</b>	Yes, Dual speakers with support for wideband audio and media play in stereo, acoustic echo cancellation
<b>QoS</b>	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
<b>Security</b>	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
<b>Multi-language</b>	English, German, French, Spanish and Chinese.
<b>Upgrade/ Provisioning</b>	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file, manual upload
<b>Power &amp; Green Energy Efficiency</b>	2-pin DC input: 12VDC/1A Integrated PoE: IEEE 802.3af Class 3, power consumption <10W Micro USB input: 5VDC/2A
<b>Temperature and Humidity</b>	Operation: -10°C to 50°C, Storage: -20°C to 60°C, Humidity: 10% to 90% Non-condensing
<b>Package Contents</b>	GSC3570 Intercom Phone, quick installation guide, wall mount bracket, and desktop stand (optional)
<b>Compliance</b>	FCC, CE, RCM, IC



## GETTING STARTED

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

### Equipment Packaging

Table 3: Equipment Packaging

GSC3570
<ul style="list-style-type: none"> <li>• 1x GSC3570.</li> <li>• 1x Installation Bracket</li> <li>• 1x PH2.0-10P Alarm cable</li> <li>• 2x Self-tapping Screws</li> <li>• 6x Self-tapping Screw Anchors</li> <li>• 6x Self-tapping Screws</li> <li>• 1x Quick Installation Guide</li> </ul>

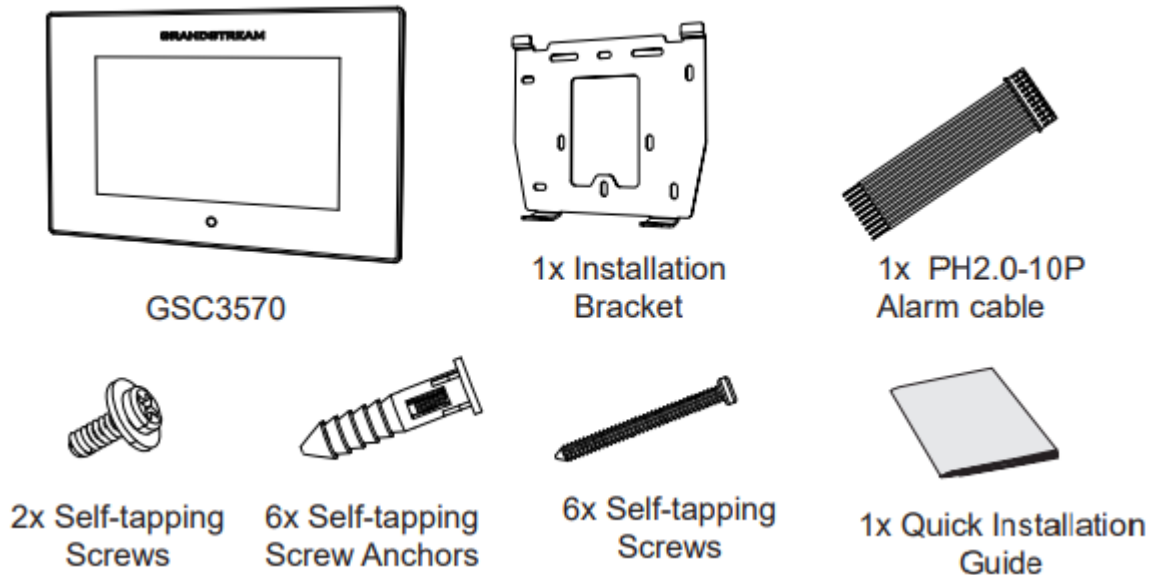


Figure 1: GSC3570 Package Content

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



## GSC3570 Wiring Connection

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

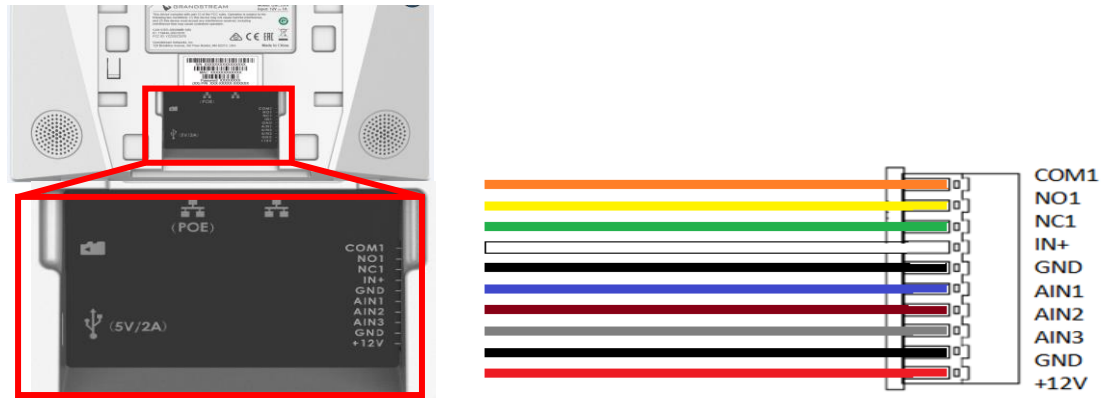


Figure 2: GSC3570 Wiring Connection

Table 4: 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	NCO1	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 Setup

The GSC3570 can be attached to the wall or in-wall using the slots for wall mounting.

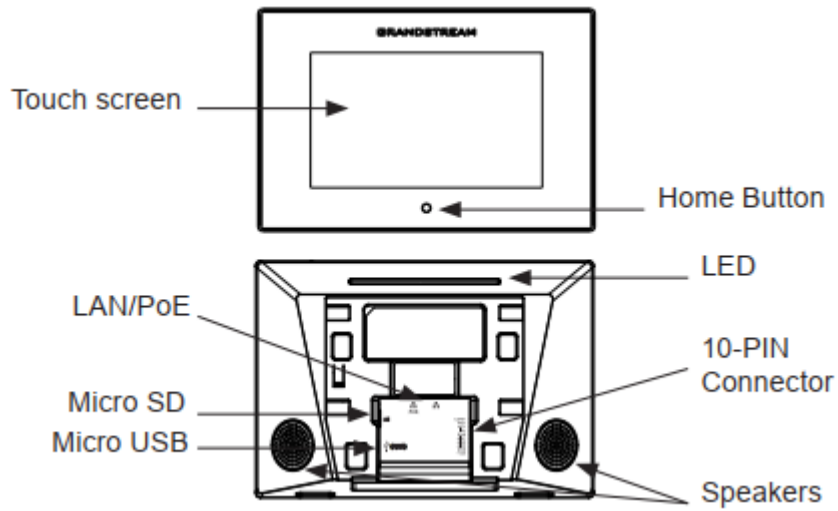


Figure 3: Built in Stand and Mounting Slots on The GSC3570.

## On-Wall Mounting

The GSC3570 can be mounted on the wall or on the desktop (desktop bracket is sold separately). Please refer to the following steps for 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.

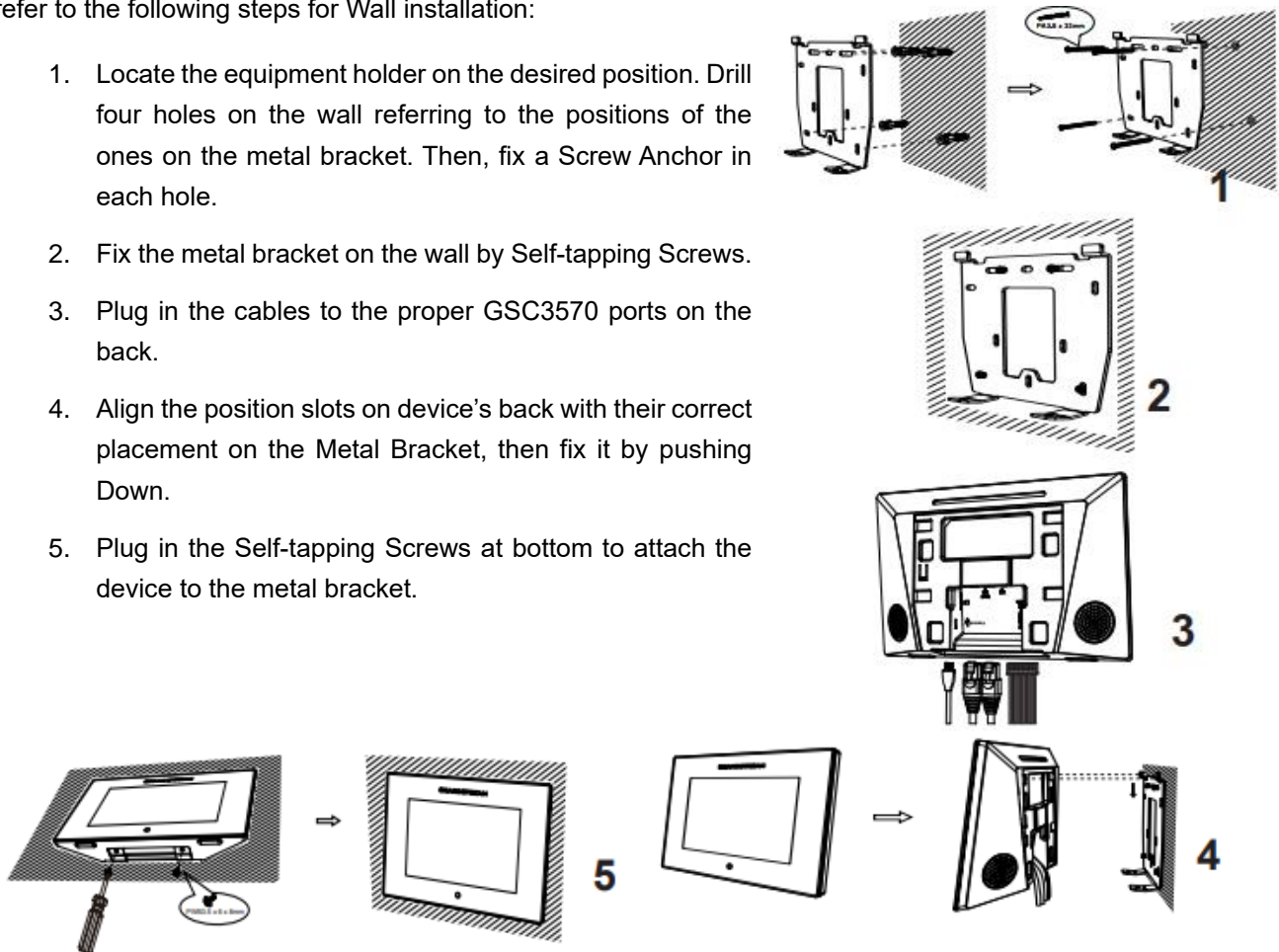


Figure 4: On-Wall Mounting

## 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.

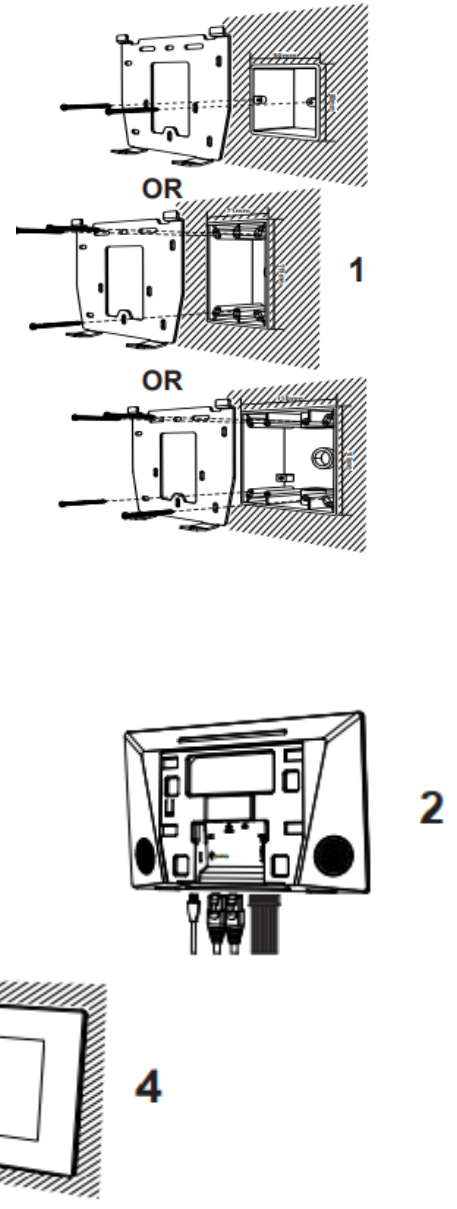


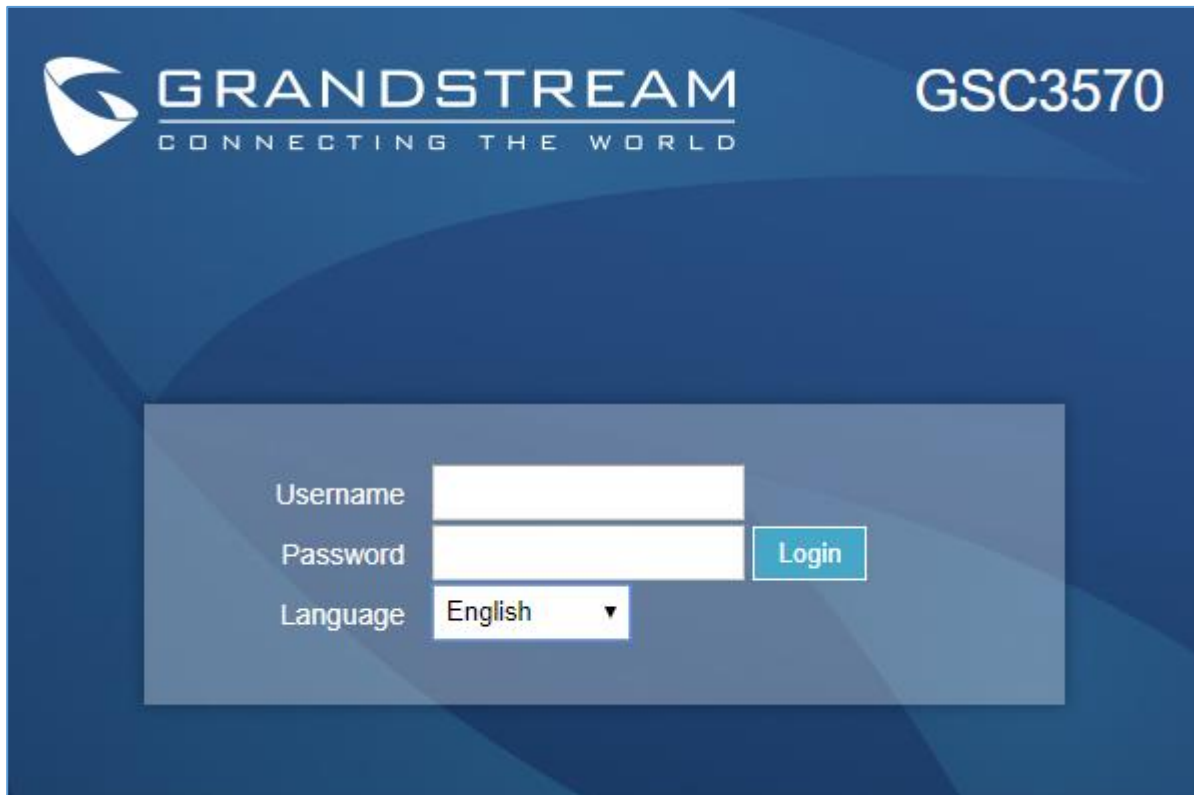
Figure 5: In-Wall Mounting

## Connecting the GSC3570

To setup 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 "Setting"
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 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.



**Figure 6: GSC3570 web interface**

To setup 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 "Setting". Browse the GSC3570 MENU for Status, Network information, Features and Basic/Advanced Settings...
3. Press "Home" Button to go back to Idle screen.

## Alarm IN/OUT

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

Alarm\_Out device could use 3<sup>rd</sup> party Siren and Strobe Light, or Electric Door Striker, etc.

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

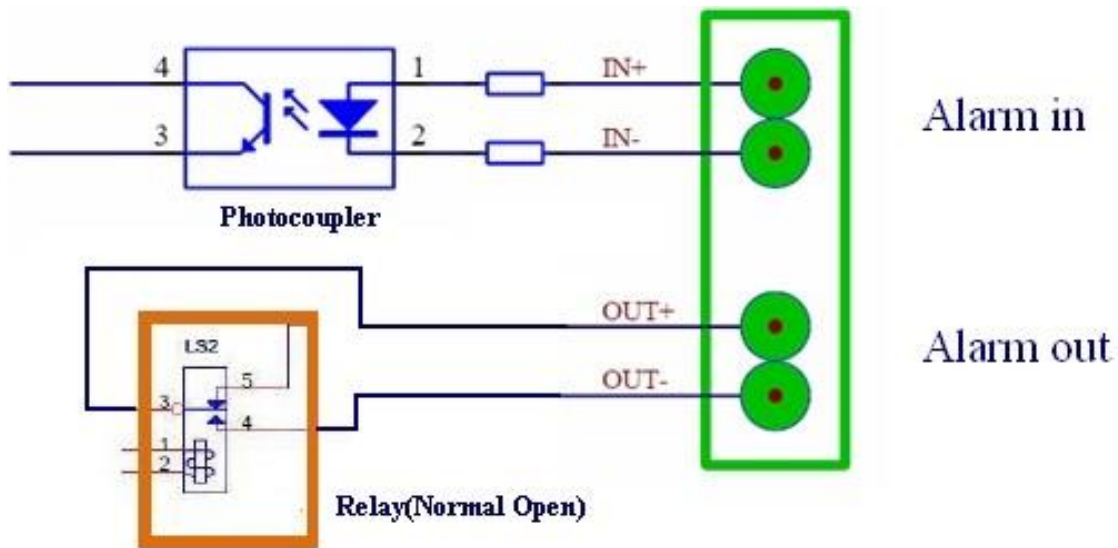


Figure 7: Alarm\_In/Out Circuit for GDS3710

### Notes:

- The Alarm\_In and Alarm\_Out circuit for the GSC3570 should meet the following requirement:

<b>Alarm Input</b>	9V<V <sub>in</sub> <15V, PINs (1.02KΩ)
<b>Alarm Output</b>	125VAC/0.5A, 30VDC/2A, Normal Open, PINs

- The Alarm\_In circuit, if there is any voltage change between 9V and 15V, as specified in the table above, the GSC3570 Alarm\_In port will detect it and trigger the action and event.
- Higher voltage and wrong polarity connection are prohibited because this will damage the devices.

## Connection Examples

### GSC3570 Connection & Wiring Diagrams - "Fail Secure" Electric Strike, POE Power Supply

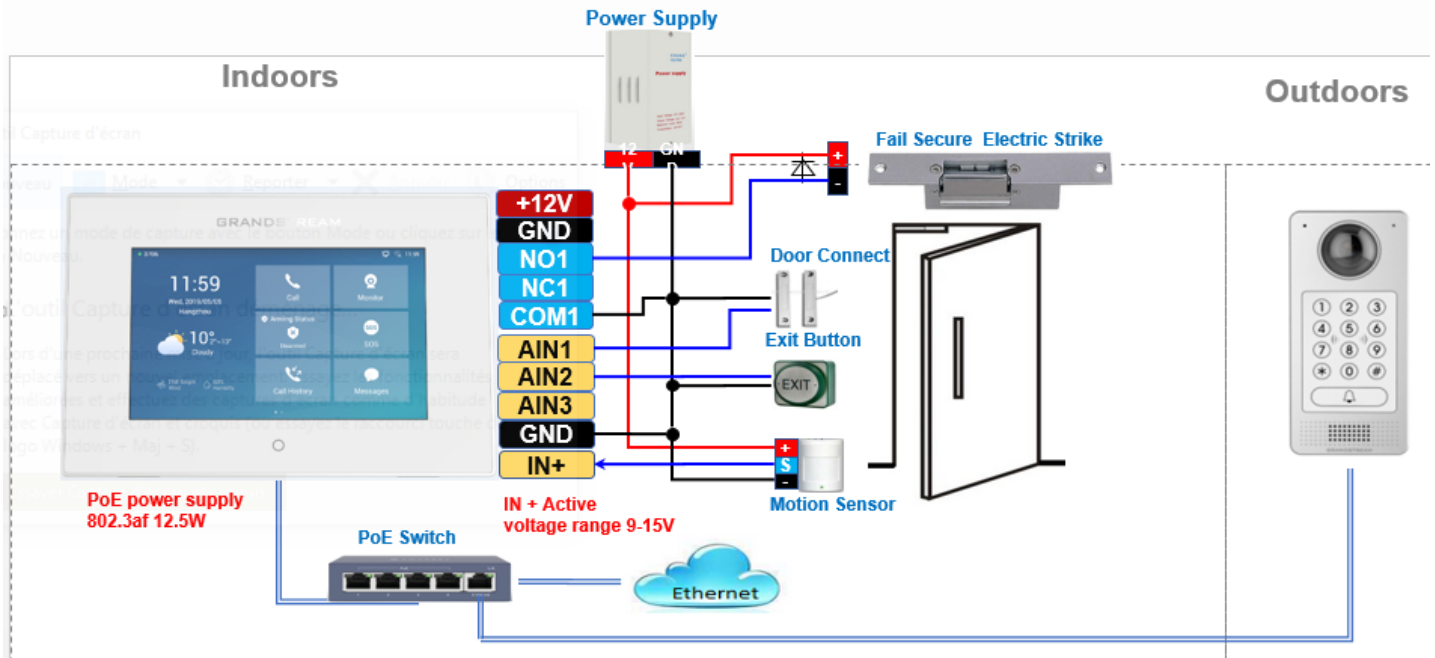


Figure 8: "Fail Secure" Electric Strike, POE Power Supply

### GSC3570 Connection & Wiring Diagrams - "Fail Safe" Electric lock, 3rd Party Power Supply

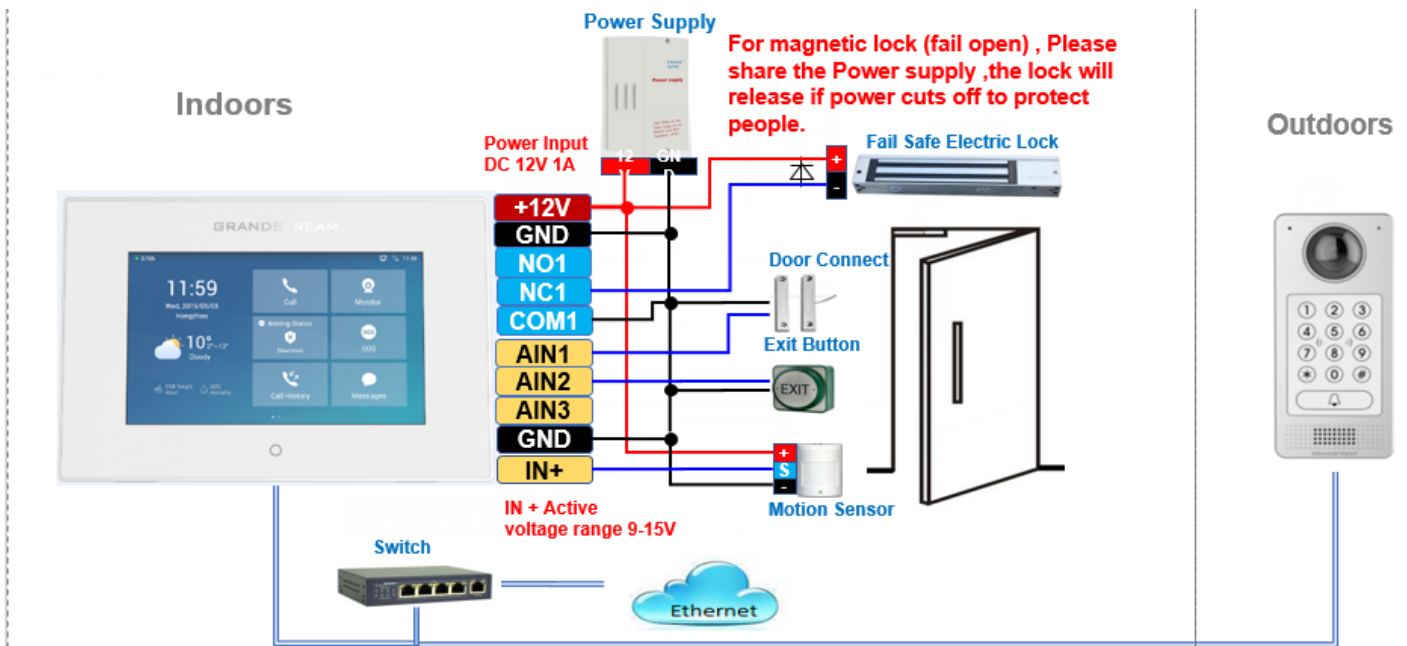


Figure 9: "Fail Safe" Electric lock, 3rd Party Power Supply





## GSC3570 Connection & Wiring Diagrams - "Fail Safe" Electric lock, Power Supply and Wi-Fi

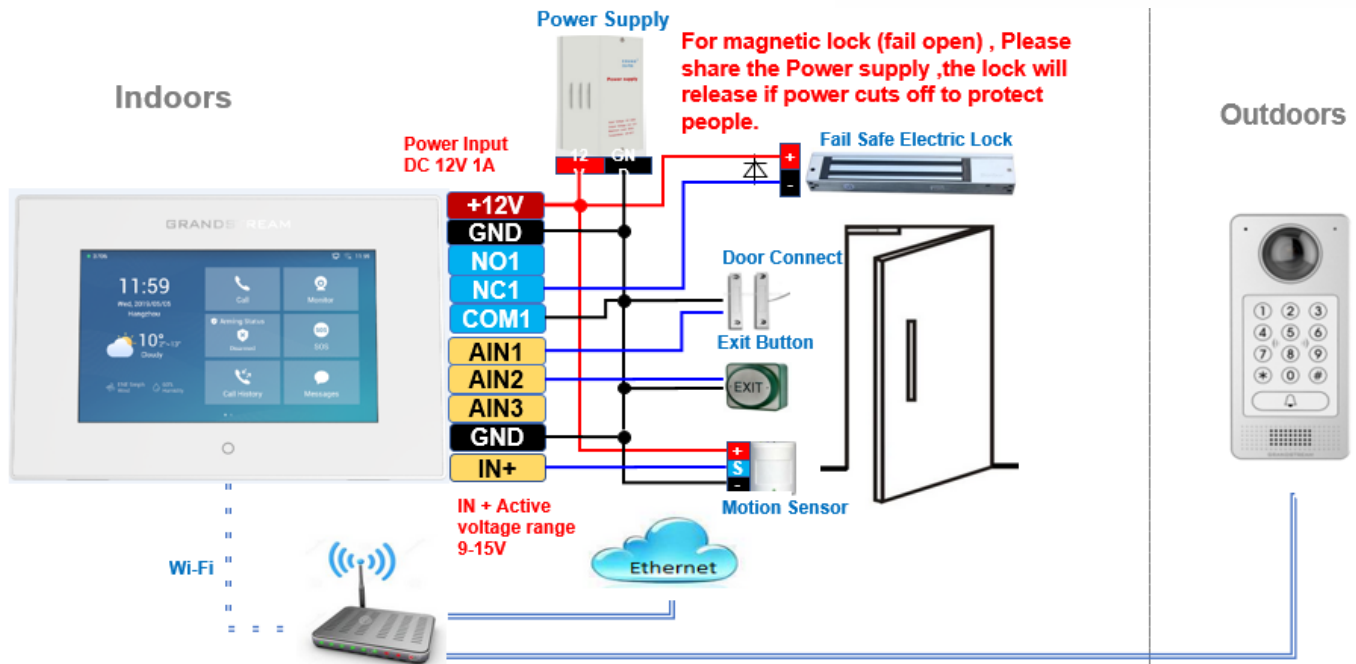


Figure 10: "Fail Safe" Electric lock, 3rd Party Power Supply, Wi-Fi

## Connecting GDS37xx with GSC3570

The GSC3570 can be configured with up to 10 GDS37xx devices allowing two doors remote control per GDS, the configuration is done as follow:

### Web interface configuration:

1. Access **Settings**→ **External Service**.
2. Select **Account** on which the remote door opening with softkey will be applied on.
3. Enter name of the GDS unit in **System Identification**. (not a mandatory field)
4. Set GDS SIP Number (or IP address in case of the peering scenario) on **System Number**.
5. Enter **Door 1 name**. (not a mandatory field)
6. Enter the **Remote PIN to Open Door 1** configured in the GDS in **Door 1 Access Password**.
7. Enter the **Remote PIN to Open Door 2** configured in the GDS in **Door 2 Access Password**.
8. Click on Save and Apply.



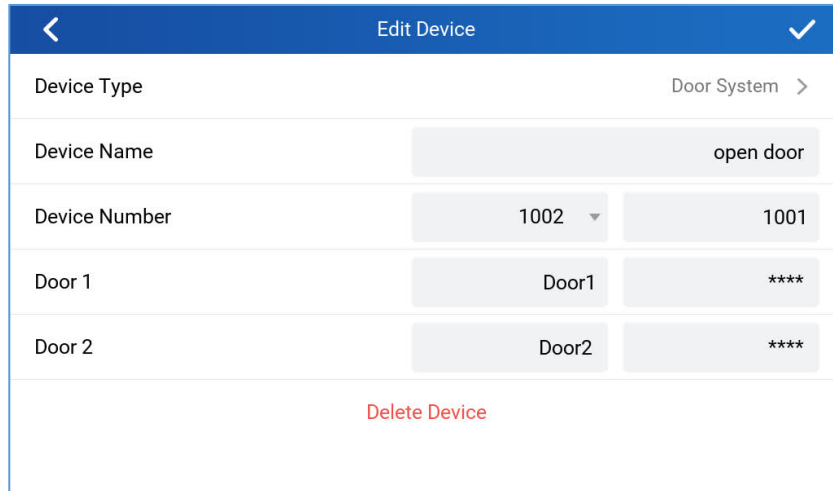


Order	Account	System Identification	System Number	Door 1 Name	Door 1 Access Password	Door 2 Name	Door 2 Access Password
1	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	Account 1 ▼	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Figure 11: External Service: Web Configuration

### LCD configuration:

1. Tap the menu button if GSC3570 is in 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 **Device Name** field.
5. Select the Account which will have the remote door opening feature and enter GDS SIP extension (or IP address in case of peering scenario) in **Device Number** field.
6. Enter the **Door Name** for Door 1 and **Remote PIN to Open Door 1** configured in the GDS in **Password** Field.
7. Enter the **Door Name** for Door 2 and **Remote PIN to Open Door 2** configured in the GDS in **Password** Field.



Edit Device	
Device Type	Door System >
Device Name	open door
Device Number	1002 1001
Door 1	Door1 ****
Door 2	Door2 ****
Delete Device	

Figure 12: External Service: LCD Configuration

## Connecting IP Camera with GSC3570

The GSC3750 can be configured with up to 32 IP Camera devices allowing two doors remote control per GDS, the configuration is done as follow:

### Web interface configuration:

1. Access **Settings**→ **IPC**.
2. Enter name of the IP Camera unit in **System Identification**. (not a mandatory field)
3. Select SIP protocol 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 outgoing call towards the IP Camera under **Account**.
6. Click on Save and Apply.

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 ▼

Figure 13: 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 **Device Name** field.
5. Select which Account to make outgoing call towards the IP Camera and enter the IP Camera's SIP extension (or IP address in case of peering scenario) in **Device Number** field.

<
Edit Device
>

Device Type IP Camera >

---

Device Name GXV3610

---

Device Number 1002 ▼ 1003

---

Delete Device

Figure 14: IPC: LCD Configuration

## Arming Mode

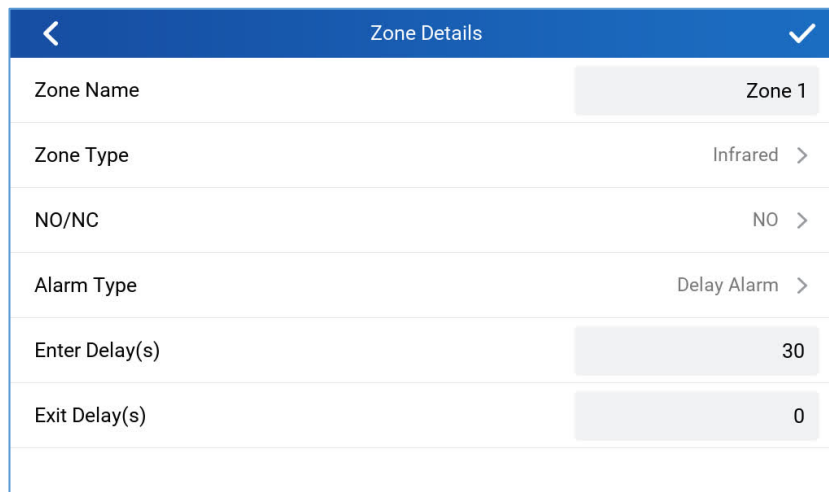
The GSC3750 can be connected to 1 Active Alarm IN and up to 3 Passive Alarm IN inputs. Each detector input is linked to a Zone that can be set with different Alarm Action (instant, delayed, 24h alarm).

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

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

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 24h 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

Figure 15: Features: Zone Settings

### Notes:

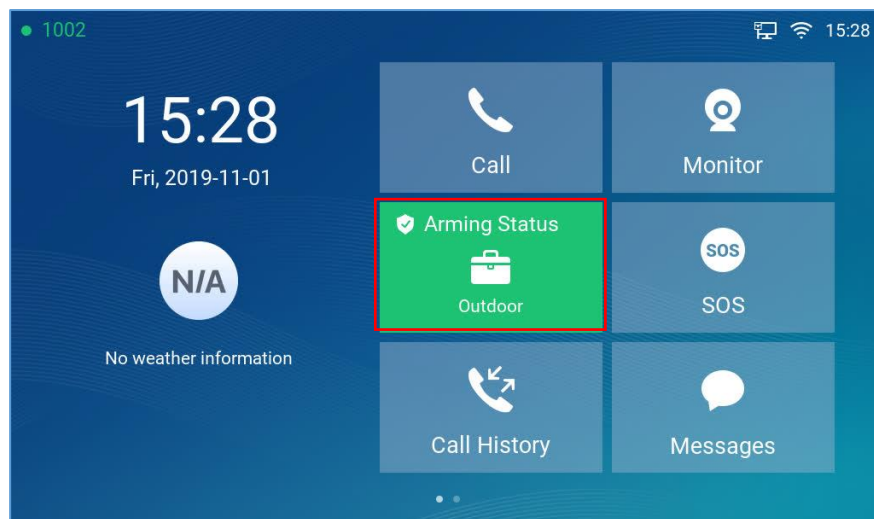
- Both the Entering/Exiting Delay duration got a range from 0s to 60s.
- The GSC3570 supports up to 4 zones.
- Once the Zone(s) is configured, proceed from **Features** → **Arming Mode**:  
 On each **Profile** (Outdoor, Indoor, Sleeping, Custom) User can enable the zones.



Arming Mode				
Outdoor	Zone Name	Zone Type	NO/NC	Alarm Type
Indoor	Zone 1	Infrared	NO	Delay Alarm 30s / 0s <input type="checkbox"/>
	Zone 2	Infrared	NO	Delay Alarm 30s / 0s <input type="checkbox"/>
Sleeping	Zone 3	Infrared	NO	Delay Alarm 30s / 0s <input type="checkbox"/>
Custom	Zone 4	Infrared	NO	Delay Alarm 30s / 0s <input type="checkbox"/>

**Figure 16: Features: Arming Mode**

- User can activate the arming profile from the LCD Menu as follow as a quick arming procedure by tapping Arming Status and scrolling the current Arming profiles:



**Figure 17: Features: Arming Status**

## Alarm & SOS Calling

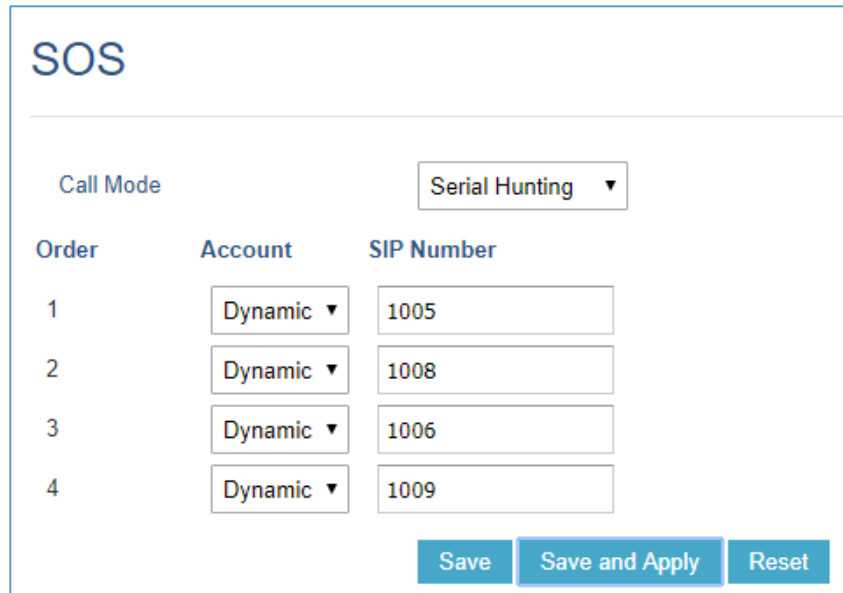
The GSC3750 can be configured with a SOS key as when this key is hold the GSC3570 will trigger will be ringing the extension(s) configured under SOS panel from either the web GUI or LCD Menu.

### 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 in the order from 1-4 after 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.



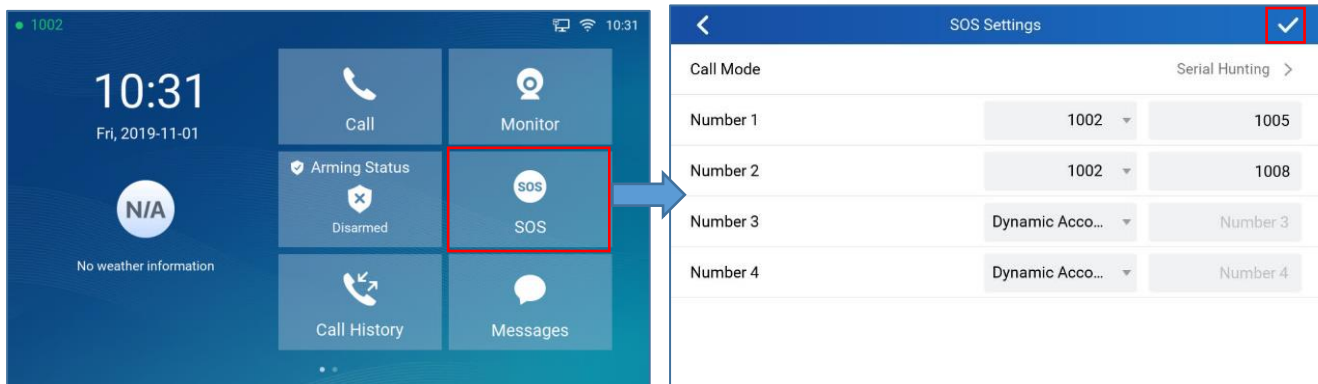
Order	Account	SIP Number
1	Dynamic ▼	1005
2	Dynamic ▼	1008
3	Dynamic ▼	1006
4	Dynamic ▼	1009

Figure 18: 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 in the order from 1-4 after 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 Save button.

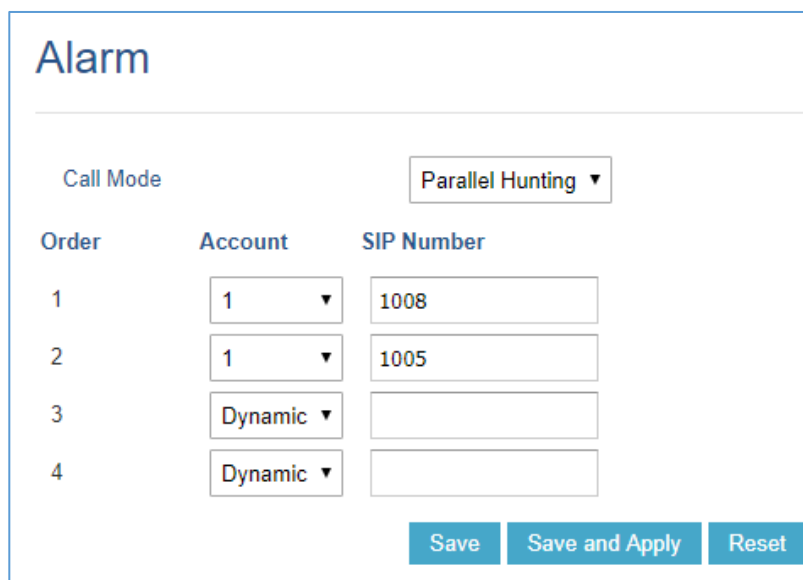
The GSC3570 can be set with trigger button to execute the Alarm output action and numbers configured on Alarm panel on either the web interface will be ringing as well.



**Figure 19: 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 in the order from 1-4 after 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.

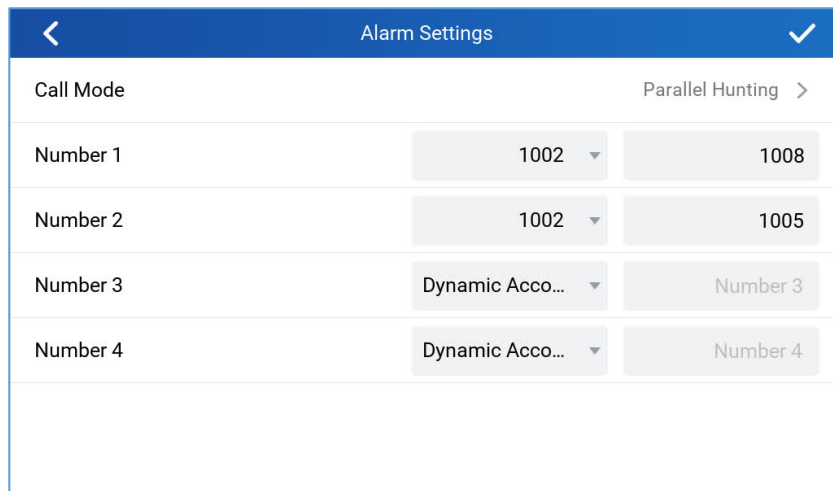


**Figure 20: Alarm: Web Configuration**



### LCD configuration:

1. Tap the menu button if GSC3570 is in 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 in the order from 1-4 after 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 Save icon.



Alarm Settings	
Call Mode	Parallel Hunting >
Number 1	1002 ▾ 1008
Number 2	1002 ▾ 1005
Number 3	Dynamic Acco... ▾ Number 3
Number 4	Dynamic Acco... ▾ Number 4

Figure 21: Alarm: LCD Configuration



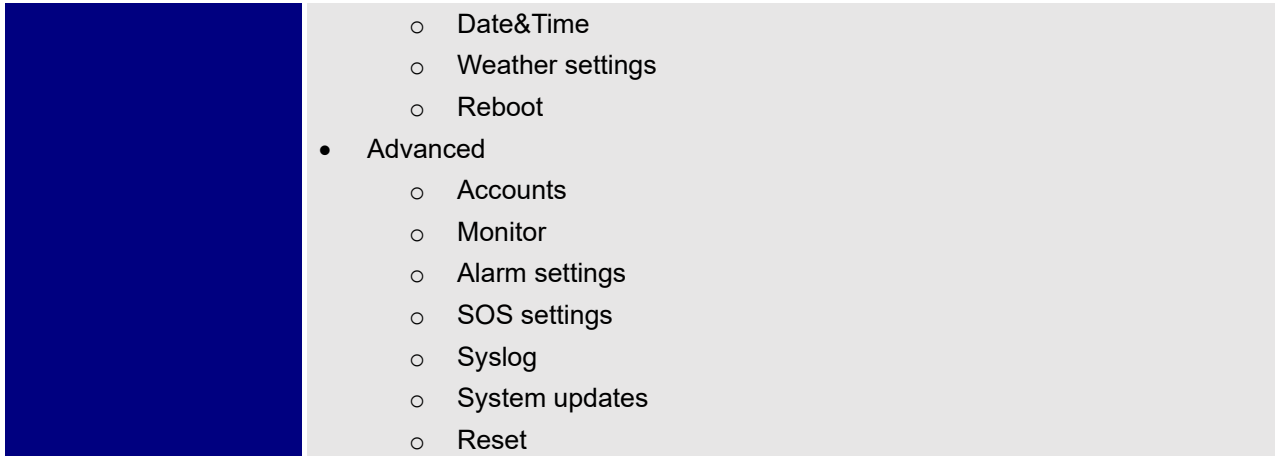
## GSC3570 LCD SETTINGS

The GSC3570 LCD MENU provides an 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.

**Table 5: GSC3570 LCD Menu**

<b>Call</b>	<ul style="list-style-type: none"> <li>• Audio/Video call</li> <li>• IP call</li> <li>• Paging</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Door System</li> <li>• IP Camera</li> </ul>
<b>Arming Status</b>	<ul style="list-style-type: none"> <li>• Arming Mode</li> </ul>
<b>SOS</b>	<ul style="list-style-type: none"> <li>• Call Mode</li> <li>• Numbers (1-4) to be called</li> </ul>
<b>Call History</b>	<ul style="list-style-type: none"> <li>• All</li> <li>• Missed</li> <li>• Outgoing</li> <li>• Incoming</li> </ul>
<b>Message</b>	<ul style="list-style-type: none"> <li>• Voice Mail</li> <li>• Alarm</li> </ul>
<b>Contacts</b>	<ul style="list-style-type: none"> <li>• Favorite</li> <li>• Local</li> <li>• Group</li> <li>• LDAP</li> </ul>
<b>Setting</b>	<ul style="list-style-type: none"> <li>• Status               <ul style="list-style-type: none"> <li>○ Account Status</li> <li>○ Network Status</li> <li>○ System Info</li> </ul> </li> <li>• Network               <ul style="list-style-type: none"> <li>○ Ethernet Settings</li> <li>○ Wi-Fi</li> </ul> </li> <li>• Features               <ul style="list-style-type: none"> <li>○ Auto answer</li> <li>○ DND</li> <li>○ Arming Mode</li> <li>○ Zone settings</li> </ul> </li> <li>• Basic               <ul style="list-style-type: none"> <li>○ Sound</li> <li>○ Display</li> <li>○ Language</li> </ul> </li> </ul>





## Access LCD Settings

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



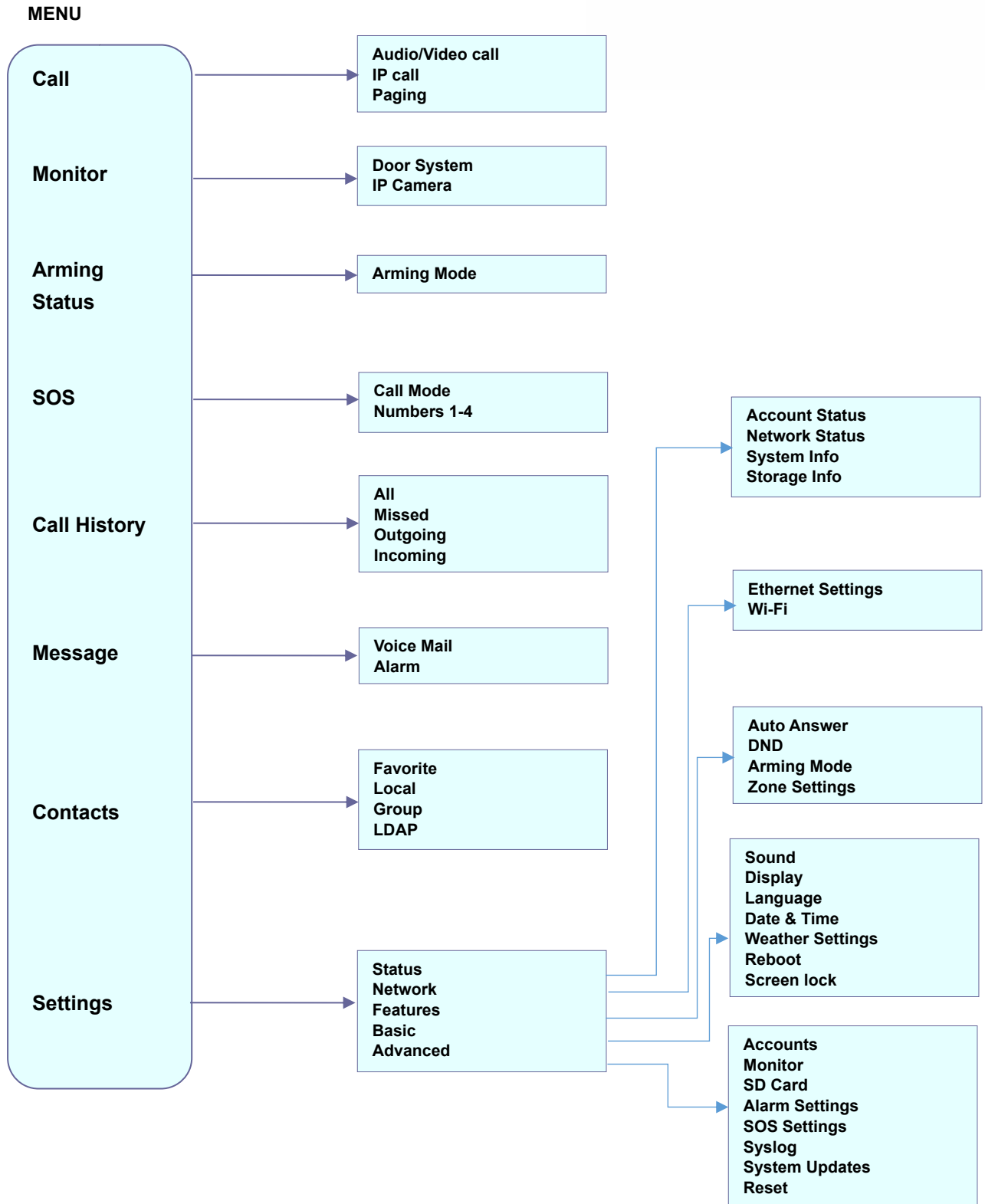
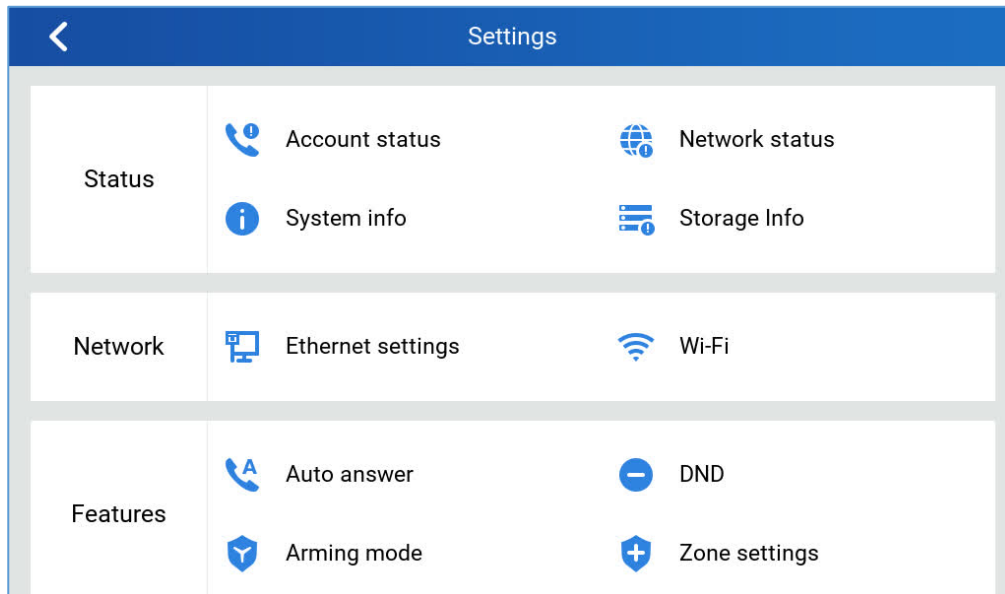


Figure 22: MENU Configuration

To open the settings menu, you should:

- Tap on  **Settings** app on the screen.



**Figure 23: GSC3570 System Settings**

## Status

### Account Status

This page displays all available accounts on the phone with 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

### 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 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, roll to the end of the Wi-Fi list and select "Add Network". Then Enter SSID, Security type, password and set up address type (DHCP/Static IP) in the prompt dialog. The phone will reboot with Wi-Fi network connected.

## 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
  - ❖ Drmagnet (door lock)
  - ❖ Urgency
  - ❖ Others
- **NO/NC:** Match the alarm type:
  - ❖ **NO:** Normally Open device
  - ❖ **NC:** Normally Close device
- **Alarm Type:** Select the **Type** of the Alarm **arming**:
  - ❖ **Delay Alarm:** Enter the **Enter Delay/Exit Delay** (Duration between 0-60 seconds)
  - ❖ **Instant Alarm:** Alarm is armed instantly when triggered.
  - ❖ **24h Alarm:** Alarm is always armed when triggered.

## 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 ringing volume
- **Ringtone:** Select phone's ringtone for incoming call.



- **Door Ringtone:** Select the Door ringtone when 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.
- **Enable back LED indicator:** Enable/disable the back LED indicator.

## Language

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

## Date & Time

- **NTP server:** Assign the URL or IP Address of 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. 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.

## Weather Settings

- **City:** Select either **Auto** which is based on the location detected or **Self-Defined City:**
  - ❖ Self-Defined City: Enter the city name manually.



- **Temperature Settings:** Set to either **Auto** or Manually to either °C or °F.
- **Automatic Update:** Enable the weather update feature.
- **Update Interval:** Configure the weather update interval in minutes. Default is 15 minutes.

## Reboot

- Reboot the GSC3570.

## Screen Lock

- Enable/Disable screen lock and define the 6-digits password.

## Advanced

### Accounts

Set up to 4 SIP accounts. Account Settings page allows to configure SIP settings for each account. Tap on Account# to access the settings, when configured press ✓ sign (on the top right corner) to confirm the changes or press back button to cancel them. Users can press Empty configuration on the bottom of the page to clear all the settings. Following settings can be configured for each account. Refer to [Account/General Settings] for 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 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 Call to GDS37xx.
  - ❖ **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 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 Call to 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 configured from which account to make calls when 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.

## SOS Settings

- Select the Call Mode and configured from which account to make calls when 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 initiate 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. 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 network connection, the phone will send the syslog packets to this server address.
- **System log keyword filtering:** Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to "SIP" to filter SIP log.



## System Update

- Configure the Firmware server path and protocol. Click on Update Now button to start 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's IE.

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.

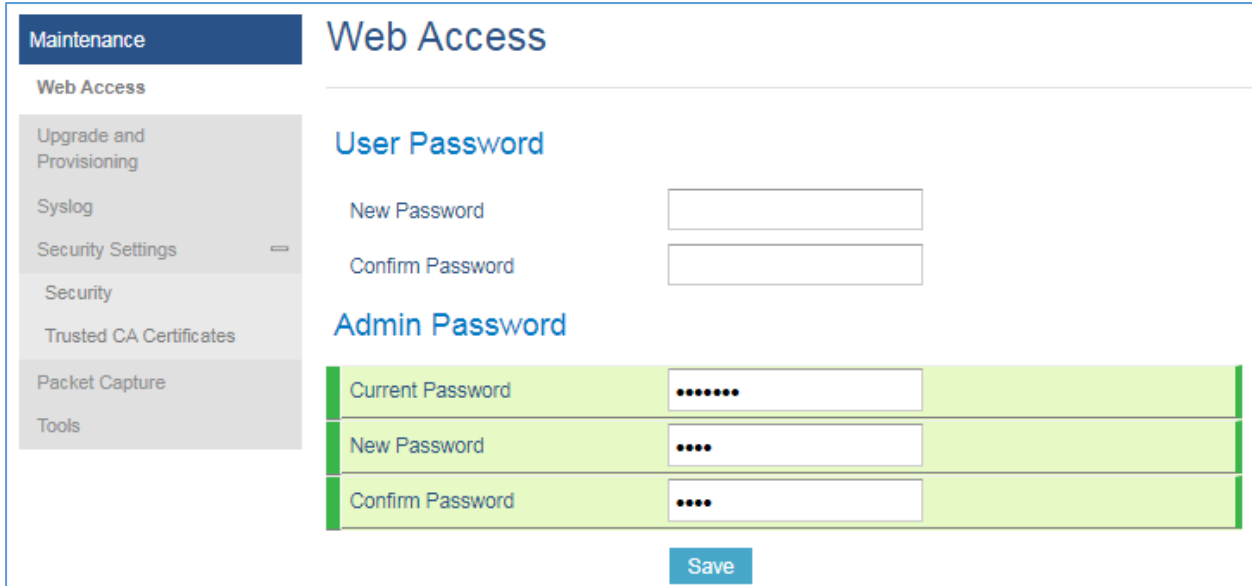
### Notes:

- 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 connected to. In 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 **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 IP address 192.168.40.154, please enter "http://192.168.40.154" in the address bar of the browser.
- There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed
End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	Random Password	Browse all pages

- When accessing the GSC3570, 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 strong password including letters, digits and special characters is recommended for better security.





**Figure 24: Change Password**

- When changing any settings, always SUBMIT them by pressing the “Save” or “Save and Apply” button on the bottom of the page. If the change is saved only but not applied, after making all the changes, click on the “APPLY” button on 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 “Accounts” page and “Phonebook” page do not require reboot. Most of the options under “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, ring tone, 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

Table 6: Status Page Definitions

Status → Account Status	
<b>Account</b>	Account index. For GSC3570: up to 4 SIP accounts
<b>SIP User ID</b>	Displays the configured SIP User ID for the account.
<b>SIP Server</b>	Displays the configured SIP Server address, URL or IP address, and port of the SIP server.
<b>SIP Registration</b>	Displays SIP registration status for the SIP account, it will display Yes/No with Green/Red background.
Status → Network Status	
<b>MAC Address</b>	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.
<b>IP Setting</b>	The configured address type: DHCP, Static IP.
<b>IPv4 Address</b>	The IPv4 address obtained on the GSC3570.
<b>IPv6 Address</b>	The IPv6 address obtained on the GSC3570.
<b>OpenVPN IP</b>	The OpenVPN IP obtained on the GSC3570.
<b>Subnet Mask</b>	The subnet mask obtained on the GSC3570.
<b>Gateway</b>	The gateway address obtained on the GSC3570.
<b>DNS Server 1</b>	The DNS server address 1 obtained on the GSC3570.
<b>DNS Server 2</b>	The DNS server address 2 obtained on the GSC3570.
<b>PPPoE Link Up</b>	PPPoE Link status
<b>NAT Type</b>	Displays the configured NAT type
<b>NAT Traversal</b>	Display the status of NAT connection for each account on the GSC3570.
Status → System Info	
<b>Product Model</b>	Product model of the GSC3570.
<b>Part Number</b>	Product part number.
<b>Software Version</b>	<ul style="list-style-type: none"> <li>• <b>Boot:</b> boot version number.</li> <li>• <b>Core:</b> core version number.</li> <li>• <b>Base:</b> base version number.</li> <li>• <b>Prog:</b> program version number. This is the main firmware release number, which is always used for identifying the software system of the GSC3570.</li> </ul>



	<ul style="list-style-type: none"> <li>• <b>Locale:</b> locale version number.</li> <li>• <b>Recovery:</b> recovery version number.</li> </ul>
<b>IP Geographic Information</b>	<ul style="list-style-type: none"> <li>• <b>City:</b> displaying GSC3570 location.</li> <li>• <b>Language:</b> displaying language.</li> <li>• <b>Time Zone:</b> displaying time zone.</li> <li>• <b>Country Code:</b> displaying the country code;</li> </ul>
<b>Special Feature</b>	<ul style="list-style-type: none"> <li>• <b>OpenVPN® Support</b></li> </ul>
<b>System Time</b>	<ul style="list-style-type: none"> <li>• <b>System Up Time:</b> System up time since the last reboot.</li> <li>• <b>System Time:</b> Current system time on the GSC3570 system.</li> </ul>
<b>Service Status</b>	GUI and Phone service status.
<b>System Information</b>	Download system information
<b>User Space</b>	Shows the percentage of the user space used and the status of the Database
<b>Core Dump</b>	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

Table 7: Account Page Definitions

Account x → General Settings	
<b>Account Active</b>	This field indicates whether the account is active. The default setting is “Yes”.
<b>Account Name</b>	The name associated with each account to be displayed on the LCD.
<b>SIP Server</b>	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (ITSP).
<b>Secondary SIP Server</b>	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).
<b>Outbound Proxy</b>	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.
<b>Backup Outbound Proxy</b>	IP address or Domain name of the Secondary Outbound Proxy which will be used when the primary proxy cannot be connected.



<b>SIP User ID</b>	<p>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.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>• 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)</li> <li>• The server domain will not be included in the SIP from header.</li> </ul>
<b>Authenticate ID</b>	<p>SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.</p>
<b>Authenticate Password</b>	<p>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.</p>
<b>Name</b>	<p>The SIP server subscriber's name (optional) that will be used for Caller ID display.</p>
<b>Voice Mail Access Number</b>	<p>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.</p>
<b>Account x → Dial Plan</b>	
<b>Name</b>	<p>Enter the name for the configured rules.</p>
<b>Rule</b>	<p>Enter the rule settings (number pattern, prefix to add ...etc.).</p>
<b>Type</b>	<p>Choose the type of the rule:</p> <ul style="list-style-type: none"> <li>• Pattern</li> <li>• Block</li> <li>• Dial now</li> <li>• Prefix</li> <li>• Second tone</li> </ul>
<b>Account x → Network Settings</b>	
<b>DNS Mode</b>	<p>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".</p> <p>If the user wishes to locate the server by DNS SRV, the user may select "SRV" or "NATPTR/SRV".</p> <p>If "Use Configured IP" is selected, please fill in the three fields below:</p>



	<ul style="list-style-type: none"> <li>• <b>Primary IP:</b></li> <li>• <b>Backup IP 1.</b></li> <li>• <b>Backup IP 2.</b></li> </ul> <p>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.</p> <p>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.</p> <p>If SIP server is already an IP address, GSC3570 will use it directly even “User Configured IP” is selected.</p>
<b>Primary IP</b>	Configures the primary IP address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>Backup IP1</b>	Configures the backup IP1 address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>Backup IP2</b>	Configures the backup IP2 address where the GSC3570 sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>NAT Traversal</b>	<p>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.</p> <p>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&amp;SDP messages.</p> <p>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.</p>
<b>Proxy-Require</b>	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.
<b>Account x → SIP Settings → Basic Settings</b>	
<b>TEL URI</b>	<p>If the GSC3570 has an assigned PSTN phone number, this field should be set to “user=phone”.</p> <p>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.</p>





	If set to "Enabled", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable".
<b>SIP Registration</b>	Selects whether the GSC3570 will send SIP Register messages to the proxy/server. The default setting is "Yes".
<b>Unregister on Reboot</b>	<p>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".</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• If set to "Instance", the SIP user will be unregistered on current GSC3570 only.</li> <li>• If set to "No", the GSC3570 will not unregister the SIP account when rebooting.</li> </ul>
<b>Register Expiration</b>	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).
<b>Subscribe Expiration</b>	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.
<b>Reregister Before Expiration</b>	Specifies the time frequency (in seconds) that the GSC3570 sends re-registration request before the Register Expiration. The default value is 0.
<b>Enable OPTIONS Keep Alive</b>	Enable OPTIONS Keep Alive to check SIP Server.
<b>OPTIONS Keep Alive Interval</b>	Time interval for OPTIONS Keep Alive feature in Second.
<b>OPTIONS Keep Alive Max Lost</b>	Number of max lost packets for OPTIONS Keep Alive feature before the GSC3570 re-registration.
<b>Local SIP Port</b>	<p>Defines the local SIP port used to listen and transmit.</p> <p>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.</p>



<b>SIP Registration Failure Retry Wait Time</b>	<p>Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600.</p> <p>The default value is 20 seconds.</p>
<b>SIP T1 Timeout</b>	<p>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.</p>
<b>SIP T2 Timeout</b>	<p>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.</p>
<b>SIP Transport</b>	<p>Determines the network protocol used for the SIP transport. Users can choose from TCP, UDP and TLS. The default setting is “UDP”.</p>
<b>SIP URI Scheme when using TLS</b>	<p>Specifies if “sip” or “sips” will be used when TLS/TCP is selected for SIP Transport. The default setting is “sips”.</p>
<b>Use Actual Ephemeral Port in Contact with TCP/TLS</b>	<p>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”.</p>
<b>Outbound Proxy Mode</b>	<p>The Outbound proxy mode is placed in the route header when sending SIP messages, or they can be always sent to outbound proxy.</p>
<b>Support SIP Instance ID</b>	<p>Defines whether SIP Instance ID is supported or not.</p> <p>Default setting is “Yes”.</p>
<b>SUBSCRIBE for MWI</b>	<p>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”.</p>
<b>SUBSCRIBE for Registration</b>	<p>When set to “Yes”, a SUBSCRIBE for Registration will be sent out periodically. The default setting is “No”.</p>
<b>Enable 100rel</b>	<p>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”.</p>
<b>Callee ID Display</b>	<p>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”.</p>



	When set to “To Header”, caller ID will not be updated and displayed as To Header.
<b>Caller ID Display</b>	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”.
<b>Add Auth Header on Initial REGISTER</b>	To define whether authorization Header will be added on initial REGISTER from the first REGISTER. The default setting is “No”.
<b>Allow SIP Reset</b>	This is used to perform a factory reset through SIP NOTIFY. When the GSC3570 receives the NOTIFY with <b>event:reset</b> , the GSC3570 should perform a factory reset after the authentication. The default setting is “No”.
<b>Ignore Alert-Info header</b>	This option is used to configure default ringtone. If set to “Yes”, configured default ringtone will be played. The default setting is “No”.
<b>Account x → SIP Settings → Custom SIP Headers</b>	
<b>Use Privacy Header</b>	Controls whether the Privacy header will present in the SIP INVITE message or not, whether the header contains the caller info. When set to “Default”, the Privacy Header will show in INVITE only when “Huawei IMS” special feature is on. 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”.
<b>Use P-Preferred-Identity Header</b>	Controls whether the P-Preferred-Identity Header will present in the SIP INVITE message. The default setting is “default”: The P-Preferred-Identity Header will show in INVITE unless “Huawei IMS” special feature is on. 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.
<b>Use X-Grandstream-PBX Header</b>	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”.
<b>Use P-Access-Network-Info Header</b>	Enables / disables the use of P-Access-Network-Info header in SIP request. When disabled, the SIP message sent from the GSC3570 will not include the selected header. Default setting is “Yes”.
<b>Use P-Emergency-Info Header</b>	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”.



<b>Use MAC Header</b>	<p>If <b>Yes except REGISTER</b>, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header;</p> <p>If <b>Yes to all SIP</b>, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP message including REGISTER will attach the MAC address to the User-Agent header;</p> <p>If <b>No</b>, neither will the MAC header be included in the register or unregister message nor the MAC address be attached to the User-Agent header for any outgoing SIP message.</p> <p>The default setting is “No”.</p>
<b>Account x → SIP Settings → Advanced Features</b>	
<b>Music on Hold URI</b>	Configures Music on Hold URI to call when a call is on hold. This feature must be supported on the server side.
<b>Omit charset=UTF-8 in MESSAGE</b>	Omit charset=UTF-8 in MESSAGE content-type
<b>Allow Unsolicited REFER</b>	Allow Unsolicited REFER to accomplish an outgoing call.
<b>Special Feature</b>	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, Sylanro, Huawei IMS, PhonePower and UCM Call center depending on the server type. The default setting is “Standard”.
<b>Session Timer</b>	
<b>Enable Session Timer</b>	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”.
<b>Session Expiration</b>	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.



<b>Min-SE</b>	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
<b>Caller Request Timer</b>	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”.
<b>Callee Request Timer</b>	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”.
<b>Force Timer</b>	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”.
<b>UAC Specify Refresher</b>	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”.
<b>UAS Specify Refresher</b>	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”.
<b>Force INVITE</b>	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

<b>Check Domain Certificates</b>	Choose whether the domain certificates will be checked or not when TLS/TCP is used for SIP Transport. The default setting is “No”.
<b>Validate Certificate Chain</b>	Validate certification chain when TCP/TLS is configured. Default setting is “No”.
<b>Validate Incoming Messages</b>	Choose whether the incoming messages will be validated or not. The default setting is “No”.
<b>Check SIP User ID for Incoming INVITE</b>	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”.



<b>Accept Incoming SIP from Proxy Only</b>	When set to “ <b>Yes</b> ”, 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 “ <b>No</b> ”.
<b>Authenticate Incoming INVITE</b>	If set to “ <b>Yes</b> ”, the GSC3570 will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. Default setting is “ <b>No</b> ”.
<b>Account x → Codec Settings</b>	
<b>Audio Settings</b>	
<b>Preferred Vocoder</b>	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.
<b>Use First Matching Vocoder in 200OK SDP</b>	When it is set to “ <b>Yes</b> ”, the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is “ <b>No</b> ”.
<b>Codec Negotiation Priority</b>	Configures the GSC3570 to use which codec sequence to negotiate as the callee. When set to “ <b>Caller</b> ”, the GSC3570 negotiates by SDP codec sequence from received SIP Invite. When set to “ <b>Callee</b> ”, the GSC3570 negotiates by audio codec sequence on the GSC3570. Default is “ <b>Callee</b> ”.
<b>Disable Multiple m line in SDP</b>	When it is set to “ <b>No</b> ”, the device will reply with multiple m lines; Otherwise, it will reply 1 m line. The default setting is “ <b>No</b> ”.
<b>SRTP Mode</b>	Enable SRTP mode based on your selection from the drop-down menu. The default setting is “ <b>Disabled</b> ”.
<b>SRTP Key Length</b>	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
<b>Crypto Lifetime</b>	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 “ <b>Yes</b> ”.
<b>Symmetric RTP</b>	Defines whether symmetric RTP is supported or not. Default setting is “ <b>No</b> ”.
<b>Silence Suppression</b>	Controls the silence suppression/VAD feature of the audio codecs except for G.723 (pending) and G.729. If set to “ <b>Yes</b> ”, a small quantity of RTP packets containing comfort noise will be sent during the periods of silence. If set to “ <b>No</b> ”, this feature is disabled. Default setting is “ <b>No</b> ”
<b>Jitter Buffer Type</b>	Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is “ <b>Adaptive</b> ”.
<b>Jitter Buffer Length</b>	Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is “ <b>300ms</b> ”.



<b>Voice Frames Per TX</b>	Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the “ptime” value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is 2.
<b>G723 Rate</b>	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”.
<b>iLBC Frame Size</b>	This option determines the iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is “30ms”.
<b>iLBC Payload Type</b>	This option is used to specify iLBC payload type. Valid range is 96 to 127. The default setting is “97”.
<b>OPUS Payload Type</b>	Specifies OPUS payload type. Valid range is 96 to 127. Cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
<b>DTMF Payload Type</b>	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
<b>Send DTMF</b>	This parameter specifies the mechanism to transmit DTMF digits. There are 3 supported modes: <ul style="list-style-type: none"> <li>• <b>In audio:</b> DTMF is combined in the audio signal (not reliable with low-bit-rate codecs).</li> <li>• <b>RFC2833</b> sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.</li> <li>• <b>SIP INFO</b> uses SIP INFO to carry DTMF.</li> </ul> Default setting is “RFC2833”.
<b>DTMF Delay</b>	Configures the delay between sending DTMF (in milliseconds). Default is 250 ms.
<b>Video Settings</b>	
<b>H.264 Image Size</b>	Sets the H.264 image size. It can be selected from the dropdown list. <ul style="list-style-type: none"> <li>• <b>720P</b></li> <li>• <b>4CIF</b></li> <li>• <b>VGA</b></li> <li>• <b>CIF</b></li> <li>• <b>QVGA</b></li> </ul>





	<ul style="list-style-type: none"> <li>• <b>QCIF</b></li> </ul> <p><b>Note:</b> 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.</p> <p>The default setting is 720P.</p>
<b>H.264 Profile Type</b>	<p>Selects the H.264 profile type from the dropdown list.</p> <ul style="list-style-type: none"> <li>• <b>Baseline Profile</b></li> <li>• <b>Main Profile</b></li> <li>• <b>High Profile</b></li> <li>• <b>BP/MP/HP</b> (Default Setting)</li> </ul> <p><b>Note:</b> 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”.</p> <p>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.</p>
<b>Video Bit Rate</b>	<p>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.</p> <p><b>Note:</b> 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.</p> <p>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.</p>
<b>H264 Payload Type</b>	<p>Specifies the H.264 codec message payload type format. The default setting is 99. The valid range is from 96 to 127.</p>
<b>Account x → Call Settings</b>	
<b>Send Anonymous</b>	<p>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”.</p>





<b>Anonymous Call Rejection</b>	If set to “Yes”, anonymous calls will be rejected. The default setting is “No”.
<b>Auto Answer</b>	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”.
<b>Disable Call Waiting</b>	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

<b>Allow Auto Answer by Call-Info/Alert-Info</b>	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”.
<b>Mute on answer Intercom call</b>	When enabled, the GSC3570 will mute the incoming intercom call.
<b>Custom Alert-Info for Auto Answer</b>	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

<b>Swap Account Settings</b>	Allows users to swap the two accounts that they have configured. This will increase the flexibility of account management. <b>Note:</b> Make sure to press “Start” to complete the process.
------------------------------	--

## Settings Page Definitions

Table 8: Settings Page Definitions

Settings → General Settings	
<b>Local RTP Port</b>	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 <code>_value</code> for RTP; channel 1 will use <code>port_value+2</code> for RTP. Local RTP port ranges from 1024 to 65400 and must be even. Default value is 5004.
<b>Local RTP Port Range</b>	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.



<b>Use Random Port</b>	<p>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”</p> <p><b>Note:</b> This parameter must be set to “No” for Direct IP Calling to work.</p>
<b>Keep-alive Interval</b>	<p>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.</p>
<b>Use NAT IP</b>	<p>The NAT IP address used in SIP/SDP messages. This field is blank at the default settings. It should ONLY be used if it is required by your ITSP.</p>
<b>STUN Server</b>	<p>The IP address or Domain name of the STUN server.</p> <p>STUN resolution results are displayed in the STATUS page of the Web GUI.</p> <p>Only non-symmetric NAT routers work with STUN.</p>
<b>Test Password Strength</b>	<p>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:</p> <ol style="list-style-type: none"> <li>1) Numeric (0-9)</li> <li>2) Capital letters (A-Z)</li> <li>3) Lower case (a-z)</li> <li>4) Special characters (!, @, #, \$, %, ^, &amp;, *, (, ), etc.)</li> </ol> <p>Default setting is “No”.</p>
<b>Settings → External Service</b>	
<b>Order</b>	<p>Displays the order of the service.</p>
<b>Account</b>	<p>Specifies the account on which the service will be applied.</p>
<b>System Identification</b>	<p>Specifies the name to identify the service.</p>
<b>System Number</b>	<p>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.</p>
<b>Door 1 Name</b>	<p>Specifies the name of door 1.</p>
<b>Door 1 Access Password</b>	<p>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.</p>
<b>Door 2 Name</b>	<p>Specifies the name of door 2.</p>
<b>Door 2 Access Password</b>	<p>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.</p>



**Settings → Alarm**

<b>Call Mode</b>	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.
<b>Order (1-4)</b>	Displays the order of the service.
<b>Account</b>	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.
<b>SIP Number</b>	Enter the Number to receive the call. User can set up to 4 SIP Numbers.

**Settings → SOS**

<b>Call Mode</b>	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.
<b>Order (1-4)</b>	Displays the order of the service.
<b>Account</b>	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.
<b>SIP Number</b>	Enter the Number to receive the call. User can set up to 4 SIP Numbers.

**Settings → IPC**

<b>Order (1 – 32)</b>	Displays the order of the IP camera
<b>System Identification</b>	Specifies the name to identify the IP camera.
<b>Connection Type</b>	Select the signaling protocol to be used. Default is SIP.
<b>System Number</b>	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.
<b>Account</b>	Specifies the account on which this feature will be applied.

**Settings → Call Features**

<b>Bypass Dial Plan Through Call History and Directories</b>	Enable/Disable the dial plan check while dialing through the call history and any Phonebook directories. The default setting is “No”.
--	---



<b>Disable Call Waiting</b>	Disables the call waiting feature. The default setting is “No”.
<b>Disable Call Waiting Tone</b>	Disables the call waiting tone when call waiting is on. Default setting is “No”.
<b>Enable Auto Unmute</b>	If the option is enabled, automatically unmute phone when a user resumes the call or establishes a new call. Default is “No”.
<b>Do Not Escape # as %23 in SIP URI</b>	Specifies whether to replace # by %23 or not for some special situations. The default setting is “No”.
<b>Return Code When Refusing Incoming Call</b>	When refusing the incoming call. The GSC3570 will send the selected type of SIP message of the call. Default setting is “Busy 486”. <ul style="list-style-type: none"> <li>• Busy (486)</li> <li>• Temporarily unavailable (480)</li> <li>• Not Found (404)</li> <li>• Decline (603)</li> </ul>
<b>User-Agent Prefix</b>	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.
<b>Settings → Preferences → Date and Time</b>	
<b>NTP Server</b>	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”.
<b>Secondary NTP Server</b>	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.
<b>NTP Update Interval</b>	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.
<b>Allow DHCP Option 42 Override NTP Server</b>	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is “Yes”.
<b>Time Zone</b>	Configures the date/time used on the GSC3570 according to the specified time zone.
<b>Allow DHCP Option 2 to Override Time Zone Setting</b>	Defines whether DHCP Option 2 should override time zone or not. The default setting is “Yes”.



<b>Self-Defined Time Zone</b>	<p>This parameter allows the users to define their own time zone.</p> <p>The syntax is: <b>std offset dst [offset], start [/time], end [/time]</b></p> <p>Default is set to: <b>MTZ+6MDT+5,M4.1.0,M11.1.0</b></p> <p><b>MTZ+6MDT+5</b></p> <p>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.</p> <p><b>M4.1.0,M11.1.0</b></p> <p>The 1<sup>st</sup> number indicates Month: 1,2, 3..., 12 (for Jan, Feb, ..., Dec)</p> <p>The 2<sup>nd</sup> number indicates the n<sup>th</sup> iteration of the weekday: (1<sup>st</sup> Sunday, 3<sup>rd</sup> Tuesday...)</p> <p>The 3<sup>rd</sup> number indicates weekday: 0,1, 2...,6 (for Sun, Mon, Tues, ... ,Sat)</p> <p>Therefore, this example is the DST which starts from the First Sunday of April to the 1<sup>st</sup> Sunday of November.</p>
<b>Date Display Format</b>	<p>Configures the date display format on the LCD.</p> <p>The following formats are supported:</p> <ul style="list-style-type: none"> <li>• yyyy-mm-dd: 2012-07-02</li> <li>• mm-dd-yyyy: 07-02-2012</li> <li>• dd-mm-yyyy: 02-07-2012</li> <li>• dddd, MMMM dd: Friday, October 12</li> <li>• MMMM dd, dddd: October 12, Friday</li> </ul> <p>The default setting is yyyy-mm-dd.</p>
<b>Time Display Format</b>	<p>Configures the time display in 12-hour or 24-hour format on the LCD. The default setting is in 12-hour format.</p>
<b>Settings → Preferences → Language</b>	
<b>Display Language</b>	<p>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.</p> <p>The default setting is “Auto”.</p>
<b>Settings → Preferences → LCD Display</b>	
<b>Active Backlight Timeout</b>	<p>Allows user to set up the backlight time (in minutes) for the extension board. Valid range from 0 to 90. Default value is 1.</p> <p><b>Note:</b> When Active Backlight Timeout is set to 0, the backlight will be constantly on.</p>



<b>Screensaver Timeout</b>	Configures the minutes of idle before the screensaver activates. Valid range is 3 to 6. The default time is 3 minutes.
<b>Settings → Preferences → Ring Tone</b>	
<b>Call Progresses Tones</b> <ul style="list-style-type: none"> <li>• <i>Second Dial Tone</i></li> <li>• <i>Message Waiting</i></li> <li>• <i>Speaker Ring Volume</i></li> </ul>	<p>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.</p> <p><b>Syntax:</b> f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]];          (Frequencies are in Hz and cadence on and off are in 10ms)</p> <p>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.</p> <p>Speaker volume range is 0-7 (default is 5)</p>

## Network Page Definitions

Table 9: Network Page Definitions

<b>Network → Basic Settings</b>	
<b>IPv4 Address</b>	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”.
<b>Host name (Option 12)</b>	Specifies the name of the client. This field is optional but may be required by some Internet Service Providers.
<b>DHCP Vendor Class ID (Option 60)</b>	Used by clients and servers to exchange vendor class ID. The default setting is “Grandstream GSC3570” for GSC3570.
<b>IPv4 Address</b>	Enter the IP address when static IP is used.
<b>Subnet Mask</b>	Enter the Subnet Mask when static IP is used for IPv4.
<b>Gateway</b>	Enter the Default Gateway when static IP is used for IPv4.
<b>DNS Server 1</b>	Enter the DNS Server 1 when static IP is used for IPv4.
<b>DNS Server 2</b>	Enter the DNS Server 2 when static IP is used for IPv4.
<b>Preferred DNS Server</b>	Enters the Preferred DNS Server for IPv4.
<b>Network → Advanced Settings</b>	
<b>802.1X mode</b>	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.



<b>802.1X Identity</b>	Enter the Identity information for the 802.1x mode. <b>Note:</b> Valid input needs to match <b>[a-zA-Z0-9]*</b>
<b>MD5 Password</b>	Enter the MD5 Password for the 802.1X mode. <b>Note:</b> Valid input needs to match <b>[a-zA-Z0-9]*</b>
<b>802.1X CA Certificate</b>	Uploads / deletes the 802.1X CA certificate to the GSC3570; or delete existed 802.1X CA certificate from the GSC3570.
<b>802.1X Client Certificate</b>	Uploads / deletes 802.1X Client certificate to the GSC3570; or delete existed 802.1X Client certificate from the GSC3570.
<b>HTTP Proxy</b>	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.
<b>HTTPS Proxy</b>	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.
<b>Bypass Proxy For</b>	Enter host names that do not require a proxy to reach. Commas should separate those names.
<b>Layer 3 QoS for SIP</b>	Defines the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 26.
<b>Layer 3 QoS for RTP</b>	Defines the Layer 3 QoS parameter for RTP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 46.
<b>Enable DHCP VLAN</b>	Enables auto configure for VLAN settings through DHCP. Disabled by default.
<b>Enable Manual VLAN Configuration</b>	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".
<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assigns the VLAN Tag of the Layer 2 QoS packets. The default value is 0.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assigns the priority value of the Layer2 QoS packets. The default value is 0.
<b>Enable CDP</b>	Enables/Disables CDP "Cisco Discovery Protocol". The default setting is "Enabled".
<b>Enable LLDP</b>	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is "Enabled".
<b>LLDP TX Interval</b>	Defines LLDP TX Interval (in seconds). Valid range is 1 to 3600. The default value is 60.





<b>Maximum Transmission Unit (MTU)</b>	Configure custom MTU. Default is 1500.
<b>Network → OpenVPN® Settings</b>	
<b>OpenVPN® Enable</b>	Enable/Disable OpenVPN® feature. Default is No.
<b>OpenVPN® Server Address</b>	Specify the IP address or FQDN for the OpenVPN® Server.
<b>OpenVPN® Port</b>	Specify the listening port of the OpenVPN® server. Default is 1194.
<b>OpenVPN® Transport</b>	Specify the Transport Type of OpenVPN® whether UDP or TCP. Default is UDP.
<b>OpenVPN® CA</b>	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.
<b>OpenVPN® Certificate</b>	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.
<b>OpenVPN® Client Key</b>	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.
<b>OpenVPN® Cipher Method</b>	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.
<b>OpenVPN® Username</b>	Configures the optional username for authentication if the OpenVPN server supports it.
<b>OpenVPN® Password</b>	Configures the optional password for authentication if the OpenVPN server supports it.
<b>Additional Options</b>	Additional options to be appended to the OpenVPN® config file, separated by semicolons. For example, comp-lzo no;auth SHA256 <b>Note:</b> Please use this option with caution. Make sure that the options are recognizable by OpenVPN® and do not unnecessarily override the other configurations above.
<b>Network → SNMP Settings</b>	
<b>Enable SNMP</b>	Enables/Disables the SNMP feature. Default settings is <b>No</b> .





<b>Version</b>	SNMP version. <ul style="list-style-type: none"> <li>• Version 1</li> <li>• Version 2</li> <li>• Version 3 (Default)</li> </ul>
<b>Port</b>	SNMP port (Default 161).
<b>Community</b>	Enters SNMP Community.
<b>SNMP Trap Version</b>	SNMP Trap Version <ul style="list-style-type: none"> <li>• Trap Version 1</li> <li>• Trap Version 2 (Default)</li> <li>• Trap Version 3</li> </ul>
<b>SNMP Trap IP</b>	IP address of the SNMP trap receiver.
<b>SNMP Trap Port</b>	Port of the SNMP trap receiver (Default 162)
<b>SNMP Trap Interval</b>	The interval between each trap sent to the trap receiver
<b>SNMP Trap Community</b>	Community string associated to the trap. It must match the community string of the trap receiver.
<b>SNMP Username</b>	Username for SNMPv3
<b>Security Level</b>	<ul style="list-style-type: none"> <li>• <b>noAuthUser:</b> Users with security level noAuthnoPriv and context name as noAuth.</li> <li>• <b>authUser:</b> Users with security level authNoPriv and context name as auth.</li> <li>• <b>privUser:</b> Users with security level authPriv and context name as priv.</li> </ul>
<b>Authentication Protocol</b>	Select the Authentication Protocol: "None" or "MD5" or "SHA".
<b>Privacy Protocol</b>	Select the Privacy Protocol: "None" or "DES" or "AES".
<b>Authentication Key</b>	Enter the Authentication Key.
<b>Privacy Key</b>	Enter the Privacy Key.
<b>SNMP Trap Username</b>	Username for SNMPv3 Trap.
<b>Trap Security Level</b>	<ul style="list-style-type: none"> <li>• <b>noAuthUser:</b> Users with security level noAuthnoPriv and context name</li> </ul>



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

## Maintenance Page Definitions

Table 10: Maintenance Page Definitions

<b>Maintenance → Web Access</b>	
<b>User Password</b>	
<b>New Password</b>	<p>Set new password for web GUI access as User.</p> <p><b>Note:</b> This field is case sensitive.</p>



<b>Confirm Password</b>	Enter the new User password again to confirm.
<b>Admin Password</b>	
<b>Current Password</b>	The current admin password is required for setting a new admin password.
<b>New Password</b>	Set new password for web GUI access as Admin. <b>Note:</b> This field is case sensitive.
<b>Confirm Password</b>	Enter the new Admin password again to confirm.
<b>Maintenance → Upgrade and Provisioning</b>	
<b>Upgrade Firmware</b>	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.
<b>Firmware Upgrade and Provisioning</b>	Specifies how firmware upgrading and provisioning request 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”.
<b>Always Authenticate Before Challenge</b>	Only applies to HTTP/HTTPS. If enabled, the GSC3570 will send credentials before being challenged by the server. The default setting is “No”.
<b>Validate Hostname in Certificate</b>	After enabling this feature, device validate the hostname in the SSL certificate. The default setting is “No”.
<b>Allow DHCP Option 43 and Option 66 to Override Server</b>	Default setting is “Yes”. DHCP option 66 originally was only designed for TFTP server. Later, it was extended to support an HTTP URL. GSC3570 supports both TFTP and HTTP server via option 66. Users can also use DHCP option 43 vendor specific option to do this. 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.
<b>Additional Override DHCP Option</b>	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 this option will be effective only when option “Allow DHCP Option 43 and Option 66 to Override Server” is enabled. The default setting is “None”.
<b>Allow DHCP Option 120 to override SIP Server</b>	Enables DHCP Option 120 from local server to override the SIP Server on the GSC3570. The default setting is “No”.
<b>3CX Auto Provision</b>	Enables automatic provision feature (PNP) on the GSC3570. The default setting is “Yes”.



<b>Automatic Upgrade</b>	<p>Specifies when the firmware upgrade process will be initiated; there are 4 options:</p> <ul style="list-style-type: none"> <li>• <b>No:</b> The GSC3570 will only do upgrade once at boot up.</li> <li>• <b>Check every X minutes:</b> User needs to specify a period in minutes.</li> <li>• <b>Check every day:</b> User needs to specify "Hour of the day (0-23)".</li> <li>• <b>Check every week:</b> User needs to specify "Hour of the day (0-23)" and "Day of the week (0-6)". (Day of week is starting from Sunday).</li> </ul> <p>Default is No.</p>
<b>Randomized Automatic Upgrade</b>	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).
<b>Hour of the Day (0-23)</b>	Defines the hour of the day to check the HTTP/TFTP/FTP server for firmware upgrades or configuration files changes. The default value is 1.
<b>Day of the Week (0-6)</b>	Defines the day of the week to check HTTP/TFTP/FTP server for firmware upgrades or configuration files changes. The default value is 1.
<b>Disable SIP NOTIFY Authentication</b>	Device will not challenge NOTIFY with 401 when set to "Yes". Default setting is "No".
<b>Firmware Upgrade Confirmation</b>	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. If set to "No", the GSC3570 will automatically upgrade without user input.
<b>Config</b>	
<b>Config Upgrade Via</b>	Allows users to choose the config upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is "HTTPS".
<b>Config Server Path</b>	Defines the server path for provisioning. Default is "fm.grandstream.com/gs"
<b>Config Server Username</b>	The username for the Config server.
<b>Config Server Password</b>	The password for the Config server.
<b>Config File Prefix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the GSC3570.
<b>Config File Postfix</b>	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the GSC3570.



<b>XML Config File Password</b>	The password for encrypting XML configuration file using OpenSSL. This is required for the GSC3570 to decrypt the encrypted XML configuration file.
<b>Authenticate Conf File</b>	Sets the GSC3570 system to authenticate configuration file before applying it. When set to “Yes”, the configuration file must include value P1 with GSC3570 system’s administration password. If it is missed or does not match the password, the GSC3570 system will not apply it. Default setting is “No”.
<b>Download Device Configuration</b>	Click to download GSC3570’s configuration file in .txt format. <b>Note:</b> The file does not include passwords or CA/Custom certificate
<b>Download Device Configuration (XML)</b>	Click to download GSC3570’s configuration file in .xml format. <b>Note:</b> The file does not include passwords or CA/Custom certificate
<b>User protection</b>	When user protection is on, p-values that user sets will not be changed by provision or provider. <ul style="list-style-type: none"> <li>• If “User protection” is OFF, everyone (Provider, user, or admin) has access to most of the P-values.</li> <li>• If “User protection” is ON, only those (normally user or admin) who have privilege can modify the configuration.</li> </ul>
<b>Download and Process All Available Config Files</b>	By default, 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 inverse the downloading process to cfg.xml > cfgGSC3570.xml > cfgMAC.bin > cfgMAC.xml. The following files will override the files that has already been load and processed.
<b>Download User Configuration</b>	This allows users to download part of the configuration that does not include any personal settings like Username and Passwords. Also, it will include all the changes manually made by user from web UI, or config file uploaded from “Upload Device Configuration”, but not include the changes from the server provision via TFTP/FTP/FTPS/HTTP/HTTPS.
<b>Upload Device Configuration</b>	Uploads configuration file to GSC3570.
<b>Export backup Package</b>	Export backup package which contains device configuration along with personal data.
<b>Restore from Backup package</b>	Click to upload backup package and restore.
<b>Firmware</b>	



<b>Firmware Upgrade Via</b>	Allows users to choose the firmware upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is “HTTP”.
<b>Firmware Server Path</b>	Defines the server path for the firmware server. Default is “fm.grandstream.com/gs”
<b>Firmware Server Username</b>	The username for the Firmware server.
<b>Firmware Server Password</b>	The password for the Firmware server.
<b>Firmware File Prefix</b>	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.
<b>Firmware File Postfix</b>	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the GSC3570.

### Maintenance → Syslog

<b>Syslog Protocol</b>	If set to SSL/TLS, the syslog messages will be sent through secured TLS protocol to syslog server. Default setting is UDP. <b>Note:</b> The CA certificate is required to connect with the TLS server.
<b>Syslog Server</b>	URL or IP address of the syslog server for the GSC3570 to send syslog to. <b>Note:</b> By adding 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.
<b>Syslog Level</b>	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: <ul style="list-style-type: none"> <li>• Product model/version on boot up (INFO level).</li> <li>• NAT related info (INFO level).</li> <li>• sent or received SIP message (DEBUG level).</li> <li>• SIP message summary (INFO level).</li> <li>• inbound and outbound calls (INFO level).</li> <li>• registration status change (INFO level).</li> <li>• negotiated codec (INFO level).</li> <li>• Ethernet link up (INFO level).</li> <li>• SLIC chip exception (WARNING and ERROR levels).</li> <li>• Memory exception (ERROR level).</li> </ul>



<b>Syslog Keyword Filtering</b>	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.
<b>Send SIP Log</b>	Configures whether the SIP log will be included in the syslog messages. The default setting is "No". <b>Note:</b> By setting Send SIP Log to Yes, the GSC3570 will still send SIP log from syslog even when Syslog Level set to NONE.
<b>Maintenance → Security Settings → Security</b>	
<b>Validate Server Certificates</b>	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.
<b>SIP TLS Certificate</b>	SSL Certificate used for SIP Transport in TLS/TCP.
<b>SIP TLS Private Key</b>	SSL Private key used for SIP Transport in TLS/TCP.
<b>SIP TLS Private Key Password</b>	SSL Private key password used for SIP Transport in TLS/TCP.
<b>Custom Certificate</b>	The uploaded custom certificate will be used for SSL/TLS communication instead of the GSC3570 default certificate.
<b>Web Access Mode</b>	Sets the protocol for web interface. <ul style="list-style-type: none"> <li>• HTTPS</li> <li>• HTTP</li> <li>• Disabled</li> <li>• Both HTTP and HTTPS</li> </ul> The default setting is "HTTP".
<b>HTTP Web Port</b>	Configures the HTTP port under the HTTP web access mode. Default is 80.
<b>HTTPS Web Port</b>	Configures the HTTPS port under the HTTPS web access mode. Default setting is "443".
<b>Disable SSH</b>	Disables SSH access. The default setting is "No".
<b>SSH Public Key</b>	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. <b>Note:</b> This will allow upcoming SSH access without password.
<b>Web Session Timeout</b>	Configures timer to logout web session during idle. Default is 10 min. Range is 2-60 min.
<b>Web Access Attempt Limit</b>	Configures attempt limit before lockout. Default is 5. Range is 1-10.



**Maintenance → Security Settings → Trusted CA Certificates**

<b>Trusted CA Certificates</b>	Allows to upload and delete the CA Certificate file to GSC3570. <b>Note:</b> Users can either upload the file directly from web or they can choose to provision it from their cfg.xml file.
<b>Load CA Certificates</b>	Users can specify which certificate they are going to use: <ul style="list-style-type: none"> <li>• <b>Default Certificates:</b> (Default) Built-in Certificates.</li> <li>• <b>Custom Certificates:</b> Uploaded Certificates.</li> <li>• <b>All Certificates:</b> Both built-in and uploaded Certificates.</li> </ul>

**Maintenance → Packet Capture**

<b>Status</b>	Displays packet capture status. When user starts to capture trace file, it will show "RUNNING" status, otherwise, it will show "STOPPED".
<b>With RTP Packets</b>	Defines whether the packet capture file contains RTP or not. Default is No

**Maintenance → Tools**

<b>Provision</b>	Launch provision process.
<b>Factory Reset</b>	Reset device.
<b>Ping</b>	Start ping on a destination.
<b>Traceroute</b>	Start Traceroute on a destination.

## Directory Page Definitions

Table 11: Directory Page Definitions

**Phonebook → Contacts**

<b>Search Bar</b>	Allows users searching for Phonebook entries.
<b>Add Contact</b>	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. <b>Note:</b> 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.
<b>Edit Contact</b>	Edits selected contact.
<b>Delete All Contacts</b>	Deletes all contacts from Phonebook. <b>NOTE:</b> 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	
<b>Add Group</b>	Specifies Group's name to add new group and select a default ringtone for this group. Up to 30 Groups can be added.
<b>Edit Group</b>	Edits selected group.
Phonebook → Phonebook Management	
<b>Enable Phonebook XML Download</b>	Configures to enable Phonebook XML download. Users could select HTTP/HTTPS/TFTP to download the Phonebook file. The default setting is "Disabled".
<b>HTTP/HTTPS Username</b>	The username for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	The password for the HTTP/HTTPS server.
<b>Phonebook XML Server Path</b>	Configures the server path to download the Phonebook XML. This field could be IP address or URL, with up to 256 characters.
<b>Phonebook Download Interval</b>	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.
<b>Remove Manually edited Entries on Download</b>	If set to "Yes", when XML Phonebook is downloaded, the entries added manually will be automatically removed. The default setting is "Yes".
<b>Import Group Method</b>	When set to " <b>Replace</b> ", existing groups will be completely replaced by imported one; When set to " <b>Append</b> ", the imported groups will be attended with the current one.
<b>Download XML Phonebook</b>	Click on "Download" to download the XML Phonebook file to local PC
<b>Upload XML Phonebook</b>	Click on "Upload" to upload local XML Phonebook file to the GSC3570.
<b>Default search mode</b>	<p>Configures default phonebook search mode.</p> <ul style="list-style-type: none"> <li>• <b>Quick Match:</b> 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.</li> <li>• <b>Exact Match:</b> 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.</li> </ul> <p>The default setting is "Quick Match".</p>



Phonebook → Call History	
<b>Delete</b>	Users can select an entry, then click “Delete” to remove it from the list.
<b>Delete All</b>	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	
<b>LDAP Protocol</b>	Configures the LDAP protocol to LDAP or LDAPS. The default setting is “LDAP”. LDAPS is a feature to support LDAP over TLS.
<b>Server Address</b>	Configures the IP address or DNS name of the LDAP server.
<b>Port</b>	Configures the LDAP server port. The default port number is “389”.
<b>Base</b>	Configures the LDAP search base. This is the location in the directory where the search is requested to begin. <u>Example:</u> dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com
<b>Username</b>	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
<b>Password</b>	Configures the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
<b>LDAP Number Filter</b>	Configures the filter used for number lookups. <u>Examples:</u> (!(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.
<b>LDAP Name Filter</b>	Configures the filter used for name lookups. <u>Examples:</u> (!(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.
<b>LDAP Version</b>	Selects the protocol version for the GSC3570 to send the bind requests. The default setting is "Version 3".
<b>LDAP Name Attributes</b>	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. <u>Example:</u>



	gn cn sn description
<b>LDAP Number Attributes</b>	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. <u>Example:</u> telephoneNumber telephoneNumber Mobile
<b>LDAP Display Name</b>	Configures the entry information to be shown on Intercom's LCD. Up to 3 fields can be displayed. <u>Example:</u> %cn %sn %telephoneNumber
<b>Max. Hits</b>	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.
<b>Search Timeout</b>	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.
<b>Sort Results</b>	Specifies whether the searching result is sorted or not. Default setting is "No".

## NAT Settings

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

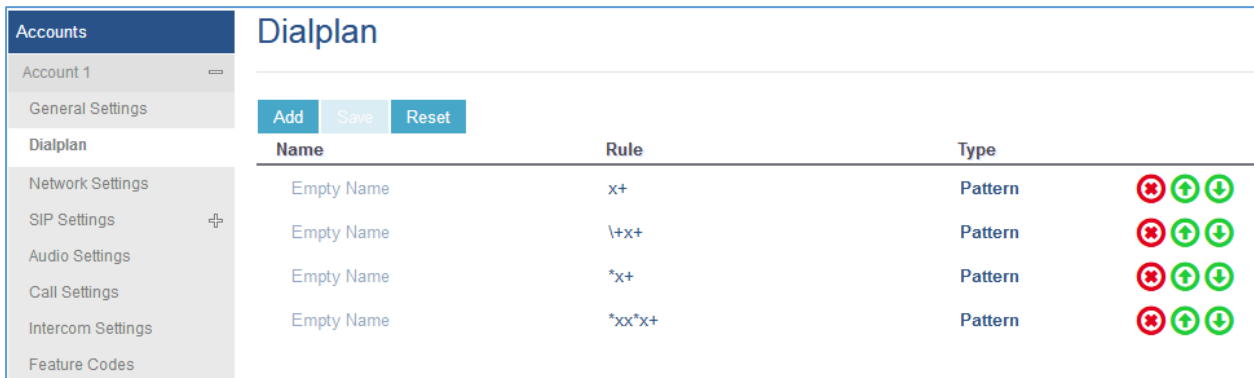
- STUN Server**  
 Under **Settings**→**General Settings**, enter a STUN Server IP (or FQDN) that you may have, or look up a free public STUN Server on the internet and enter it on this field. If using Public IP, keep this field blank.
- Use Random Ports**  
 It is under **Settings**→**General Settings**. 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**. Default setting is "No". Enable the device to use NAT traversal when it is behind 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 type of calls or change the number format before dialing out. Users can configure dial plan rules through a simple and well-designed interface under menu “**Account X → Dial Plan**”.

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















Accounts		Dialplan		
Account 1				
General Settings		Add	Save	Reset
Dialplan		Name	Rule	Type
Network Settings		Empty Name	x+	Pattern   
SIP Settings		Empty Name	\+x+	Pattern   
Audio Settings		Empty Name	*x+	Pattern   
Call Settings		Empty Name	*xx*x+	Pattern   
Intercom Settings				
Feature Codes				

Figure 25: Dial Plan Configuration

The current interface features are as follow:

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.
  - i. **Pattern:** The general rule and it will not change the dial plan you configured.
  - ii. **Block:** The rules you set in combination with this type will be blocked.
  - iii. **Dial Now:** The rules you set in combination with this type will be dialed out once the DTMF matches the Dial Plan.
  - iv. **Prefix:** The rules you set in combination with this type will include configured prefix automatically. If Replaced was set, your used prefix will replace the “Replaced” value.



**Replaced:**

**Used:**

**Rule:**

Prefix  

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



<b>Replaced:</b>	<input type="text" value="3"/>	
<b>Used:</b>	<input type="text" value="123"/>	Prefix ▾
<b>Rule:</b>	<input type="text" value="xxx"/>	

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

<b>Trigger:</b>	<input type="text" value="1,2,3,4,5,6,7,8,9,0"/>	
<b>Rule:</b>	<input type="text" value="1,2,3,4,5,6,7,8,9,0 , * , # , A,a,B,b,C,c,D,d"/>	Second tone ▾

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

**Note:**

- 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 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.)

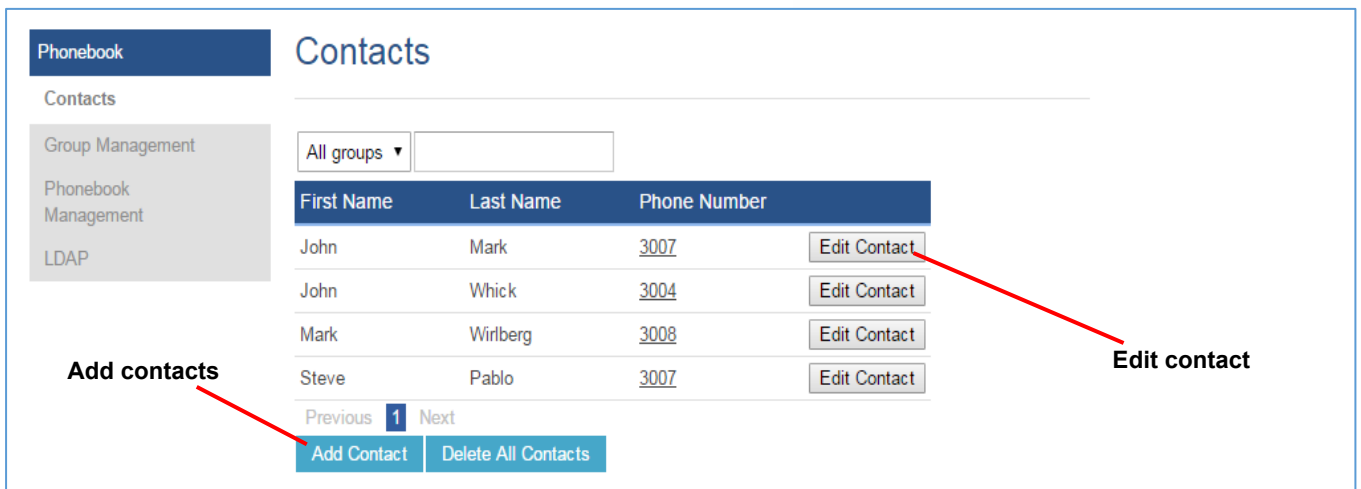


Figure 26: Edit contacts

## 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.

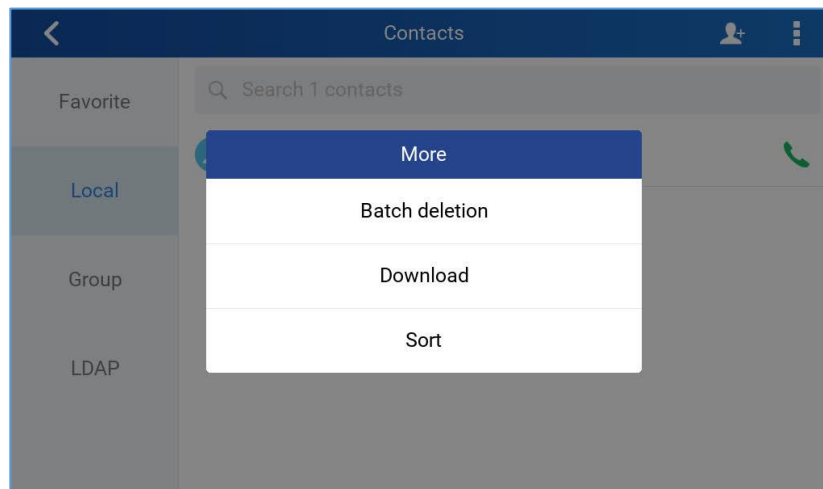


Figure 27: Download XML phonebook

- **Phonebook Download Interval:**

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



## Saving Configuration Changes

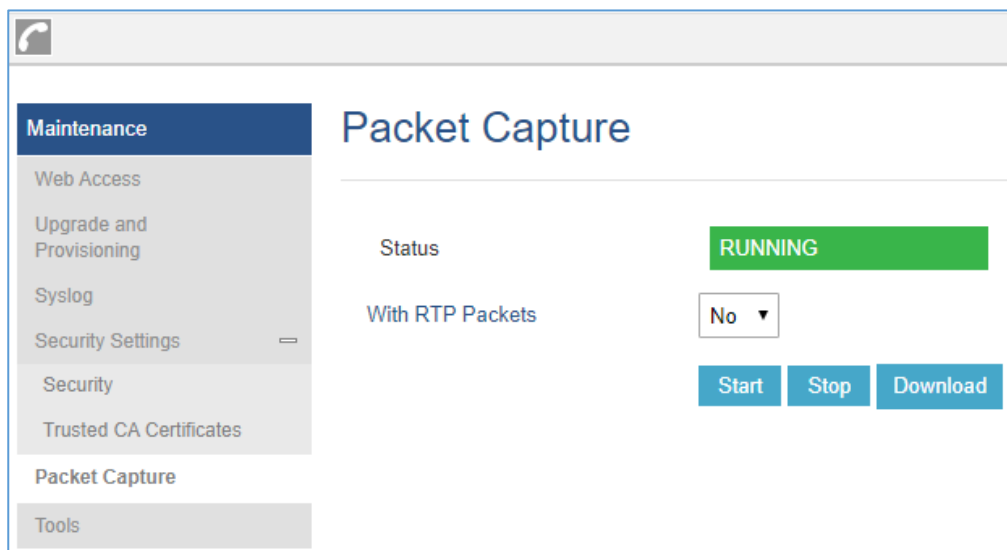
After users makes changes to the configuration, press the "Save" button will save but not apply the changes until the "Apply" button on the top of web GUI page is clicked. Or, users could directly press "Save and Apply" button. We recommend rebooting or powering cycle the GSC3570 after applying all the 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 packet capture function. The related options are under **Maintenance**→**Packet Capture**.



**Figure 28: Packet Capture**

User can also define whether RTP packets will be captured or not from **With RTP Packets** option. When the capture configuration is set, press **Start** button to start packet capture. The Status will become **RUNNING** while capturing. Press **Stop** button to end capture. Press **Download** button to download capture file to 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 name can be FQDN or IP address.

### Examples of valid URLs:

[firmware.grandstream.com/BETA](http://firmware.grandstream.com/BETA)

[fw.mycompany.com](http://fw.mycompany.com)

There are two ways to setup 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 LCD menu:

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

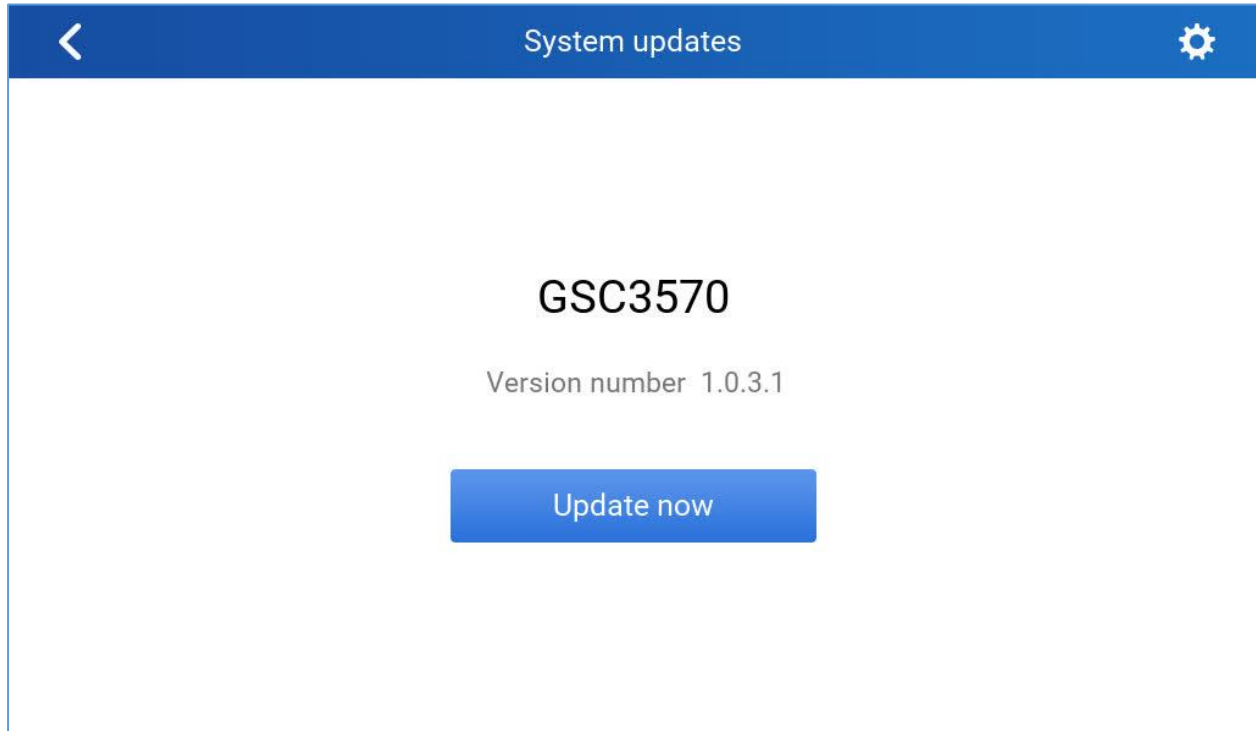


Figure 29: LCD upgrade



## Upgrade via Web GUI

Open a web browser on PC and enter the IP address of the GSC3570. Then, login with the administrator username and password. Go to Maintenance→Upgrade and Provisioning page, enter the IP address or the FQDN for the upgrade server in "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 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 that 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:

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

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

[http://www.solarwinds.com/products/freetools/free\\_tftp\\_server.aspx](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 numeric 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 "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:

[http://www.grandstream.com/sites/default/files/Resources/gs\\_provisioning\\_guide.pdf](http://www.grandstream.com/sites/default/files/Resources/gs_provisioning_guide.pdf)

## 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 user to enter username and password. Once correct username and password are entered, the GSC3570 will send 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 LCD prompt, users can save the login credentials for 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 saved are correct, login window will be skipped. Otherwise, login window will be popped up to prompt users to enter correct username and password again.



## RESTORE FACTORY DEFAULT SETTINGS

---

 **Warning:**

Restoring the Factory Default Settings will delete all configuration information on the GSC3570. Please backup 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 factory reset on GSC3570 IP Intercom series which are described below.

### Restore to factory using Web GUI

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

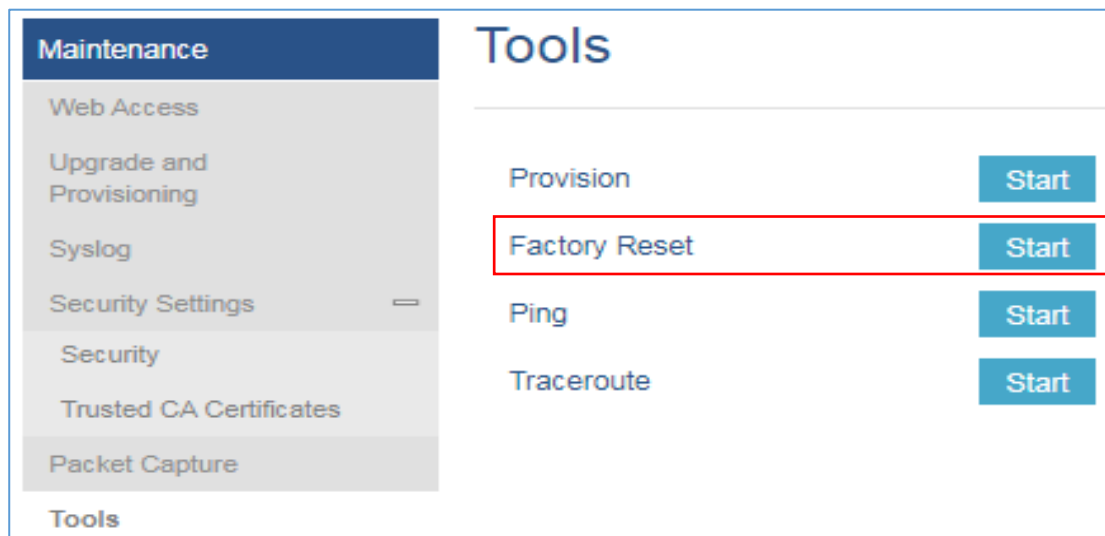


Figure 30: Factory Reset from web GUI

### Restore to factory using LCD menu

Please follow the instructions below to reset the GSC3570:

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



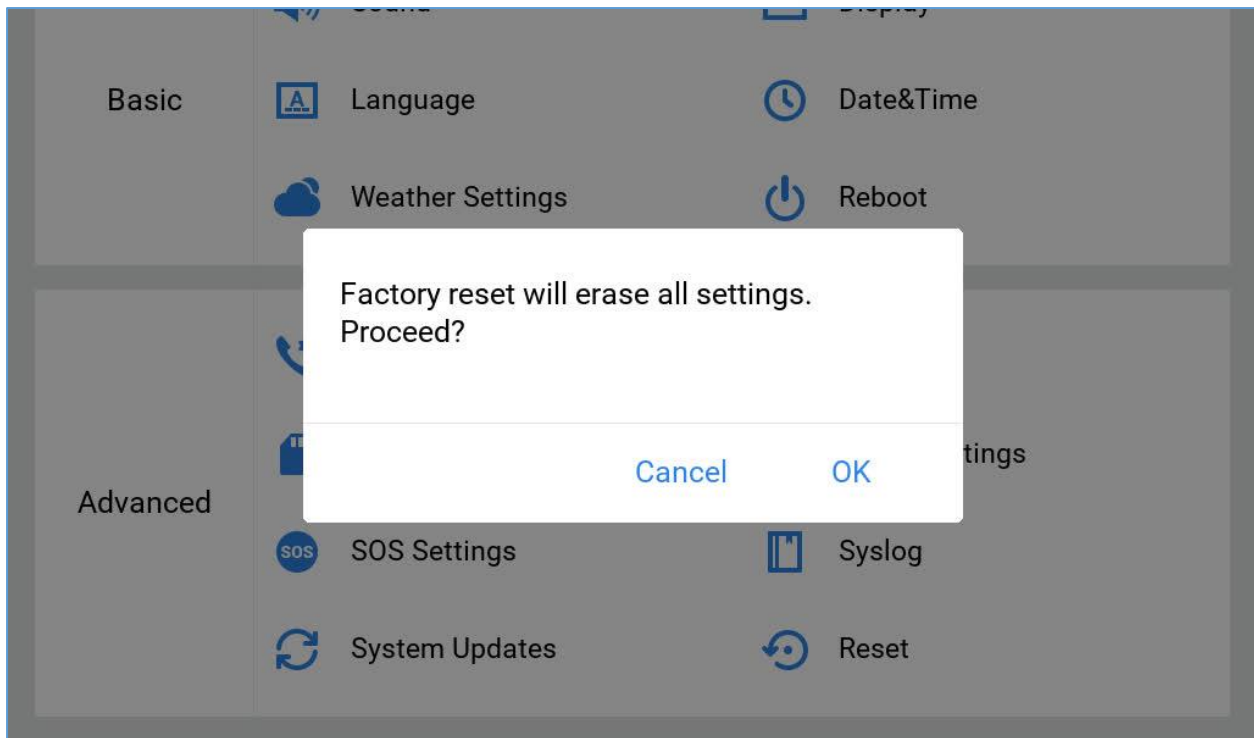


Figure 31: Factory Reset from LCD

## EXPERIENCING GSC3570

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

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

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

Thank you again for purchasing Grandstream GSC3570 IP Intercom, it will be sure to bring convenience and color to both your business and personal life.

