

# Grandstream Networks, Inc.

---

GSC35XX Series

**User Manual**



## **COPYRIGHT**

©2019 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.



## FCC Caution

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

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

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

## RF Exposure Information (SAR)

This device is designed and manufactured not to be exceeded the emission limits for exposure to radio frequency RF energy set by the Federal Communications Commission of the United States. The exposure standard for wireless devices employing a unit of measurement is known as the Specific Absorption Rate (SAR), and the SAR limit set by FCC is 1.6 W/kg.

This device is complied with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1992, and has been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C. This device has been tested and meets the FCC RF exposure guidelines when tested with the device directly contacted to the body. RF exposure compliance with anybody-worn accessory, which contains metal, was not tested and certified, and use such body-worn accessory should be avoided.

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

Hereby, Grandstream declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.



## CE Authentication



AT	BE	CY	CZ	DK	EE	FI
FR	DE	EL	HU	IE	IT	LV
LT	LU	MT	NL	PL	PT	SK
SI	ES	SE	UK	BG	RO	HR

In all EU member states, operation of 5150 - 5350 MHz is restricted to indoor use only.

Hereby, Grandstream Networks, Inc. declares that the radio equipment GSC3510/GSC3505 is in compliance with Directive 2014/53/EU.

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

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



## GNU GPL INFORMATION

GSC3510/GSC3505 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/sites/default/files/Resources/GSC35XX\\_gpl.zip](http://www.grandstream.com/sites/default/files/Resources/GSC35XX_gpl.zip)



# Table of Contents

<b>DOCUMENT PURPOSE .....</b>	<b>11</b>
<b>CHANGE LOG .....</b>	<b>12</b>
Firmware Version 1.0.0.22.....	12
Firmware Version 1.0.0.15.....	12
<b>WELCOME .....</b>	<b>13</b>
<b>PRODUCT OVERVIEW .....</b>	<b>14</b>
Feature Highlights.....	14
GSC3510/GSC3505 Technical Specifications.....	14
<b>GETTING STARTED.....</b>	<b>16</b>
Equipment Packaging .....	16
GSC3510/GSC3505 Ports.....	17
GSC3510/GSC3505 LED Indicators.....	17
Hardware Installation .....	18
<i>Wall Mount</i> .....	18
<i>Ceiling Mount</i> .....	19
<i>Anti-theft Installation</i> .....	20
Powering and Connecting GSC3510/GSC3505.....	20
<i>Connecting Wiring Seat</i> .....	21
Access GSC3510/GSC3505 Web GUI .....	21
<b>GSC3510/GSC3505 APPLICATION SCENARIOS.....</b>	<b>23</b>
GSC3510/GSC3505 SIP Two-Way/One-Way Intercom System .....	23
Multicast Paging Application.....	26
Bluetooth Speaker .....	29
2-pin Multi-Purpose Input Applications.....	30
<b>GSC3510/GSC3505 WEB GUI SETTINGS .....</b>	<b>33</b>
Status Page Definitions.....	33



<i>Account Status</i> .....	33
<i>Network Status</i> .....	33
<i>System Info</i> .....	34
<b>Account Page Definitions</b> .....	34
<i>General Settings</i> .....	34
<i>SIP Settings</i> .....	37
<i>Codec Settings</i> .....	40
<i>Call Settings</i> .....	43
<i>Advanced Settings</i> .....	45
<b>Calls Page Definition</b> .....	47
<i>Call</i> .....	47
<i>Call History</i> .....	48
<i>Call History → All</i> .....	48
<i>Call History → Intercept Record</i> .....	50
<b>Contacts</b> .....	52
<i>Contacts List</i> .....	52
<i>Group</i> .....	56
<b>Black/White List Settings</b> .....	57
<i>Whitelist</i> .....	57
<i>Blacklist</i> .....	59
<i>Blocking Rules</i> .....	60
<b>Phone Settings Page Definitions</b> .....	60
<i>General Settings</i> .....	60
<i>Call Settings</i> .....	61
<i>Ring Tone</i> .....	62
<i>Multicast Paging</i> .....	63
<b>Network Settings Page Definitions</b> .....	64
<i>Ethernet Settings</i> .....	64
<i>Bluetooth</i> .....	66
<i>Wi-Fi Settings</i> .....	66
<i>Connect to Wi-Fi Network</i> .....	66
<i>Wi-Fi Settings description</i> .....	68
<i>OpenVPN® Settings</i> .....	69
<i>Advanced Network Settings</i> .....	70



System Settings Page Definitions.....	71
<i>Time Settings</i> .....	71
<i>Security Settings</i> .....	71
<i>Preferences</i> .....	73
<i>TR-069</i> .....	73
<i>Sensor Settings</i> .....	74
<i>Backup</i> .....	74
Maintenance Page Definitions.....	76
<i>Upgrade</i> .....	76
<i>System Diagnosis</i> .....	80
<i>Event Notification</i> .....	82
Application Page Definitions.....	83
<i>LDAP Book</i> .....	83
<i>Recording</i> .....	84
Device Detection Page Definitions.....	85
<i>Audio Loop Test</i> .....	85
<i>Built-in Speaker Test</i> .....	85
<i>LED Test</i> .....	86
<i>Certificate Verify</i> .....	87
<i>Reset Button Test</i> .....	87
<b>EXPERIENCING THE GSC3510/GSC3505.....</b>	<b>88</b>





## Table of Tables

Table 1: GSC3510/GSC3505 Features in a Glance.....	14
Table 2: GSC3510/GSC3505 Technical Specifications .....	14
Table 3: Equipment Packaging.....	16
Table 4: GSC3510/GSC3505 Ports Description.....	17
Table 5: GSC3510 LED Indicators .....	17

## Table of Figures

Figure 1: GSC3510/GSC3505 Package Content.....	16
Figure 2: GSC3510/GSC3505 Ports .....	17
Figure 3: Wall Mount - Step 1.....	18
Figure 4: Wall Mount - Step 2.....	18
Figure 5: Wall Mount - Step 3.....	18
Figure 6: Wall Mount - Step 4.....	18
Figure 7: Ceiling Mount - Step 1 & 2 .....	19
Figure 8: Ceiling Mount - Step 3.....	19
Figure 9: Ceiling Mount - Step 4.....	19
Figure 10: Ceiling Mount - Step 5.....	19
Figure 11: Anti-theft Installation.....	20
Figure 12: Powering GSC3505/GSC3510 .....	20
Figure 13: Connecting Wiring Seat .....	21
Figure 14: GSC3510 Web GUI – Login .....	22
Figure 15: SIP 2-Way/1-Way Paging Diagram.....	23
Figure 16: SIP Account Configuration .....	24
Figure 17: SIP Account Status .....	24
Figure 18: Default Blocking Rules .....	25
Figure 19: Whitelisted Devices.....	25
Figure 20: Multicast paging Diagram.....	26
Figure 21: Multicast Paging Listening Addresses .....	27
Figure 22: Multicast Paging – Paging Priority Active.....	27
Figure 23: Multicast Paging - Priority Barge .....	28
Figure 24: Connecting the GSC3510/GSC3505 as a Bluetooth Speaker .....	29
Figure 25: 2-pin Multi-Purpose Input Applications.....	30
Figure 26: Sensor Settings .....	30
Figure 27: Sensor Setting – Trigger time.....	31
Figure 28: Sensor Setting - Linkage Function - Play Audio .....	32
Figure 29: Sensor Setting - Linkage Function - Make Call .....	32



Figure 30: Click-to-Dial Feature .....	47
Figure 31: Outgoing call in progress and accepted .....	48
Figure 32: Call History → All.....	49
Figure 33: Call details under Call History → All.....	49
Figure 34: Add number from call history to an existing contact .....	50
Figure 35: Call History → Intercept Record.....	50
Figure 36: Call details under Call History → Intercept Record.....	51
Figure 37: Contacts → Contacts List .....	52
Figure 38: Add New Contact .....	52
Figure 39: Contacts → Group.....	56
Figure 40: Add New Group .....	57
Figure 41: Whitelist section.....	57
Figure 42: Add phonebook contacts to whitelist.....	58
Figure 43: Add blocked numbers to whitelist .....	58
Figure 44: Add Manually to Whitelist .....	59
Figure 45: Blacklist Section.....	59
Figure 46: Add from Call History to Blacklist.....	60
Figure 47: Wi-Fi Basics Page.....	67
Figure 48: Connect to Wi-Fi Network .....	67
Figure 49: GSC3510/GSC3505 Connect to Wi-Fi-Show Advanced Options.....	68
Figure 50: GSC3510/GSC3505 Backup Page.....	75
Figure 51: Backup content selection .....	75
Figure 52: Generated Backup .....	76
Figure 53: Device Detection - Audio Loop Test.....	85
Figure 54: Device Detection - Built-in Speaker Test.....	86
Figure 55: Device Detection - LED Test.....	86
Figure 56: Device Detection - Reset Button Test .....	87



## DOCUMENT PURPOSE

This document describes how to configure the GSC3510 via web UI menu to fully manipulate device's features. Please visit <http://www.grandstream.com/support> to download the latest "GSC3510 User Manual".

This guide covers following topics:

- [Product Overview](#)
- [Getting Started](#)
- [Hardware Installation](#)
  - [Wall Mount](#)
  - [Ceiling Mount](#)
  - [Anti-theft Installation](#)
- [GSC3510/GSC3505 Application Scenarios](#)
  - [GSC3510/GSC3505 SIP two-way/one-way Intercom System](#)
  - [Multicast Paging Application](#)
  - [Bluetooth Speaker](#)
  - [2-pin Multi-Purpose Input Applications](#)
- [GSC3510 Web GUI Settings](#)
- [Experiencing the GSC3510](#)



## CHANGE LOG

This section documents significant changes from previous versions of user manual for GSC35XX Seies. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

### **Firmware Version 1.0.0.22**

- Added support for Date/Time settings. [Time Settings]
- Added volume control settings. [Preferences]
- Added support for Sensor Profile Schedule/ Profile Action. [2-pin Multi-Purpose Input Applications] [Sensor Settings]
- Added support for numbers with + on the whitelist/blacklist. [Black/White List Settings]
- Removed Red LED on missed call/voicemail when GSC3510 connected via Bluetooth. [GSC3510/GSC3505 LED Indicators]
- Removed Subscribe for MWI settings. [SIP Settings]
- Removed Voicemail Access Number settings. [General Settings]
- Removed SIP Display Name settings. [General Settings]

### **Firmware Version 1.0.0.15**

- This is the initial version.



## WELCOME

Thank you for purchasing Grandstream GSC3510/GSC3505 SIP Intercom speakers. The GSC3505 is a one-way SIP Intercom Speaker and GSC3510 is a two-way full-duplex SIP intercom speaker/microphone, both featuring one 100Mbps Ethernet port with PoE/PoE+, integrated dual-band 2.4G/5G Wi-Fi, integrated Bluetooth, high fidelity 8W speaker and a multi-purpose input port supporting a wide range of peripherals, 3 directional microphones with Multichannel Microphone Array Design (MMAD) available for GSC3510 only. Both GSC3505 and GSC3510 with their Hi-Fi speaker delivers full-band audio, while GSC3510 adds a state-of-art microphone array with pickup distance up to 4.2 meters. The built-in whitelist and blacklist features enable easy filtering of unwanted calls from the Internet. Its modern industrial design and rich features make it ideal for classrooms, hospitals, apartments, dormitories and much more.

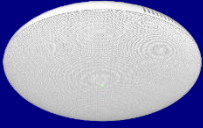


## PRODUCT OVERVIEW

### Feature Highlights

The following table contains the major features of the GSC3510/GSC3505:

**Table 1: GSC3510/GSC3505 Features in a Glance**

 <p><b>GSC3510</b> <b>GSC3505</b></p>	<ul style="list-style-type: none"> <li>• Up to 16 SIP accounts.</li> <li>• Ethernet RJ45 10/100Mbps, PoE/PoE+, Integrated Bluetooth, Wi-Fi.</li> <li>• Both GSC3505 and GSC3510 HD with their Hi-Fi speaker delivers full-band audio, Hands-free speakerphone with HD acoustic chamber, advanced acoustic echo cancellation, while GSC3510 adds a state-of-art microphone array with pickup distance up to 4.2 meters.</li> </ul>
--	---

### GSC3510/GSC3505 Technical Specifications

The following table resumes all the technical specifications including the protocols / standards supported, voice codecs, telephony features, languages and upgrade/provisioning settings for GSC3510/GSC3505.

**Table 2: GSC3510/GSC3505 Technical Specifications**

<b>Protocols/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 Interfaces</b>	Ethernet RJ45 10/100Mbps ports with integrated PoE/PoE+.
<b>Bluetooth</b>	Yes, integrated. Bluetooth.
<b>Wi-Fi</b>	Yes, dual-band 2.4 & 5GHz with 802.11 a/b/g/n.
<b>Alarm Input</b>	1 Alarm Input Port.
<b>Voice Codec</b>	G.711μ/a, G.722 (wide-band), G.722.1, G.722.1C, G.726-32, iLBC, Opus, G.729A/B in-band and out-of-band DTMF (In audio, RFC2833, SIP INFO).

<b>Telephony Features</b>	Hold, transfer, forward (unconditional/no-answer/busy), call park/pickup, downloadable contacts, call record, call log, auto answer, click-to-dial, flexible dial plan.
<b>HD Audio</b>	Yes, HD speakerphone with support for wideband audio.
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS.
<b>Security</b>	User and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control.
<b>Multi-languages</b>	English, Chinese and Portuguese.
<b>Upgrade/ Provisioning</b>	Firmware upgrade via TFTP / HTTP / HTTPS or local HTTP upload, mass provisioning using TR-069 or AES encrypted XML configuration file.
<b>Power and Green Energy Efficiency</b>	Integrated PoE* 802.3af Class 3, PoE+ 802.3at, Class 4.
<b>Package Content</b>	GSC3510/GSC3505, Metal Bracket, Plastic Bracket, Wiring Seat, Hang rope plate, 3x Screw (PM 3 x 50), 3x Screw (PA 3.5 x 20), 1 x Screw (M3 x 15), Hexagonal Screwdriver, 3 x Plastic Expansion Bolt, 3 x M3 NUT, Quick Installation Guide, GPL license.

## GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the GSC3510/GSC3505.

### Equipment Packaging

Table 3: Equipment Packaging

GSC3510/GSC3505
<ul style="list-style-type: none"> <li>• 1x GSC3510/GSC3505 Main Case.</li> <li>• 1x Metal Bracket.</li> <li>• 1x Plastic Bracket.</li> <li>• Wiring Seat.</li> <li>• Hang rope plate.</li> <li>• 3x Screw (PM 3x50)</li> <li>• 3x Screw (PA 3.5 x20).</li> <li>• 1x Screw (M3x15)</li> <li>• Hexagonal Screwdriver.</li> <li>• 3x Plastic Expansion Bolt.</li> <li>• 3x M3 NUT.</li> <li>• 1x Quick Installation Guide.</li> <li>• 1x GPL license.</li> </ul>

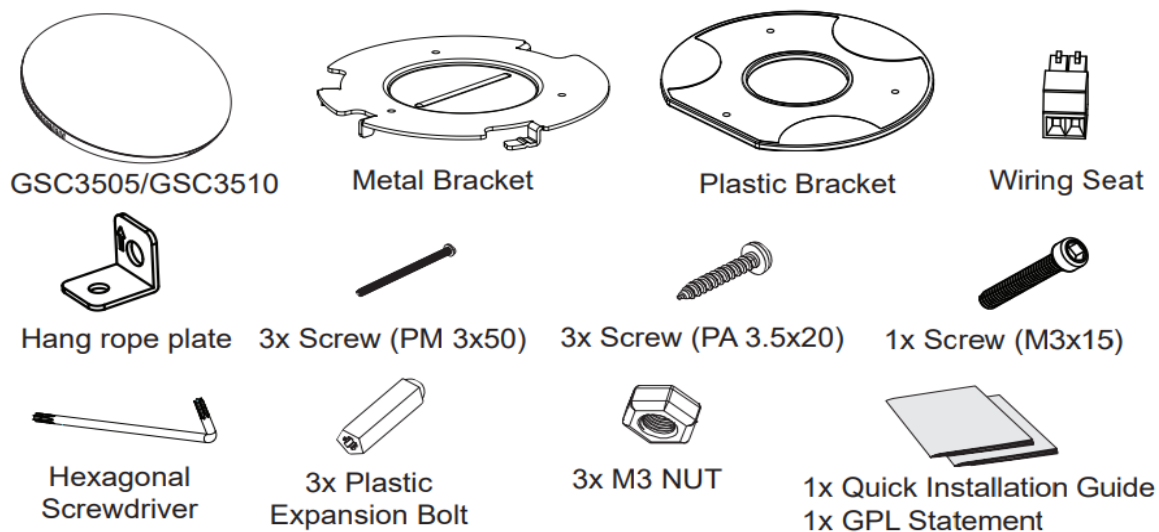


Figure 1: GSC3510/GSC3505 Package Content

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



## GSC3510/GSC3505 Ports

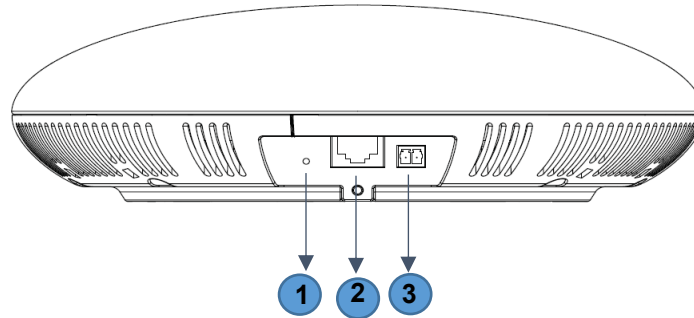


Figure 2: GSC3510/GSC3505 Ports

Table 4: GSC3510/GSC3505 Ports Description

NO.	Name	Description
1	RESET	Factory reset button. Press for 10 seconds to reset factory default settings.
2	NET/PoE	Ethernet RJ45 port (10/100Mbps) supporting PoE/PoE+.
3	2-PIN Port	2-PIN Multi-Purpose Input Port.

## GSC3510/GSC3505 LED Indicators

The GSC3510/GSC3505 contains 4 types of colored LEDs (Red, Green, White and Blue light) that are used in some specific situations and operations. Please, refer to the following table describing each one of the LED Indicators status:

Table 5: GSC3510 LED Indicators

Color	LED Indicator Status	Description
Red Light	Fast Flashing (every 1s)	Rebooting/factory resetting
	Slow Flashing (On 1s, Off 2s)	Unhandled event: (Included Missed call(s), new voice mails, new SIP messages). <b>Note:</b> In case the GSC3510/3505 is connected via Bluetooth, Missed Call/Voicemail Red LED will not light and will remain flashing in blue.
	Solid Red	The contacts/storage space is full
Green Light	Fast Flashing (every 1s)	Incoming/outgoing call
	Slow Flashing (On 1s, Off 2s)	Call on hold.
	Solid Green	During the call.

<b>White Light</b>	Fast Flashing (every 1s)	Upgrading the firmware.
<b>Blue Light</b>	Fast Flashing (every 1s)	Bluetooth pairing.

## Hardware Installation

GSC3510/GSC3505 can be mounted on the wall or ceiling. Please refer to the following steps for the appropriate installation

### Wall Mount

1. Locate the equipment holder on the desired position with arrow up. Drill three holes on the wall referring to the positions of holes on the metal bracket.
2. Fix the metal bracket on the wall by expansion screws.
3. Align the position line on device's back cover with the positioning slot.
4. Rotate the device clockwise until it is locked on the right position.

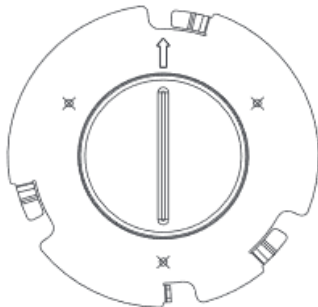


Figure 3: Wall Mount - Step 1

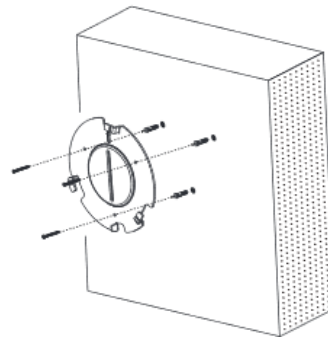


Figure 4: Wall Mount - Step 2

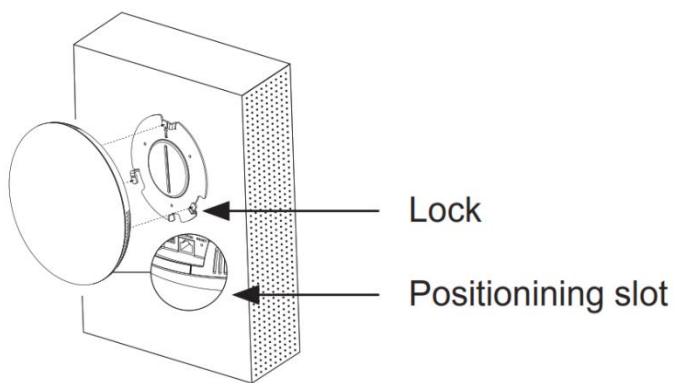


Figure 5: Wall Mount - Step 3

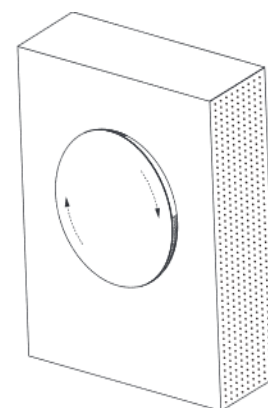


Figure 6: Wall Mount - Step 4

## Ceiling Mount

1. Put the ceiling mounting (metal bracket) in the ceiling's center and mark the position of the three screws holes.
2. Drill a round hole with a diameter of 18mm for Ethernet cable. The distance between its center and the highlighted hole on the plastic bracket should be 35mm.
3. Fix the plastic and metal brackets on the ceiling with flat-head screws and locknuts. Then place and Ethernet cable pass through the 18mm-round hole.
4. Align the position line on device's back cover with the positioning slot. —
5. Rotate the device clockwise until it is locked on the right position.

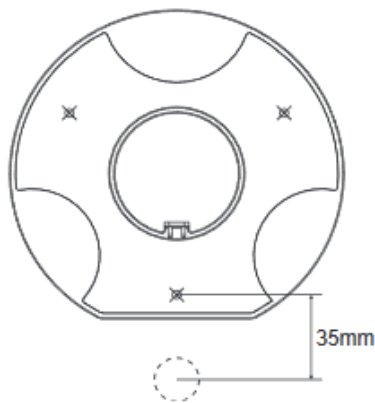


Figure 7: Ceiling Mount - Step 1 & 2

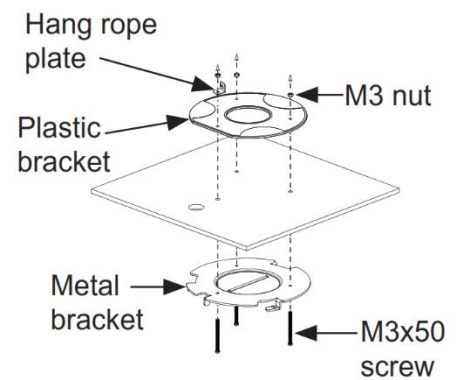


Figure 8: Ceiling Mount - Step 3

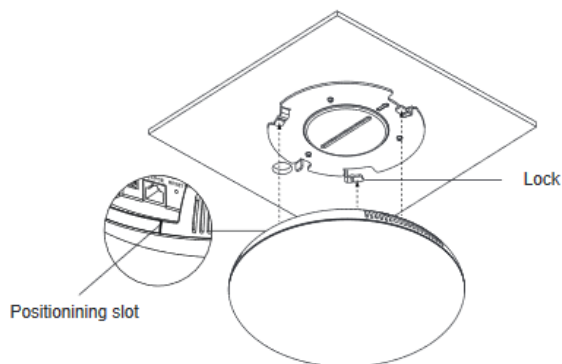


Figure 9: Ceiling Mount - Step 4

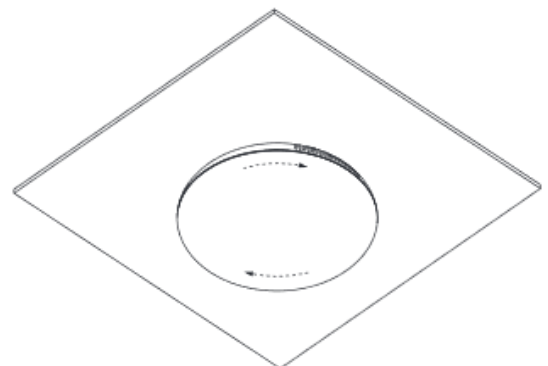


Figure 10: Ceiling Mount - Step 5

## Anti-theft Installation

After the device is assembled with the metal bracket support on the wall or ceiling, use the anti-detachable screw (M3x15) in order to prevent theft.

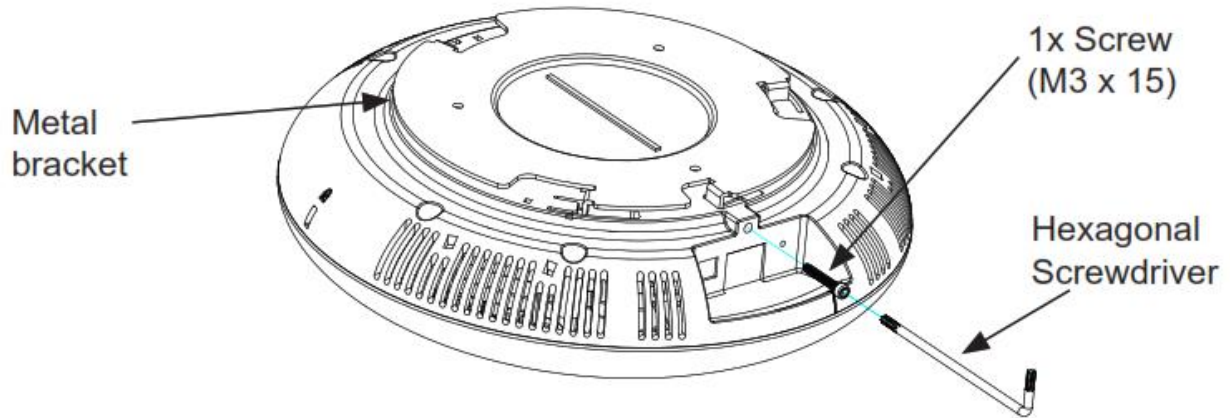


Figure 11: Anti-theft Installation

## Powering and Connecting GSC3510/GSC3505

The GSC3510/GSC3505 can be powered on using PoE/PoE+ switch or PoE injector using following steps:

- **Step 1:** Plug a RJ45 Ethernet cable into the network port of the GSC3510/GSC3505.
- **Step 2:** Plug the other end into the power over Ethernet (PoE) switch or PoE injector.

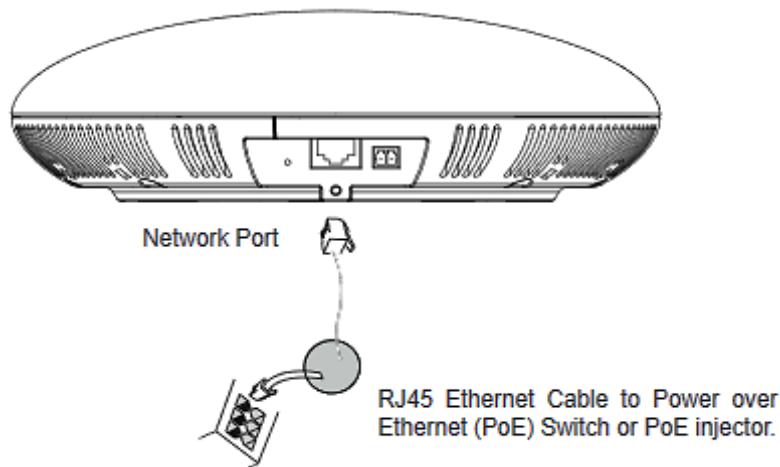


Figure 12: Powering GSC3505/GSC3510

## Connecting Wiring Seat

GSC3505/GSC3510 support to connect a “Key & LED” or “Normal Key” to the 2-pin port via Wiring Seat using following steps:

- **Step 1:** Take the wiring seat from the install kits.
- **Step 2:** Connect the “Key & LED” or “Normal Key” with the wiring seat (as shown in the figure below)

**Note:** This port supports the parallel connection of an incandescent lamp (with less than 1W) or an LED lamp (with less than 100mA).

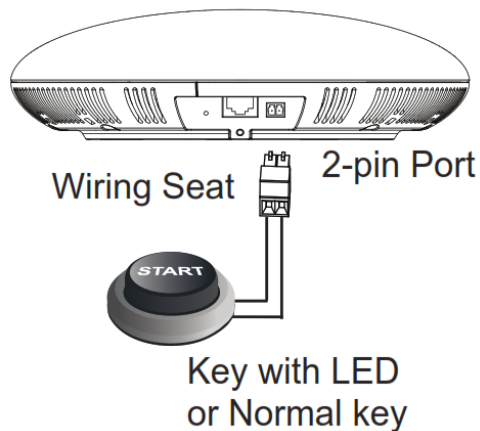


Figure 13: Connecting Wiring Seat

## Access GSC3510/GSC3505 Web GUI

The GSC3510/GSC3505 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the application phone through a Web browser such as Microsoft's IE, Mozilla Firefox, Google Chrome and etc.



**Figure 14: GSC3510 Web GUI – Login**

Users can use a computer connected to the same network as the GSC3510/GSC3505 to discover and access the GSC3510/GSC3505 Configuration Interface using its MAC Address.

Please, refer to the following steps in order to access the GSC3510/GSC3505 Web GUI:

1. Locate the MAC address on the MAC tag of the unit, which is on the underside of the device, or on the package.
2. From a computer connected to same network as the GSC3510/GSC3505, type in the following address using the GSC3510/GSC3505's MAC address on your browser: **https://gsc\_<mac>.local**

**Example:** if a GSC3510/GSC3505 has the MAC address C0:74:AD:xx:xx:xx, this unit can be accessed by typing `https://gsc_c074adxxxxxx.local` on the browser.

## GSC3510/GSC3505 APPLICATION SCENARIOS

### GSC3510/GSC3505 SIP Two-Way/One-Way Intercom System

GSC3510/GSC3505 can be used as an Intercom System using built-in SIP accounts, once the SIP account registered the device can receive paging/intercom calls and it will automatically answer calls coming from whitelisted numbers.

**Note:** GSC3505 is SIP one-way Intercom, while GSC3510 is two-way Intercom.

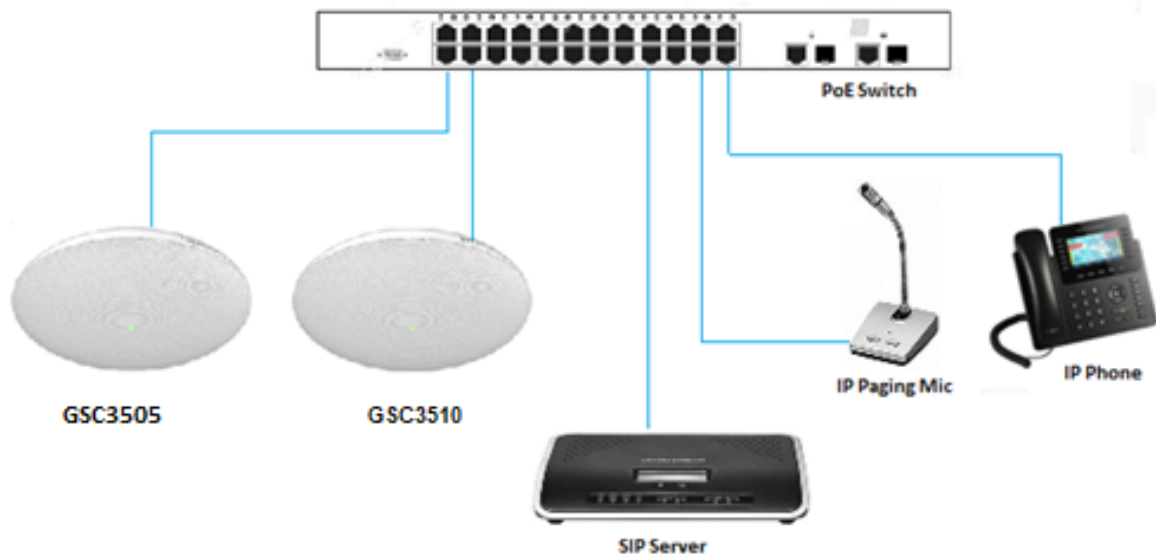


Figure 15: SIP 2-Way/1-Way Paging Diagram

To register a SIP account on the GSC3510/GSC3505 the user needs to go under **Account** → **Account X** → **General Settings**, and enter the account information as below, then save and apply the configuration.

[General Settings](#) | [SIP Settings](#) | [Codec Settings](#) | [Call Settings](#) | [Advanced Settings](#)

---

**Account Registration**

Account Active

Account Name

SIP Server

SIP User ID

SIP Authentication ID

SIP Authentication Password

Display Name

Tel URI

Voice Mail Access Number

**Figure 16: SIP Account Configuration**

Once the account registered correctly, the GSC3510/GSC3505 will show the account status as **“Registered”** under **Status → Account Status**.

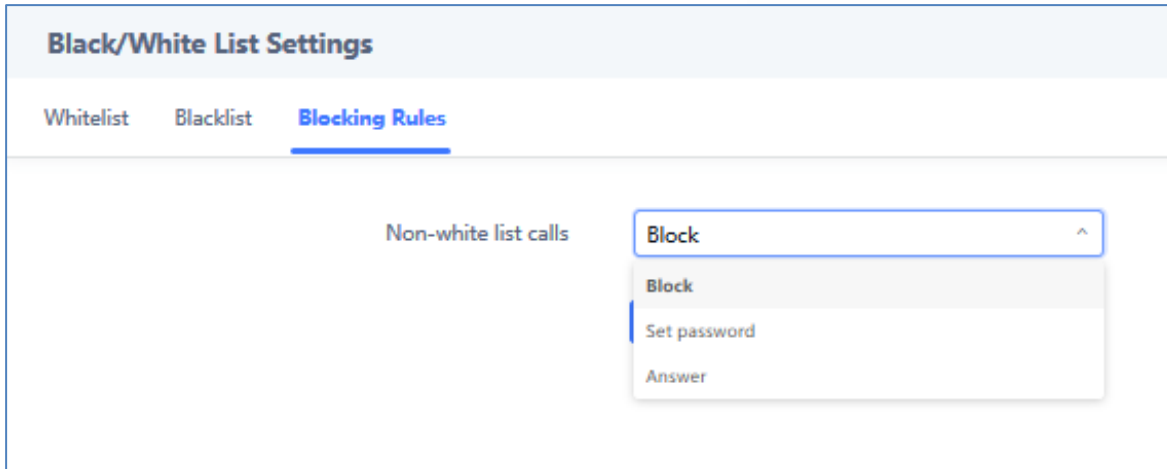
Account Status			
Account	Number	SIP Server	Status
Account 1	1000	192.168.5.161	Registered
Account 2	-	-	Unregistered
Account 3	-	-	Unregistered
Account 4	-	-	Unregistered
Account 5	-	-	Unregistered
Account 6	-	-	Unregistered
Account 7	-	-	Unregistered
Account 8	-	-	Unregistered
Account 9	-	-	Unregistered
Account 10	-	-	Unregistered
Account 11	-	-	Unregistered
Account 12	-	-	Unregistered
Account 13	-	-	Unregistered

**Figure 17: SIP Account Status**

By default, the GSC3510/GSC3505 Blocks non-whitelisted number under **Calls → Black/White List Settings → Blocking Rules**, user needs to either allow Non-White list calls or to set up a Whitelist that contains the number that will be allowed to call the GSC3510/GSC3505.

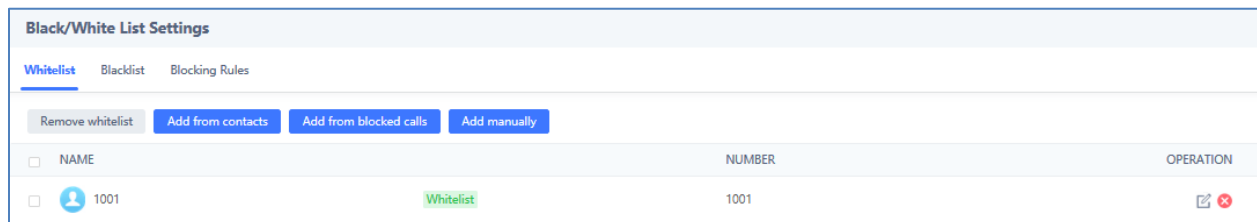






**Figure 18: Default Blocking Rules**

On the screenshot below, only number 1001 is allowed to call GSC3510/GSC3505:



**Figure 19: Whitelisted Devices**

As soon as a SIP call is received by the GSC3510/GSC3505, it first checks if the Caller ID number is allowed on the Whitelist and then answers automatically.

**Notes:**

- GSC3510/GSC3505 is an intercom system and auto-answers all whitelisted numbers.
- By default, GSC3510/GSC3505 plays a Warning tone when auto answering incoming calls, this warning tone can be disabled under **Account** → **Account X** → **Call Settings**, “Play Warning Tone for Auto Answer Intercom”.



## Multicast Paging Application

Multicast paging is an approach to let different SIP users to listen for paging calls from a common multicast IP address. In multicast page call, an audio connection will be set up from sender to receiver, but the receiver will be only able to receive audio, a one-way communication. The 2 entities, Sender/Receiver, must be located on same LAN (same broadcast domain).

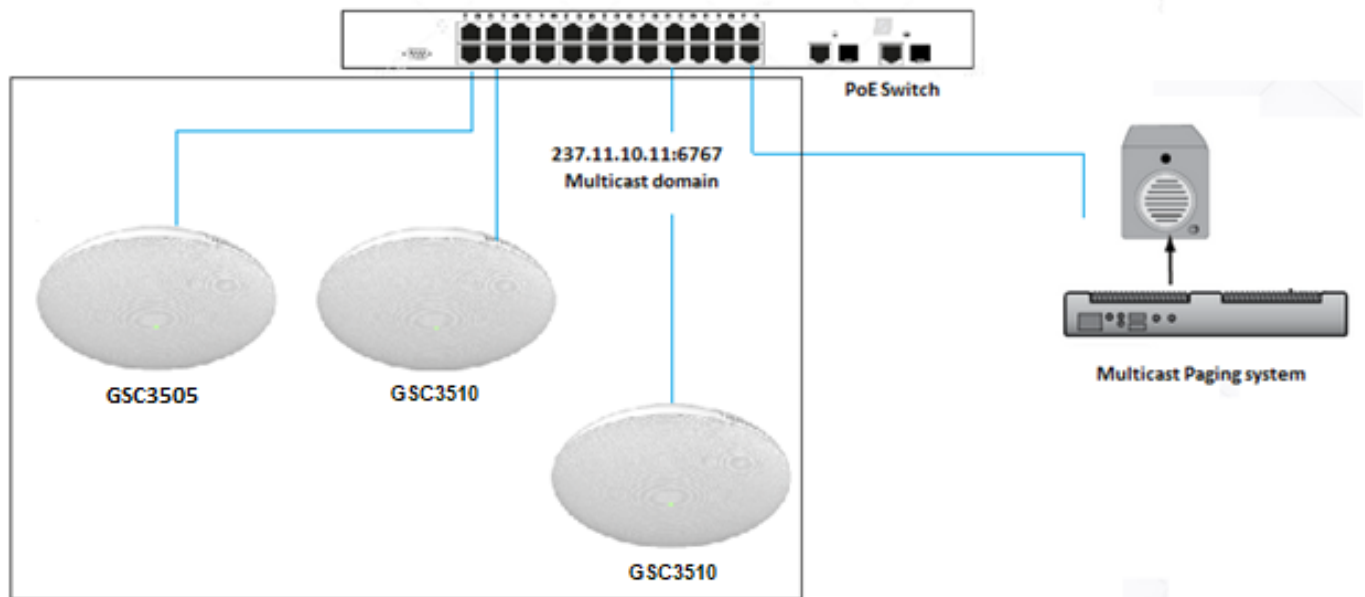


Figure 20: Multicast paging Diagram

To receive multicast page, GSC3510/GSC3505 must be well configured to listen to the right address and port. The configuration is located under **Phone Settings → Multicast Paging**. Up to 10 listening addresses are supported with priority levels from 1 to 10.

**Note:** Multicast paging configuration requires a reboot to take effect.

### Multicast Paging

Multicast Paging
Multicast Listening

Priority	Listening Address		Label
1	<input type="text" value="237.11.10.11:6767"/>	?	<input type="text" value="Sales"/>
2	<input type="text" value="237.11.10.11:6768"/>	?	<input type="text" value="Support"/>
3	<input type="text" value="237.11.10.11:6769"/>	?	<input type="text" value="HR"/>
4	<input type="text" value="237.11.10.11:6770"/>	?	<input type="text" value="Management"/>
5	<input type="text" value="237.11.10.11:6771"/>	?	<input type="text" value="Marketing"/>
6	<input type="text" value="237.11.10.11:6772"/>	?	<input type="text" value="Production"/>
7	<input type="text" value="237.11.10.11:6773"/>	?	<input type="text" value="Finance"/>
8	<input type="text" value="237.11.10.11:6774"/>	?	<input type="text" value="Accounting"/>
9	<input type="text" value="237.11.10.11:6775"/>	?	<input type="text" value="Developers"/>
10	<input type="text" value="237.11.10.11:6776"/>	?	<input type="text" value="Direction"/>

**Figure 21: Multicast Paging Listening Addresses**

In above screenshot, Listening Address “237.11.10.11:6767” with label “Sales” has the highest priority.

Users can enable “Paging Priority Active” option (under Multicast Paging tab) to accept incoming paging calls during active multicast paging. The paging call with higher priority than active one will be accepted.

### Multicast Paging

Multicast Paging
Multicast Listening

Paging Barge ?

Disable

Paging Priority Active ?

Multicast Paging Codec ?

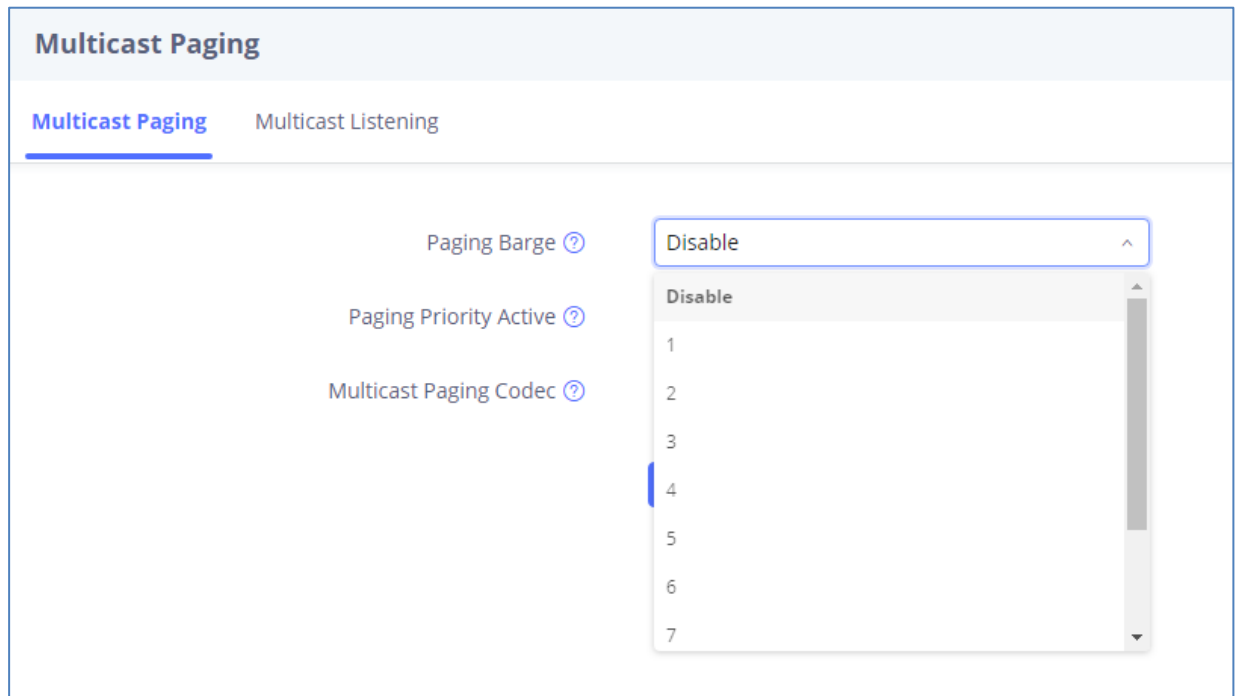
PCMU

**Figure 22: Multicast Paging – Paging Priority Active**



In the case of receiving a multicast paging call while on a unicast SIP call, the GSC3510/GSC3505 can choose to either keep the SIP call or to hold this last and allow the multicast call depending on paging call priority.

This is can be set using “Paging Barge” option. If the option is set to “Disabled” all incoming multicast paging calls will be dropped while on a SIP call. If the multicast paging call has higher priority than the value set on “Paging Barge”, the SIP call will be put on hold and GSC3510/GSC3505 will the incoming multicast paging.



**Figure 23: Multicast Paging - Priority Barge**

## Bluetooth Speaker

The GSC3510/GSC3505 can be used as a Bluetooth speaker for another device and it needs to be connected via Bluetooth to that device. Users need to turn on GSC3510/GSC3505's Bluetooth function first. The first time when using a new Bluetooth device with the GSC3510/GSC3505, "pair" the device with GSC3510/GSC3505 so that both devices know how to connect securely to each other.

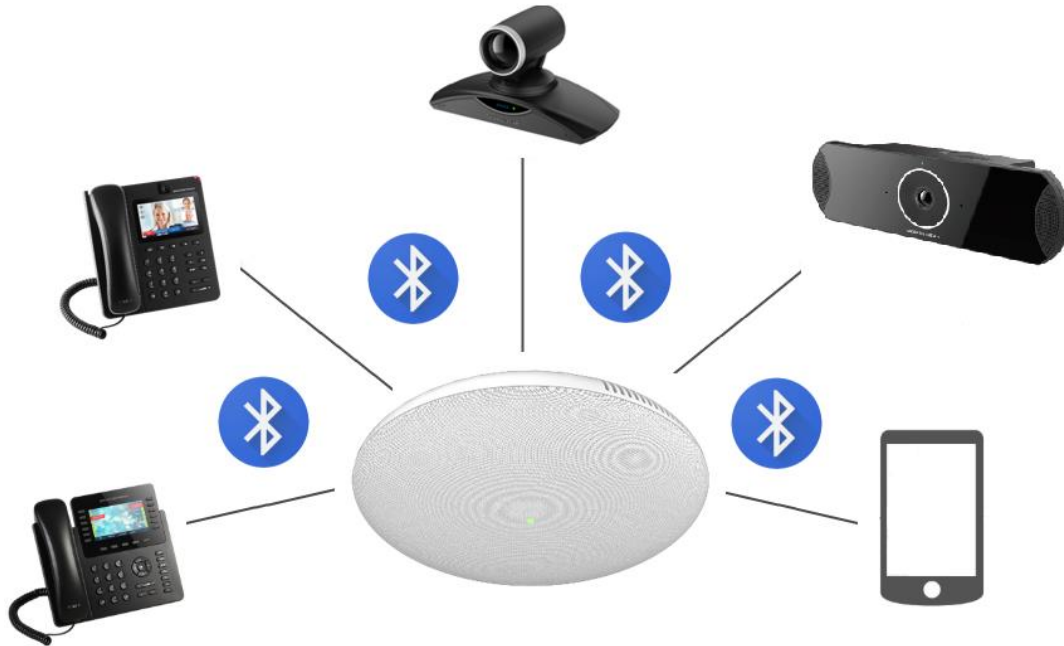


Figure 24: Connecting the GSC3510/GSC3505 as a Bluetooth Speaker

Please, refer to the following steps in order to pair and connect the GSC3510/GSC3505 to the device:

1. Go to GSC3510/GSC3505 Web GUI → Network Settings → Bluetooth Settings.
2. Enable "Bluetooth Settings" function, and enable the option "Visible to Nearby Bluetooth Device" in order to make the GSC3510/GSC3505 visible for other devices for 2 minutes (When the 2 minutes are achieved, and you still didn't connect it, please enable again the option to keep it visible)
3. Go to your Device's Bluetooth settings in order to search for visible devices. The GSC3510/GSC3505 is going to be listed within the visible devices with the "Device Name" configured on the Web GUI.
4. Click on the GSC3510/GSC3505 device's name in order to pair and connect it to the device

**Note:** The GSC3510/GSC3505 will only play the role of a speaker when it is connected to another device via Bluetooth. Users cannot use the GSC3510/GSC3505 to take control of calls made/received by the device connected to it.

## 2-pin Multi-Purpose Input Applications

GSC3510/GSC3505 supports 2-pin multi-purpose input that can connect a “Key with LED” or “Normal Key”. By configuring the sensor settings users can enable the GSC3510/GSC3505 to play an audio file (.wav/.mp3 format), trigger a SIP call to a pre-configured extension, or to start recording audio locally when triggered.

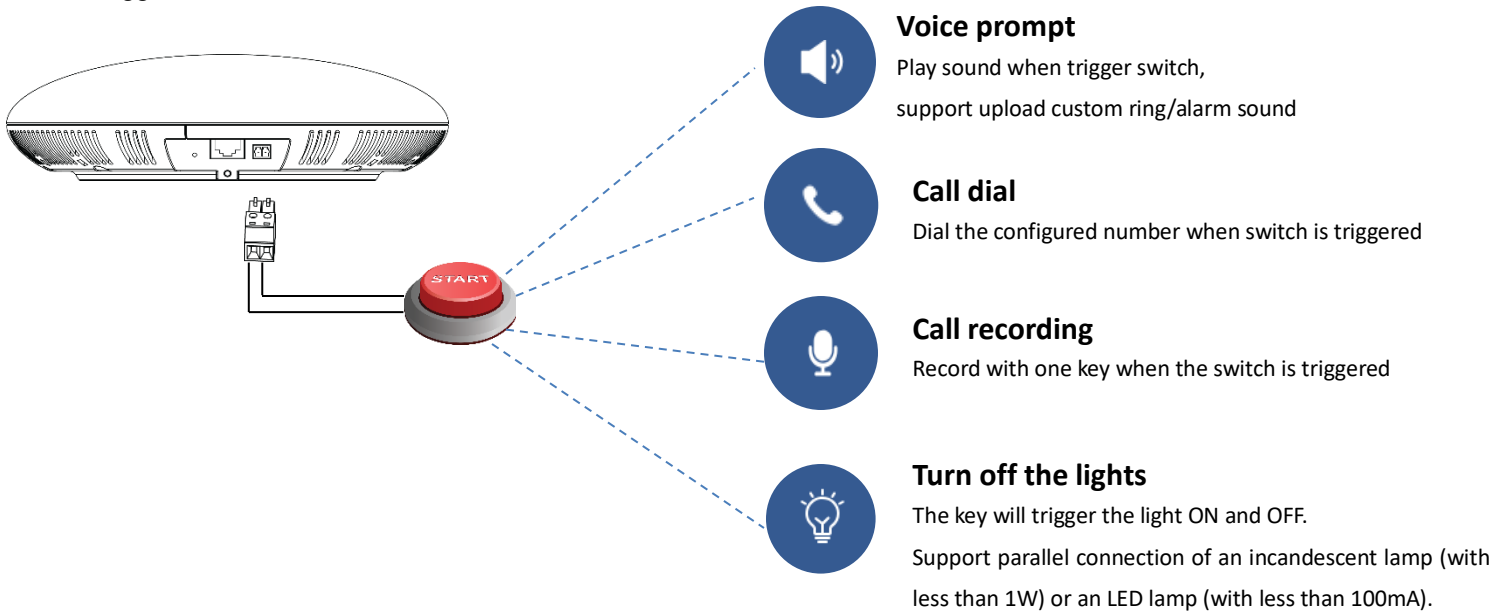


Figure 25: 2-pin Multi-Purpose Input Applications

To configure sensor settings, access to web UI → System Settings → Sensor Setting.

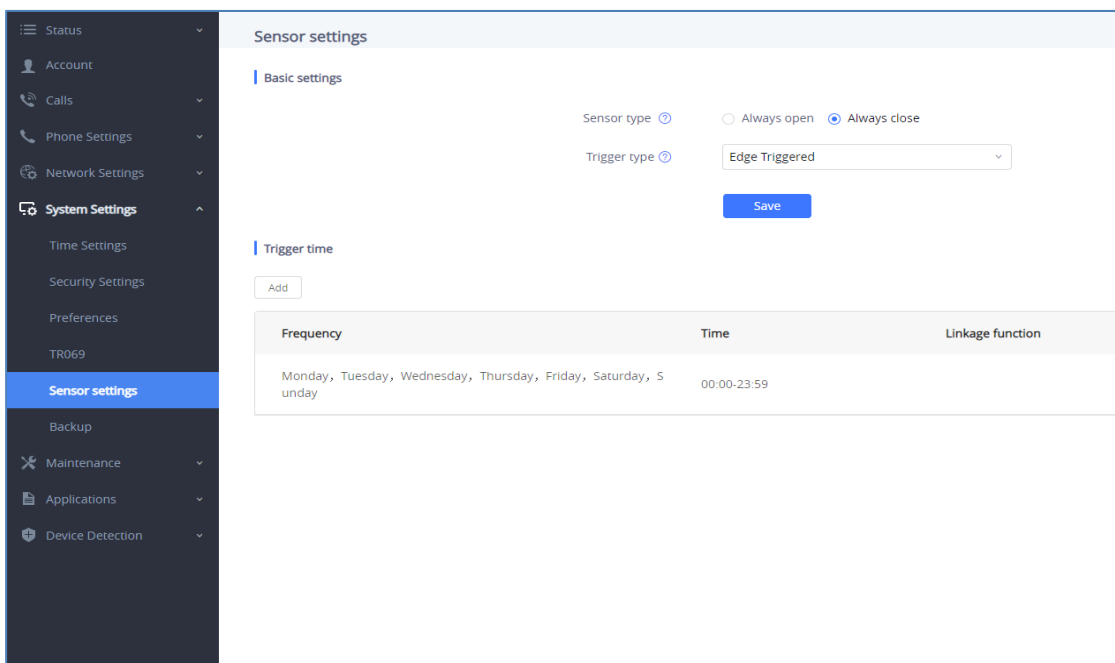


Figure 26: Sensor Settings

Under Basic Setting section, users can set “Sensor Type” and “Trigger Type”.

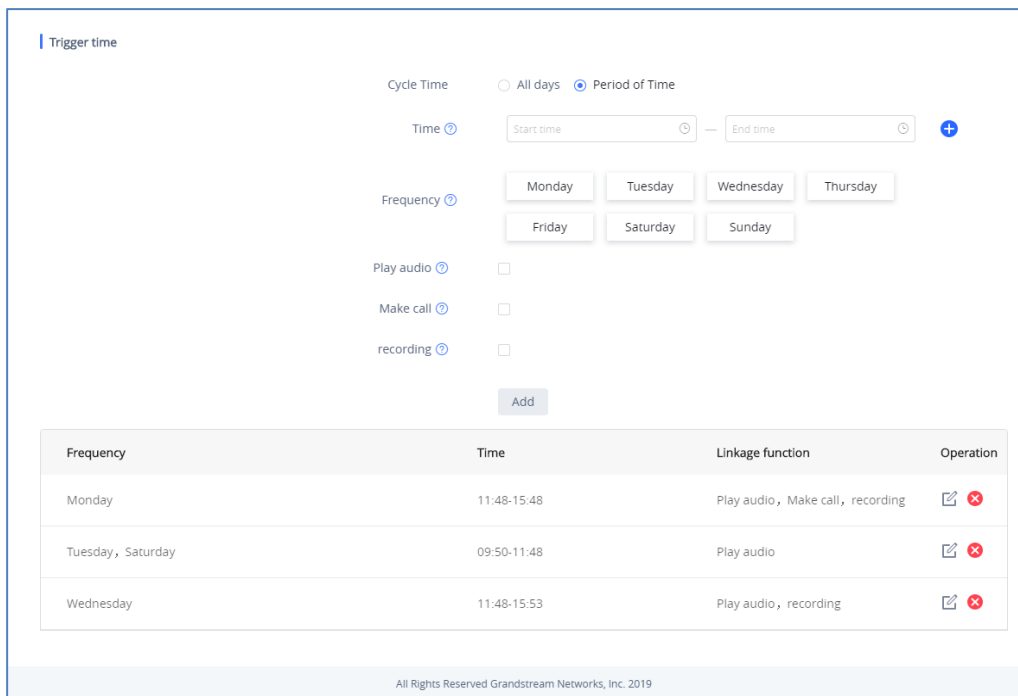
Two states are supported by the Input circuit for the “**Sensor Type**”:

1. **Normally Open** where the contact is disconnected when there is no electricity
2. **Normally Close** where the contact is connected when there is no electricity.

Users could set “**Trigger Type**” to:

1. **Edge Triggered:** When selected, the notification is triggered only when the level changes (high level to low level, or low level to high level).
2. **Level Triggered:** When selected, only high level (1) will trigger the notification.

Under “Trigger time” section, users can click on “**Add**” in order to configure different schedules and a trigger profile for each one as shown in the figure below:

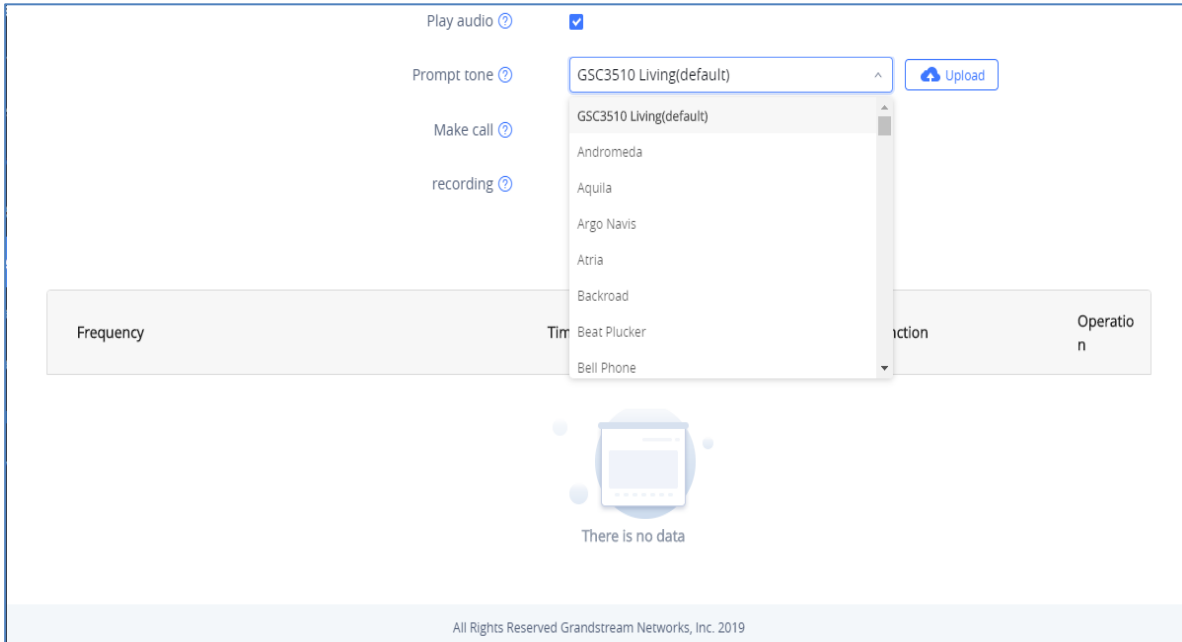


Frequency	Time	Linkage function	Operation
Monday	11:48-15:48	Play audio, Make call, recording	
Tuesday, Saturday	09:50-11:48	Play audio	
Wednesday	11:48-15:53	Play audio, recording	

All Rights Reserved Grandstream Networks, Inc. 2019

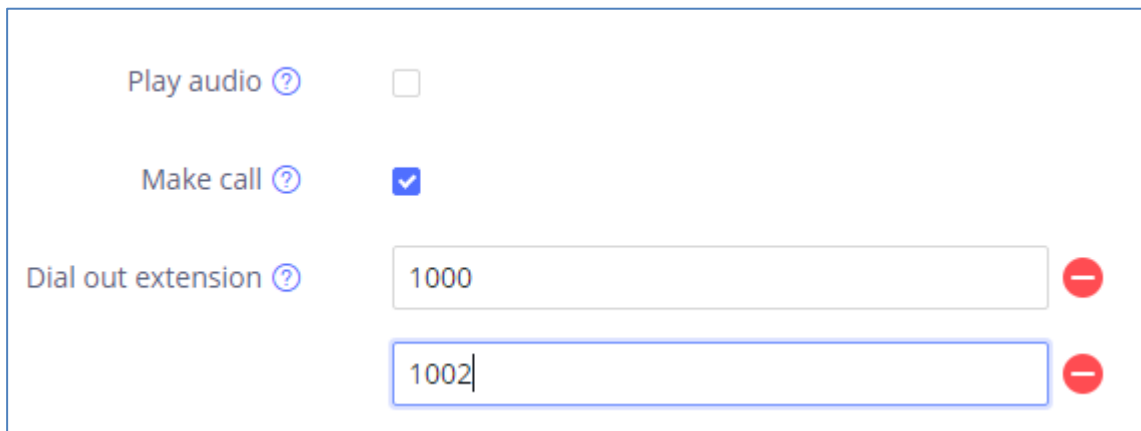
**Figure 27: Sensor Setting – Trigger time**

- **Cycle Time:** The alarm can be configured to be triggered all days of the week, in this case “**All days**” option needs to be checked. Or to some specific days of the week with Start and End time, in this case “**Period of Time**” option needs to be checked for users to be able to configure **Time** and **Frequency** options.
- **Play Audio:** If checked, GSC3510/GSC3505 will play a sound when the switch is triggered during the schedule. Users can select a “Prompt Tone” from available tones or upload a customized tone.



**Figure 28: Sensor Setting - Linkage Function - Play Audio**

- **Make Call:** If checked, GSC3510/GSC3505 will dial out configured numbers on “Dial out extension” fields (up to 2 numbers supported) when the switch is triggered during the schedule.



**Figure 29: Sensor Setting - Linkage Function - Make Call**

- **Recording:** If selected, GSC3510/GSC3505 will record audio using built-in microphones. Recorded files can be found under **Applications → Recording**

**Note:** Up to 7 different Alarm Schedule/Linkage function can be configured in the GSC3510/GSC3505. the list of schedules and linkage functions will be shown in the lower section of the page (as shown in figure **Figure 27: Sensor Setting – Trigger time**), users can edit or delete the Alarm schedule by clicking on **Edit** or **Delete** buttons respectively.





## GSC3510/GSC3505 WEB GUI SETTINGS

The GSC3510/GSC3505 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the application phone through a Web browser such as Microsoft's IE, Mozilla ,Firefox, Google Chrome and etc.

### Status Page Definitions

#### Account Status

<b>Account</b>	16 SIP accounts on the device.
<b>Number</b>	SIP User ID for the account.
<b>SIP Server</b>	URL or IP address, and port of the SIP server.
<b>Status</b>	Registration status for the SIP account.

#### 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>NAT Type</b>	Type of NAT connection used by the device.
<b>Address Type</b>	Configured address type: DHCP, Static IP or PPPoE.
<b>IPv4 Address</b>	IP address of the device.
<b>Subnet Mask</b>	Subnet mask of the device.
<b>Default Gateway</b>	Default gateway of the device.
<b>DNS Server 1</b>	DNS Server 1 of the device.
<b>DNS Server 2</b>	DNS Server 2 of the device.
<b>IPv6 Address Type</b>	Configured address type: DHCP, Static IP or PPPoE.
<b>IPv6 Address</b>	IPv6 address of the device.
<b>IPv6 DNS Server 1</b>	IPv6 DNS Server 1 of the device.
<b>IPv6 DNS Server 2</b>	IPv6 DNS Server 2 of the device.



## System Info

<b>Product Model</b>	Product model of the device: GSC3510/GSC3505.
<b>Hardware Revision</b>	Hardware version number.
<b>Part Number</b>	Product part number.
<b>System Version</b>	Firmware version ID. This is the main software release version, which is used to identify the software system of the device.
<b>Recovery Version</b>	Recovery image version.
<b>Boot Version</b>	Boot code version.
<b>Kernel Version</b>	The kernel version.
<b>System Up Time</b>	System up time since the last reboot.

## Account Page Definitions

GSC3510/GSC3505 has 16 independent SIP accounts. Each SIP account has an individual configuration page.

### General Settings

Account Registration	
<b>Account Active</b>	Indicates whether the account is active. 1 <sup>st</sup> account active by default.
<b>Account Name</b>	Configures the name associated with each account.
<b>SIP Server</b>	Specifies the URL or IP address, and port of the SIP server. This should be provided by VoIP service provider (ITSP).
<b>SIP User ID</b>	Configures user account information provided by your VoIP service provider (ITSP). It's usually in the form of digits similar to phone number or actually a phone number.
<b>SIP Authentication ID</b>	Configures the SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
<b>SIP Authentication Password</b>	Configures the account password required for the device to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purpose.
<b>Display Name</b>	Configures the subscriber's name (optional) that will be used for Caller ID display.
<b>Tel URI</b>	Indicates E.164 number in "From" header by adding "User=Phone" parameter or using "Tel:" in SIP packets, if the device has an assigned PSTN Number.



	<ul style="list-style-type: none"> <li>• <b>Disabled:</b> Will use "SIP User ID" information in the Request-Line and "From" header.</li> <li>• <b>User=Phone:</b> "User=Phone" parameter will be attached to the Request-Line and "From" header in the SIP request to indicate the E.164 number. If set to "Enable".</li> <li>• <b>Enabled:</b> "Tel:" will be used instead of "sip:" in the SIP request.</li> </ul> <p>Please consult your carrier before changing this parameter. Default is "Disabled".</p>
--	--

### Network Settings

<b>Outbound Proxy</b>	Configures the IP address or the domain name of the primary outbound proxy, media gateway or session border controller. It's used by the device 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>Secondary Outbound Proxy</b>	Sets IP address or domain name of the secondary outbound proxy, media gateway or session border controller. The device will try to connect the Secondary outbound proxy only if the primary outbound proxy fails.
<b>DNS Mode</b>	<p>Defines which DNS service will be used to lookup IP address for SIP server's hostname. There are three modes:</p> <ul style="list-style-type: none"> <li>• A Record</li> <li>• SRV</li> <li>• NATPTR/SRV</li> </ul> <p>To locate the server by DNS SRV set this option to "SRV" or "NATPTR/SRV". Default setting is "A Record".</p>
<b>DNS SRV Fail-over Mode</b>	<p>The option will decide which IP is going to be used in sending subsequent SIP packets (ex: Register refresh requests) after the list of IPs for SIP server host is resolved with DNS SRV.</p> <ul style="list-style-type: none"> <li>• <b>Default (prefer server with lowest SRV priority):</b></li> </ul> <p>The device will always prefer to send SIP requests to the available server having the lowest priority, and in case it's down it contacts the next one, but once the server having lowest priority is UP again, the device will switch over to this one.</p> <ul style="list-style-type: none"> <li>• <b>Saved one until DNS TTL (Stay on responding IP until DNS timeout):</b></li> </ul>



	<p>On this mode, the device will resolve DNS SRV records and tries to send the request to the server having lowest priority and if it doesn't respond, it will move on to the next IP until one of the servers responds, once this happen the device will keep contacting this responding IP until DNS timeout (30 minutes) before starting over.</p> <ul style="list-style-type: none"><li>• <b>Saved one until no response (Stay on responding IP until its failure):</b></li></ul> <p>On this mode, the device will send SIP requests to the last responding IP, and it doesn't failover/switchover to the next one until this responding server is down.</p>
<b>NAT Traversal</b>	<p>Specifies which NAT traversal mechanism will be enabled on the device. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"><li>• NAT NO</li><li>• STUN</li><li>• Keep-alive</li><li>• UPnP</li><li>• Auto</li><li>• OpenVPN</li></ul> <p>If the outbound proxy is configured and used, it can be set to "NAT NO". If set to "STUN" and STUN server is configured, the device will periodically send STUN message to the SUTN server to get the public IP address of its NAT environment and keep the NAT port open. STUN will not work if the NAT is symmetric type.</p> <p>If set to "Keep-alive", the device will send the STUN packets to maintain the connection that is first established during registration of the device. The "Keep-alive" packets will fool the NAT device into keeping the connection open and this allows the host server to send SIP requests directly to the registered phone.</p> <p>If it needs to use OpenVPN to connect host server, it needs to set it to "VPN". If the firewall and the SIP device behind the firewall are both able to use UPnP, it can be set to "UPnP". The both parties will negotiate to use which port to allow SIP through. The default setting is "Keep-alive".</p>
<b>Proxy-Require</b>	<p>Adds the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server.</p>



## SIP Settings

SIP Basic Settings	
<b>SIP Registration</b>	Allows the device to send SIP REGISTER messages to the proxy/server. The default setting is "Yes".
<b>Unregister before New Registration</b>	<p>Controls whether to clear SIP user's information by sending un-register request to the proxy server.</p> <ul style="list-style-type: none"> <li>When set to "All", the un-registration is performed by sending a REGISTER message with "Contact" header set to * and Expires=0 parameters to the SIP server when the device starts pre-registration after rebooting.</li> <li>If set to "Instance", the device only cleans the current SIP user's info by sending REGISTER message with "Contact" header set to concerned SIP user's info and Expires=0 parameters to the SIP server.</li> </ul> <p>The default setting is "Instance".</p>
<b>Register Expiration (m)</b>	Configures the time period (in minutes) in which the device refreshes its registration with the specified registrar. The default setting is 60. The maximum value is 64800 (about 45 days).
<b>Subscribe Expiration (m)</b>	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified register. The maximum value is 64800 (about 45 days).
<b>Re-register before Expiration (s)</b>	Specifies the time frequency (in seconds) that the device sends re-registration request before the Register Expiration. The default setting is 0. The range is from 0 to 64,800.
<b>Registration Retry Wait Time (s)</b>	Configures the time period (in seconds) in which the device will retry the registration process in the event that is failed. The default setting is 20. The maximum value is 3600 (1 hour).
<b>Add Auth Header On RE-REGISTER</b>	<p>Configure if the SIP account needs to add Auth header in RE-REGISTER.</p> <ul style="list-style-type: none"> <li>If the option is checked, device will always add authentication header in REGISTER.</li> <li>If the option is unchecked, device will only send authentication for the first REGISTER.</li> </ul>
<b>Enable SIP OPTIONS Keep Alive</b>	Enables SIP OPTIONS to track account registration status so the device will send periodic OPTIONS message to server to track the connection status with the server. The default setting is "No".



<b>SIP OPTIONS Keep Alive Interval (s)</b>	Configures the time interval when the device sends OPTIONS message to SIP server. The default value is 30 seconds, in order to send an OPTIONS message to the server every 30 seconds. The default range is 1-64800.
<b>SIP OPTIONS Keep Alive Maximum Tries</b>	Configures the maximum times of sending OPTIONS message consistently from the device to server. Phone will keep sending OPTIONS messages until it receives response from SIP server. The default setting is "3", which means when the device sends OPTIONS message for 3 times, and SIP server does not respond this message, the device will send RE-REGISTER message to register again. The valid range is 3-10.
<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. Do not use the privacy header fields by default in Huawei IMS mode. If set to "Yes", the Privacy Header will always show in INVITE. If set to "No", the Privacy Header will not show in INVITE.
<b>Use P-Preferred-Identity Header</b>	Controls whether the P-Preferred-Identity header will present in the SIP INVITE message or not, whether the header contains the caller info. Do not use the P-Preferred-Identity header fields by default in Huawei IMS mode. 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>SIP Transport</b>	Determines which network protocol will be used to transport the SIP message. It can be selected from TCP/UDP/TLS. Default setting is "UDP".
<b>Local SIP Port</b>	Determines the local SIP port used to listen and transmit. The default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4, 5068 for Account 5, and 5070 for Account 6. The valid range is from 5 to 65535.
<b>SIP URI Scheme When Using TLS</b>	Defines which SIP header, "sip" or "sips", will be used if TLS is selected for SIP Transport. The default setting is "sip".
<b>Use Actual Ephemeral Port in Contact with TCP/TLS</b>	Determines the port information in the Via header and Contact header of SIP message when the device use TCP or TLS. If set to No, these port numbers will use the permanent listening port on the device. Otherwise, they will use the ephemeral port for the particular connection. The default setting is "No".



<b>Support SIP Instance ID</b>	Determines if the device will send SIP Instance ID. The SIP instance ID is used to uniquely identify the device. If set to "Yes", the SIP Register message Contact header will include +sip.instance tag. Default is "Yes".
<b>SIP T1 Timeout</b>	Defines an estimate of the round-trip time of transactions between a client and server. If no response is received in T1, the figure will increase to 2*T1 and then 4*T1. The request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 sec.
<b>SIP T2 Interval</b>	Specifies the maximum retransmit time of any SIP request messages (excluding the SIP INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. The default setting is 4 sec.
<b>SIP Timer D Interval</b>	Defines the amount of time that the server transaction can remain when unreliable response (3xx-6xx) received. The valid value is 0-64 seconds. The default value is 0.
<b>Remove OBP from Route</b>	Configures the device to remove the outbound proxy URI from the Route header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall. If it is set to "Yes", it will remove the Route header from SIP requests. The default setting is "No".
<b>Enable 100rel</b>	Activates PRACK (Provisional Acknowledgment) method. PRACK improves the network reliability by adding an acknowledgement system to the provisional Responses (1xx). It is set to "Yes", the device will response to the 1xx response from the remote party. Default is "No".
<b>Session Timer</b>	
<b>Enable Session Timer</b>	Allows the device to use the session timer, when set to "Yes", it will be added in the SIP INVITE message to notify the server.
<b>Session Expiration (s)</b>	Configures the device's SIP session timer. It 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 (s)</b>	Determines the minimum session expiration timer (in seconds) if the device act as a timer refresher. Default is 90. The valid range is from 90 to 64800.
<b>UAC Specify Refresher</b>	Sets which party will refresh the active session if the device makes outbound calls. If it is set to "UAC" and the remote party does not support Refresher feature, the device will refresh the active session.



	If it is set to "UAS", the remote party will refresh it. If it is set to "Omit", the header will be omitted so that it can be selected by the negotiation mechanism. The default setting is "Omit".
<b>UAS Specify Refresher</b>	Specifies which party will refresh the active session if the device receives inbound calls. If it is set to "UAC", the remote party will refresh the active session. If it is set to "UAS" and the remote party does not support refresh feature, the device will refresh it. The default setting is "UAC".
<b>Caller Request Timer</b>	Sets the caller party to act as refresher by force. If set to "Yes" and both party support session timers, the device will enable the session timer feature when it makes outbound calls. The SIP INVITE will include the content "refresher=uac". The default setting is "No".
<b>Callee Request Timer</b>	Sets the callee party to act as refresher by force. If set to "Yes" and the both parties support session timers, the device will enable the session timer feature when it receives inbound calls. The SIP 200 OK will include the content "refresher=uas". The default setting is "No".
<b>Force Timer</b>	<p>Configures the session timer feature on the device by force.</p> <ul style="list-style-type: none"> <li>• If it is set to "Yes", the device will use the session timer even if the remote party does not support this feature.</li> <li>• If set to "No", the device will enable the session timer only when the remote party supports this feature. To turn off the session timer, select "No".</li> </ul> <p>The default setting is "No".</p>
<b>Force INVITE</b>	Sets the SIP message type for refresh the session. If it is set to "Yes", the Session Timer will be refreshed by using the SIP INVITE message. Otherwise, the device will use the SIP UPDATE or SIP OPTIONS message. Default is "No".

## Codec Settings

Preferred Vocoder	
<b>Preferred Vocoder</b>	Lists the available and enabled Audio codecs for this account. Users can enable the specific audio codecs by moving them to the selected box and set them with a priority order from top to bottom. This configuration will be included with the same preference order in the SIP SDP message.





<b>Codec Negotiation Priority</b>	Configures the device to use which codec sequence to negotiate as the callee. When set to "Caller", the device negotiates by SDP codec sequence from received SIP Invite; When set to "Callee", the device negotiates by audio codec sequence on the device. The default setting is "Callee".
<b>Use First Matching Vocoder in 200OK SDP</b>	Configures the device to use the first matching codec in the 200OK message. The default value is 0.
<b>iLBC Frame Size</b>	Sets the iLBC (Internet Low Bitrate Codec) frame size if iLBC is used. Users can select it from 20ms or 30ms. The default setting is 30ms.
<b>G726-32 ITU Payload Type</b>	Configures G726-32 payload type for ITU packing mode. Payload 2 is static and payload dynamic is dynamic. The default setting is "2".
<b>G726-32 Dynamic Payload Type</b>	Specifies the G726-32 payload type, and the valid range is 96 to 127. The default setting is "126".
<b>Opus Payload Type</b>	Defines the desired value (96-127) for the payload type of the Opus codec. The default value is 123.
<b>DTMF</b>	<p>Specifies the mechanism to transmit DTMF (Dual Tone Multi-Frequency) signals.</p> <p>There are 3 supported modes: in audio, RFC2833, or SIP INFO.</p> <ul style="list-style-type: none"> <li>• <b>In audio</b>, which means DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs);</li> <li>• <b>RFC2833</b>, which means to specify DTMF with RTP packet. Users could know the packet is DTMF in the RTP header as well as the type of DTMF.</li> <li>• <b>SIP INFO</b>, which uses SIP INFO to carry DTMF. The defect of this mode is that it's easily to cause desynchronized of DTMF and media packet if the SIP and RTP messages are required to transmitted respectively.</li> </ul> <p>The default setting is "RFC2833".</p>
<b>DTMF Payload Type</b>	Configures the RTP payload type that indicates the transmitted packet contains DTMF digits. Valid range is from 96 to 127. Default value is 101.
<b>Jitter Buffer Type</b>	Selects either Fixed or Adaptive based on network conditions.
<b>Enable Audio RED with FEC</b>	If set to "Yes", FEC will be enabled for audio call. The default setting is "No".
<b>Audio FEC Payload Type</b>	Configures audio FEC payload type. The valid range is from 96 to 127. The default value is 121.
<b>Audio RED Payload Type</b>	Configures audio RED payload type. The valid range is from 96 to 127. The default value is 124.



<b>Silence Suppression</b>	Enables the silence suppression/VAD feature. If it is set to “Yes”, when silence is detected, a small quantity of VAD packets (instead of audio packets) will be sent during the period of no talking. If set to “No”, this feature is disabled. The default setting is “No”.
<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>RTP Settings</b>	
<b>SRTP Mode</b>	Sets if the device will enable the SRTP (Secured RTP) mode. It can be selected from dropdown list: <ul style="list-style-type: none"> <li>• <b>Disable</b></li> <li>• <b>Enabled but not forced</b></li> <li>• <b>Enabled and forced</b></li> </ul> SRTP uses encryption and authentication to minimize the risk of denial of service. (DoS). If the server allows to use both RTP and SRTP, it should be configured as “Enabled but not forced”.  The default setting is “Disable”.
<b>SRTP Key Length</b>	Configures all the AES (Advanced Encryption Standard) key size within SRTP. It can be selected from dropdown list: <ul style="list-style-type: none"> <li>• <b>AES128&amp;256 bit</b></li> <li>• <b>AES 128 bit</b></li> <li>• <b>AES 256 bit</b></li> </ul> If it is set to “AES 128&256 bit”, the device will provide both AES 128 and 256 cipher suite for SRTP. If set to “AES 128 bit”, it only provides 128-bit cipher suite; if set to “AES 256 bit”, it only provides 256-bit cipher suite. The default setting is “AES128&256 bit”.
<b>Enable SRTP Key Life Time</b>	Defines the SRTP key life time. When this option is set to be enabled, during the SRTP call, the SRTP key will be valid within $2^{31}$ SIP packets, and phone will renew the SRTP key after this limitation.  The default setting is “Yes”.
<b>RTCP Destination</b>	Configures a remote server URI where RTCP messages will be sent to during an active call.



<b>Symmetric RTP</b>	<p>Configures if the device enables the symmetric RTP mechanism.</p> <p>If it is set to “Yes”, the device will use the same socket/port for sending and receiving the RTP messages.</p> <p>The default setting is "No".</p>
<b>RTP IP Filter</b>	<p>Receives the RTP packets from the specified IP address and Port by communication protocol. If it is set to “IP Only”, the device only receives the RTP packets from the specified IP address based on the communication protocol; if it is set to “IP and Port”, the device will receive the RTP packets from the specified IP address with the specified port based on the communication protocol.</p> <p>The default setting is “Disable”.</p>

## Call Settings

<b>Call Features</b>	
<b>Play Warning Tone for Auto Answer Intercom</b>	<p>When this option is enabled, the device will play a warning tone When auto-answering intercom. The default setting is “yes”.</p>
<b>Send Anonymous</b>	<p>If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous, essentially blocking the Caller ID to be displayed.</p>
<b>Intercept Anonymous Calls</b>	<p>If set to "Yes", anonymous calls will be rejected.</p>
<b>Call Log</b>	<p>Categorizes the call logs saved for this account. If it is set to “Log All”, all the call logs of this account will be saved.</p> <p>If set to “Log Incoming/Outgoing Calls (Missed Calls Not Record)”, the whole call history will be saved other than missed call.</p> <p>If it is set to “Disable Call All”, none of the call history will be saved. If it is set to “Don’t Prompt Missed Call”, the device will log the missed call histories, but there is no prompt to indicate the missed calls.</p> <p>The default setting is “Log All”.</p>
<b>Ring Timeout (s)</b>	<p>Defines the expiration timer (in seconds) for the rings with no answer. The default setting is 60. The valid range is from 10 to 300.</p>
<b>Refer-To Use Target Contact</b>	<p>Sets the device to use the target’s Contact header tag to the Refer-To header in the SIP REFER message during an attended transfer.</p> <p>The default setting is “No”.</p>
<b>Dial Plan</b>	
<b>Dial Plan Prefix</b>	<p>This parameter can be configured to define the prefix added to each dialed number.</p>



<b>Disable DialPlan</b>	<p>Enables/disables the Dial plan mechanism for different cases. If the specific case is checked, the Dial plan mechanism will be disabled.</p> <ul style="list-style-type: none"> <li>• <b>Dial Page:</b> It controls the pattern of dialing numbers from the call page.</li> <li>• <b>Contact:</b> It controls the pattern of dialing numbers from local, LDAP and Broadsoft contacts.</li> <li>• <b>Incoming Call History:</b> It controls the pattern of dialing numbers from inbound call logs.</li> <li>• <b>Outgoing Call History:</b> It controls the pattern of dialing numbers from outbound call logs.</li> </ul>
<b>DialPlan</b>	<p>Configures the dial plan to establish the expected number and pattern of digits for a telephone number. This parameter configures the allowed dial-plan for the device.</p> <p><u>Dial Plan Rules:</u></p> <ol style="list-style-type: none"> <li>1. Accepted Digits: 1,2,3,4,5,6,7,8,9,0 , * , #, A,a,B,b,C,c,D,d,+</li> <li>2. Grammar: x – any digit from 0-9;             <ol style="list-style-type: none"> <li>a) xx+ or xx. – at least 2-digit numbers</li> <li>b) xx – only 2-digit numbers</li> <li>c) ^ - exclude</li> <li>d) [3-5] – any digit of 3, 4, or 5</li> <li>e) [147] – any digit of 1, 4, or 7</li> <li>f) &lt;2=011&gt; - replace digit 2 with 011 when dialing</li> <li>g)   - the OR operand</li> <li>h) \+ - add + to the dialing number</li> </ol> </li> </ol> <ul style="list-style-type: none"> <li>• Example 1: {[369]11   1617xxxxxxx}</li> </ul> <p>Allow 311, 611, and 911 or any 10-digit numbers with leading digits 1617</p> <ul style="list-style-type: none"> <li>• Example 2: {^1900x+   &lt;=1617&gt;xxxxxxx}</li> </ul> <p>Block any number of leading digits 1900 or add prefix 1617 for any dialed 7-digit numbers</p> <ul style="list-style-type: none"> <li>• Example 3: {1xxx[2-9]xxxxxx   &lt;2=011&gt;x+}</li> </ul> <p>Allow any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR allow any length of numbers with leading digit 2, replacing the 2 with 011 when dialed.</p>



3. Default: Outgoing – { x+ | \+x+ | \*x+ | \*xx\*x+ }

Allow any number of digits, OR any number with a leading +, OR any number with a leading \*, OR any number with a leading \* followed by a 2-digit number and a \*.

Example of a simple dial plan used in a Home/Office in the US:

{^1900x. | <=1617>[2-9]xxxxxx | 1[2-9]xx[2-9]xxxxxx | 011[2-9]x. | [3469]11 }

Explanation of example rule (reading from left to right):

- ^1900x. – prevents dialing any number started with 1900
- <=1617>[2-9]xxxxxx – allow dialing to local area code (617) numbers by dialing 7 numbers and 1617 area code will be added automatically
- 1[2-9]xx[2-9]xxxxxx |- allow dialing to any US/Canada Number with 11 digits length
- 011[2-9]x. – allow international calls starting with 011
- [3469]11 – allow dialing special and emergency numbers 311, 411, 611 and 911

**Note:** In some cases, where the user wishes to dial strings such as \*123 to activate voice mail or other applications provided by their service provider, the \* should be predefined inside the dial plan feature. An example dial plan will be: { \*x+ } which allows the user to dial \* followed by any length of numbers.

## Advanced Settings

### Security Settings

<b>Check Domain Certificates</b>	Sets the device to check the domain certificates if TLS/TCP is used for SIP Transport. The default setting is "No".
<b>Validate Certification Chain</b>	Configures whether to validate certification chain, when TLS/TCP is configured for SIP Transport. If this is set to "Yes", phone will validate server against the new certificate list. The default setting is "No".
<b>Validate Incoming SIP Messages</b>	Specifies if the device will check the incoming SIP messages caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
<b>Allow Unsolicited REFER</b>	It is used to configure whether to dial the number carried by Refer-to after receiving SIP REFER request actively.



	<p>If it is set to "Disabled", the device will send error warning and stop dialing. If it is set to "Enabled/Force Auth", the device will dial the number after sending authentication, if the authentication failed, then the dialing will be stopped. If it is set to "Enabled", the device will dial up all numbers carried by SIP REFER. The default is "Disabled".</p>
<b>Only Accept SIP Requests from Known Servers</b>	<p>Answers the SIP request from saved servers when set to "Yes", only the SIP requests from saved servers will be accepted; and the SIP requests from the unregistered server will be rejected. The default setting is "No".</p>
<b>Check SIP User ID for Incoming INVITE</b>	<p>Configures the device to check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it doesn't match the device's SIP User ID, the call will be rejected. The default setting is "No".</p>
<b>Allow SIP Reset</b>	<p>It is used to configure whether to allow SIP Notification message to perform factory reset on the device. The default setting is "No".</p>
<b>Authenticate Incoming INVITE</b>	<p>Configures the device to authenticate the SIP INVITE message from the remote party. If set to "Yes", the device will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. Default is "No".</p>
<b>SIP Realm used for Challenge INVITE &amp; NOTIFY</b>	<p>Configure this item to validate incoming INVITE, but you must enable authenticate incoming INVITE first to make it take effect. You can verify the NOTIFY information for the provision, including check-sync, resync and reboot, but only when SIP NOTIFY authentication enabled first to make it take effect.</p>

## MOH

<b>Upload Local MOH Audio File (Music on Hold)</b>	<p>Loads the MOH file to the device. Click on "Browse" button to upload the music file from local PC. The MOH audio file has to be in .wav or .mp3 format. <b>Note:</b> Please be patient while the audio file is being uploaded. It could take more than 3 minutes to finish the uploading especially the file size is large. The button will show as "Processing" during the uploading. Once done, it will show as "Browse" again. Click on "Save" on the bottom of the web page and "Apply" on the top of the web page to save the change.</p>
<b>Enable Local MOH</b>	<p>Plays local MOH file if the call is being hold by the device. Default is "No".</p>

## Advanced Features

<b>Virtual Account Group</b>	<p>It is used to set to categorize accounts in server mode groups, the accounts in the same group will be combined as one and the account widget will display the Caller ID in the account with lowest ID. The device can answer any incoming calls to each account in groups.</p>
------------------------------	--




	<p>If user makes an outbound call, the device will use the lowest ID account by default. If the account fails or SIP INVITE message is timeout, the device will failover to the next account in the group with higher account ID.</p> <p>If all the accounts are not available in the group, the device will traverse all the accounts in the group and notify the users the session is failed.</p>
<b>Special Feature</b>	<p>Configures phone's settings to meet different vendors' server requirements. Users can choose from Standard, NEC, WorldStone, BroadSoft, China Mobile, ZTE IMS, Mobotix, ZTE NGN, or Huawei IMS depending on the server type.</p>

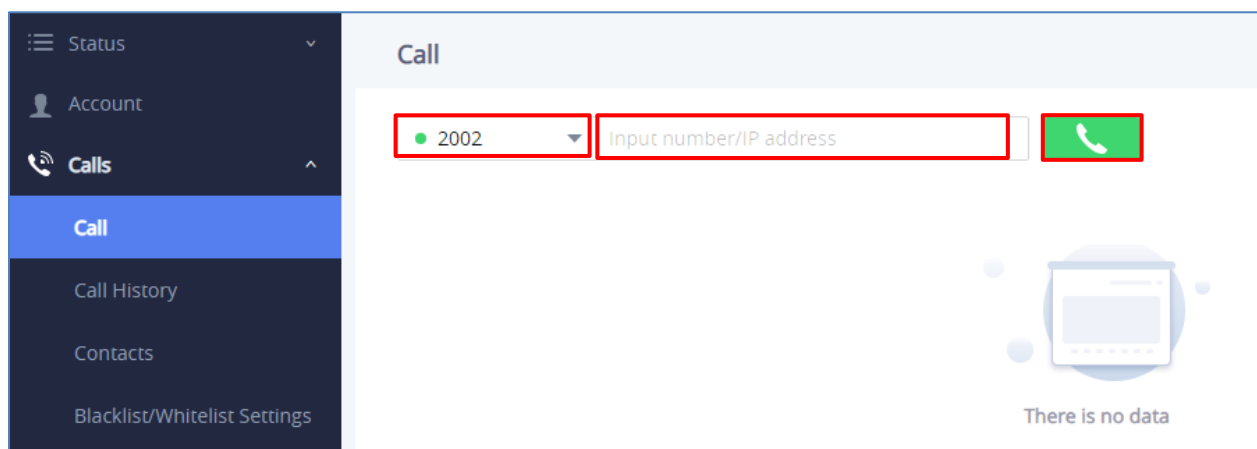
## Calls Page Definition

### Call

***This page is available for the GSC3510 only.***

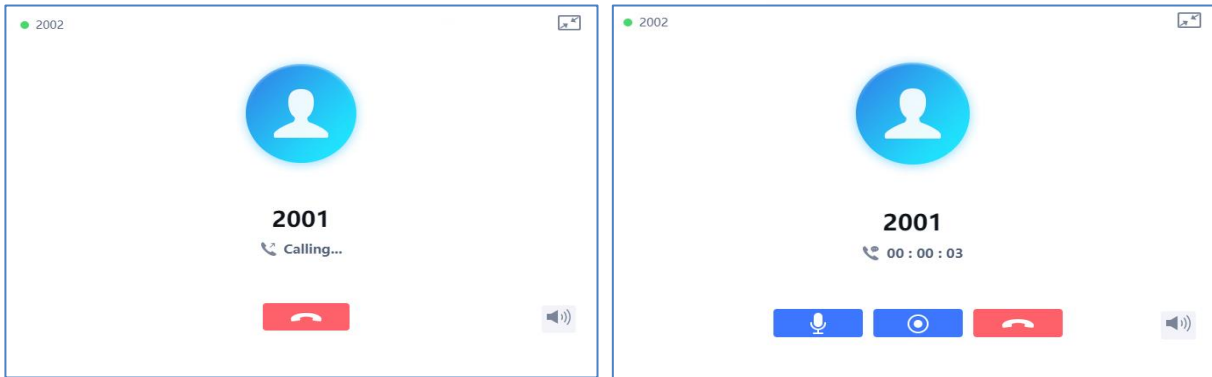
The GSC3510 allows users to manage their calls using the Click to Dial feature which permits to initiate and receive calls using the Web GUI. To use the Click to Dial feature, please refer the following steps:

1. Go under the GSC3510 Web GUI → Calls → Call.
2. Select the account to be used.
3. Type the number / IP Address to call and press **Dial** button  as displayed on the following screenshots:



**Figure 30: Click-to-Dial Feature**

Once the number / IP address is dialed or a Call is received, a window pops up showing the call information and gives the user the ability to do the following operations:



**Figure 31: Outgoing call in progress and accepted**



: Reduce the window to a bar at the top of Web GUI interface.



: Adjust the ringing volume.



: Mute the GSC3510 Mic.



: Start recording the call.



: End the in-progress call.

## Call History

***This page is available for the GSC3510 only.***

The GSC3510 Call History is divided into two sections: “All” and “Intercepted Record”:

### Call History → All

This section shows all the calls that have been made or answered. Users can find two types of calls under “Call History → All”:



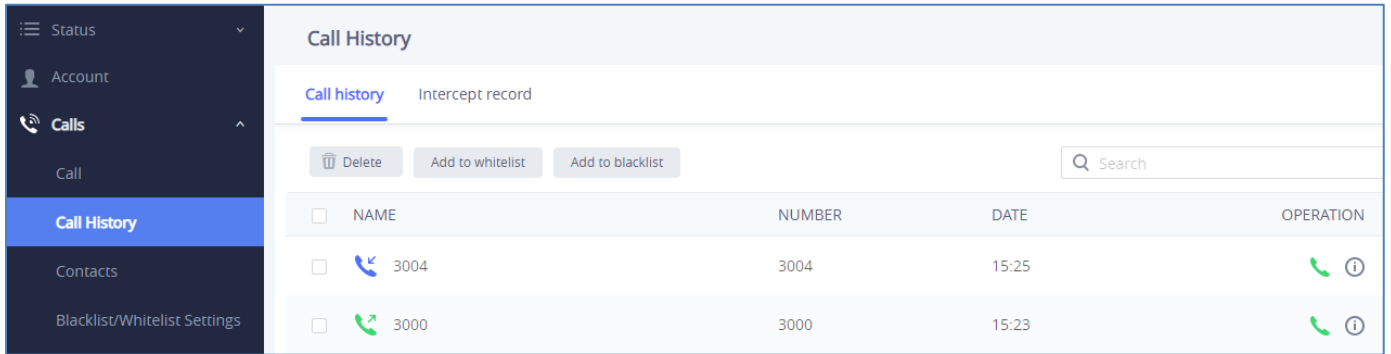
Outgoing Calls.



Answered Calls.









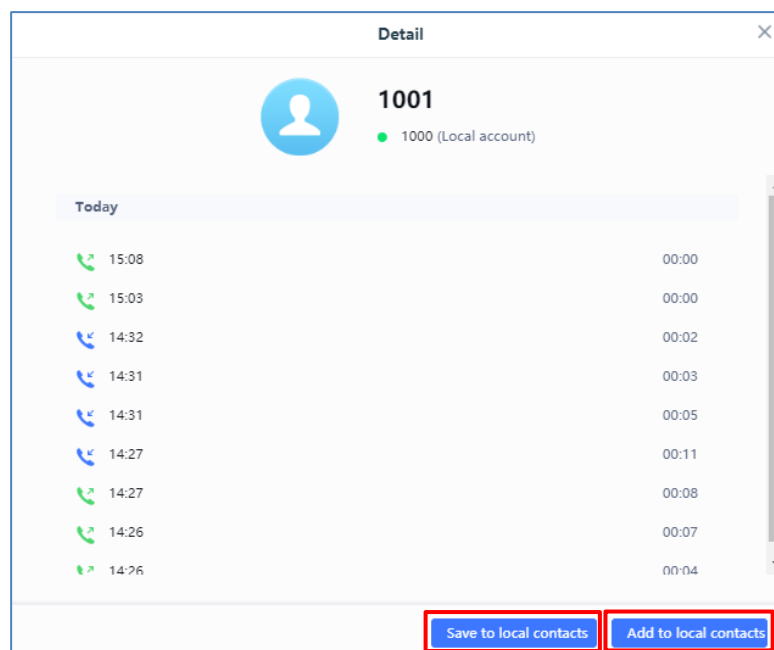
**Figure 32: Call History → All**

By Tapping on the checkbox to select the call history entries, users can do the following operations:

- **Delete Call History:** Users need to press the button **Delete** after selecting the call history entries.
- **Add entries to Whitelist:** Users may select the entries to be allowed to call the GSC3510/GSC3505 by clicking on the button **Add to whitelist** after selecting the right entries.
- **Add entries to Blacklist:** Users can block the calls of some entries by selecting them and pressing the button **Add to blacklist**.

The following operations can be done as well:

- **Make a call to one of the call history entries:** Users can directly make a call to a number listed in the call history by clicking directly on the button  under “OPERATION”.
- **Show calls details:** users can show the calls details of a number by clicking on the button  and a window will pop up to show all the calls sent/received with the selected number.

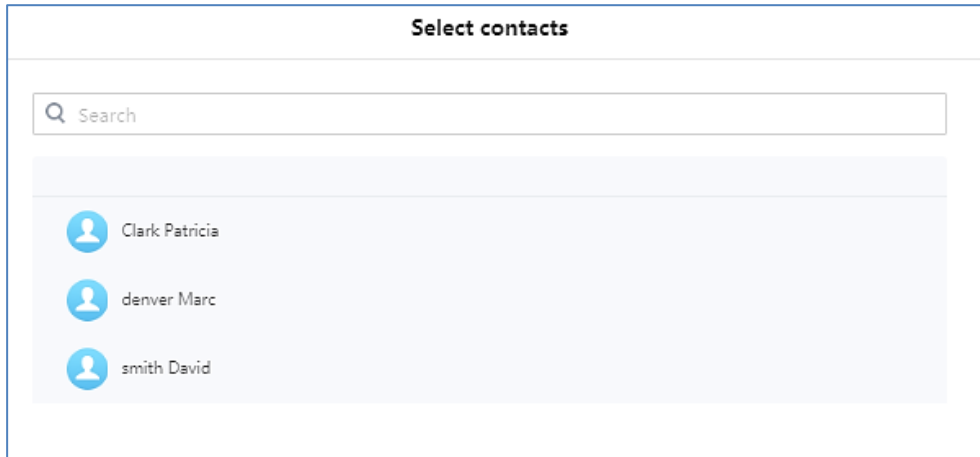


**Figure 33: Call details under Call History → All**



From the Call details window, users can also add the number selected to local contacts by creating a new contact [Add to local contacts](#) , or by adding it to an existing contact [Save to local contacts](#) .

- **Add number to an existing contact:** Users can click on “Save to local contacts” in order to show a window with all the contacts already registered in the GSC3510/GSC3505 local contacts and to choose one of the contacts to link the selected number with:



**Figure 34: Add number from call history to an existing contact**

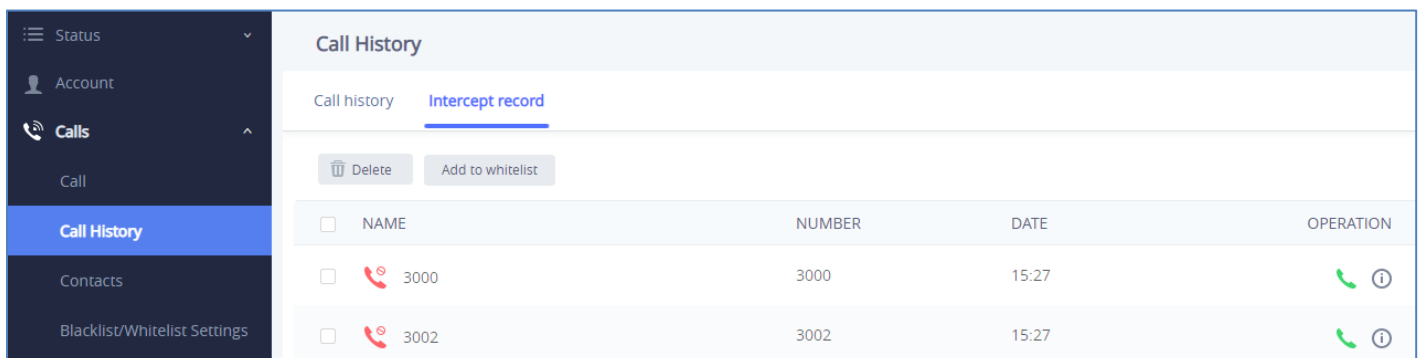
- **Create a new contact:** user can click on “Add to local contacts” in order to show a window where all the information about the contact need to be entered.

**Note:** Please, refer to the next section “**Contacts**” for more information about creating a new contact or editing an existing one.

### Call History → Intercept Record

This section shows all the calls that have been blocked when received because of not having the permission to make a call to the GSC3510/GSC3505. Users can find only one type of calls under “Call History → Intercept Record”:


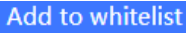
 Blocked Calls





**Figure 35: Call History → Intercept Record**



By checking the checkbox to select entries, users can do the following operations:

- **Delete Blocked Numbers Call History:** Users need to press the button  **Delete** after selecting the call history entries.
- **Add entries to Whitelist:** Users may select the blocked entries to give them permission to call the GSC3510/GSC3505 by clicking on the button  **Add to whitelist** after selecting the right entries.

The following operations can be done as well:

- **Make a call to one of the entries:** Users can directly make a call to a number listed in call history → Intercept Record, by clicking directly on the button  under “OPERATION”.
- **Show calls details:** users can show the calls details of a number by clicking on the button  and a window will pop up to show all the blocked calls received from the selected number.

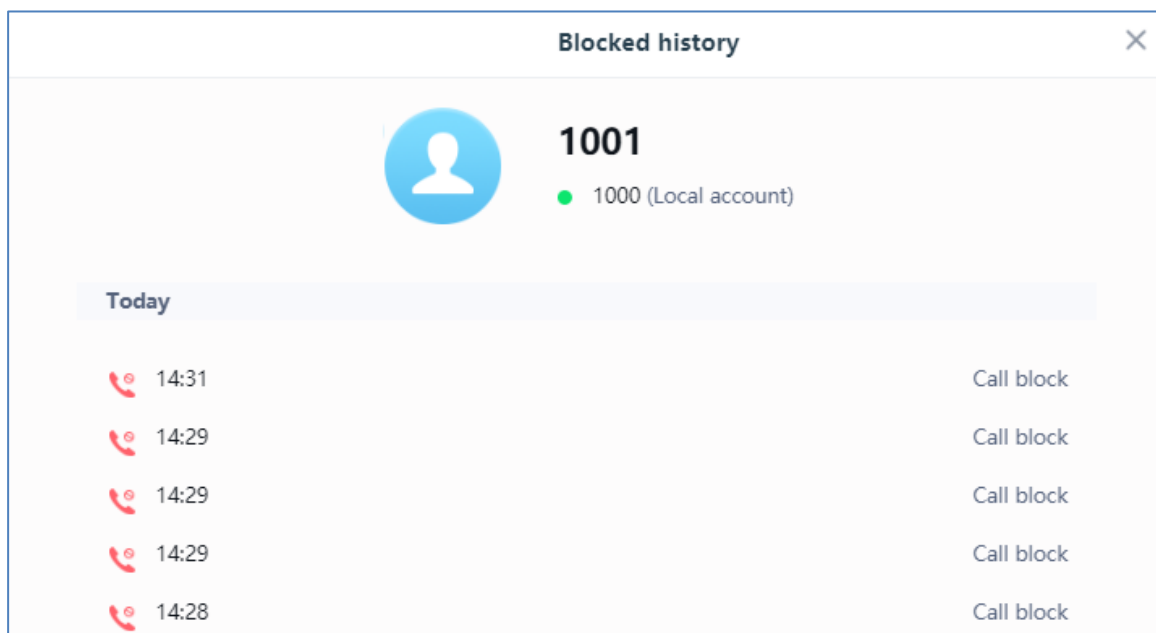


Figure 36: Call details under Call History → Intercept Record

## Contacts

Contacts section is divided into two sections: “Contacts List” and “Group”.

### Contacts List

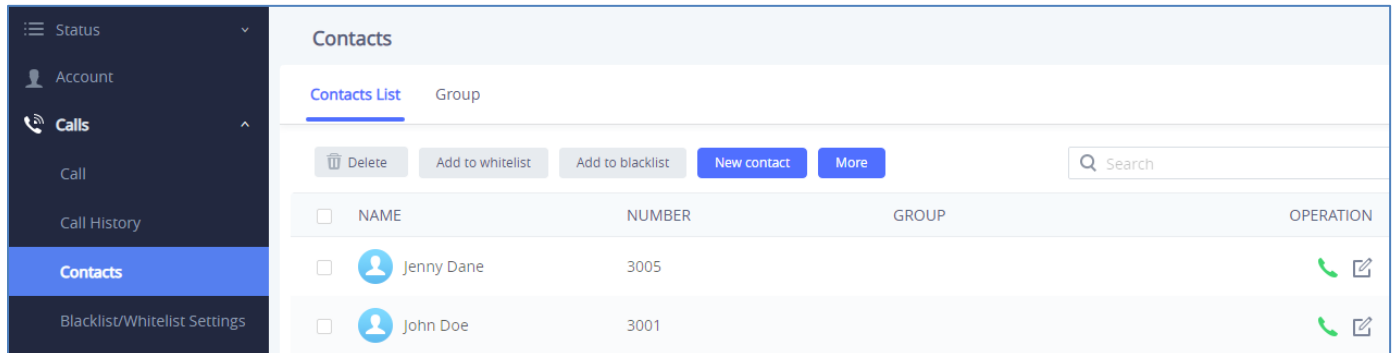


Figure 37: Contacts → Contacts List

- Dial Contact (Available for GSC3510 only).
- Edit contact details.
- **Delete**: Users can select one or a bench of contacts and click on the “Delete” button order to delete all the selected contacts.
- **Add to whitelist**: Users can select one or bench of contacts and click on the “Add to Whitelist” button in order to directly add the selected contacts to the list of contacts allowed to call the GSC3510/GSC3505.
- **Add to blacklist**: Users can select one or bench of contacts and click on the “Add to blacklist” button in order to remove the permission to call the GSC3510/GSC3505 from the selected contacts.
- **New contact**: Users can create a new contact by clicking on the “New contact” button, then a window pops up (Please, refer to the following figure) in order to enter the new contact’s details.

### New contact

Name	<input type="text" value="First Name"/>	<input type="text" value="Last Name"/>
Number	<input style="border-bottom: 1px solid #ccc;" type="text" value="Use active account"/> <span style="font-size: 0.8em;">▼</span>	<input style="width: 100%;" type="text"/> <span style="float: right; color: #007bff; font-weight: bold;">+</span>
Email	<input style="width: 100%;" type="text"/> <span style="float: right; color: #007bff; font-weight: bold;">+</span>	

Figure 38: Add New Contact



- **More**: Users need to click on the “More” button for more operations (Import contacts, Export contacts, Download contacts).

Import Contacts	
<b>Clear The Old List</b>	Determines if the device will delete the previous contacts when a new contact file is imported. If set to "Yes", the previous contacts will be removed. The default setting is "No".
<b>Clear Old History Mode</b>	If set to "Clear all", the device will delete all previous records before importing the new records. If set to "Keep Local Contacts", the new-added local new contacts will not be deleted when importing new records.
<b>Replace Duplicate Items</b>	Configures the device to keep the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the device will replace the original entries to the new one. Otherwise, the device will save both contact entries.  The default setting is "No".
<b>Replace Duplicate Entries Mode</b>	If set to "Replace by name", replace the records of the same name automatically when importing new records. If set to "Replace by number", replace the records of the same number automatically when importing new records.
<b>File Encoding</b>	Specifies the encoding format for contacts file importing. It can be selected from the dropdown list: <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• GBK</li> <li>• UTF-16</li> <li>• UTF-32</li> <li>• Big5</li> <li>• Big5-HKSCS</li> <li>• Shift-JIS</li> <li>• ISO8859-1</li> <li>• ISO8859-15</li> <li>• Windows-1251</li> <li>• EUC-KR</li> </ul> <p>The default setting is UTF-8.</p>



<b>File Type</b>	<p>Sets the type format for contacts file importing. It can be selected from the dropdown list.</p> <ul style="list-style-type: none"> <li>• XML</li> <li>• vCard</li> </ul> <p>The default setting is "XML".</p>
<b>Import Local File</b>	Uploads the contact files from PC to the device.
<b>Export Contacts</b>	
<b>File Encoding</b>	<p>Specifies the encoding format for contacts file exporting. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• GBK</li> <li>• UTF-16</li> <li>• UTF-32</li> <li>• Big5</li> <li>• Big5-HKSCS</li> <li>• Shift-JIS</li> <li>• ISO8859-1</li> <li>• ISO8859-15</li> <li>• Windows-1251</li> <li>• EUC-KR</li> </ul> <p>The default setting is UTF-8.</p>
<b>File Type</b>	<p>Sets the type format for contacts file exporting. It can be selected from the dropdown list.</p> <ul style="list-style-type: none"> <li>• XML</li> <li>• vCard</li> </ul> <p>The default setting is "XML".</p>
<b>Export</b>	Downloads the contacts file from the device to PC.
<b>Download Contacts (XML Contacts)</b>	
<b>Clear The Old List</b>	<p>Sets the device to delete the previous contacts when a new contact file is downloaded. If set to "Yes", the previous contacts will be removed. The default setting is "No".</p>
<b>Clear Old History Mode</b>	<p>If set to "Clear all", the device will delete all previous records before downloading the new records. If set to "Keep Local Contacts", the new-added local new contacts will not be deleted when downloading new records.</p>



<b>Replace Duplicate Items</b>	Keeps the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the device will replace the original entries to the new one. Otherwise, the device will save both contact entries. The default setting is "No".
<b>Replace Duplicate Entries Mode</b>	If set to "Replace by name", replace the records of the same name automatically when downloading new records. If set to "Replace by number", replace the records of the same number automatically when downloading new records.
<b>Download Mode</b>	Enables the device to download contacts file and select the server and protocol to download the contacts file. It can be selected from TFTP, HTTP, and HTTPS. The default setting is "OFF".
<b>File Encoding</b>	<p>Selects the encoding format for contacts file download. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> <li>• UTF-8</li> <li>• GBK</li> <li>• UTF-16</li> <li>• UTF-32</li> <li>• Big5</li> <li>• Big5-HKSCS</li> <li>• Shift-JIS</li> <li>• ISO8859-1</li> <li>• ISO8859-15</li> <li>• Windows-1251</li> <li>• EUC-KR</li> </ul> <p>The default setting is UTF-8.</p>
<b>Download Server</b>	<p>Configures the server URL to download the contacts file.</p> <p>The device will send a request to the server to download the contacts file with filename <b><i>contacts.xml</i></b>.</p>
<b>HTTP/HTTPS Username</b>	Configures username for HTTP/HTTPS server to download the contacts file.
<b>HTTP/HTTPS Password</b>	Specifies password for HTTP/HTTPS server to download contacts file.



<b>Automatic Download Interval</b>	Determines how the device to send the request to the server to download the contacts file. It can be selected from the dropdown list: <ul style="list-style-type: none"> <li>• None</li> <li>• 2 Hour</li> <li>• 4 Hour</li> <li>• 6 Hour</li> <li>• 8 Hour</li> <li>• 12 Hour</li> </ul>
<b>Download Now</b>	Starts downloading the XML contacts to the device immediately.

## Group

Users could manage the groups of the existing contacts that can be found in “Contacts List”.

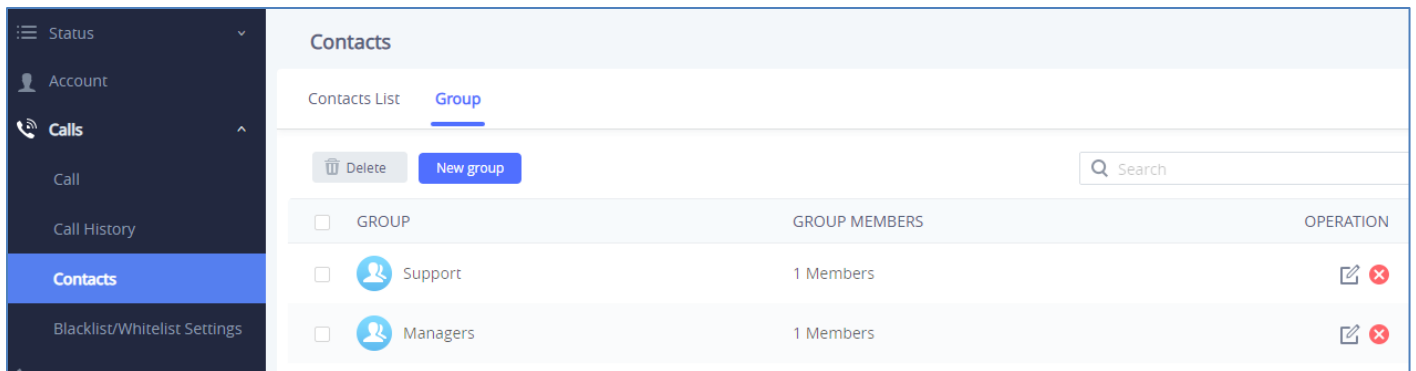


Figure 39: Contacts → Group

Users has the ability to do two operations in this section:

- **Delete**: Users can select one or a bench of groups and click on the “Delete” button in order to delete all the selected groups.
- **New group**: Users can create a new group by clicking on the “New group” button, then a window pops up (Please, refer to the following figure) in order to enter the group’s name and specify the contacts that will be included in it.



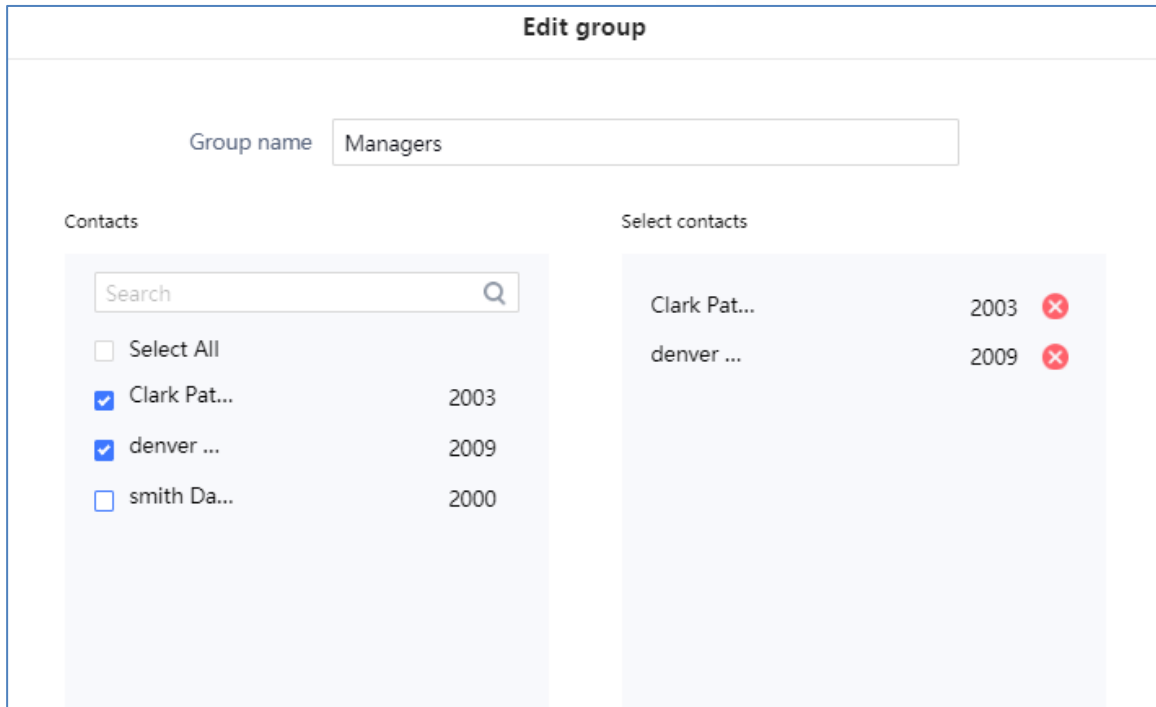


Figure 40: Add New Group

## Black/White List Settings

This section is for managing calling permissions to the GSC3510/GSC3505. Users can give or remove the permission to call the GSC3510/GSC3505, this can be managed under the following three subsections:

### Whitelist

Users can specify the numbers allowed to call the GSC3510/GSC3505 and every time a number is added it is listed in the below list:

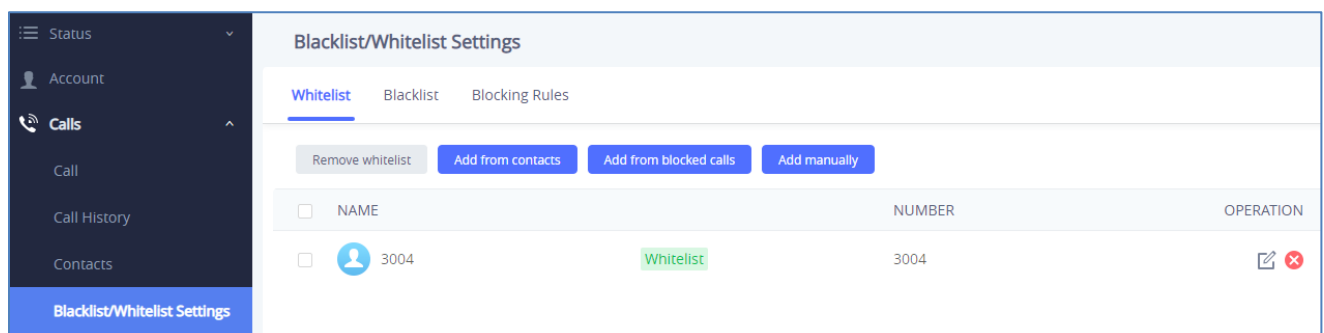
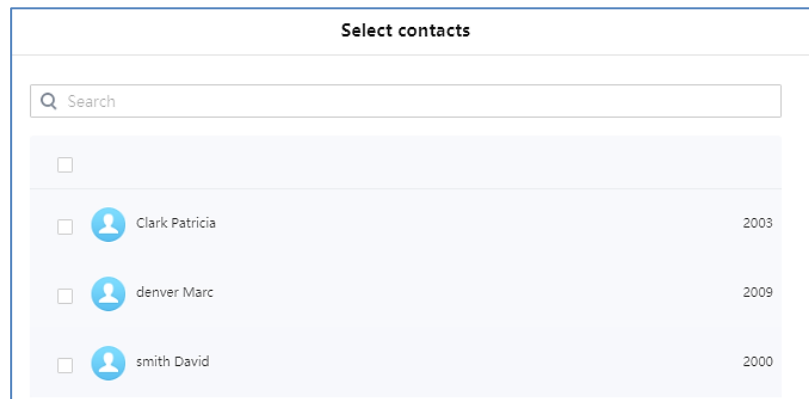


Figure 41: Whitelist section

- **Remove whitelist:** Users can remove one or a group of numbers from whitelist by clicking in “Remove Whitelist” button.

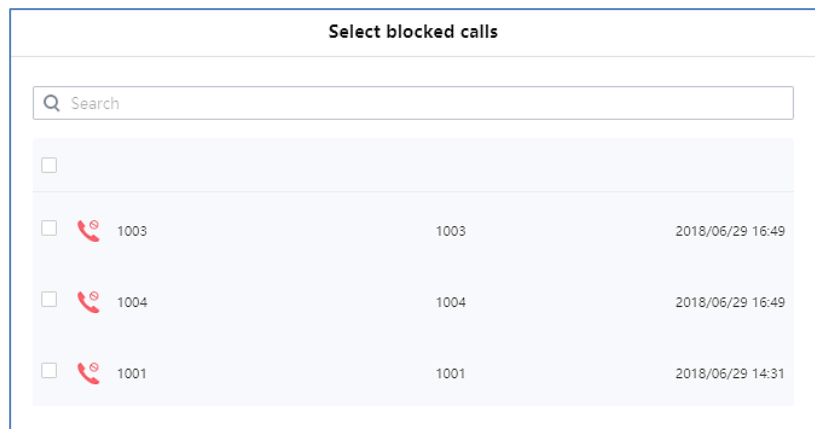
**Note:** Users can also press on to remove one specific contacts from whitelist.

- Add from contacts**: Users can add the phonebook contacts to the whitelist by clicking on “Add from contacts” button. A window pops up showing the existing contacts so that users can select the ones wishing to give permission to.



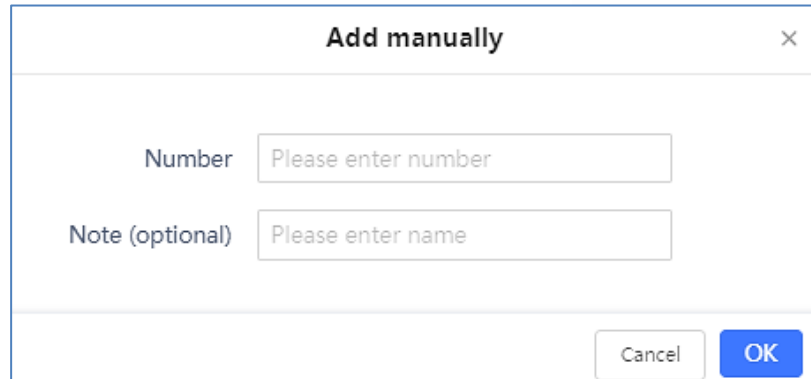
**Figure 42: Add phonebook contacts to whitelist**

- Add from blocked calls**: Users can add the numbers that the GSC3510/GSC3505 is blocking to the Whitelist by clicking on “Add from blocked calls”. A window pops up showing all the blocked numbers.



**Figure 43: Add blocked numbers to whitelist**

- Add manually**: Users can add numbers manually to whitelist by clicking on “Add manually” button. A window pops up allowing users to enter the number and its name.




**Add manually** ✕

Number

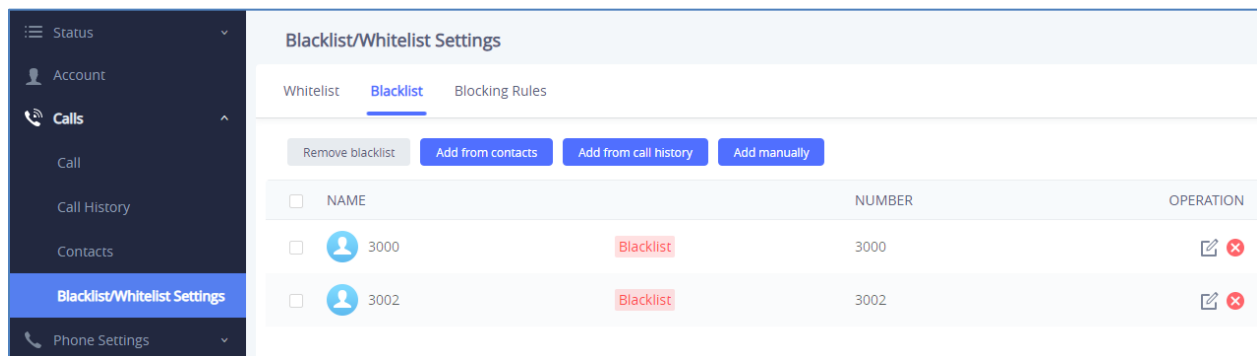
Note (optional)

**Figure 44: Add Manually to Whitelist**

**Note:** Users can modify the name of the number listed in the Whitelist by clicking on .







## Blacklist

Users can specify the numbers to be blocked by the GSC3510/GSC3505 for incoming calls, and every time a number is added to the blacklist, it is listed in the below list:




**Blacklist/Whitelist Settings**

Whitelist **Blacklist** Blocking Rules

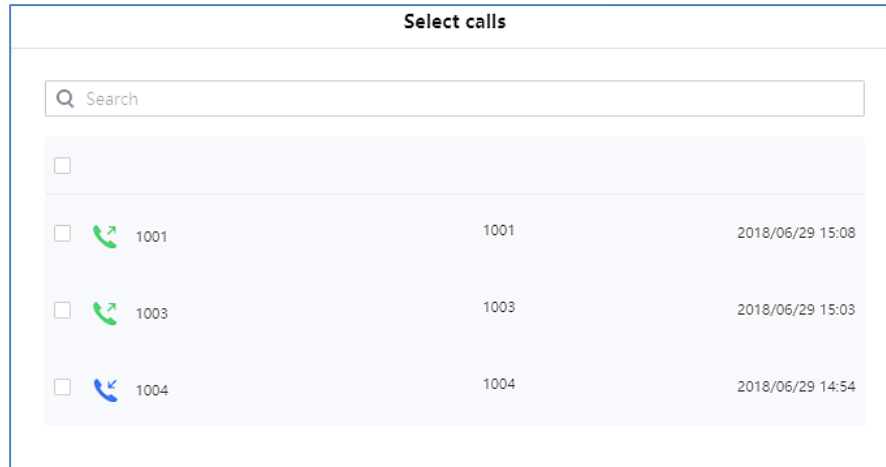
<input type="checkbox"/>	NAME	NUMBER	OPERATION
<input type="checkbox"/>	 3000	3000	<span style="color: red;">Blacklist</span>  
<input type="checkbox"/>	 3002	3002	<span style="color: red;">Blacklist</span>  

**Figure 45: Blacklist Section**

- Remove blacklist:** Users can remove one or a group of numbers from blacklist by clicking in “Remove blacklist” button.
 


**Note:** Users can also press on  to remove one specific contacts from blacklist.
- Add from contacts:** Users can add phonebook contacts to the blacklist by clicking on “Add from contacts” button. A window pops up showing the existing contacts so that users may select the ones wishing to give permission to (*Please, refer to Figure 23*).
- Add from call history:** Users can add numbers from Call History to the blacklist by clicking on “Add from call history” button. A window pops up showing all the calls listed in the GSC3510/GSC3505 call history.





**Figure 46: Add from Call History to Blacklist**

- **Add manually**: Users can add numbers manually to blacklist by clicking on “Add manually” button. A window pops up allowing users to enter the number and its name (*Please, refer to Figure 25*).

**Note:** Users can modify the name of the number listed in the blacklist by clicking on .

## Blocking Rules

This sub-section allows the user to define the blocking rules for Non-white list calls. The blocking rules available for the users are:

- **Block:** Configures the GSC3510/GSC3505 to block all the numbers that are not listed in the Whitelist.
- **Answer:** Configures the GSC3510/GSC3505 to allow all the calls received from any number but the number listed in the blacklist.

## Phone Settings Page Definitions

### General Settings

#### Available for the GSC3510 Only

Basic Settings	
<b>Local RTP Port</b>	Defines the local RTP port pair used to listen and transmit. The default value is 5004. The valid range is from 1024 to 65400.
<b>Use Random Port</b>	Forces the device to use random ports for both SIP and RTP messages. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is “No”.  <b>Note:</b> This parameter must be set to “No” for Direct IP Calling to work.



<b>Keep-alive Interval (s)</b>	Specifies how the device will send a Binding Request packet to the SIP server in order 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.
<b>STUN Server</b>	Configures the URI of STUN (Simple Traversal of UDP for NAT) server. The device will send STUN Binding Request packet to the STUN server to learn the public IP address of its network. Only non-symmetric NAT routers work with STUN. The default setting is “stun.ipvideotalk.com”.
<b>TURN Server Username</b>	Fill in the username to validate TURN server.
<b>TURN Server Password</b>	Fill in the password to validate TURN server.
<b>Use NAT IP</b>	Configures the IP address for the Contact header and Connection Information in the SIP/SDP message. It should <b>ONLY</b> be used if it's required by your ITSP. The default setting is keep the box blank.

## Call Settings

### *Available for the GSC3510 Only*

<b>Enable Call Waiting</b>	Enables call waiting feature. If it is disabled, the GSC3510 will reject the second incoming call during an active session without user's knowledge. But this missed call record will be saved to remind users. The default setting is checked (enabled).
<b>Enable Call Waiting Tone</b>	Sets the GSC3510 to play the call waiting tone along with LED indicator if there is another incoming call. If unchecked, only LED will indicate another incoming call. The default setting is checked (enabled).
<b>Auto Mute on Entry</b>	<p>Configures whether to mute the call on entry automatically.</p> <ul style="list-style-type: none"> <li>• If set to "<b>Disable</b>", then do not use auto mute function.</li> <li>• If set to "<b>Auto Mute on Outgoing Call</b>", then mute automatically when the other party answers the outgoing call.</li> <li>• If set to "<b>Auto Mute on Incoming Call</b>", then mute automatically when answers the incoming call;</li> <li>• If set to "<b>Mute on Incoming &amp; Outgoing Call</b>", then mute automatically when the call gets through.</li> </ul> <p><b>Note:</b> This function only take effect when the device is from the idle status to call status. Users could click the Mute button on call interface to cancel the current mute status.</p>



<b>Virtual Account Group Avaya Mode</b>	<p>If set to "Yes", when processing SIP Register 3XX Response, it will parse the address site in 3XX, modify the account server info "SIP Server: port" &amp; "SIP Transaction" in virtual account group and initiate registration again. This feature is designed for the Avaya customers.</p>
<b>Filter Characters</b>	<p>Sets the characters for filter when dial out numbers. Users could set up multiple characters. For example, if set to "[()-]", when dial (0571)-8800-8888, the character "()-" will be automatically filtered and dial 057188008888 directly.</p>
<b>Escape # as %23 in SIP URI</b>	<p>Determines which characters will be included in the SIP INVITE URI if end users input #. If it is set to "Yes", the device will replace the # by %23. Otherwise, it will include # in the SIP INVITE message. The default setting is "Yes".</p>
<b>Record Mode</b>	<p>Configures phone recording mode. If set to "Record locally", then will use the local tape recorder for call recording, and the audio file will be saved in accordance with the tape recorder setup. If set to "Record on PortaOne", then will send the specified SIP messages to the corresponding server; If set to "Record on UCM", then will send the recording feature code to the UCM server to request for recording, and the recording function will be executed by the server.</p>
<b>Environment</b>	<p>Sets operating environment for the device.</p> <ul style="list-style-type: none"> <li>• When set to "Small and medium size room &amp; used on desk", the sound pickup range is increased and ENC is reduced;</li> <li>• When set to "Large room &amp; used on empty area", the sound pickup range is reduced and ENC is increased.</li> </ul> <p>The default value is "Large room &amp; used on empty area".</p>

## Ring Tone

*Available for the GSC3510 only*

<b>Auto Config CPT by Region</b>	<p>Configures whether to choose Call Progress Tone automatically by region. If set to "Yes", the device will configure CPT (Call Progress Tone) according to different regions automatically. If set to "No", you can manual configure CPT parameters. The default setting is "No".</p>
----------------------------------	---



<b>Call Progress Tones:</b> <ul style="list-style-type: none"> <li>• <b>Dial Tone</b></li> <li>• <b>Second Dial Tone</b></li> <li>• <b>Ring Back Tone</b></li> <li>• <b>Busy Tone</b></li> <li>• <b>Reorder Tone</b></li> <li>• <b>Confirmation Tone</b></li> <li>• <b>Call-Waiting Tone</b></li> </ul>	<p>Configures tone frequencies according to user preference. By default, the tones are set to North American frequencies. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds.</p> <ul style="list-style-type: none"> <li>• <b>Syntax:</b> f1=val,f2=val [,c=on1/off1[-on2/off2[-on3/off3]]];</li> </ul> <p>(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. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeats the pattern.</p> <p>Please refer to the document below to determine your local call progress tones: <a href="http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf">http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf</a></p>
<b>Call-Waiting Tone Gain</b>	Adjusts the call waiting tone volume. Users can select "Low", "Medium" or "High". The default setting is "Low".
<b>Default Ring Cadence</b>	Defines the ring cadence for the device. The default setting is: c=2000/4000.

## Multicast Paging

Multicast Paging	
<b>Paging Barge</b>	Sets the threshold of paging calls. If the paging call's priority is higher than the threshold, the existing call will be hold and the paging call will be answered. Otherwise, the existing call does not be affected. If it is set to Disable, any paging call will not be answered. The default setting is "Disable".
<b>Paging Priority Active</b>	Determines if a new paging call whose priority is higher than the existing paging call will be answered. If it is checked, this feature will be enabled. The default setting is disabled.
<b>Multicast Paging Codec</b>	Selects the codec type for the multicast paging call. This list includes PCMU, PCMA, G726-32, G722, and G729A/B, iLBC, Opus.
Multicast Listening	
<ul style="list-style-type: none"> <li>• <b>Priority</b></li> <li>• <b>Listening Address</b></li> <li>• <b>Label</b></li> </ul>	<p>Configures the IP address and port number for monitoring multicast paging call. Reboot the device to make changes take effect.</p> <p>The valid IP address range is from 224.0.0.0 to 239.255.255.255. Users may also fill the label for each listening address corresponding to priority.</p>



## Network Settings Page Definitions

### Ethernet Settings

<b>Preferred Internet Protocol</b>	<p>If IPv4 is selected, the device will be using IPv4 addressing, otherwise, it will be using IPv6 addressing.</p> <p>Default is Prefer IPv4.</p>
<b>Different Networks for Data and VoIP Calls</b>	<p>Configures whether to set up different networks for the phone data and the call. If set to "Yes", you need to configure the data network and VoIP network respectively.</p> <p><b>Note:</b> Reboot is required to take effect.</p>
<b>IPv4</b>	
<b>IPv4 Address Type</b>	<p>Allows users to configure the appropriate network settings on the device. Users could select "DHCP", "Static IP" or "PPPoE".</p> <ul style="list-style-type: none"> <li>• <b>DHCP:</b> Obtain the IP address via one DHCP server in the LAN. All domain values about static IP/PPPoE are unavailable (although some domain values have been saved in the flash.)</li> <li>• <b>PPPoE:</b> Configures PPPoE account/password. Obtain the IP address from the PPPoE server via dialing. (When "Different Networks for Data and VoIP Calls" is set to Yes; it will be available for "Network Configuration of Data" only).</li> <li>• <b>Static IP:</b> Manually configures IP Address, Subnet Mask, Default Router's IP Address, DNS Server 1 and DNS Server 2.</li> </ul> <p>By default, it is set to "DHCP".</p>
<b>DHCP VLAN Override</b>	<p>DHCP Option 132 defines VLAN ID and DHCP Option 133 defines priority tag ID.</p> <p>GSC3510/GSC3505 supports DHCP VLAN override via DHCP Option 132 and DHCP Option 133, or encapsulated DHCP option 132 and DHCP option 133 in DHCP option 43.</p> <ul style="list-style-type: none"> <li>• Users could select "<b>Disable</b>", "DHCP Option 132 and DHCP Option 133", or "Encapsulated in DHCP Option 43".</li> <li>• When set to "<b>DHCP Option 132 and DHCP Option 133</b>", the GSC3510/GSC3505 will get DHCP Option 132 as VLAN ID and get DHCP Option 133 as VLAN priority, from the DHCP server directly.</li> </ul>






	<ul style="list-style-type: none"> <li>When set to “<b>Encapsulated in DHCP Option 43</b>”, the GSC3510/GSC3505 will get VLAN ID and VLAN priority value from the DHCP Option 43 which has DHCP Option 132 and DHCP Option 133 encapsulated. In this case, please make sure the option “Allow DHCP Option 43 and Option 66 to Override Server” is enabled under GSC3510/GSC3505 web UI → <b>Maintenance</b> → <b>Upgrade</b>.</li> </ul> <p>By default, it is set to “Encapsulated in DHCP Option 43”:</p>
<b>Host name (Option 12)</b>	Sets the name of the client in the DHCP request. It is optional but may be required by some Internet Service Providers.
<b>Vendor Class ID (Option 60)</b>	Configures the vendor class ID header in the DHCP request. Default setting is “Grandstream GSC3510” or “Grandstream GSC3505”.
<b>Layer 2 QoS 802.1Q/VLAN Tag (Ethernet)</b>	Assigns the VLAN Tag of the Layer 2 QoS packets for Ethernet. The Default value is 0. <b>Note:</b> When “Different Networks for Data and VoIP Calls” is set to Yes, user needs to set “Layer 2 QoS 802.1Q/VLAN Tag (Ethernet) for Data” and “Layer 2 QoS 802.1Q/VLAN Tag (Ethernet) for VoIP Calls”.
<ul style="list-style-type: none"> <li>for Data</li> <li>for VoIP Calls</li> </ul>	
<b>Layer 2 QoS 802.1p Priority Value (Ethernet)</b>	Assigns the priority value of the Layer 2 QoS packets for Ethernet. The Default value is 0. <b>Note:</b> When “Different Networks for Data and VoIP Calls” is set to Yes, user needs to set “Layer 2 QoS 802.1p Priority Value (Ethernet) for Data” and “Layer 2 QoS 802.1p Priority Value (Ethernet) for VoIP Calls”.
<ul style="list-style-type: none"> <li>for Data</li> <li>for VoIP Calls</li> </ul>	
<b>IPv6</b>	
<b>IPv6 Address</b>	Configures the appropriate network settings on the device. Users could select from "Auto-configured" or “Statically configured”.
<b>Preferred DNS Server</b>	Configures the Preferred DNS Server.
<b>DNS Server 1</b>	Configures the primary DNS IP address.
<b>DNS Server 2</b>	Configures the secondary DNS IP address.
<b>Static IPv6 Address</b>	Enter the static IPv6 address in "Statically configured" IPv6 address type.
<b>IPv6 Prefix Length</b>	Enter the IPv6 prefix length in "Statically configured" IPv6 address type. Default is 64.
<b>802.1x Mode</b>	
<b>802.1x mode</b>	Enables and selects the 802.1x mode for the device. The supported 802.1x modes are: <ul style="list-style-type: none"> <li><b>EAP-MD5</b></li> </ul>



	<ul style="list-style-type: none"> <li>• <b>EAP-TLS</b></li> <li>• <b>EAP-PEAP</b></li> </ul> <p>The default setting is "Disable".</p>
<b>802.1x Identity</b>	Enters the identity information for the selected 802.1x mode. (This setting will be displayed only if 802.1 X mode is enabled).
<b>802.1x Secret</b>	Enters the secret for the 802.1x mode. This option will appear when 802.1x mode is EAP-MD5 or EAP-PEAP.
<b>CA Certificate</b>	Uploads the CA Certificate file to the device. (This setting will be displayed only if the 802.1 X mode is enabled)
<b>Client Certificate</b>	Loads the Client Certificate file to the device. (This setting will be displayed only if the 802.1 X TLS mode is enabled)
<b>Private Key</b>	Loads the private key file to the device. (This setting will be displayed only if the 802.1 X TLS mode is enabled)

## Bluetooth

<b>Bluetooth Settings</b>	Enable or Disable Bluetooth on GSC3510/GSC3505
<b>Visible to Nearby Bluetooth Devices</b>	Enable the GSC3510/GSC3505 to be visible via Bluetooth by nearby devices for a duration of 2 minutes.
<b>Device Name</b>	Configures the name that will be shown to other Bluetooth devices.
<b>Paired devices</b>	Lists paired devices.  Press  to unpair/remove the device from the list.

## Wi-Fi Settings

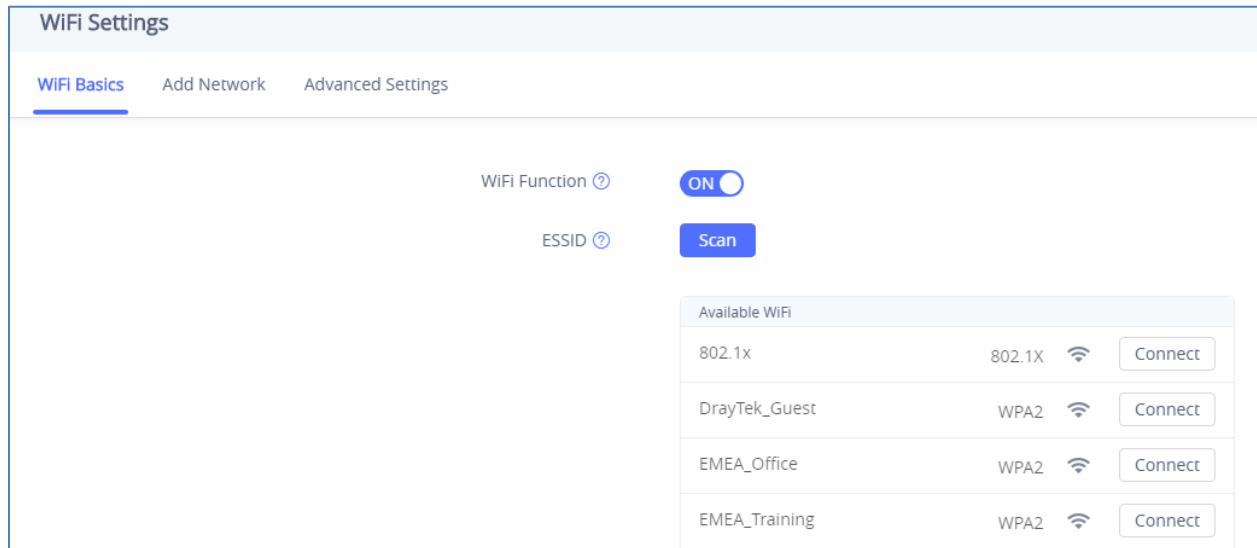
### Connect to Wi-Fi Network

Users can connect wirelessly to a network using Wi-Fi under **GSC3510/GSC3505 Web GUI → Network Settings → Wi-Fi Settings**. In order to connect to a network using Wi-Fi, please, refer to the following steps:

1. Go to **GSC3510/GSC3505 Web GUI → Network Settings → Wi-Fi Settings → Wi-Fi Basics**.
2. Enable **Wi-Fi Function** by turning the option on.
3. Click on **Scan** to show the list of Wi-Fi networks available around the GSC3510/GSC3505

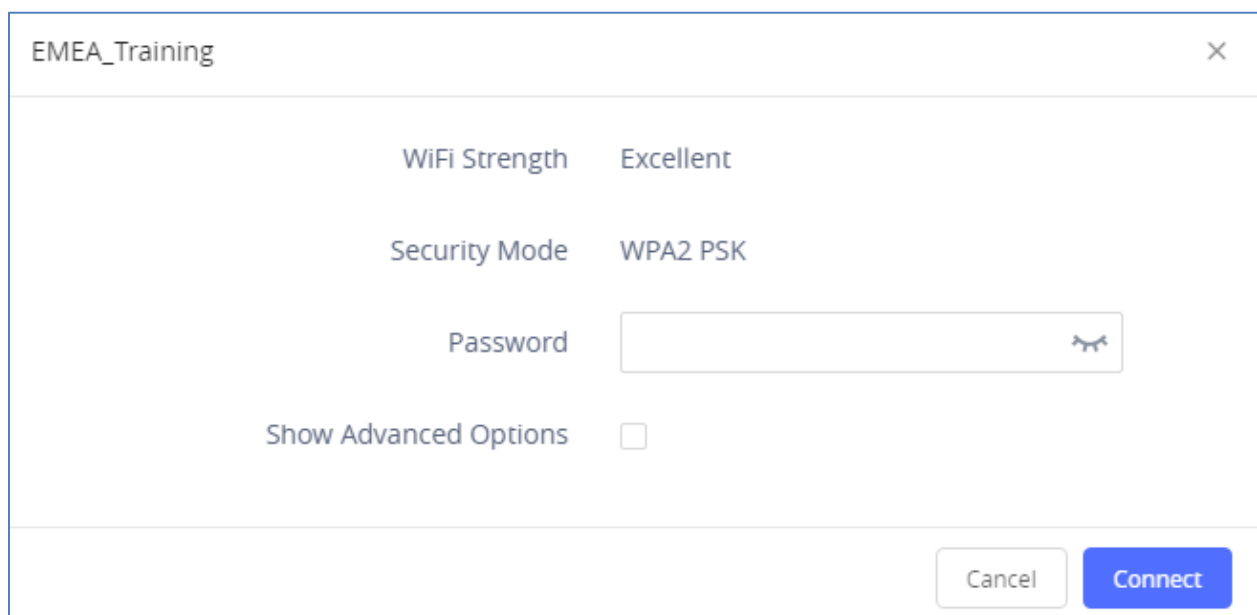
**Note:** The list of Wi-Fi Networks refreshes automatically every 15 seconds and user can force to refresh by clicking again on "Scan".





**Figure 47: Wi-Fi Basics Page**

4. Identify the Wi-Fi network's SSID and click on "Connect", then enter the correct password information to connect to the selected network:



**Figure 48: Connect to Wi-Fi Network**

5. Users can check the Wi-Fi parameters and change the setting by checking the "Show advanced options" in the bottom.

EMEA\_Training
✕

WiFi Strength    Excellent

Security Mode    WPA2 PSK

Password   

Show Advanced Options   

IP Address Type     DHCP     Static IP

Cancel

Connect

Figure 49: GSC3510/GSC3505 Connect to Wi-Fi-Show Advanced Options

### Wi-Fi Settings description

Wi-Fi Basics	
<b>Wi-Fi Function</b>	Enables/disables the Wi-Fi feature. The default setting is "Disable".
<b>ESSID</b>	Permits to scan and select the available Wi-Fi networks within the range if the Wi-Fi feature is enabled. Click on "Connect" to select the Wi-Fi network and to enter the needed password if it is required.
Add Network	
<b>ESSID</b>	Configures the hidden ESSID name.
<b>Security Mode for Hidden SSID</b>	Defines the security mode used for the wireless network when the SSID is hidden. Default is "None". Users can choose: WEP, WPA/WPA2 PSK or 802.1x EAP.
<b>Password</b>	Configures the hidden ESSID password.
Advanced Settings	
<b>Layer 2 QoS 802.1p Priority Value (Wi-Fi)</b>	Assigns the priority value of the Layer 2 QoS packets for Wi-Fi. The Default value is 0.
<b>Country Code</b>	Configures Wi-Fi country code. The default value is "United States of America". <b>Note:</b> Reboot is requested to take effect.

## OpenVPN® Settings

OpenVPN® Settings	
<b>Enable OpenVPN®</b>	<p>This enables/disables OpenVPN® functionality, and requires the user to have access to an OpenVPN® server. The default setting is No.</p> <p><b>Note:</b> To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key.</p>
<b>Enable OpenVPN® Comp-Izo</b>	<p>Configures enable/disable the LZO compression. When the LZO Compression is enabled on the OpenVPN® server, you must turn on it at the same time. Otherwise, the network will fail to connect.</p>
<b>OpenVPN® Server Address</b>	<p>The URL/IP address for the OpenVPN® server.</p>
<b>OpenVPN® Port</b>	<p>The network port for the OpenVPN® server. By default, it is set to 1194.</p>
<b>OpenVPN® Transport</b>	<p>Determines network protocol used for OpenVPN®: UDP or TCP.</p>
<b>OpenVPN® CA</b>	<p>OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.</p>
<b>OpenVPN® Client Certificate</b>	<p>OpenVPN® Client certificate file (*.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.</p>
<b>OpenVPN® Client Key</b>	<p>The OpenVPN® Client key (*.key) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.</p>
<b>OpenVPN® Cipher Method</b>	<p>The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Available methods are:</p> <ul style="list-style-type: none"> <li>• Blowfish</li> <li>• AES-128</li> <li>• AES-256</li> <li>• Triple-DES</li> </ul> <p>Default is "Blowfish"</p>
<b>OpenVPN® Username</b>	<p>OpenVPN® authentication username (optional).</p>
<b>OpenVPN® Password</b>	<p>OpenVPN® authentication password (optional).</p>



## Advanced Network Settings

Advanced Network Settings	
<b>Preferred DNS 1</b>	Sets the preferred DNS server 1 for the user.
<b>Preferred DNS 2</b>	Sets the preferred DNS server 2 for the user.
<b>Enable LLDP</b>	Enables the LLDP (Link Layer Discovery Protocol) feature on the device. If it is set to "Yes", the device will broadcast LLDP PDU to advertise its identity and capabilities and receive same from a physical adjacent layer 2 peer. The default setting is "Yes".
<b>LLDP TX Interval (s)</b>	Configures the interval the device sends LLLD-MED packet. The default setting is 30s. <b>Note:</b> Reboot the device to make changes take effect.
<b>Enable CDP</b>	Configures whether to enable CDP to receive and/or transmit information from/to CDP-enabled devices. The default setting is "No".
<b>Layer 3 QoS for SIP</b>	Defines the Layer 3 packet's QoS parameter for SIP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. Default setting is 48 which is equivalent to the DSCP name constant CS6.
<b>Layer 3 QoS for Audio</b>	Defines the Layer 3 packet's QoS parameter for RTP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. Default setting is 48 which is equivalent to the DSCP name constant CS6.
<b>HTTP/HTTPS User-Agent</b>	Sets the user-agent for contacts. <b>Note:</b> Reboot the device to make changes take effect.
<b>SIP User-Agent</b>	Sets the user-agent for SIP. Default is: <ul style="list-style-type: none"> <li>• Grandstream GSC3510 \$version</li> <li>• Grandstream GSC3505 \$version</li> </ul>
Proxy	
<b>HTTP/HTTPS Proxy Hostname</b>	Specifies the HTTP/HTTPS proxy hostname for the device to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
<b>HTTP/HTTPS Proxy Port</b>	Specifies the HTTP/HTTPS proxy port for the device to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
<b>Bypass Proxy For</b>	Defines the destination IP address where no proxy server is needed. The device will not use a proxy server when sending packets to the specified destination IP address.



## System Settings Page Definitions

### Time Settings

Time Settings	
<b>Assign NTP Server Address</b>	Defines the URL or IP address of the NTP server. The phone may obtain the current date and time information from the server. The default setting is "pool.ntp.org".
<b>DHCP Option 42 Override NTP Server</b>	Obtains NTP server address from a DHCP server using DHCP Option 42; it will override configured NTP Server. If set to "No", the phone will use configured NTP server to synchronize time and date even if a NTP server is provided by DHCP server. The default setting is "Yes". <b>Note:</b> Changes in this setting need reboot to take effect.
<b>DHCP Option 2 to Override Time Zone Settings</b>	Obtains time zone setting (offset) from a DHCP server using DHCP Option 2; it will override selected time zone. If set to "No", the phone will use selected time zone even if provided by DHCP server. The default setting is Yes. <b>Note:</b> Changes in this setting need reboot to take effect.
<b>Time Zone</b>	Specifies the local time zone for the phone. It covers the global time zones and user can selected the specific one from the drop-down list.
<b>Time Display Format</b>	Specifies which format will be used to display the time. It can be selected from 12-hour and 24-hour format.
<b>Date Display Format</b>	Determines which format will be used to display the date. It can be selected from the drop-down list. <ul style="list-style-type: none"> <li>• Normal (YYYY/M/D)</li> <li>• YYYY/MM/DD</li> <li>• MM/DD/YYYY</li> <li>• DD/MM/YYYY</li> </ul> The default setting is MM/DD/YYYY

### Security Settings

Web/SSH Access	
<b>Enable SSH</b>	Enables/disables SSH access to the device. The default setting is "Yes".
<b>SSH Port</b>	Customizes the SSH port. By default, SSH uses port 22.
<b>Access Method</b>	Determines which protocol will be used to access the device 's Web GUI. It can be selected from HTTP and HTTPS. The default setting is HTTP.
<b>Port</b>	Specifies which port to use to access the Web UI. By default, if HTTP, the port number will be 80; if HTTPS is selected, the port number will be 443.



User Info Management	
<b>Current Admin Password</b>	Enter current logged-in user's password. This field is case sensitive. The default password is "admin".
<b>New Admin Password</b>	Allows the user to change the admin password. The password field is purposely blank after clicking the "Save" button for security purpose. This field is case sensitive with a maximum length of 32 characters.
<b>Confirm Admin Password</b>	Enter the new Admin password again to confirm.
<b>New User Password</b>	Allows the administrator to set the password for user-level web GUI access. This field is case sensitive with a maximum length of 32 characters. The default password is "123".
<b>Confirm New User Password</b>	Enter the new User password again to confirm.
SIP TLS	
<b>SIP TLS Certificate</b>	Defines the SSL certificate used for SIP over TLS.
<b>SIP TLS Private Key</b>	Defines the SSL Private key used for SIP over TLS.
<b>SIP TLS Private Key Password</b>	Defines the SSL Private key password used for SIP over TLS.
Certificate Management	
CA Certificate	
<b>Import Trusted CA Certificates</b>	Allows to upload the CA Certificate file to phone. <b>Note:</b> Reboot is required to take effect.
<b>Trusted CA Certificates</b>	Lists trusted CA certificates previously uploaded. Administrator can delete a certificate from here.
User Certificate	
<b>Add User Certificate</b>	Allows to upload & Install User Certificate file to phone.
<b>User Certificates</b>	Lists Users Certificates previously uploaded. Administrator can delete a certificate from here.
Custom Certificate	
<b>Import Custom Certificate</b>	Allows to upload & Install Custom Certificate file to device.
<b>Custom Certificate</b>	Lists Custom Certificates previously uploaded. Administrator can delete a certificate from here.





## Preferences

LED Management	
<b>Disable Missed Call Indicator</b>	If set to "Yes", the LED indicator will not light up when there is missed call on the device.
<b>Disable Contact Full Indicator</b>	If set to "Yes", the LED indicator will light up when the contact storage or message storage is full.
Brightness Control	
<b>Red Light</b>	Control the intensity of the Red Color in the LED
<b>Green Light</b>	Control the intensity of the Green Color in the LED
<b>Blue Light</b>	Control the intensity of the Blue Color in the LED
Volume Settings	
<b>Call Volume</b>	Sets the volume of calls.
<b>Ringtone volume</b>	Sets the volume of ringtones.
<b>Media volume</b>	Sets the volume of media.

## TR-069

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



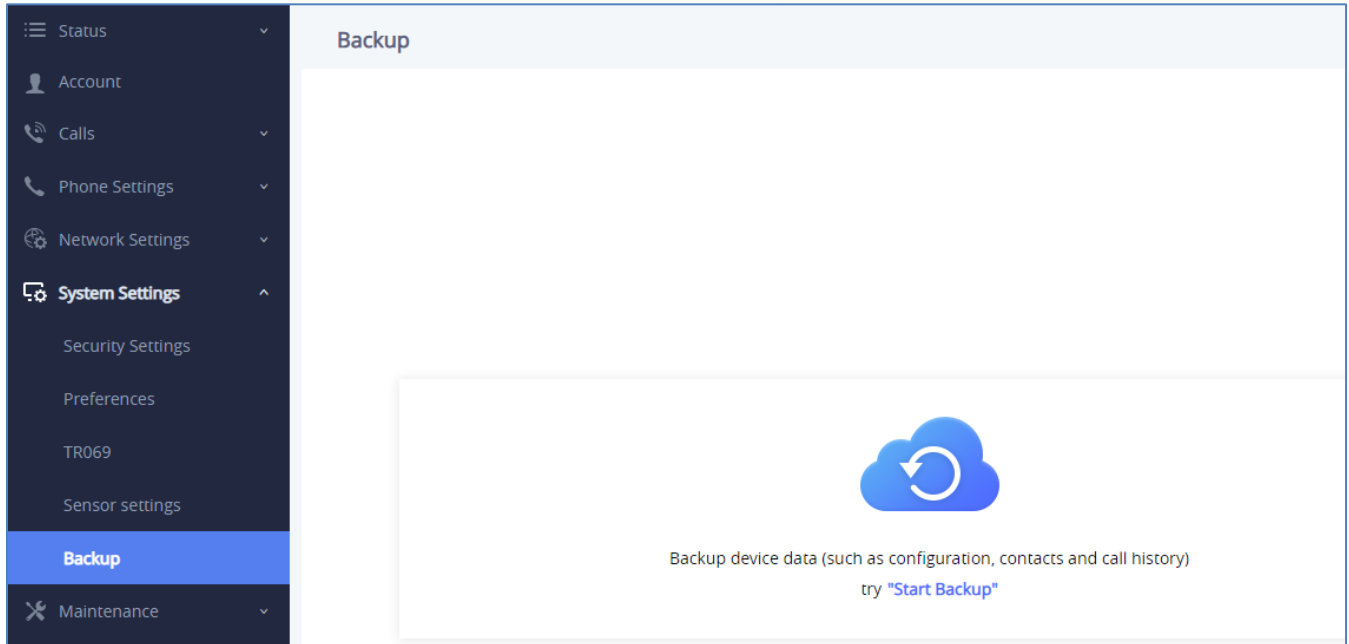
## Sensor Settings

Basic Settings	
<b>Basic Settings</b>	
<b>Sensor Type</b>	Set the initial state of the sensor, when the selection is normally open, the contact is disconnected when static; When the selection is normally closed, the contact is connected when static. The normally open will be connected when the electrical action is on the switch, and the normally closed will be disconnected. The default is normally open.
<b>Trigger Type</b>	Set the type of the trigger mode, and when the selection is level triggered, only high level (1) or low level (0) will trigger the notification. When the edge trigger is selected, the notification is triggered only when the level changes (high level to low level, or low level to high level). The default is level trigger.
<b>Trigger time</b>	
<b>Cycle Time</b>	The alarm can be configured to be triggered all days of the week, in this case " <b>All days</b> " option needs to be checked. Or to some specific schedule, in this case " <b>Period of Time</b> " option needs to be checked for users to be able to configure <b>Time</b> and <b>Frequency</b> options below.
<b>Time</b>	Set the activation time, up to 3 times. When the activation time is not set, the default time is full day.
<b>Frequency</b>	Set the activation frequency from Monday to Sunday, which can be selected from the whole week. The default value is not selected.
<b>Play audio</b>	Play a sound when the switch is triggered during the scheduled time.
<b>Prompt tone</b>	When the "voice prompt" is selected, you can upload the customized audio by clicking on "Upload" and choose the file.
<b>Make call</b>	Dial the number when the sensor is activated.
<b>Dial out extension</b>	Enter the number you need to dial, and click the "add" button to set two numbers at the same time.
<b>Recording</b>	Start recording when the sensor is activated.

## Backup

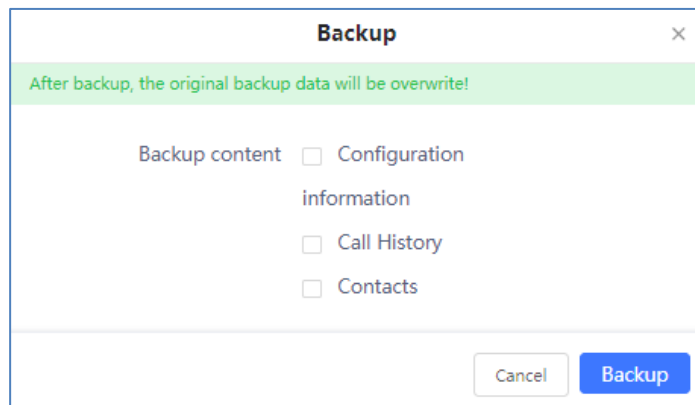
GSC3510/GSC3505 Backup page is used to back up data or import backup files to restore data. Users can start the Backup by clicking on "Start Backup".





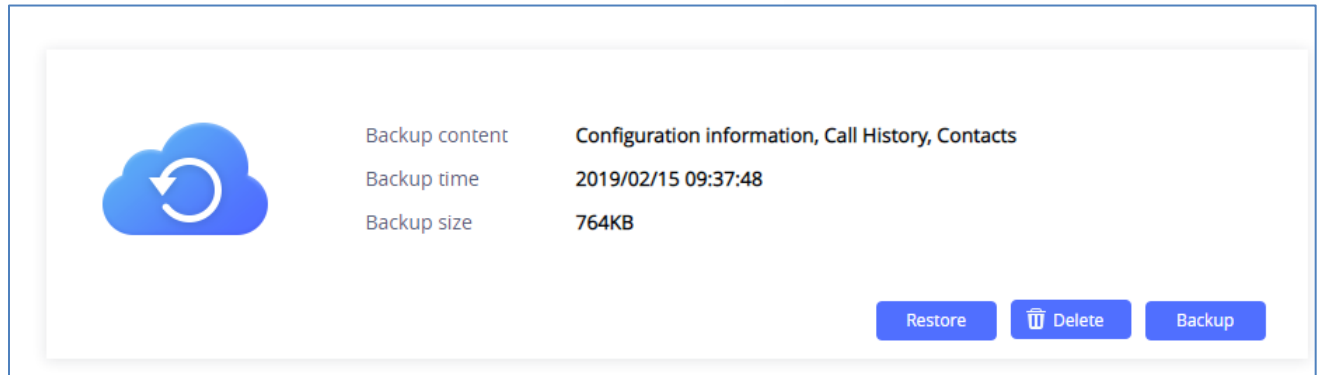
**Figure 50: GSC3510/GSC3505 Backup Page**

The following data on the GSC3510/GSC3505 can be backed up and restored to the device again using the built-in Backup application: **Contacts, Call history, Configuration information.**



**Figure 51: Backup content selection**

Once the wanted Backup contents are checked, users can generate the backup by clicking on “Backup”. The backup will be shown with all the needed information (Back Content, Backup Time and Backup Size).



**Figure 52: Generated Backup**

By generating the Backup, users can do the following operations:

- **Restore**: Users can bring back to the GSC3510/GSC3505 all the backup contents selected during Back generating operation by clicking on “Restore”.
- **Delete**: Users can delete the generated Backup by clicking on “Delete”.
- **Backup**: Users needs to click on “Backup” to generate a new backup and replace the existing one.

## Maintenance Page Definitions

### Upgrade

Firmware	
Upgrade via Manually Upload	
<b>Complete Upgrade</b>	If enabled, all files will be replaced except user data. Default setting is disabled.
<b>Upload Firmware File to Update</b>	Allows users to load the local firmware to the device to update the firmware.
Upgrade via Network	
<b>Firmware Upgrade Mode</b>	Allows users to choose the firmware upgrade method: TFTP, HTTP, HTTPS or Manual Upload. The default setting is “HTTP”.
<b>Firmware Server Path</b>	Sets IP address or domain name of firmware server. The URL of the server that hosts the firmware release. Default is “fm.grandstream.com/gs”.
<b>HTTP/HTTPS Username</b>	Enters the username for the firmware HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	Enters the password for the firmware HTTP/HTTPS server.



<b>Firmware File Prefix</b>	Checks if firmware file is with matching prefix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
<b>Firmware File Postfix</b>	Checks if firmware file is with matching postfix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
<b>Firmware Upgrade</b>	Click the " <b>Detect</b> " button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
<b>Config File</b>	
<b>Use Grandstream GAPS</b>	<p>It is used to configure the download path and update mode for the configuration file server.</p> <ul style="list-style-type: none"> <li>• If set to "<b>Yes</b>", the device will set the download path of the configuration file to "fm.grandstream.com/gs" by default and use HTTPS protocol to connect to the server.</li> <li>• If set to "<b>No</b>", then users can manually configure the path and update mode for the configuration file server.</li> </ul>
<b>Config Upgrade Via</b>	Selects provisioning method: TFTP, HTTP or HTTPS. Default setting is "HTTPS".
<b>Config Server Path</b>	Sets IP address or domain name of configuration server. The server hosts a copy of the configuration file to be installed on the device. Default is "fm.grandstream.com/gs".
<b>HTTP/HTTPS Username</b>	Configures the username for the config HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	Configures the password for the config HTTP/HTTPS server.
<b>Always send HTTP Basic Authentication Information</b>	Includes configured username and password in HTTP request before receiving authentication challenge from the server. Default is "No".
<b>Config File Prefix</b>	Checks if configuration files are with matching prefix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
<b>Config File Postfix</b>	Checks if configuration files are with matching postfix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
<b>Authenticate Conf File</b>	Sets the device to authenticate configuration file before applying it. When set to "Yes", the configuration file must include value P1 with phone system's administration password. If it is missed or does not match the password, the device will not apply it. Default setting is "No".



<b>XML Config File Password</b>	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file is using OpenSSL.
<b>Download Device Configuration</b>	Downloads the device's configuration file in text format. The config file includes all the P value parameters for phone's current settings except password for security purpose. Users can use the Grandstream configuration file generator to generate binary config file from this text file.
<b>Upload Device Configuration</b>	Uploads configuration file to the device. <b>Note:</b> The GSC35XX supports the following config file format: <ul style="list-style-type: none"> <li>• “cfgMAC.xml”, where MAC is the MAC Address.</li> <li>• “cfgGSC35XX.xml”, where GSC35XX is the Product Model.</li> </ul>
<b>Provision</b>	
<b>Automatic Upgrade</b>	
<b>Automatic Upgrade</b>	Specifies when the firmware upgrade process will be initiated; there are 4 options: <ul style="list-style-type: none"> <li>• <b>No:</b> The device will only do upgrade once at boot up.</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)”.</li> <li>• <b>Check at a period Time:</b> User needs to specify “Hour of the day (0-23)”</li> </ul> <b>Note:</b> Day of week is starting from Sunday. The default setting is “No”.
<b>Starting – Ending Hour of the Day (0 – 23)</b>	Sets the time or time period of automatic upgrade, and automatically update during the set time or time period.
<b>Firmware Upgrade and Provisioning</b>	Defines the device’s rules for automatic upgrade. It can be selected from: <ul style="list-style-type: none"> <li>• Always Check at bootup</li> <li>• Always Check at bootup, when F/W pre/suffix changes,</li> <li>• Skip the Firmware Check.</li> </ul> The default setting is “Always Check at bootup”.
<b>DHCP Option</b>	
<b>Allow DHCP option 43, option 160 and option 66 to Override Server</b>	If DHCP option 43, 160 and 66 is enabled on the LAN side, the device will reset the CPE, upgrade, network VLAN tag, and priority configuration according to option 43 sent by the server. At the same time, the update mode and server path of the configuration upgrade mode will be reset according to the option 160 and 66 sent by the server. The default setting is "on". The default setting is "Yes". <b>Notes:</b> Reboot the device to make changes take effect.



<b>DHCP Option 120 Override SIP Server</b>	<p>Configures the device to allow the DHCP offer message to override the Config Server Path via the Option 120 header.</p> <p>The default setting is "Yes".</p> <p><b>Note:</b> Reboot the device to make changes take effect.</p>
<b>Allow DHCP Option 242 (Avaya IP Phones)</b>	<p>Enables DHCP Option 242. Once enabled, the device will use the configuration info issued by the local DHCP in Option 242 to configure proxy, transport protocol and server path. The default setting is "Yes".</p> <p><b>Note:</b> Reboot the device to make changes take effect.</p>
<b>Config Provision</b>	
<b>Download and Process All Available Config Files</b>	<p>By default, the device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, and cfg.xml (corresponding to device specific, model specific, and global configs). If set to "Yes", the device will download and apply (override) all available configs in the order of cfgMAC, cfg.xml, cfgMODEL.xml, cfgMAC.xml.</p>
<b>Config Provision</b>	<p>Device will download the configuration files and provision by the configured order. Use arrow buttons to add and order configuration files.</p>
<b>PNP Feature</b>	
<b>PnP(3CX) Auto Provision</b>	<p>Sets the device to broadcast the SIP SUBSCRIBE message during booting up to allow itself to be discovered and be configured by the SIP platform.</p> <p>The default setting is "Yes".</p> <p><b>Note:</b> Reboot the device to make changes take effect.</p>
<b>Advanced Settings</b>	
<b>Disable SIP NOTIFY Authentication</b>	<p>Disables the SIP NOTIFY Authentication on the device. If set to "Yes", the GSC3510/GSC3505 will not challenge NOTIFY with 401. The default setting is "No".</p>
<b>Validate Certification Chain</b>	<p>Configures whether to validate the server certificate when download the firmware/config file.</p> <p>If it is set to "Yes", the device will download the firmware/config file only from the legitimate server. Default setting is "No".</p>
<b>mDNS Override Server</b>	<p>Sets the device to broadcast the Multicast DNS (mDNS) message during booting up to allow itself to be discovered and be configured by the SIP platform. If it is set to "User Type A", the device will broadcast the MDNS message "A_grandstream-cfg.local"; if it is set to "Use Type SRV", the MDNS message will be "SRV_grandstream-cfg.local".</p> <p>The default setting is "Use Type A".</p>
<b>Factory Reset</b>	<p>Resets the device to the default factory setting mode.</p>



## System Diagnosis

Syslog	
<b>Syslog Protocol</b>	Select the transport protocol over which log messages will be carried. <ul style="list-style-type: none"> <li>• <b>UDP:</b> Syslog messages will be sent over UDP.</li> <li>• <b>SSL/TLS:</b> Syslog messages will be sent securely over TLS connection.</li> </ul>
<b>Syslog Server</b>	Configures the URI which the device will send the syslog messages to. The default setting is "log.ipvideotalk.com".
<b>Syslog Level</b>	Selects the level of logging for syslog. The default setting is "None". There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet: <ul style="list-style-type: none"> <li>• <b>DEBUG</b> (Sent or received SIP messages).</li> <li>• <b>INFO</b> (Product model/version on boot up, NAT related info, SIP message summary, Inbound and outbound calls, Registration status change, negotiated codec, Ethernet link up).</li> <li>• <b>WARNING</b> (SLIC chip exception).</li> <li>• <b>ERROR</b> (SLIC chip exception, Memory exception).</li> </ul> <p><b>Note:</b> Changing syslog level does not require a reboot to take effect.</p>
<b>Syslog Keyword Filter</b>	Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to "SIP" to filter SIP log.
Logcat	
<b>Clear Log</b>	Clears the log files saved in the device.
<b>Log Tag</b>	Configures the filter to display the specified process log file.
<b>Log Priority</b>	Selects the log priority to display. It can be selected from list below: <ul style="list-style-type: none"> <li>• Verbose (Default Setting)</li> <li>• Debug</li> <li>• Info</li> <li>• Warning</li> <li>• Error</li> <li>• Fatal</li> <li>• Silent (suppress all output)</li> </ul>
<b>Get Log</b>	Displays the log file on the web page.





Debug	
<b>One-click Debugging</b>	
<b>One-click Debugging</b>	Capture the checked info in the debugging list, click "Start" to debug if including "Capture trace" item and click "Stop" to end, Click "Capture" in another situation. All retrieved files will be generated to a package, and the last package will be overwritten, while the trace file will stay remain.
<b>Debug Info Menu</b>	Display a list of info items that can be debugged, currently supports system logs, info log, capture package, tombstones and ANR log. The captured data can be viewed in "Debug information list". The default is all selected.
<b>Debug Info List</b>	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
<b>View Debug Info</b>	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
<b>Core Dump</b>	
<b>Enable Core Dump Generation</b>	Configures whether to generate and save the core dump file when the program crashes. The default setting is "No".  <b>Note:</b> Reboot the device to make changes take effect.
<b>Core Dump List</b>	Selects the existing core dump file in the drop-down box. Users could delete the file by pressing on "Delete" button.
<b>View Core Dump</b>	Press "List" button to view all existing core dump files. The files are listed in chronological order, users could click the file name to download the file to the local computer.
<b>Record</b>	
<b>Record</b>	Click to start capturing audio data, click the "Stop" button to end. To capture the audio data of the device can help to locate audio issues. The default is not enabled. You can record up to 1 minute audio data.
<b>Recording List</b>	Choose the existing audio file. Click the "Delete" button on the right to delete this file.
<b>View Recording</b>	Click on the "List" button to view. The captured audio data will be sorted by time. Click to download the data to the computer for analysis.
Traceroute	
<b>Target Host</b>	The IP address or URL for the Target Host of the Traceroute.  Press <b>Start</b> to send traceroute request to configured target host.  Press <b>Stop</b> to end traceroute running process.



Ping	
<b>Target Host</b>	The IP address or URL for the Target Host of the Ping. Press <b>Start</b> to send traceroute request to configured target host. Press <b>Stop</b> to end traceroute running process.
NSLookup	
<b>Hostname</b>	Enter a host name and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.

## Event Notification

Set the URL for events on phone web GUI, and when the corresponding event occurs on the device, the device will send the configured URL to SIP server. The dynamic variables in the URL will be replaced by the actual values of the device before sending to SIP server, in order to achieve the purpose of events notification. Here are the standards:

1. The IP address of the SIP server needs to be added at the beginning and separate the dynamic variables with a "/".
2. The dynamic variables need to have a "\$" at the beginning. For example: local=\$local
3. If users need to add multiple dynamic variables in the same event, users could use "&" to connect with different dynamic variables. For example: 192.168.40.207/mac=\$mac&local=\$local
4. When the corresponding event occurs on the device, the device will send the MAC address and phone number to server address 192.168.40.207.

<b>On Boot Completed</b>	Configures the event URL when phone boots up.
<b>Incoming Call</b>	Configures the event URL when phone has an incoming call.
<b>Outgoing Call</b>	Configures the event URL when phone has an outgoing call. <b>(Available for GSC3510 only)</b>
<b>Missed Call</b>	Configures the event URL when the device has new a missed call.
<b>On Connected</b>	Configures the event URL when a call is established.
<b>On Disconnected</b>	Configures the event URL when a call is disconnected.
<b>Forward On</b>	Configures the event URL when the forward feature is enabled on the device.
<b>Forward Off</b>	Configures the event URL when the forward feature is disabled on the device.
<b>On Blind Transfer</b>	Configures the event URL when users transfer a call with blind transfer on the device.



<b>On Attended Transfer</b>	Configures the event URL when users transfer a call with attended transfer on the device.
<b>Log On</b>	Configures the event URL when users log on the device successfully.
<b>Log Off</b>	Configures the event URL when users log off the device.
<b>On Register</b>	Configures the event URL when an account in the device is registered successfully.
<b>On Unregister</b>	Configures the event URL when an account in the device is unregistered.

## Application Page Definitions

### LDAP Book

<b>Connection Mode</b>	Selects which protocol will be used for LDAP searching, LDAP or LDAPS.
<b>Server Address</b>	Configures the URI of the LDAP server.
<b>Port</b>	Configures the LDAP server port. The default LDAP port number is 389.
<b>Base DN</b>	Determines 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>User Name</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>	Specifies the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
<b>LDAP Name Attributes</b>	Configures 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> cn sn description
<b>LDAP Number Attributes</b>	Configures 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 Mail Attributes</b>	Determines the "mail" attributes of each record which are returned in the LDAP search result. <u>Example:</u> mail
<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 Number Filter</b>	Defines 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 Mail Filter</b>	Determines the filter used for mail lookups. <u>Example:</u> (mail=%)
<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. Default setting is 50.
<b>Search Timeout (s)</b>	Configures the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 4 seconds.
<b>LDAP Lookup For Dial</b>	Sets the device to do the LDAP number searching when making outgoing calls. The default setting is "No".
<b>LDAP Lookup For Incoming Call</b>	Sets the device to do LDAP number searching for incoming calls. The default setting is "No".
<b>LDAP Dialing Default Account</b>	Configures the default account that being used when dialing LDAP contact. Users may choose the Account 1-16, the default setting is "Default".

## Recording

<b>File name</b>	Displays the name of the recording file.
<b>Duration</b>	Displays the duration of the device call.
<b>Date</b>	Displays the date the call was recorded on.



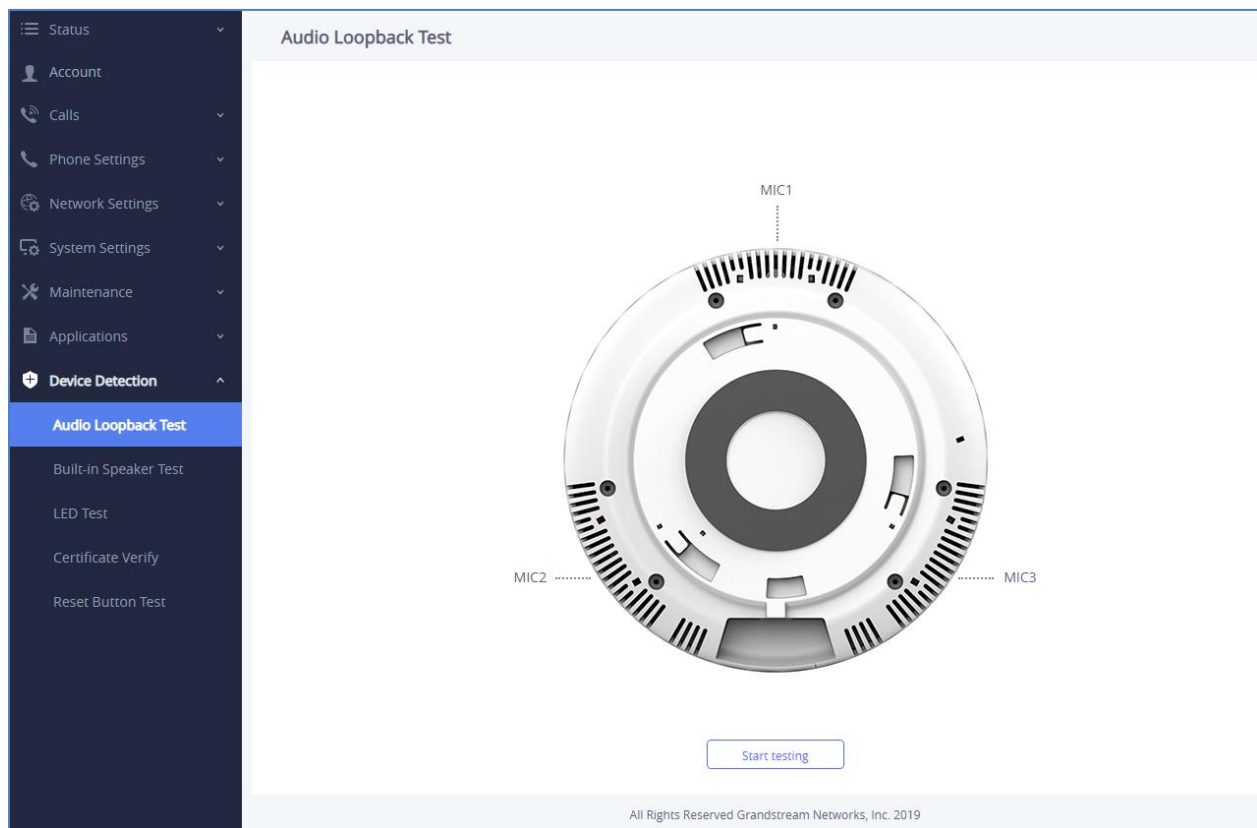
<b>Operation</b>	Delete, Modify, lock or download the recording file.  <b>Notes:</b> <ul style="list-style-type: none"> <li>• A recording file cannot be deleted if it is locked.</li> <li>• Users can delete a bench of recording files by clicking on “Delete”.</li> </ul>
------------------	---

## Device Detection Page Definitions

### Audio Loop Test

*Available for the GSC3510 only*

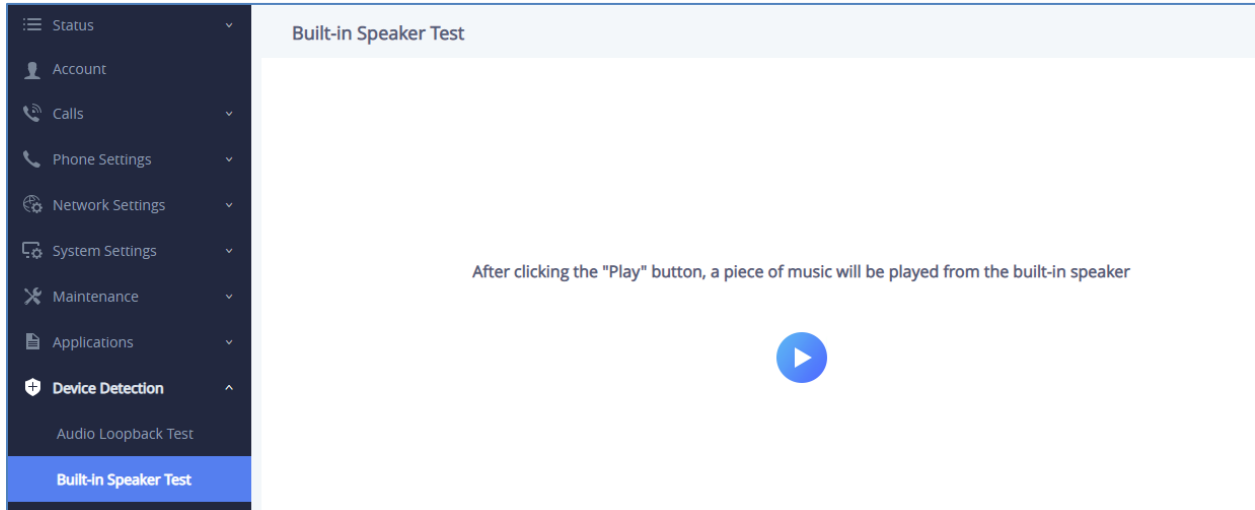
Audio loop test is used to test the three MICs available on the GSC3510. Each one of the MICs is tested separately.



**Figure 53: Device Detection - Audio Loop Test**

### Built-in Speaker Test

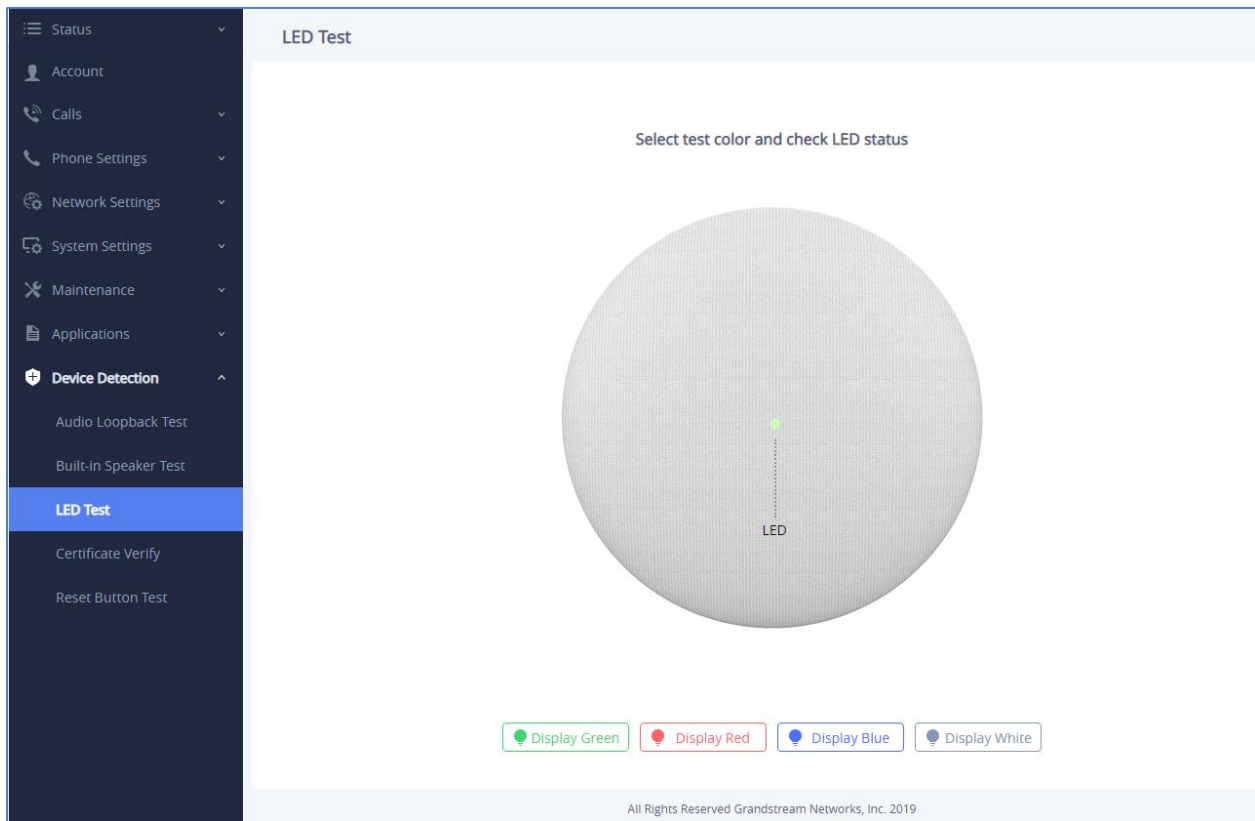
Built-in Speaker Test is used to test the GSC3510/GSC3505 by playing a piece of music in order to verify the sound quality.



**Figure 54: Device Detection - Built-in Speaker Test**

## LED Test

Led Test is used to test the availability of the four colored LEDs and their intensity. The colors of LEDs available on the GSC3510/GSC3505 are: Green, Red, Blue and White.



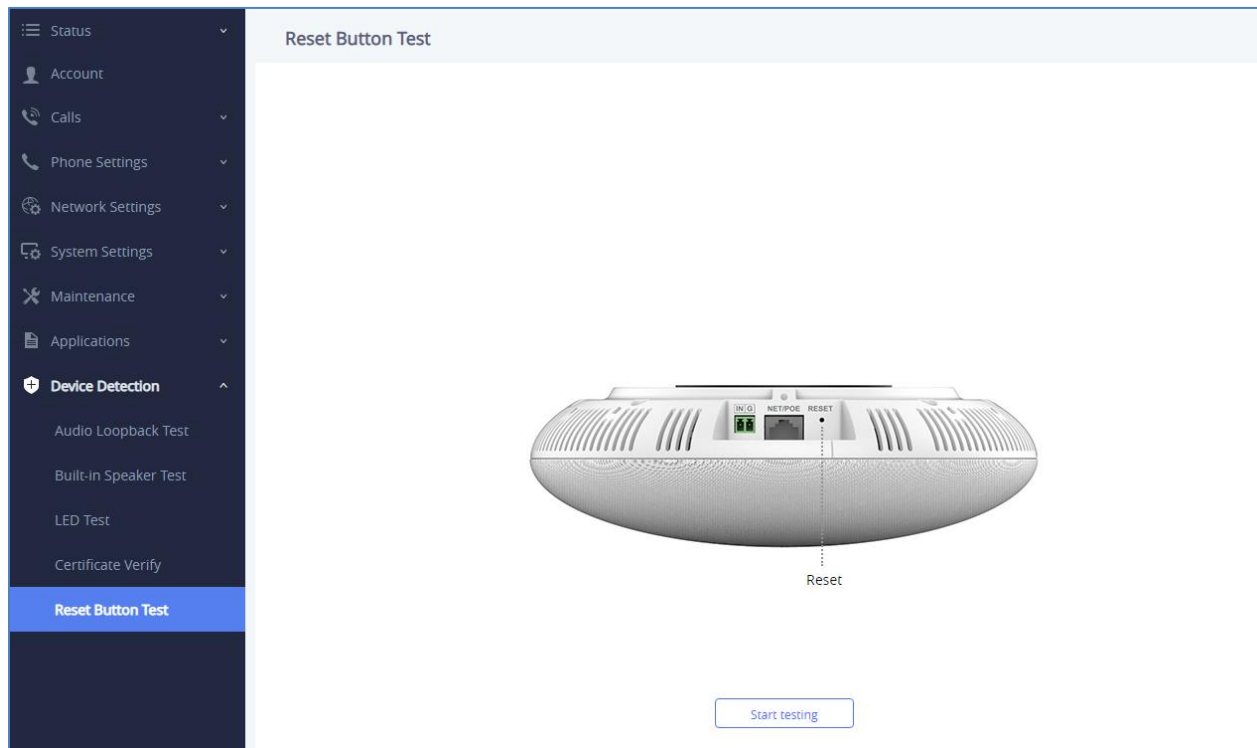
**Figure 55: Device Detection - LED Test**

## Certificate Verify

Certificate Verify is used to test the validity of the existing certificate.

## Reset Button Test

Reset Button Test is used to test the Reset button, during the test the reset button doesn't trigger factory reset, this feature allows the user to check if the button is responding.



**Figure 56: Device Detection - Reset Button Test**

## EXPERIENCING THE GSC3510/GSC3505

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 of your questions. Contact a technical support member or [submit a trouble ticket online](#) to receive in-depth support.

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

© 2002-2014 OpenVPN Technologies, Inc.

OpenVPN is a registered trademark of OpenVPN Technologies, Inc.

