Grandstream Networks, Inc.

GSC3574/75 – User Manual

WELCOME

The GSC3574/3575 is a powerful intercom and facility control station designed to provide businesses with a dedicated device to manage facility communications, door access, physical security, and more. This device can be wall-mounted as a solution for easy door control, intercom and paging communication, security camera management, and facility-wide UC integration. The GSC3574/3575 features a 7-inch touchscreen LCD and full duplex 2-way HD audio. It offers flexible network connectivity through a 100 Mbps network port with PoE or integrated dual-band Wi-Fi 6 support. This SIP intercom and facility control station is designed to seamlessly integrate with Grandstream's entire range of products, including the GDS series of Door Access devices, GSC series intercom and paging devices, security cameras, and more. The GSC3574/3575 is ideal for any deployment scenario where facility access, communications, and security need to be centrally monitored and controlled.

PRODUCT OVERVIEW

Feature Highlights

The following tables contain the major features of GSC3574/75.

 GSC3574  GSC3575	• 1x 10/100M adaptive port with integrated PoE • 7″ 1024×600 capacitive touch screen TFT LCD • 2x 1.5W, 8ohm, 99±3dB, Size 25*16mm, f0=850Hz high-fidelity speakers • 8 channels alarm in, 2 relays alarm out • Integrated Bluetooth • Wi-Fi 6 , dual-band 802.11a/b/g/n/ac/ax (2.4GHz & 5GHz) • 6 SIP account, 2-way call • Secure Boot & Data, TLS and SRTP security encryption technology to protect calls and accounts • Visual intercom • Advanced noise suppression and echo cancellation technology • One-click switch custom intelligent defense deployment

GSC3574/75 Features at a Glance

GSC3574/75 Technical Specifications

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

Protocol/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, 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, Open VPN
Network Interface	1x 10/100M adaptive port with integrated PoE
Graphic Display	7" 1024×600 capacitive touch screen TFT LCD
Memory	2GB RAM, 8GB eMMC Flash
Wi-Fi	Yes, dual-band Wi-Fi 6 802.11 a/b/g/n/ac/ax (2.4GHz & 5GHz)

Bluetooth	Yes, integrated Bluetooth
Auxilliary Ports	1x type-A USB 2.0 port, 1 x micro-SD card socket
Alarm Input	8 Channels, 6x Alarm Short-In, 2x Alarm Voltage-In
Alarm Output	2 Relays, max 125VAC/0.5A or 30VDC/2A, Normal Open or Normal Close
Device Color	GSC3574: White; GSC3575: Black
Voice Codecs and Capabilities	G.711μ/a, G.722 (wide-band), G.726-32, iLBC, Opus, G.729A/B,in-band and out-of-band, DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Video Decoders and Capabilities	H.264 BP/MP/HP and M-JPEG streaming, video resolution up to 720p, frame rate up to 30 fps, bit rate up to 2Mbps
Telephony Features	6 SIP Accounts, Hold, Call Waiting, Call Log, Auto Answer, etc.
Sample Applications	Local apps: Contacts, Call History, Settings, Voicemail, File Manager API/SDK available to allow integration with 3rd party door system products
Operating System	Android 13
HD Audio	Yes, Dual speakers with support for wideband audio and media play in stereo, one built-in microphone for improved voicer quality, acoustic echo cancellation
AI Features	Voice Recognition (glass shattering gunshot, crying, yell for help, etc.), Voice Assistant, Voice Changer(Female voice to male voice).
QoS	Layer 2 (802.1Q, 802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS Secure Boot & Data, Double images for high reliability, random administrator
Security	password, user and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES based secure configuration file, SRTP, TLS, 802.1x media access control
Multi-language	English, German, Italian, French, Spanish, Portuguese, Russian, Polish, Hebrew, Czech, Dutch, Turkish, Swedish, Ukrainian, Arabic, Chinese, Korean, Japanese and more
Upgrade/Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file, manual upload, SD card upgrade, USB upgrade
Power & Green Energy Efficiency	2-pin DC input: 12VDC/1.5A Integrated PoE : IEEE 802.3af Class 3, power consumption <13W
Temperature and Humidity	Operation: 0°C to 40°C, Storage: -10°C to 60°C, Humidity: 10% to 90% Non-condensing
Physical	Unit Weight: 408g; Package Weight: 729g Unit Size: 182mm x 122 x 26.2 Box Size: 230mm x 154 x 67
Package Contents	GSC3574/GSC3575 unit, Quick installation guide, 0°wall mount bracket, 20°desktop/ wall mount bracket, Adhesive tape, 6*expansionors anchors and 8* screws

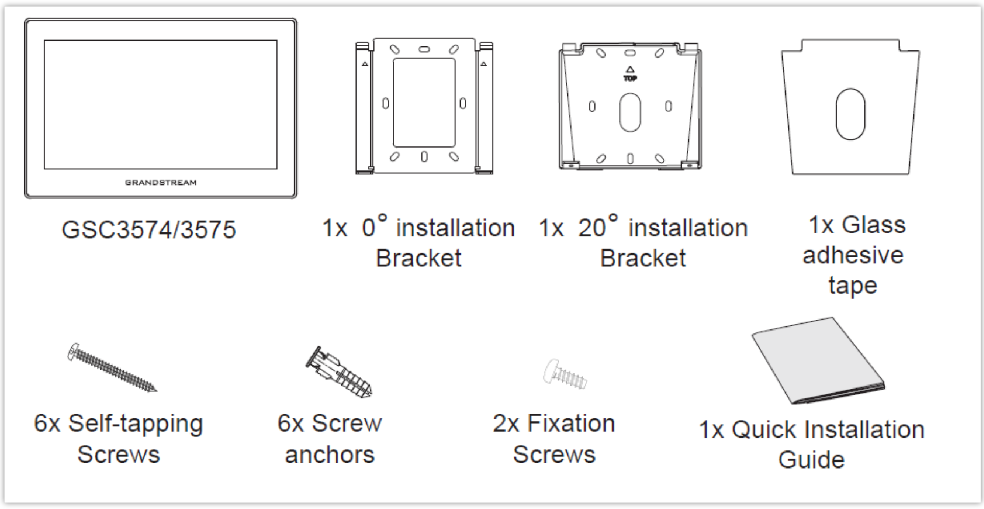
GETTING STARTED

This chapter provides basic installation instructions, including a list of the packaging contents and information for obtaining the best performance with the GSC3574/75.

Equipment Packaging

GSC3574/75
• 1x GSC3574/3575 • 1x 0° installation Bracket • 1x 20° installation Bracket • 1x Glass adhesive tape • 6x Self-tapping Screws • 6x Screw anchors • 2x Fixation Screws • 1x Quick InstallationGuide

Equipment Packaging



GSC3574/75 Package Content

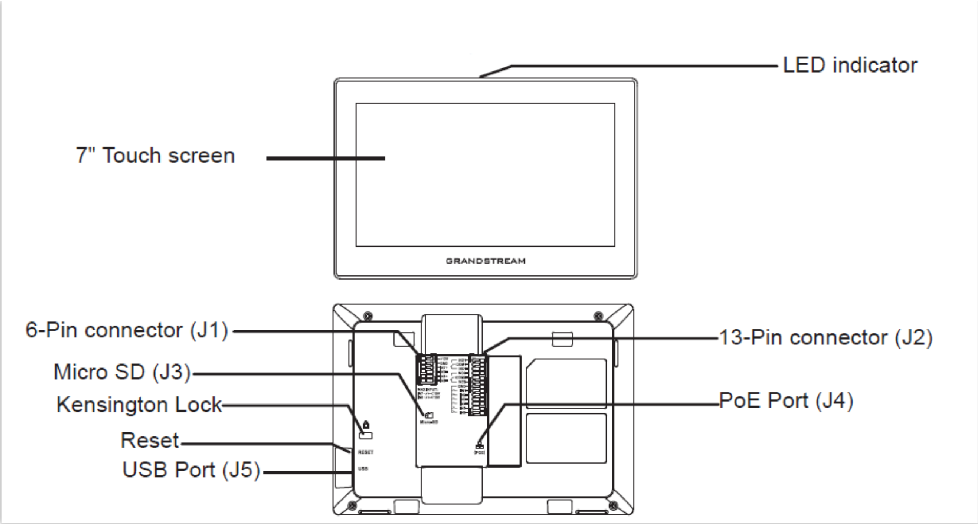
Note

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

GSC3574/75 Setup

The GSC3574/3575 can be mounted on the wall, the glass, or on the desktop using a 20 ° bracket. Please refer to the following steps for installation:

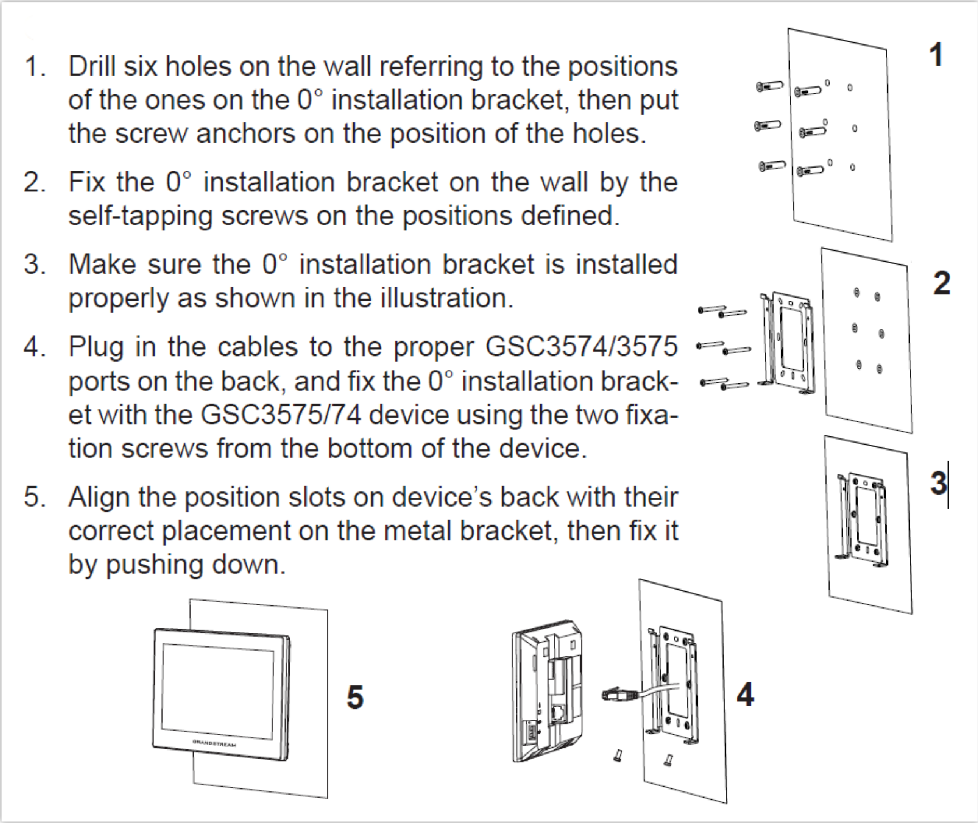
The following illustration shows the different ports and interfaces of the GSC3574/75 device.



Built-in Stand and Mounting Slots on The GSC3574/75

On-Wall 0° Mount

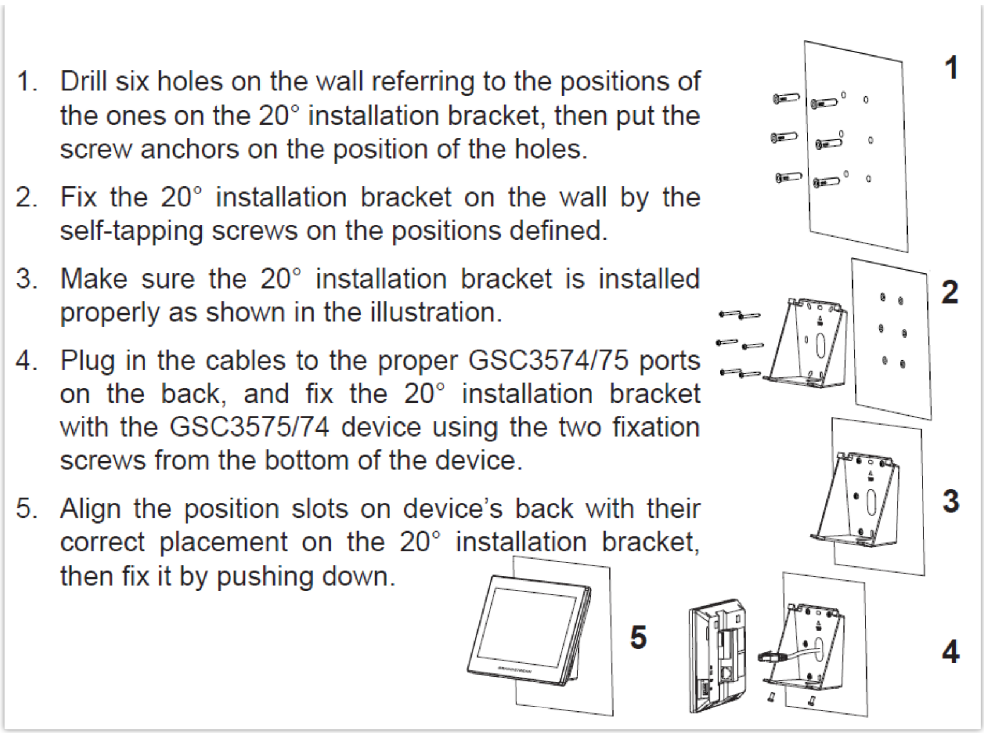
The GSC3574/75 can be mounted on the wall at 0° level. Please refer to the following steps for installation:



0 Degree On-wall Mounting

On-Wall 20° Mount

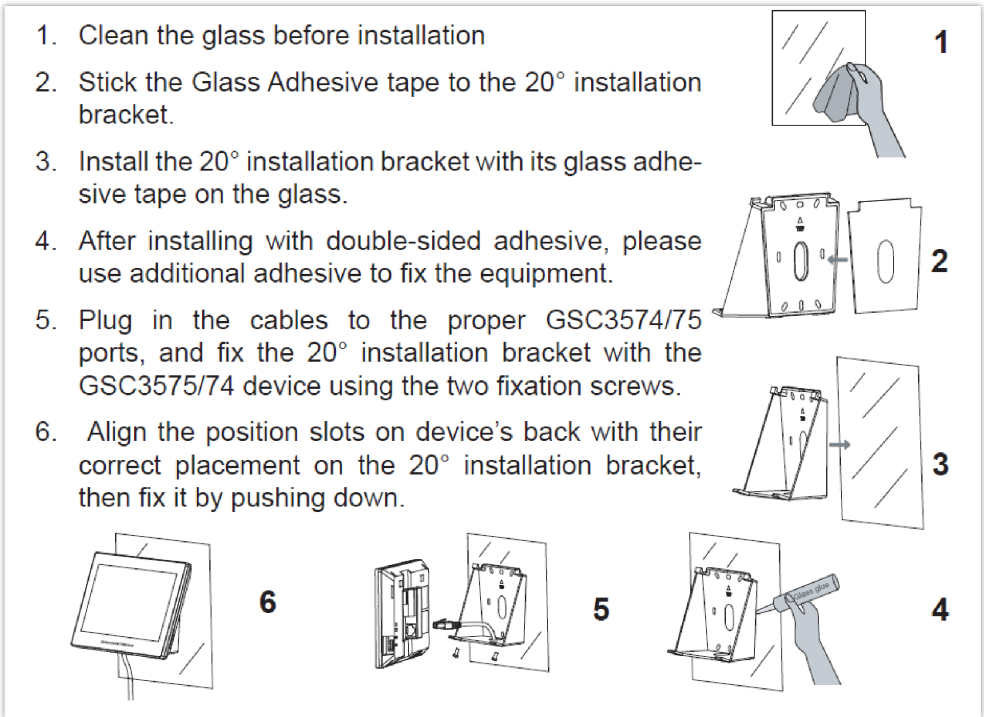
The GSC3574/75 can be mounted on the wall at a 20° angle. Please refer to the following steps for installation:



20 Degree On-Wall Mounting

On-Wall Glass Adhesive Mount

The GSC3574/75 can be mounted on a glass surface using glass adhesive tape. Please refer to the following steps for installation:



On-Wall Glass Adhesive Mount

Connecting the GSC3574/75

Note

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

To set up your GSC3574/75 from the web interface, please follow the steps below:

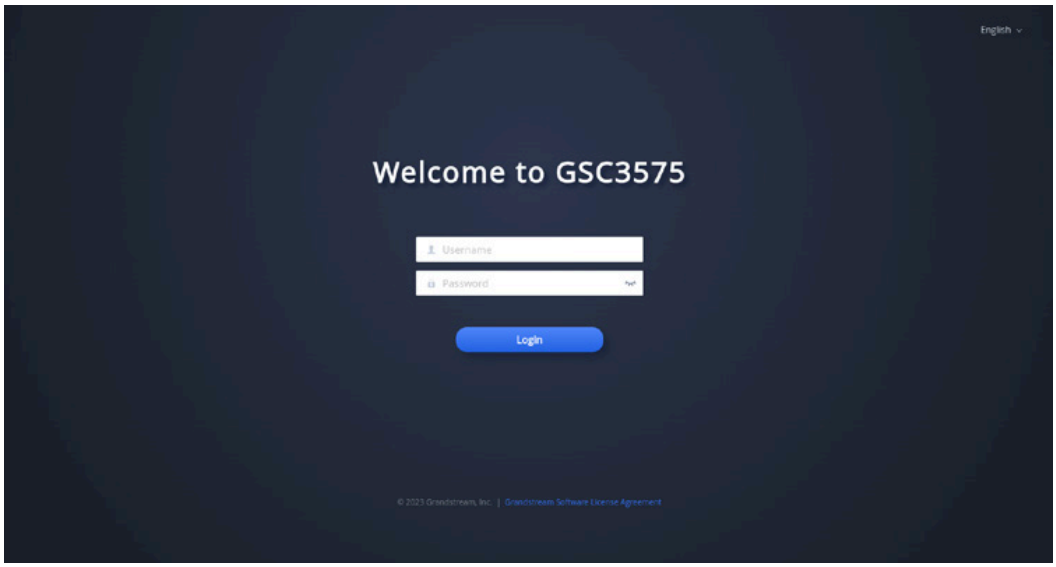
1. Ensure your device is powered up and connected to the Internet.

2. Press “Settings” on the Home Page.

3. Select “Network Status” to check the IP address.

4. Type the unit’s IP address in your PC browser. (See figure below).

5. Enter the admin’s username and password to access the configuration menu.



GSC3574/75 web interface

To set your GSC3574/75 from the LCD, please follow the steps below:

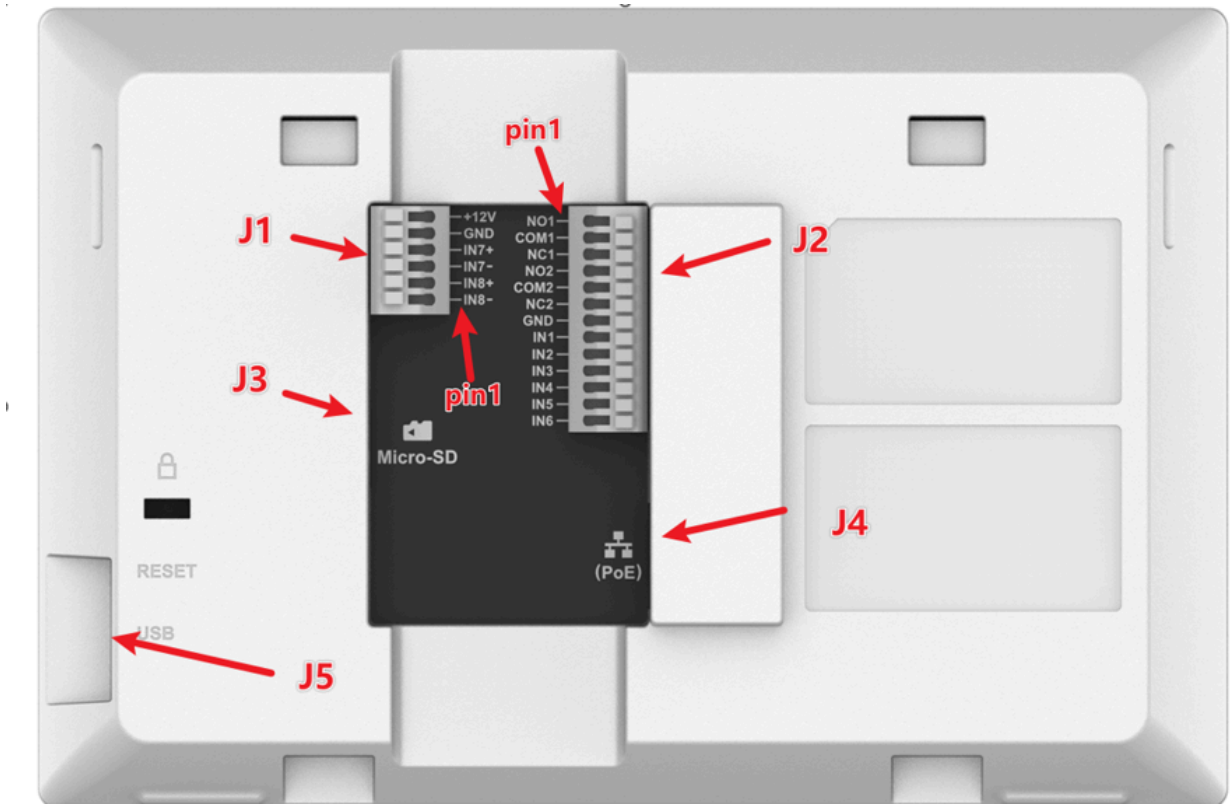
1. Make sure the device is idle.

2. Press “Settings”. Browse the GSC3574/75 MENU for Status, Network information, Features, and Basic/Advanced Settings…

3. Swipe up to go back to the idle screen.

GSC3574/75 Wiring Connection

The following figure and table show the Connection PINs available on the GSC3574/75:



Jack	Port		Function	Remark
	Pin	Signal		
J1	1	IN8-	Alarm IN8(Active)	Isolation type alarm input, used for voltage signal detection, IN+ connected to positive signal output of sensor, IN- connected to negative signal output of sensor or GND of sensor. The active voltage range is 9-15V.
	2	IN8+		
	3	IN7-	Alarm IN7 (Active)	
	4	IN7+		
	5	GND	Power Supply	DC12V recommend, input voltage rang 11-13V, current at least 1.5A@12V.
	6	+12V		
J2	1	NO1	Alarm OUT1	Relay output, normal open or close, max 125VAC/0.5A or max 30VDC/2A.
	2	COM1		
	3	NC1		
	4	NO2	Alarm OUT2	
	5	COM2		
	6	NC2		
	7	GND	Alarm GND	Voltage reference for IN(1/2/3/4/5/6).
	8	IN1	Alarm IN1(Passive)	Alarm input, used to connect devices such as buttons/ switches/ alarm sensors.
	9	IN2	Alarm IN2(Passive)	
	10	IN3	Alarm IN3(Passive)	
	11	IN4	Alarm IN4(Passive)	
	12	IN5	Alarm IN5(Passive)	
	13	IN6	Alarm IN6(Passive)	
J3	Micro-SD Port		Data Storage	Support microSD/ SDHC/ SDXC, up to 512GB.
J4	Network Port(PoE)		Ethernet and PoE Supply	Single 10/100Mbps network port, support 802.3 af PoE power supply.

J5	USB Port	Data Exchange	The USB port can be connected to USB disk (up to 2TB) / mouse/ keyboard. The default current limit is 460mA, and user can configured it to 1000mA through the web.

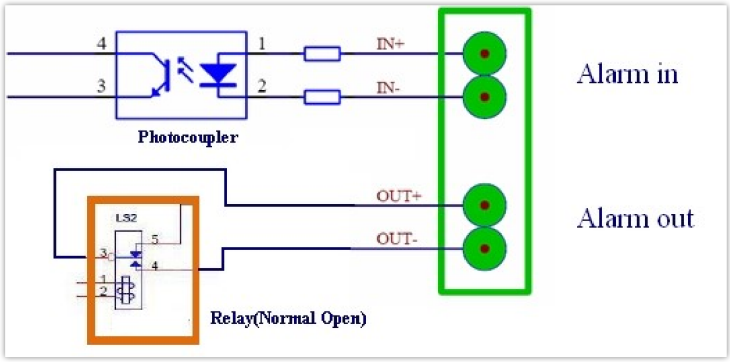
GSC3574/75 Wiring Connection

> **Warning**
>
> Please disconnect the power supply during wiring, disassembly, and other operations. Do not operate with electricity on.

Alarm IN/OUT PINS

- **Alarm_IN** pins are used to connect external sensors or detectors that detect events like motion, door/window openings, or smoke. These pins trigger the control station when an alarm condition is detected.
- **Alarm_Out** pins are used to connect to external devices such as sirens, lights, or notification systems. When the control station detects an alarm condition, it sends a signal through these pins to activate the connected external devices.

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



Alarm_In/Out Circuit

Notes:

- The Alarm_In and Alarm_Out circuit for the GSC3574/75 should meet the following requirement:

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

- In the Alarm_In circuit, if there is any voltage change between 9V and 15V, as specified in the table above, the GSC3574/75 Alarm_In port will detect it and trigger the action and event.
- Higher voltage and wrong polarity connections are prohibited because this will damage the devices.

There is also an important distinction between the two types of **Alarm_IN**, Passive, and Active:

- **Alarm In (Active):** This type of input involves sensors or detectors that actively send a signal to the control station when a specific event or condition is detected. For example, a motion sensor might actively trigger the alarm in (active) input when it detects movement in its monitored area. These sensors require power and actively transmit signals when they detect something. The pins that are responsible for **Alarm In (Active)** in the GSC3574/75 are **IN7+/IN7-** and **IN8+/IN8-**
- **Alarm In (Passive):** This refers to inputs that respond to changes in their environment without actively transmitting signals to the control station. These inputs include simple contact sensors on doors or windows. They do not actively send signals but instead rely on changes in their status (e.g., open/close) to trigger the alarm input. They don't require power to send signals, but may need power for any internal mechanisms like switches or sensors. The pins that are responsible for **Alarm In (Passive)** in the GSC3574/75 are **IN1/IN2/IN3/IN4/IN5/IN6**.

Please refer to the GSC3574/75 PIN description section for more information on the PIN functionalities.

Basic Configurations

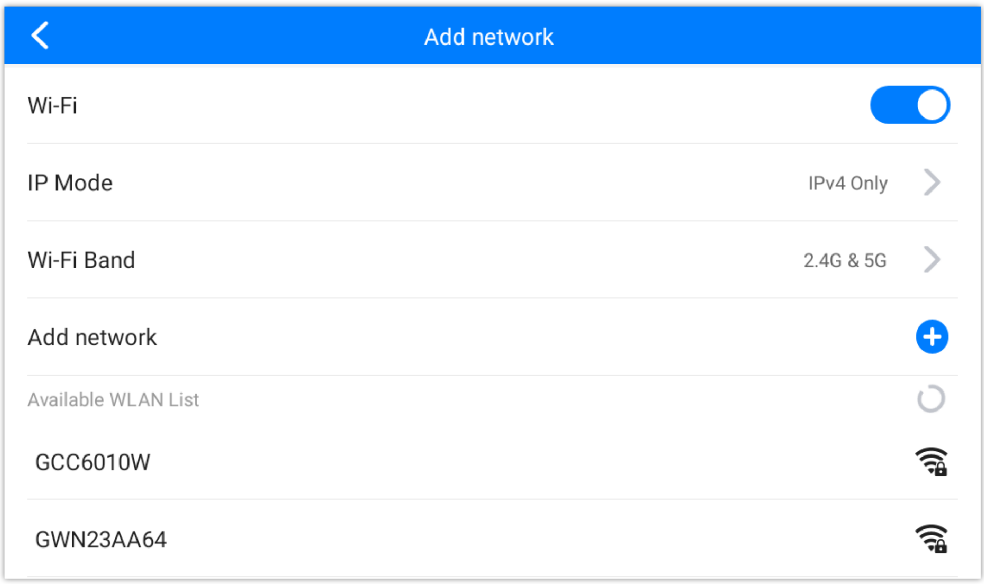
Connect to Wi-Fi

The GSC3574/75 supports Wi-Fi technology and can be connected from the LCD or the WEB UI configuration parameters.

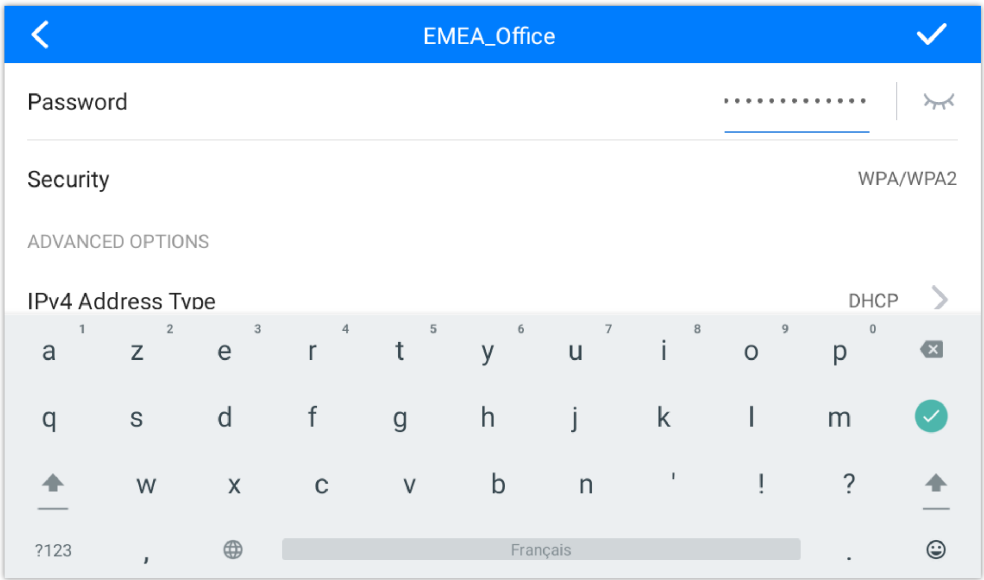
- **From LCD settings**

To connect the GSC3574/75 to Wi-Fi from the LCD settings, follow the steps below:

- Access **Settings** → **Network** → **Wi-Fi**
- Enable Wi-Fi Feature



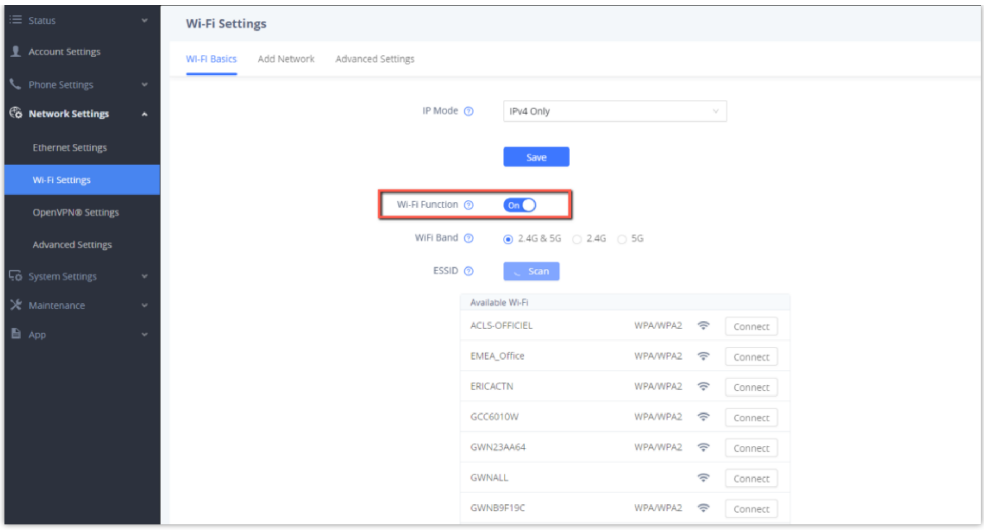
- Select the network that you want to connect to, from the list of discovered SSIDs, or manually add the SSID if it is set to be hidden.
- Provide the password, then connect to the Wi-Fi network once connected.



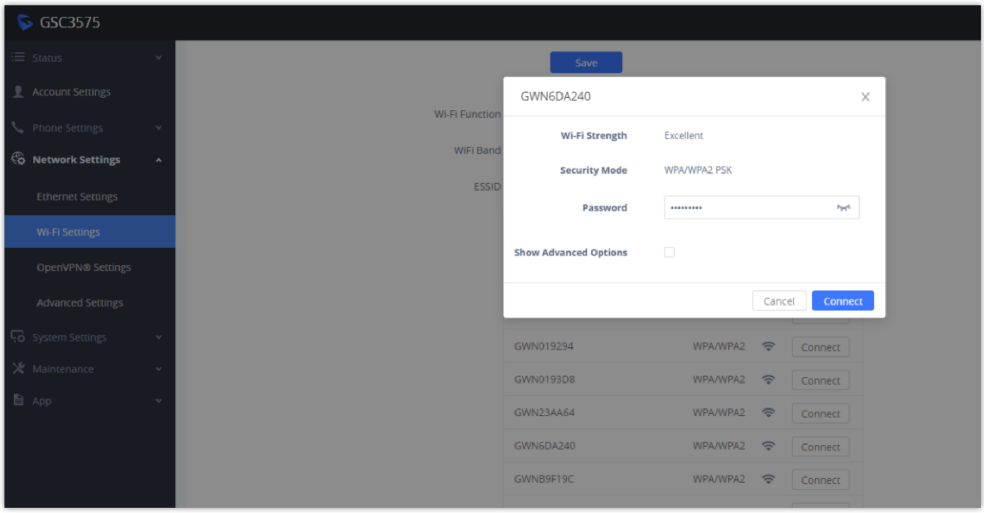
- **From the WEB UI settings**

You can connect to Wi-Fi from the network settings on the web UI. To do that:

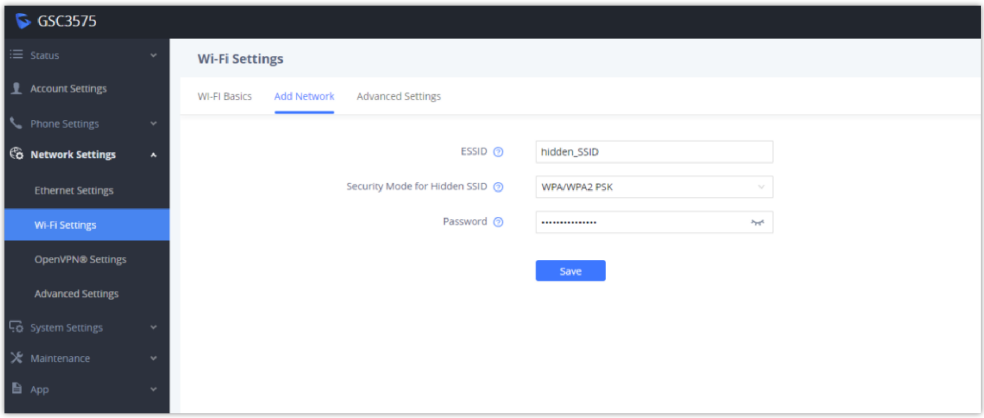
- Go to **Network Settings** → **Wi-Fi Settings** → **Wi-Fi Basics**
- Enable the **Wi-Fi function**



- Select a specific SSID you want to connect to, click on connect, then specify the security password



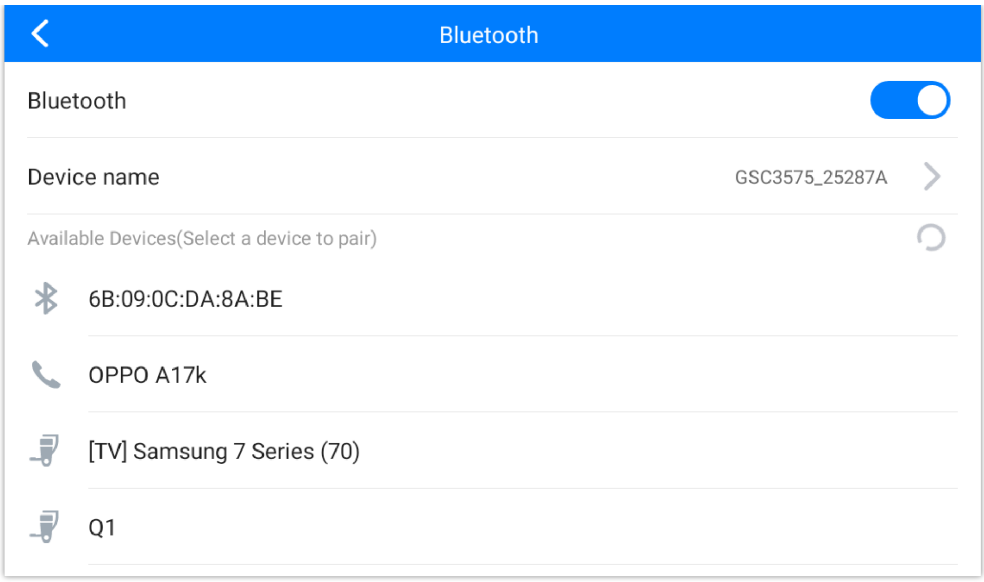
- The user can also provide the SSID manually if it is configured to be hidden



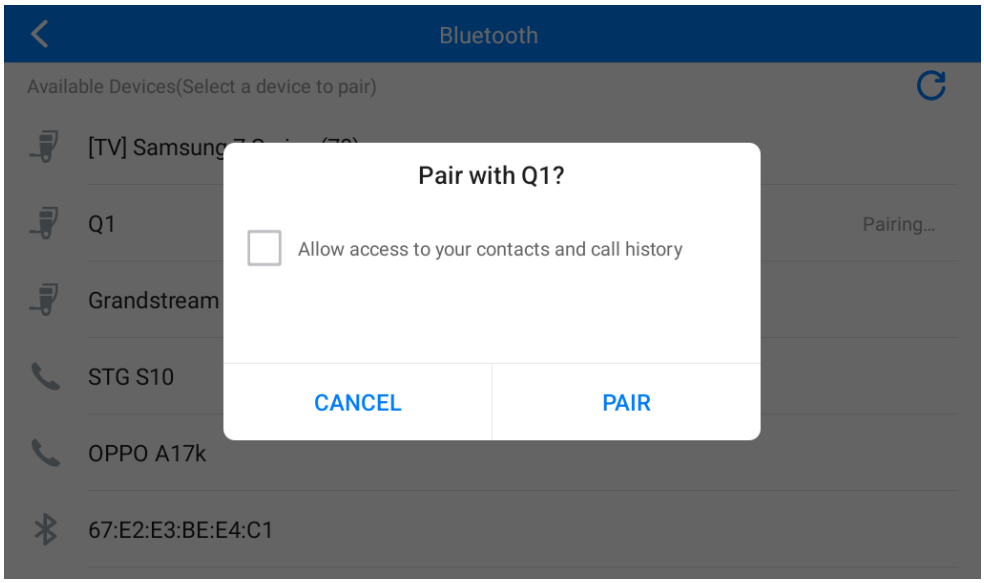
Connect to Bluetooth

The GSC3574/75 supports Bluetooth pairing to connect additional hardware devices like speakers and microphones for various purposes, to connect to Bluetooth:

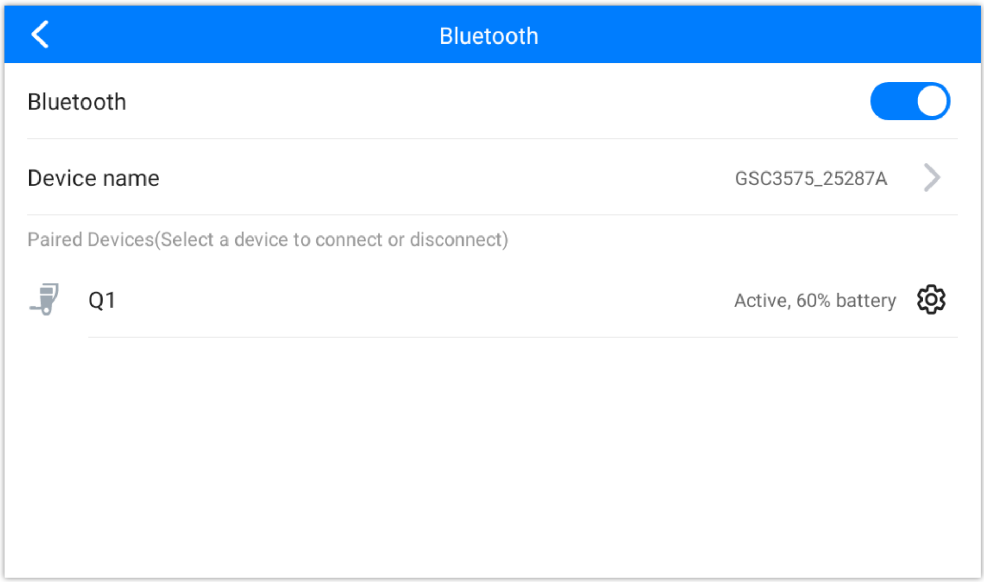
- On the LCD settings, go to **Settings → Features → Bluetooth**
- Enable Bluetooth, then select the device you want to pair, from the available list of devices.



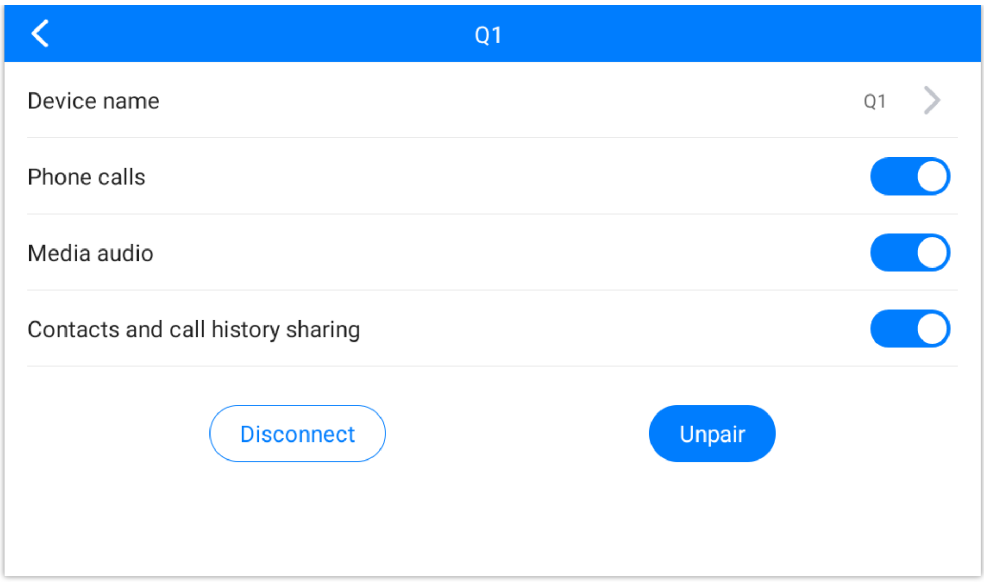
- Click on the device name to pair it, you can allow the paired device to have access to your contacts and call history



- Once connected, the device will be displayed as active and will display battery percentage information if provided from the paired device.



- Access the paired device settings to enable/disable certain authorizations.



Make a phone call

On the GSC3574/75, users can make SIP calls or direct IP calls.

1. Click the icon

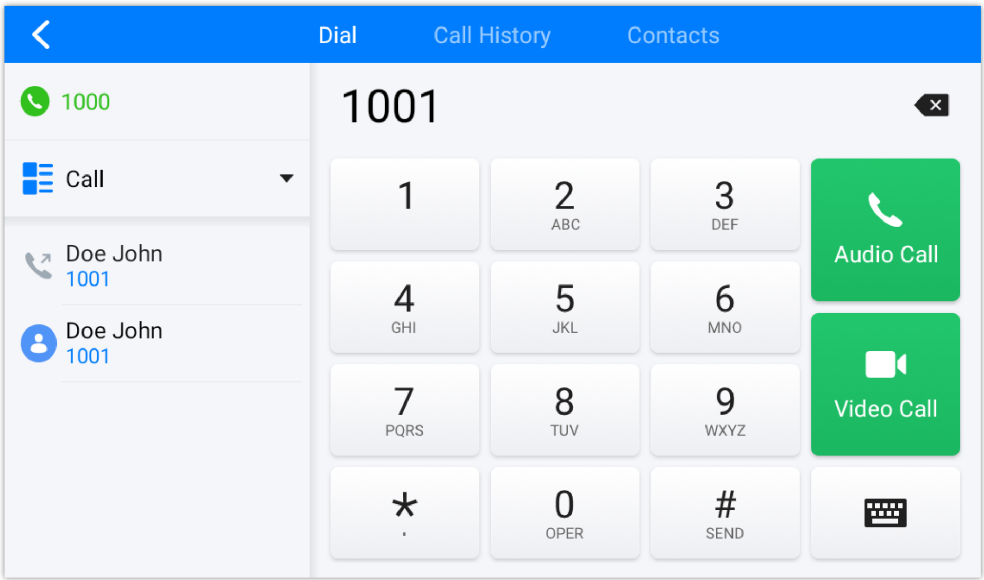
   on the home screen
2. Enter the extension number or IP address of the callee
3. Click the icon

   to initiate an audio call, or the icon

   to initiate a video call.



Make a phone call

View Call History

The call history of the GSC3574/75 can be viewed from the LCD screen.

1. Click the icon

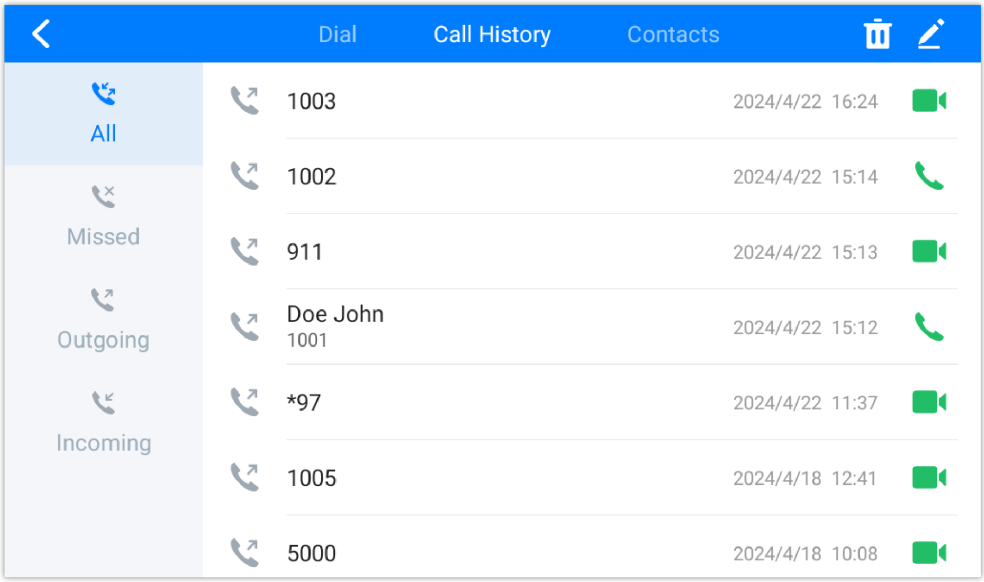
   on the home screen
2. Go to Call History, and a list of missed, outgoing, and incoming calls will be displayed, each on its tab.
3. Click the icon

   to delete all the call history, or the icon

   to select which call records to delete



View Call History

Arming Mode

The GSC3574/75 can be connected to 2 Active Alarm IN and up to 6 Passive Alarm IN inputs. Each detector input is linked to a Zone that can be set with different Alarm Actions (instant, delayed, 24-hour alarm).

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

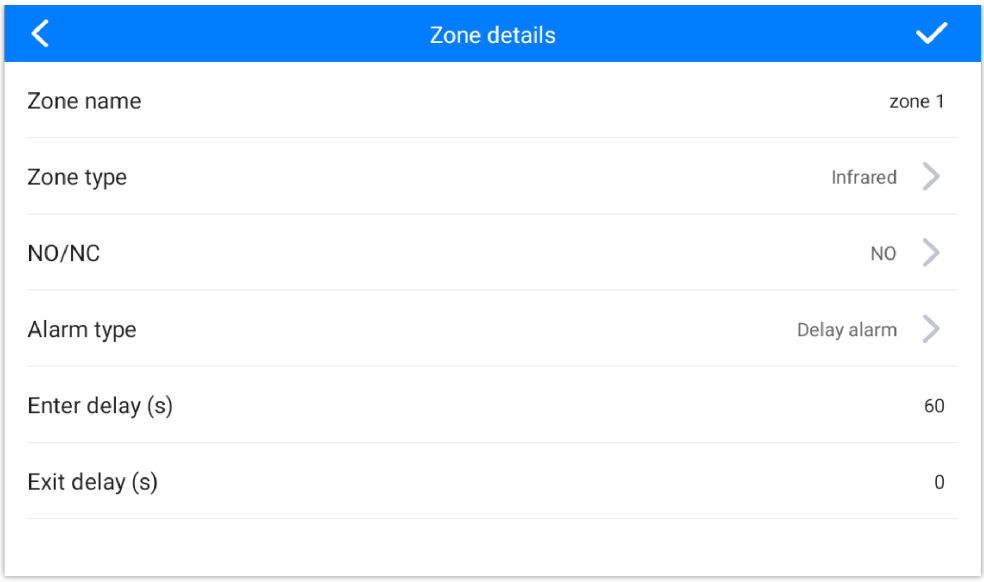
- **LCD Configuration**

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

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

1. Tap the first Zone to Edit
2. Set a new **Zone Name**.
3. Set **Zone Type** depending on the alarm input device used (Infrared, Smoke, Gas, etc.)
4. Depending on the alarm input type, you can set it to either NO or NC on **NO/NC**.
5. Set the **Alarm Type** to either choice: Instant Alarm, Delayed Alarm, or a 24h Alarm:

- **Instant Alarm:** The zone will alarm when triggered immediately.
- **Delayed Alarm:** The Enter Delay and Exit Delay will be applied.
- **24h Alarm:** The zone will be armed for 24h.

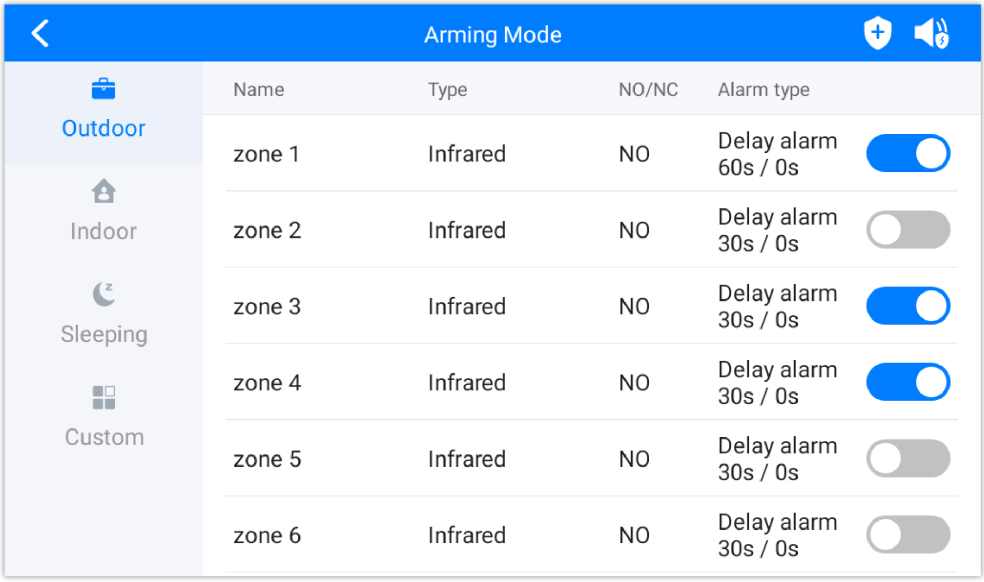


Features: Zone Settings

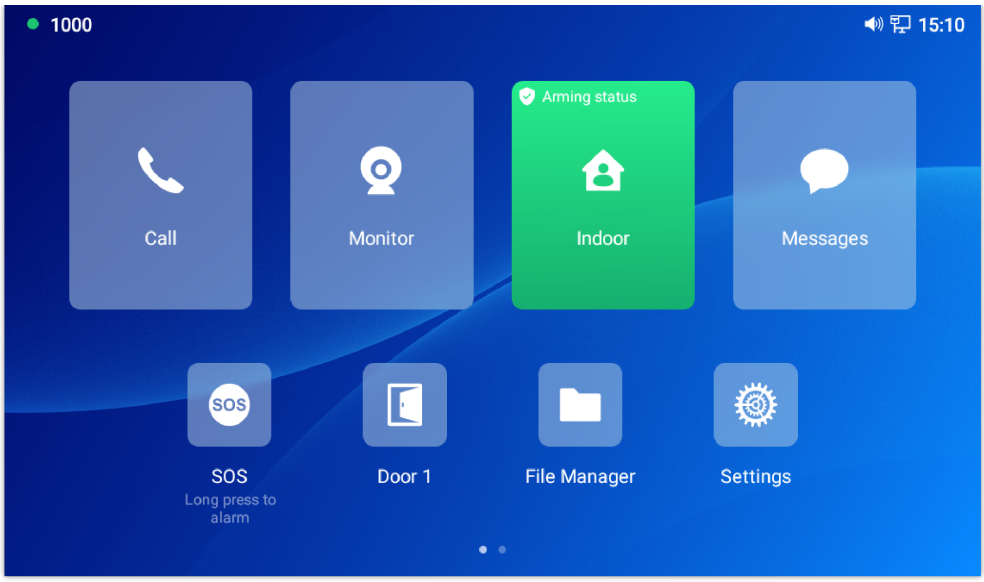
Notes:

- Both the Entering/Exiting Delay durations have a range from 0s to 60s.
- When the "Defense Zone Type" is "Open Door", then you can configure the associated "DO Settings to "Open Door Mode".
- The GSC3574/75 supports up to 8 zones.
- Once the Zone(s) are configured, proceed from **Features → Arming Mode:**

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



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



Features: Arming Status

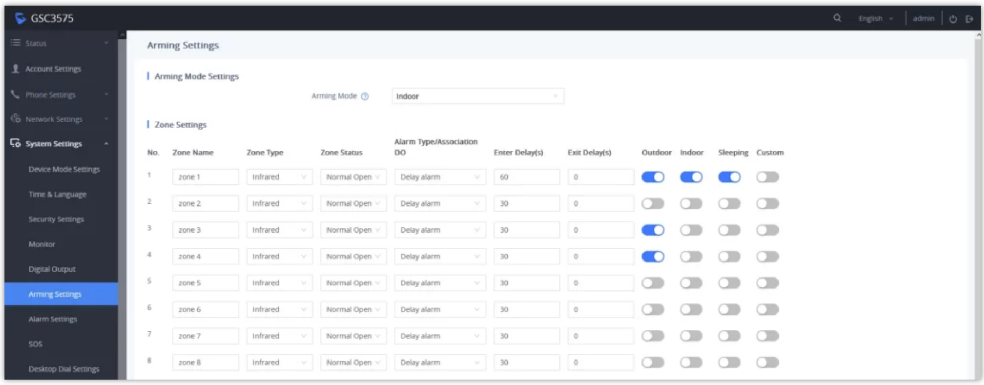
- **Web UI Configuration**

From the Web UI, you can configure the arming mode settings as shown below:

1. Go to **System Settings → Arming Settings**
2. Select the zone you want to edit.
3. Set a new **Zone Name**.
4. Set **Zone Type** depending on the alarm input device used (Infrared, Smoke, Gas, etc.)
5. Depending on the alarm input type, you can set it to either NO or NC on **NO/NC**.
6. Set the **Alarm Type and Digital Output Association** to either choice: Instant Alarm, Delayed Alarm, or a 24-hour Alarm.

- **Instant Alarm:** The zone will alarm when triggered immediately.
- **Delayed Alarm:** The Enter Delay and Exit Delay will be applied.
- **24h Alarm:** The zone will be armed for 24h.

7. Enable the zone settings for the corresponding Arming mode



Arming Mode Settings

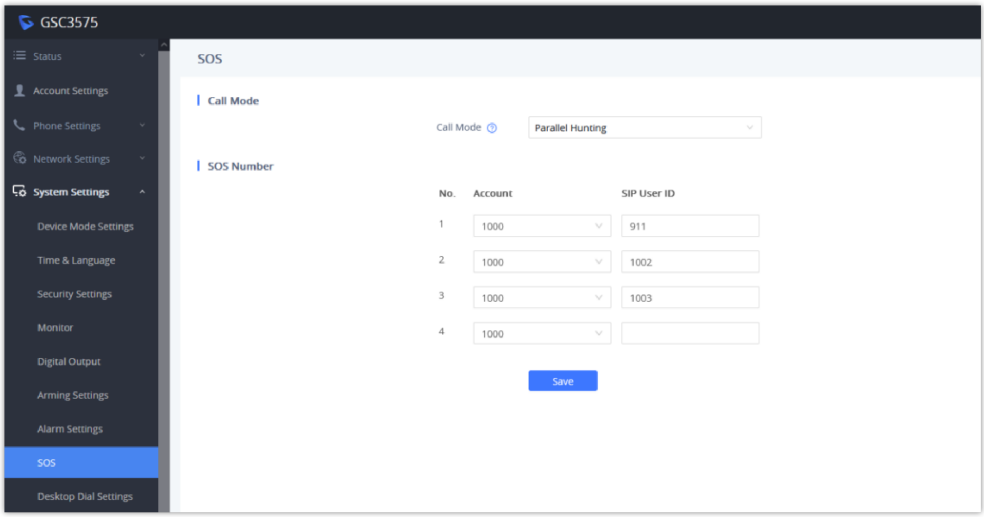
SOS Calling

The GSC3574/75 can be configured with an SOS key, as when this key is pressed, the GSC3574/75 will ring the extension(s) configured under the SOS panel from either the web GUI or LCD Menu.

- **Web interface configuration:**

1. Access **Settings → SOS.**
2. Set **Call Mode** to either Serial Hunting, where each number will be called one after one based on the order from 1-4 after the first call times out, or Parallel Huntin,g where all configured numbers receive the call simultaneously.

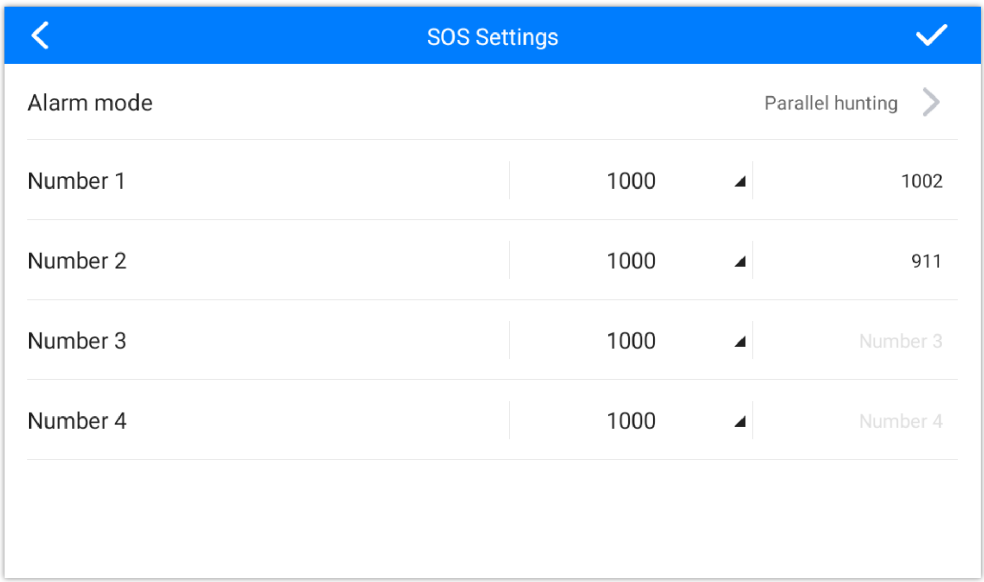
3. Select the **Account** from which the call will be made and enter the SIP extension or IP address to be called. (Default is Dynamic, so the GSC will use the first available line).
4. Click on **Save**.



SOS: Web Configuration

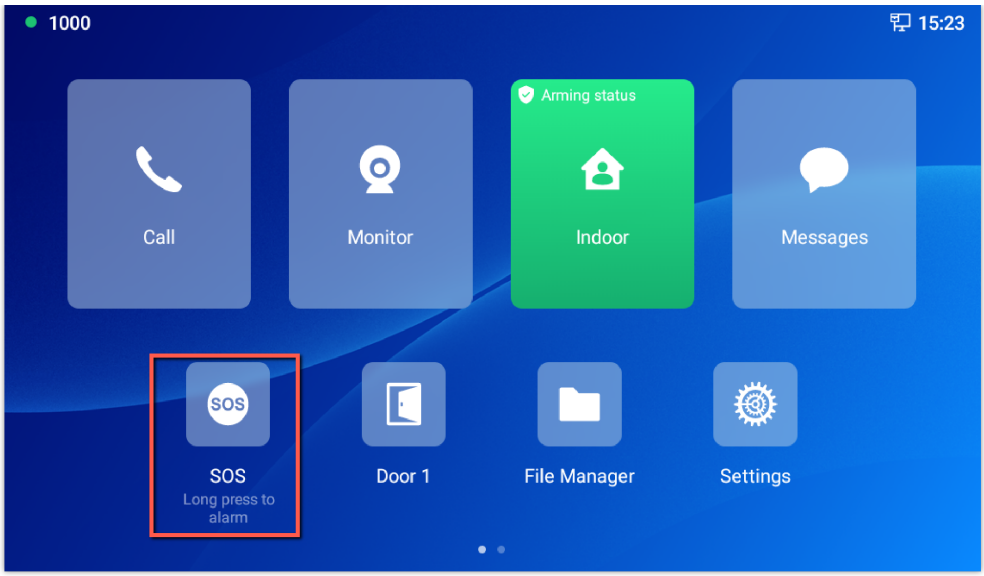
- **LCD configuration:**

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



SOS: LCD Configuration

To trigger the SOS action, long-press the SOS icon on the LCD main menu



SOS: Triggering the action

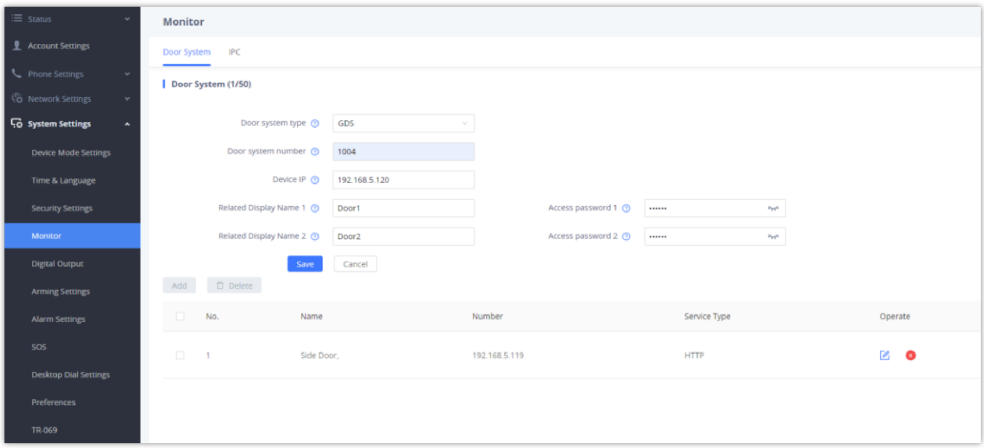
Interconnection with GDS37xx

The GSC3574/75 can be configured with up to 50 GDS37xx devices, allowing two doors of remote control per GDS. The configuration is done as follows:

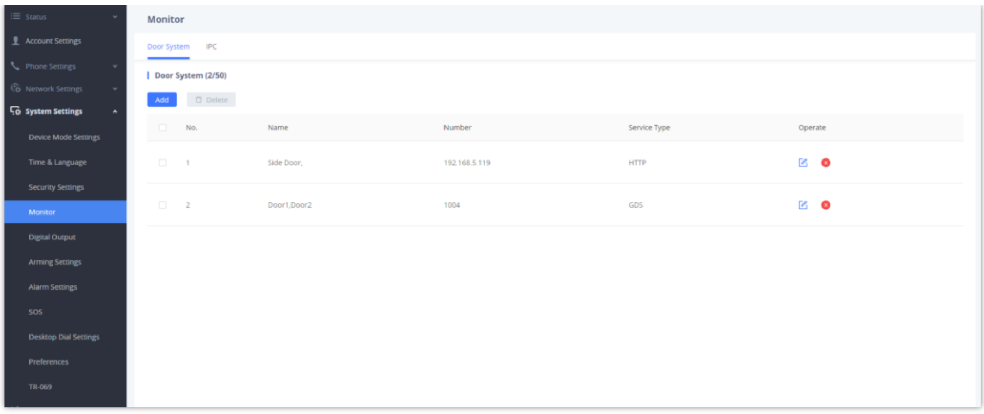
Web interface configuration:

1. Access **System Settings → Monitor.**
2. Click to add a new door system

3. Select the **Service Type**, it could be **GDS**, **Others, or HTTP** in case you want to integrate GSC3574/75 with a third-party Door Access Control system.
4. Set the GDS SIP Number (or IP address in case of the peering scenario) on the Door system number.
5. Enter **Related Display Name 1**.
6. Enter **Access Password 1**.
7. Enter **Related Display Name 2**.
8. Enter the **Access password 2**.
9. Enter the **HTTP URL** in case the service type chosen is HTTP.
10. Click on Save and Apply.

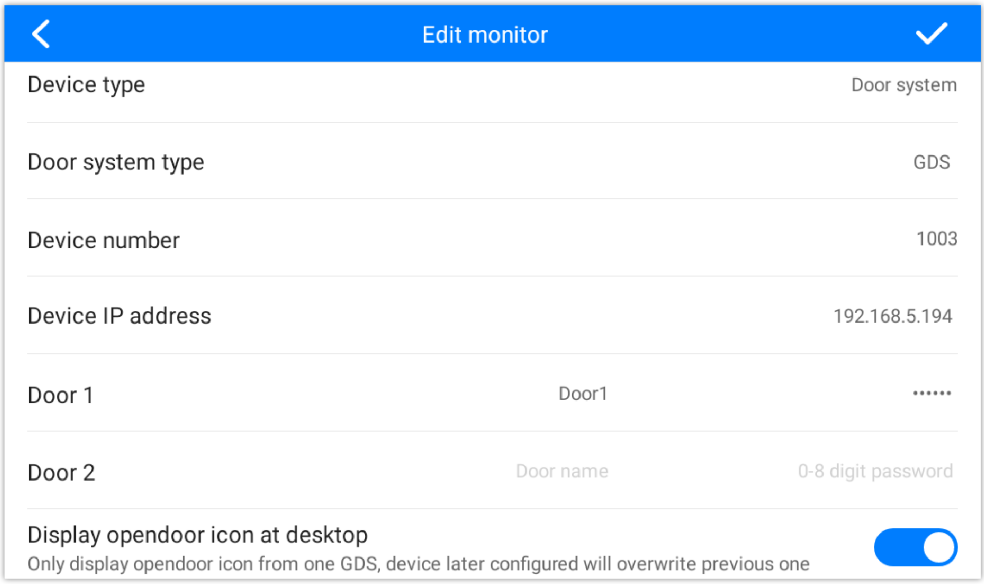


Below is a summary of all the added door systems



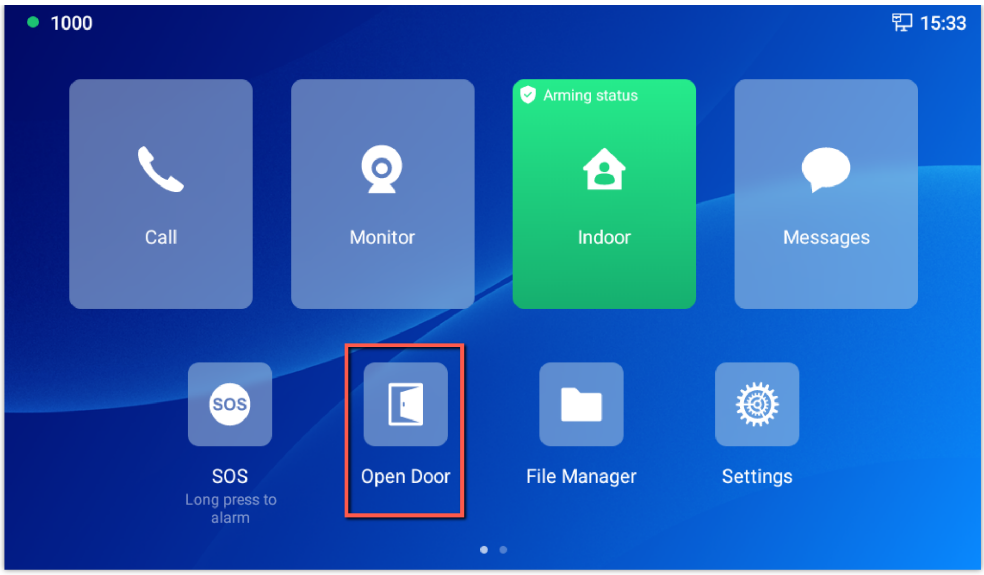
LCD configuration:

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

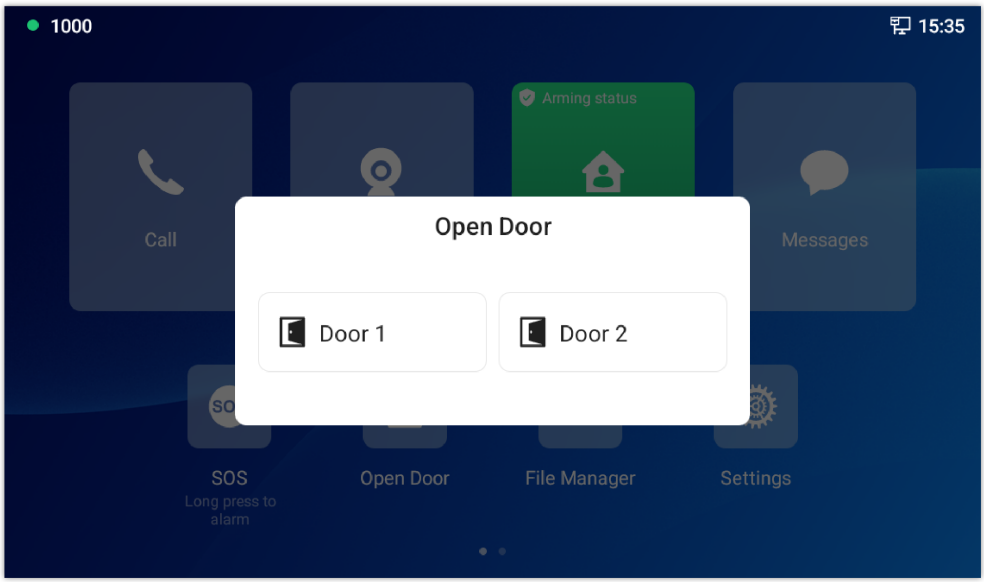


Add monitor: LCD Configuration

9. At the GSC3574/75 idle screen, once configured correctly, there will be one virtual button displayed at the lower side of the screen. If one door is configured, one button will be displayed; if two doors are configured, once you click the OpenDoor button, two doors will be displayed to choose the one to open



Open door on the GSC3574/75 idle screen – One Door



Open door on the GSC3574/75 idle screen – Two Doors

Notes

- The GSC3574/75 can be paired with 50 door machines in the Monitoring -> Door system and 2 additional door machines set by Digital Output Setting, totaling 52 door machines. All can be controlled via a desktop door-opening button.
- Only one desktop door opening button will be available, which will control the last GDS set for desktop door opening.

Open Door via GDS37xx with or without a SIP Call

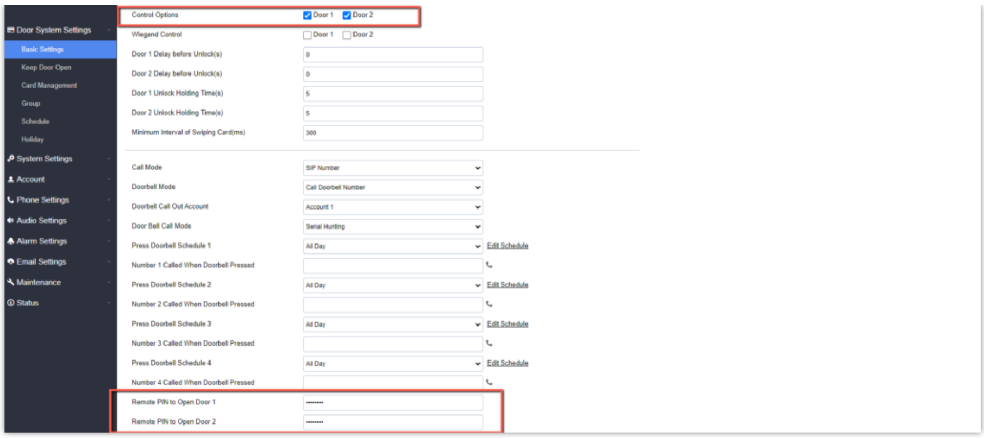
This feature is requested by customers and implemented to meet customers' application requirements, where GDS37XX paired with GSC3574/75 to open the door while no SIP call is required.

This feature needs related matching GDS37XX firmware to work.

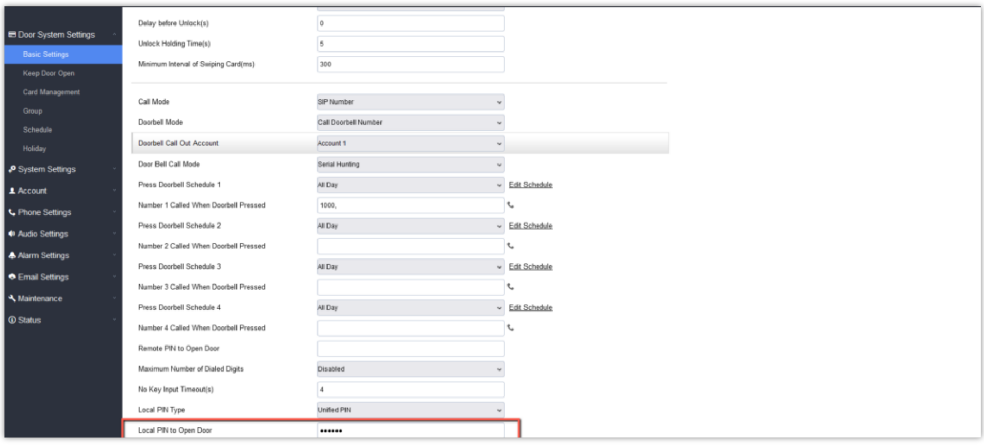
For the GDS37XX, the setup stays the same. The only change is in the number of doors controlled: With a Local Relay controlled by GDS37XX, you can handle two doors.

When you're using the GSC3574/75 Relay, you can control two doors by adjusting the digital output settings for two different GDS37XX units to open them, the PIN and other settings are similar to those for SIP remote open door or GSC3574/75 secure open door.

The difference will come out in the touch screen UI operation of GSC3574/75.



GDS37XX Configuration Example for Local Relay



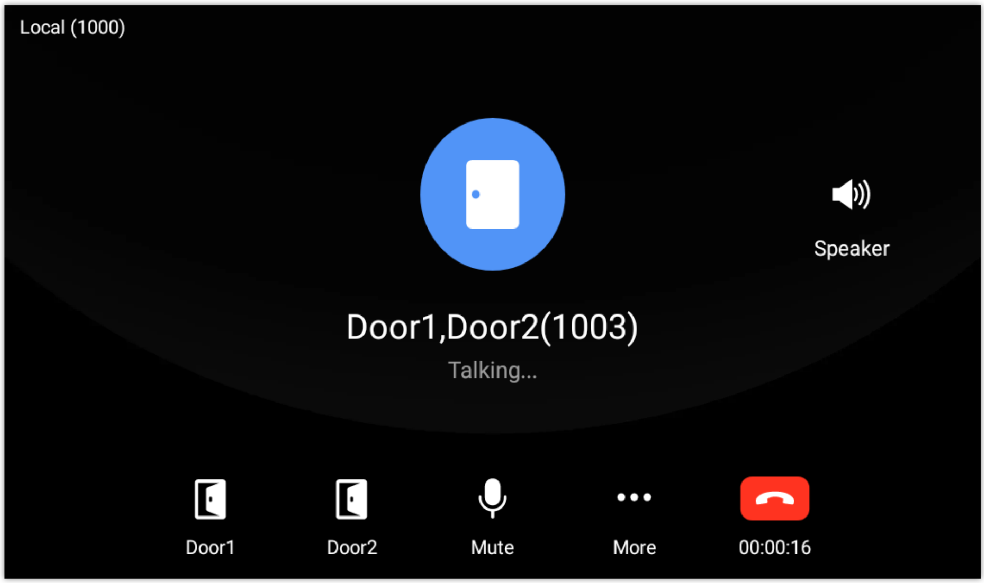
GDS37XX Configuration Example for GSC3574/75 Relay

Note

Only GDS3710/GDS3705 models support controlling two doors in the Local Relay Mode

Door opening with SIP Call:

When GSC3574/75 establishes a call with GDS37XX using its registered SIP extension or its IP Address, the screen will display virtual open door button(s), and the user will press the button to open the door:

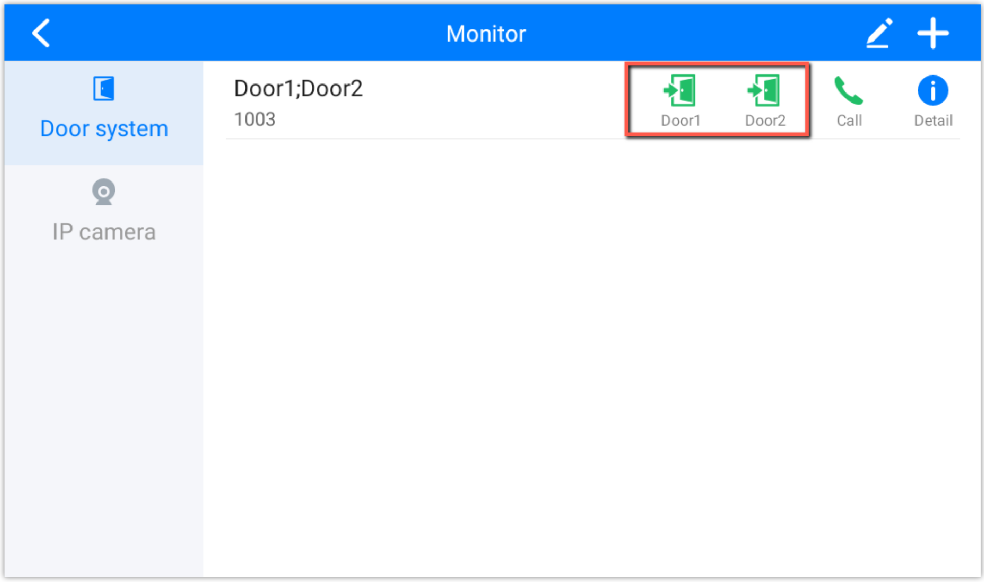


Open Door with SIP Call

GSC3574/75 Open Door NO SIP Call:

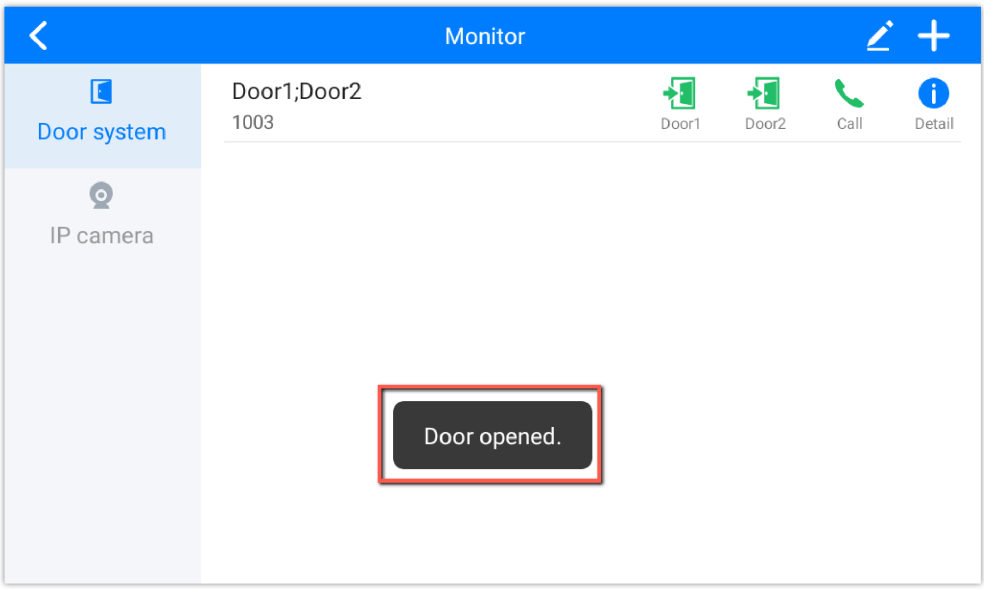
With the GSC3574/75 idle screen, press “Monitor →Door system”, and the related GDS37XX will be displayed.

Press the "Open door" icon, and the GSC3574/75 will open the door directly, and NO SIP CALL will be established. If two doors are configured, then two door icons will be displayed to open the door, as shown in the example below:



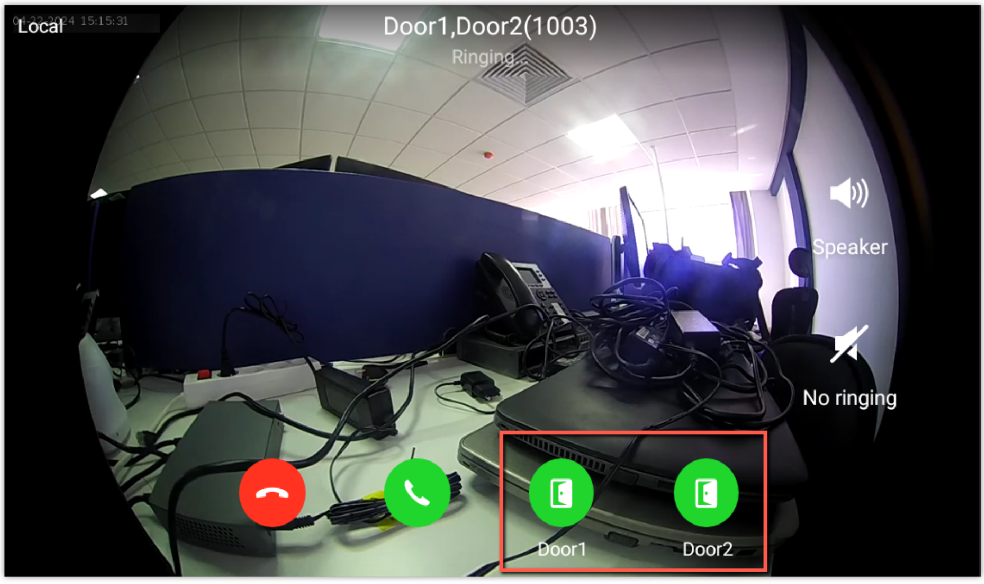
Open Door without SIP Call

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



Open Door without SIP Call

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



Door Preview

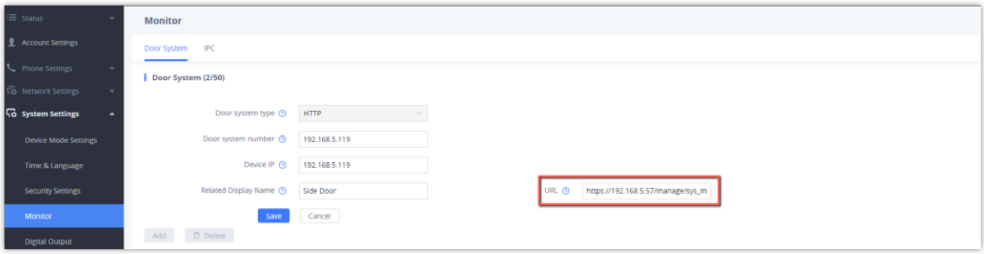
Note

If using a 3rd party Door system instead of GDS37xx , then the GSC3574/75 will send DTMF message to open door.

HTTP GET Request

By selecting HTTP as the service type, the user can use a button from the touch screen to generate an HTTP GET request to open the door.

When the device in the door system list calls, an open door button appears corresponding to the URL specified under the field HTTP URL.



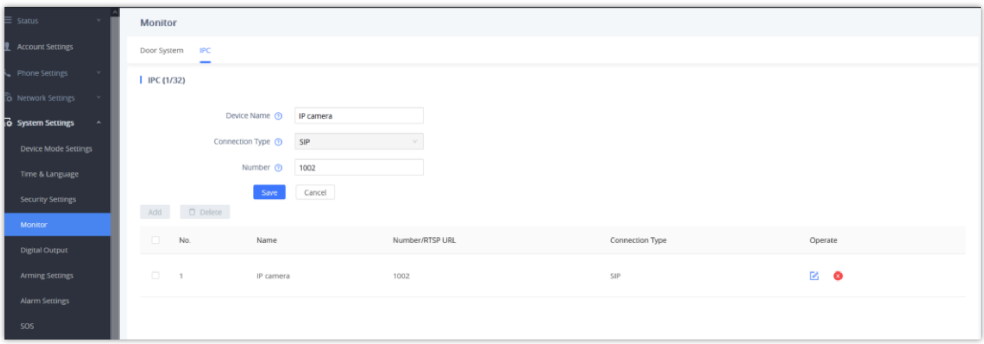
HTTP GET request

Connecting IP Camera with GSC3574/75

The GSC3574/75 can be configured with up to 32 IP cameras. The configuration is done as follows:

Web interface configuration:

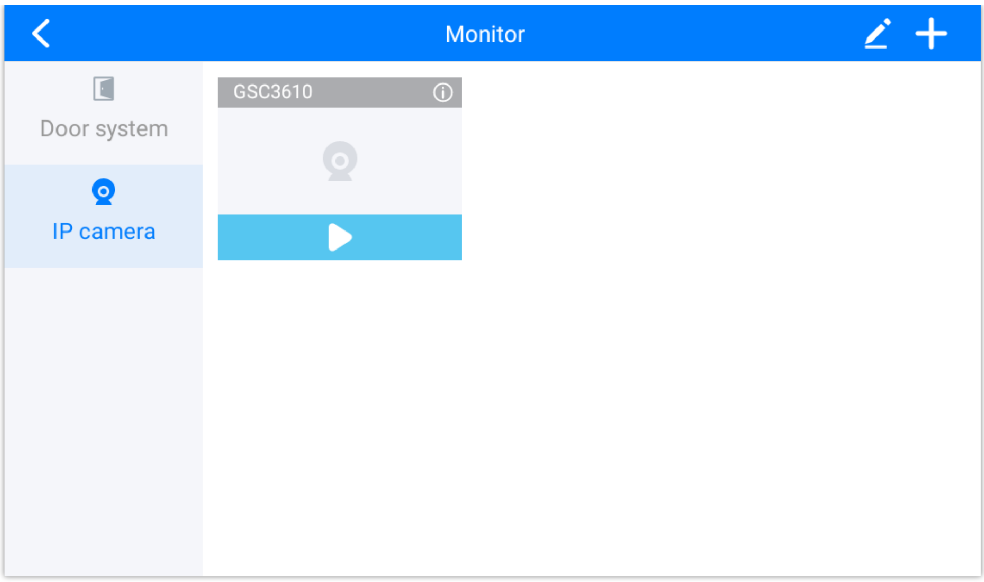
1. Access **Settings → IPC.**
2. Enter the name of the IP Camera unit in **System Identification**.
3. Select SIP or RTSP on the **Connection Type**.
4. Enter the IP Camera's SIP extension (or IP address in case of peering mode) in **Number**.
5. Click on Save.



IPC: Web Configuration

LCD configuration:

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



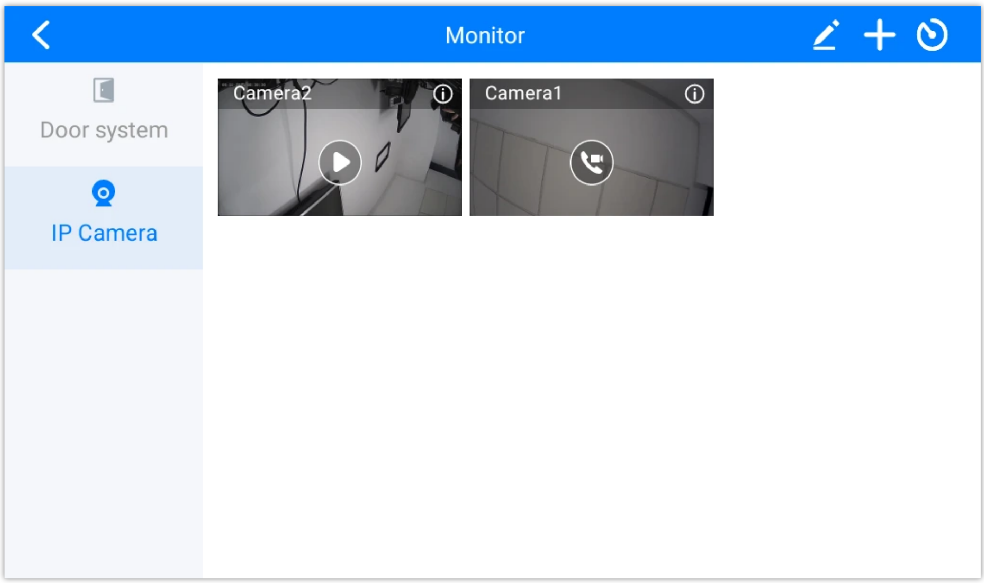
IPC: LCD Configuration

Automatic Thumbnail Update

The monitoring app **automatically updates thumbnails** for connected cameras (RTSP/TCP/UDP streams or SIP connection type), eliminating the need for manual refreshes.

When users view a video stream, the monitor app saves the last viewed frame as the thumbnail. To update a thumbnail:

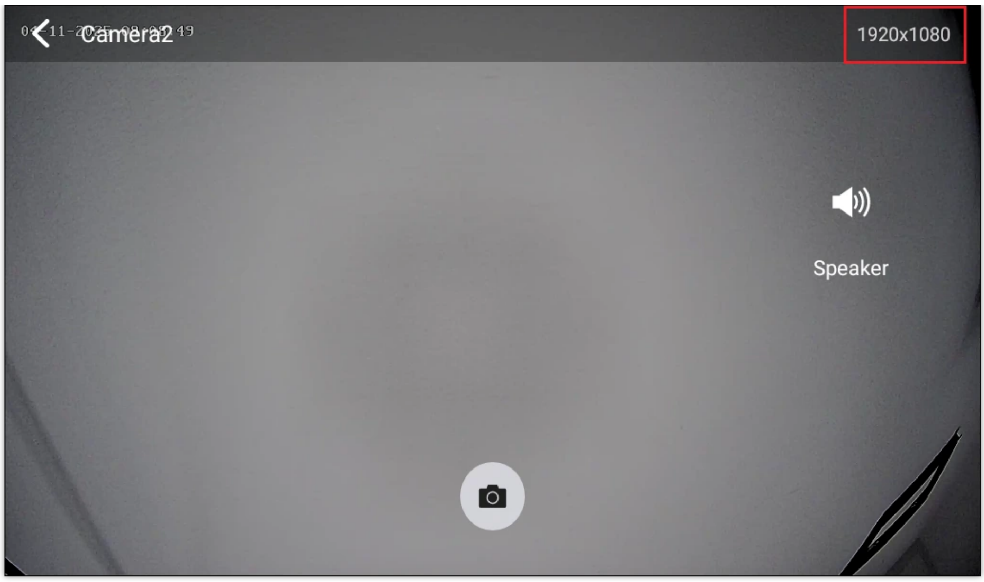
1. Open the camera's live view.
2. Exit the preview, and the last frame becomes the new thumbnail.



IPC Thumbnail

Live Stream Video Resolution Display

The monitor app shows the current video resolution (e.g., 1920×1080) in the upper-right corner of live streams, allowing users to verify the RTSP stream quality.



Video Resolution Display

Scan Nearby Devices

The GSC3574/75 has the option to scan for nearby GSC36xx IP cameras and GDS37xx Door Systems, which are available on the same subnet. Once discovered, they can be automatically added.

- **Adding GDS37xx**

Under **Monitor** → **Door System**, click the icon to display discovered devices

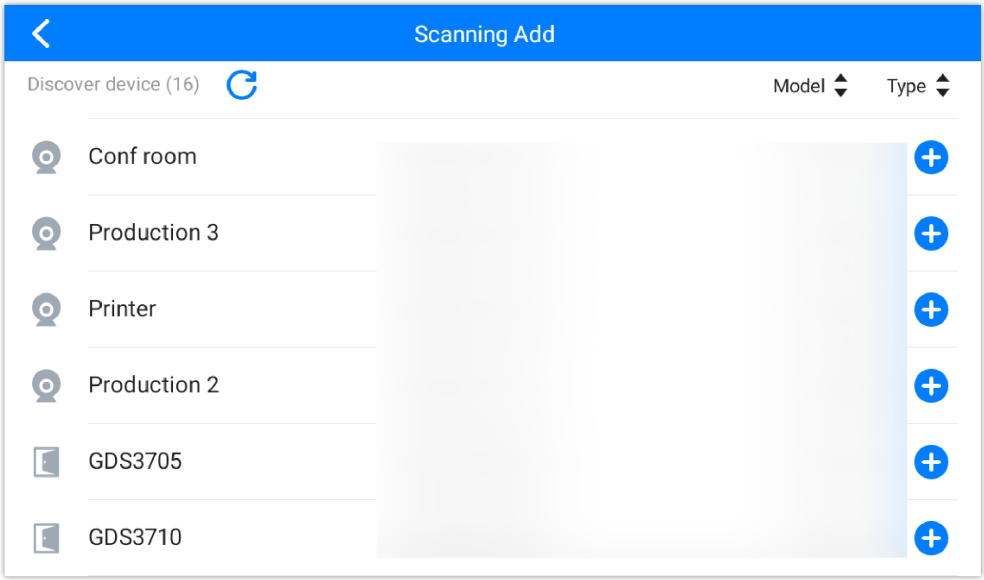
Once displayed, click the icon to add the device to the list of monitored Door Systems. You will need to provide the door name and number to allow the door open features

- **Adding GSC36xx**

Under **Monitor** → **IP Camera**, click the icon to display discovered IP Cameras

Select the one you would like to add, then click the .

Define the RTSP username and password to view the RTSP stream from the GSC3574/75.

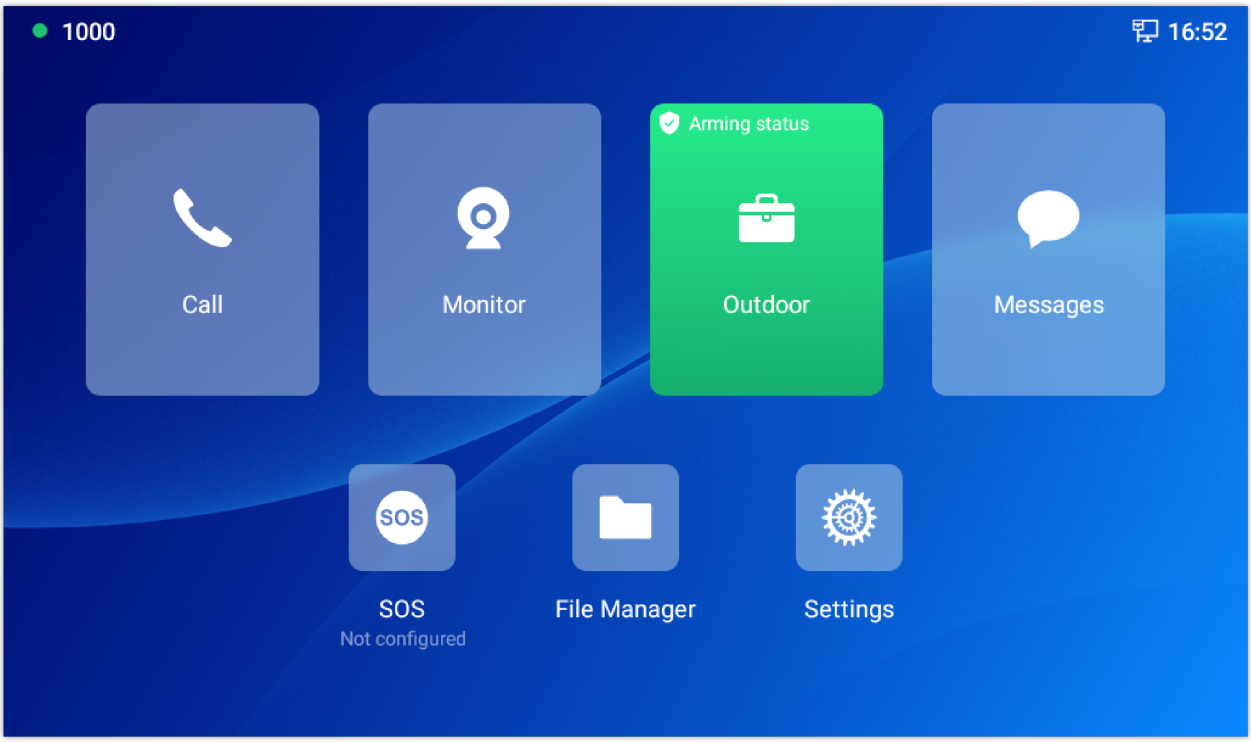


Scan Nearby Devices

GSC3574/75 Meeting Room Panel Mode

GSC3574/75 has the option to alter the device mode based on the required functions. The user can choose between the following two options:

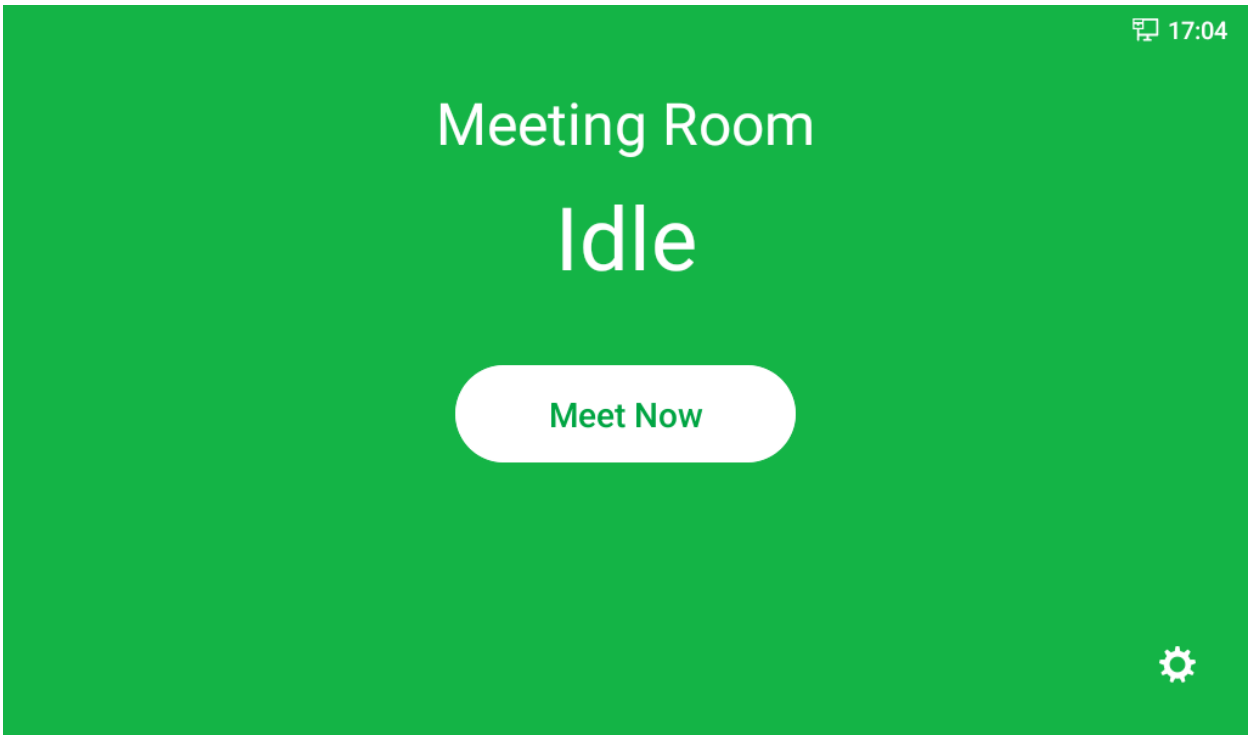
- **Control Station Mode (Default):** In this mode, the GSC3574/75 functions as a normal control station of the on-premise security control, where it is usually deployed with other IP surveillance cameras such as the GSC36xx devices, and Door systems, such as the GDS37xx device models, in this mode the main functionalities deployed are the open door features, the "Monitor" feature, used to display the video feed of the cameras, in addition to some functionalities related to alarm out/in settings, this mode is the default mode of the GSC3574/75.



Control Station Mode view

- **Meeting Room Panel Mode:** In this mode, the GSC3574/75 can function as an extension of the UCM63xx model for in-person meetings or as a standalone device for hosting local meetings independently, eliminating the necessity of connecting to a UCM, if used as a UCM63xx extension, it will display the organized onsite meetings from the UCM platform, through the control interface, users can monitor room occupancy status, reserve meeting times by choosing slots from the displayed timeline, adjust meeting duration, and receive a 10 minutes countdown notification as scheduled meetings approach.

> **Note**
>
> For more information on the configuration and setup of the Meeting Room Panel Mode, please refer to the guide: GSC357x: Meeting Room Panel Mode User Guide.



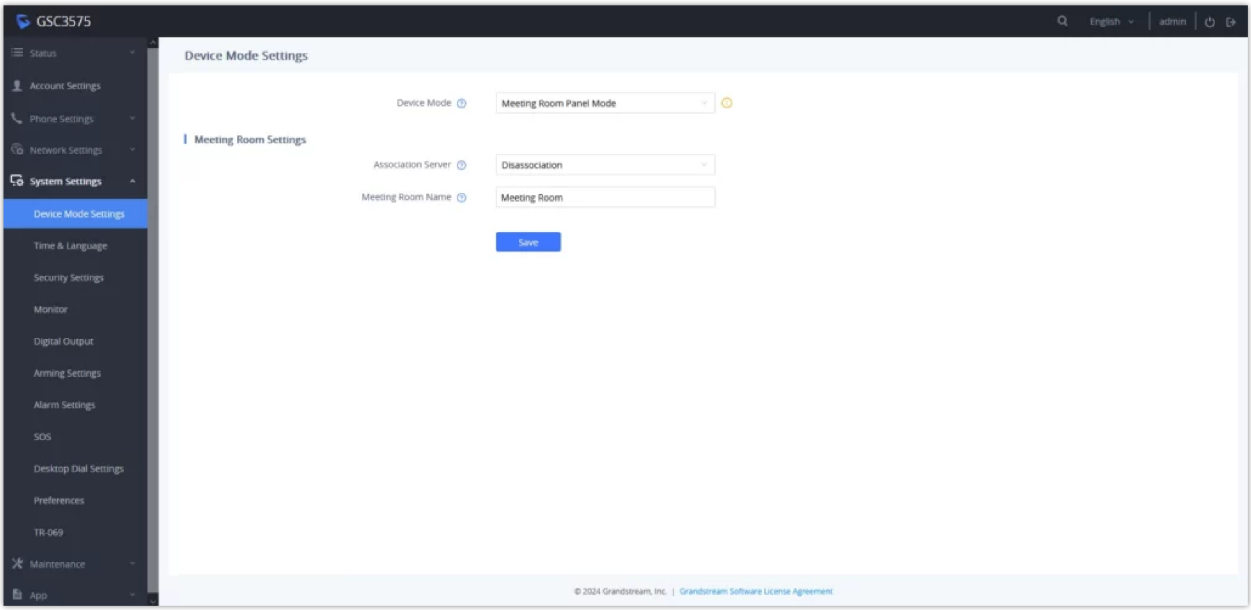
Meeting Room Panel Mode view

Note

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

Meeting Room Panel Mode Web UI view

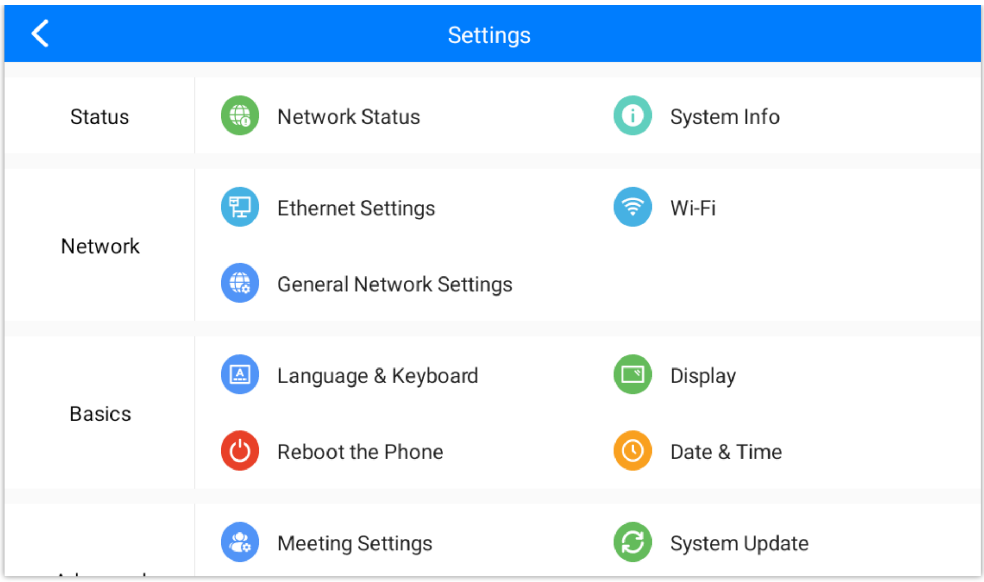
The settings available on the GSC3574/75 Meeting Room Panel Mode are limited and different from the control station mode. Here is a general view of the available settings:



Web UI Settings

Meeting Room Panel Mode LCD settings view

Some functionalities are not available on the LCD settings; the available settings are :



Meeting Room Panel Mode LCD settings view

GSC3574/75 LCD SETTINGS

The GSC3574/75 LCD MENU provides easy access to the settings on the GSC3574/75. Some of the settings from the Web GUI could be configured via the LCD as well. The following table shows the LCD menu options.

- **Control Station Mode**

Status	1. Account status 2. Network status 3. System info 4. Storage info
Network	1. Ethernet settings 2. WI-FI 3. General networking settings
Features	1. Auto answer 2. Do Not Disturb 3. Arming mode 4. Zone settings 5. DO settings 6. Bluetooth
Basic	1. Sound&Vibration 2. Display 3. Language&Keyboard 4. Date&Time 5. Security Settings 6. Desktop shortcut settings 7. Reboot the Device 8. Gesture Guide
Advanced	1. Account Settings 2. Monitor 3. Alarm settings 4. SOS Settings 5. System Update

	6. System Security

GSC3574/75 Control Station Mode LCD SETTINGS

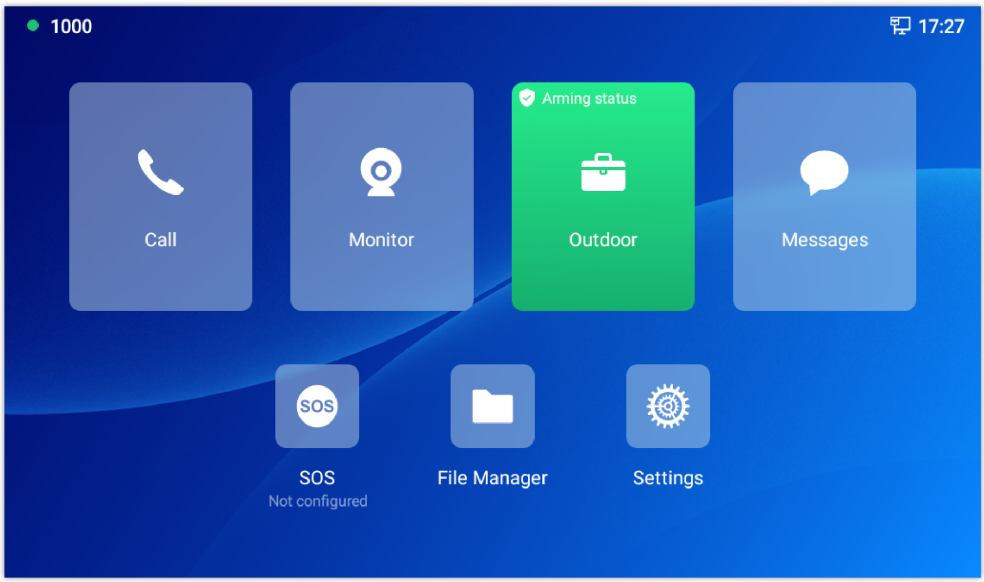
- **Meeting Room Panel Mode**

Status	1. Account status 2. Network status
Network	1. Ethernet settings 2. WI-FI 3. General networking settings
Basic	1. Language & Keyboard. 2. Display 3. Reboot the Phone 4. Date&Time
Advanced	1. Meeting Settings 2. System update 3. System Security

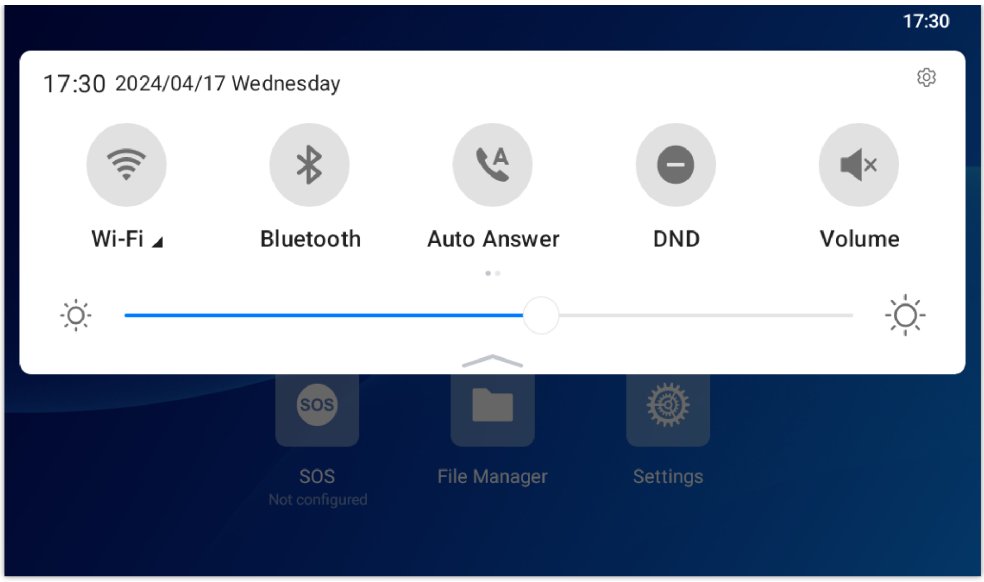
GSC3574/75 Meeting Room Panel Mode LCD SETTINGS

Idle Screen

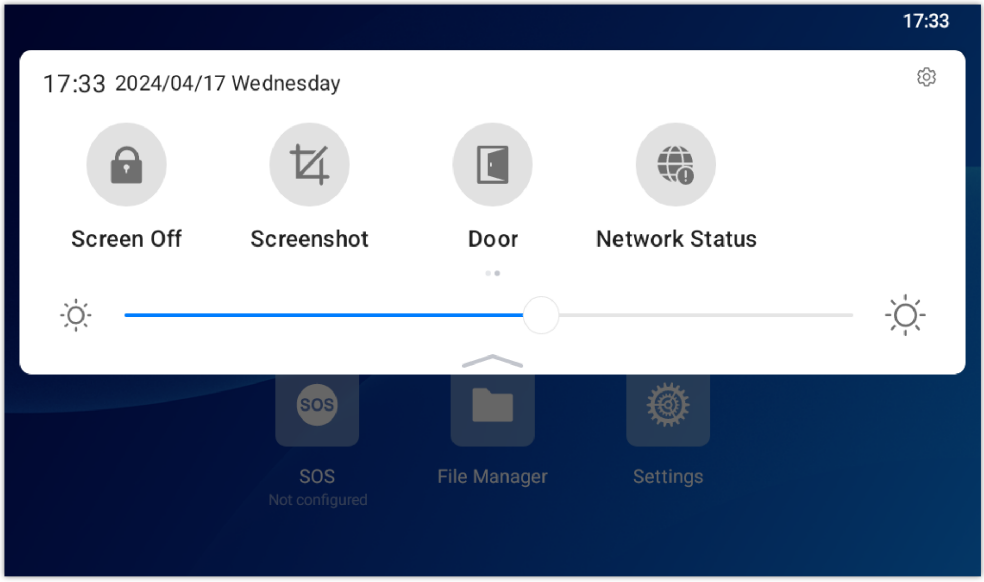
The Idle home screen provides convenient access to user-selected options configured in the Settings Menu, such as accessing Wi-Fi Settings, Bluetooth settings, Door Open Settings, and Settings, among others. Furthermore, pulling down the notification bar reveals an enhanced Panel, offering detailed information about the GSC3574/75.



Idle Home Screen



Idle Home Screen – Toolbar 1



Idle Home Screen – Toolbar 2

You can access the full settings menu by clicking the icon in the top right corner.

Note

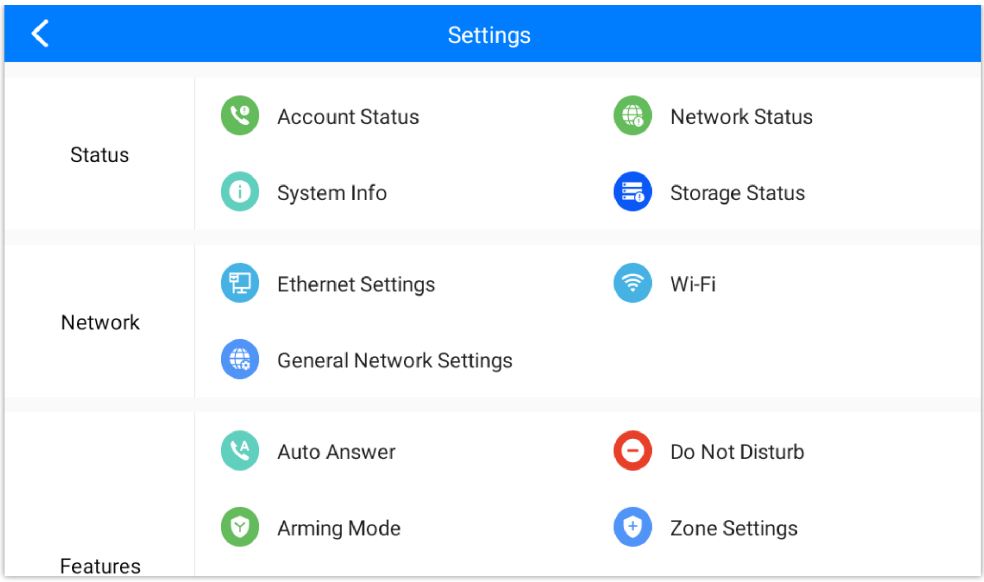
- Ensure to pull down the panel twice, once to initiate the action and then again to fully expand it.
- When the LCD is turned OFF and in energy saving mode, but a secure open door event happens, the LCD will be turned ON to light up and display the open door icon with a long “beep” to notify the user of an open door event.

Settings Menu

To open the settings menu:

- Tap on

  Settings app on the screen.

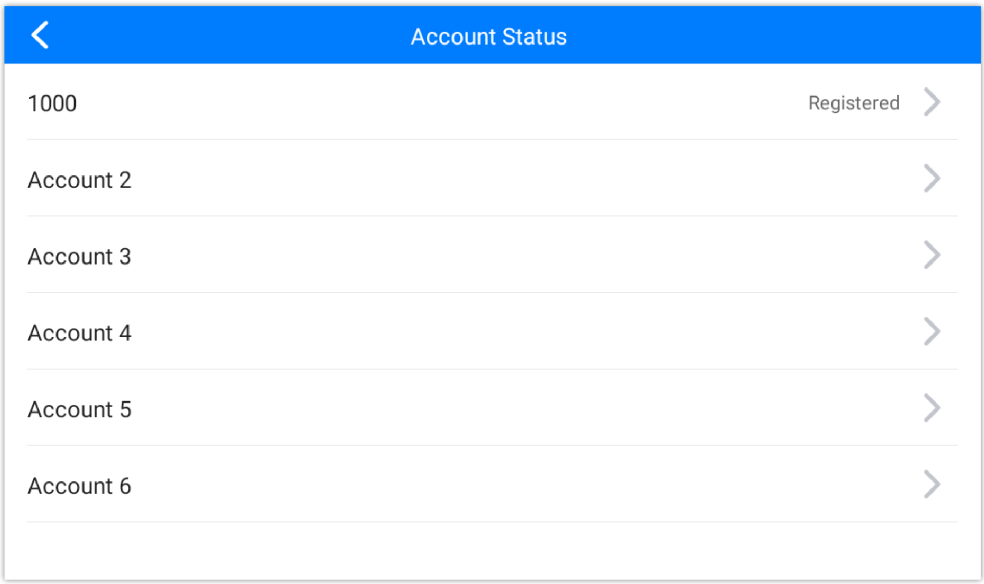


GSC3574/75 LCD Settings

Status

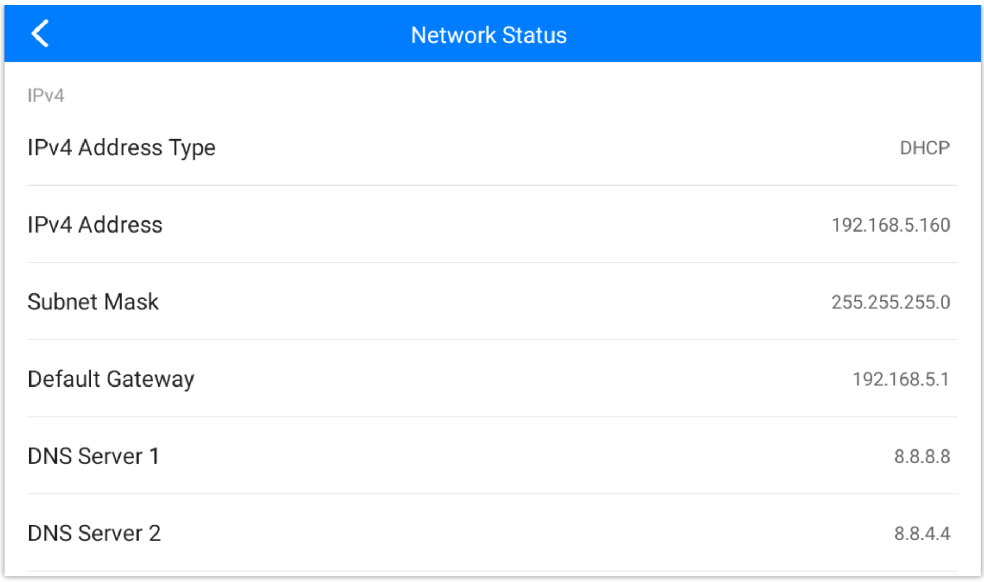
Account Status

This page displays all available accounts on the phone with their respective statuses (Configured/Not Configured and Registered/Unregistered). The GSC3574/75 supports up to 6 accounts.



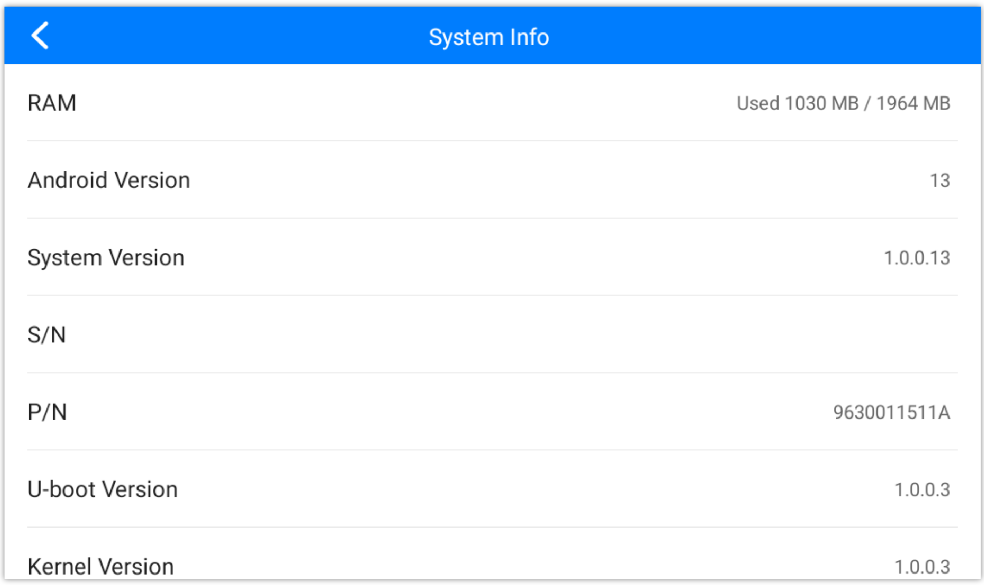
Network Status

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



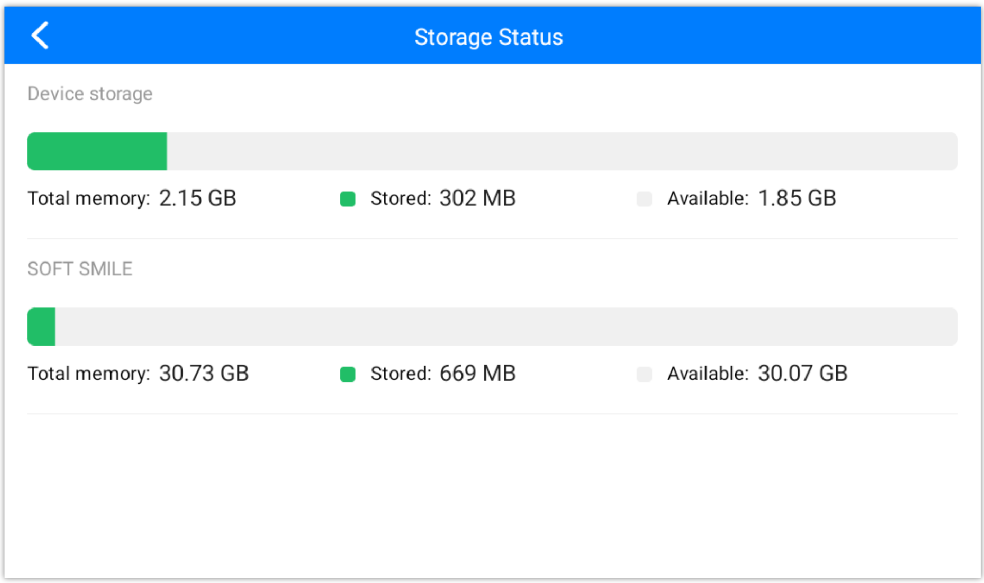
System Info

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



Storage Status

This page shows the local storage info, as well as the external storage info (for both the SD card and the USB key)

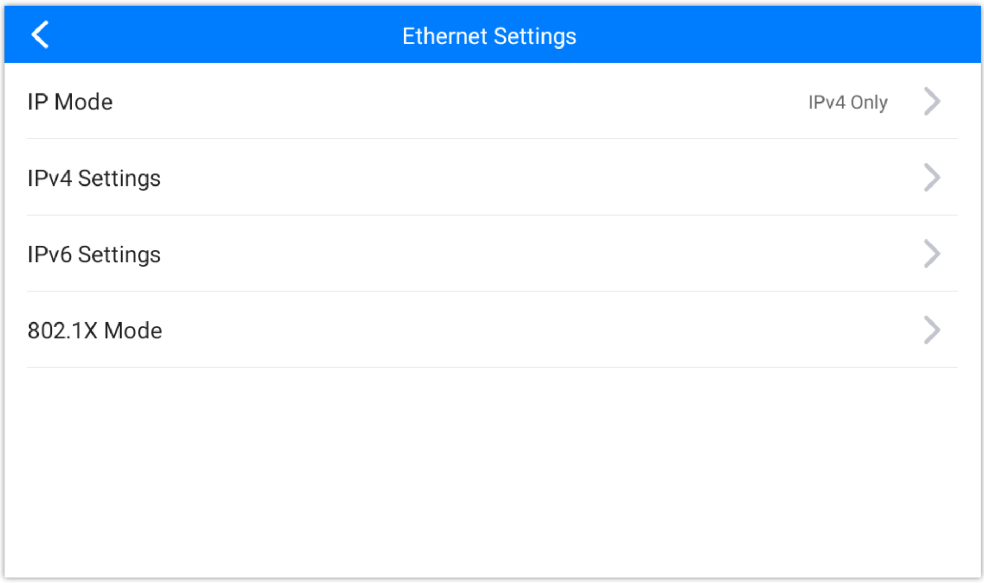


Network

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

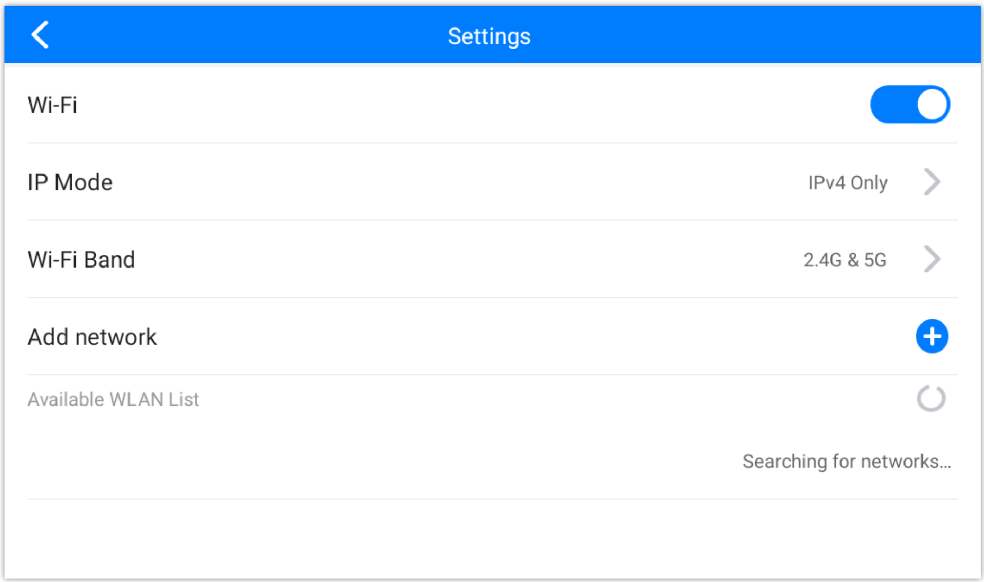
Ethernet Settings

- **IPv4**/IPv6 Settings: Here user can configure the IPv4/IPv6 address type for both data and VoIP calls. For network configuration of data, if DHCP is selected, the phone will get an IP address automatically from the DHCP server in the network. This is the default mode. If Static IP is selected, manually enter the information for IP Address, Subnet Mask, Default Gateway, DNS Server, and Alternative DNS Server.
- **802.1x mode:** This option allows the user to enable/disable 802.1x mode on the phone. The default setting is disabled. To enable 802.1x mode, select the 802.1x mode and enter the required configuration depending on the 802.1x mode chosen. The available modes are **EAP-MD5**, **EAP-TLS**, and **EAP-PEAP**



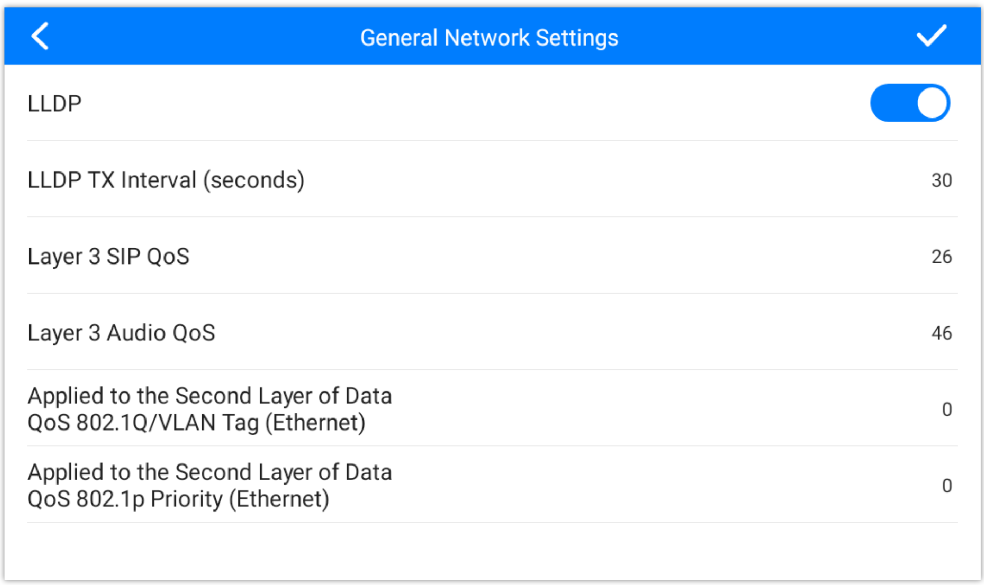
Wi-Fi

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



General Networking Settings

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

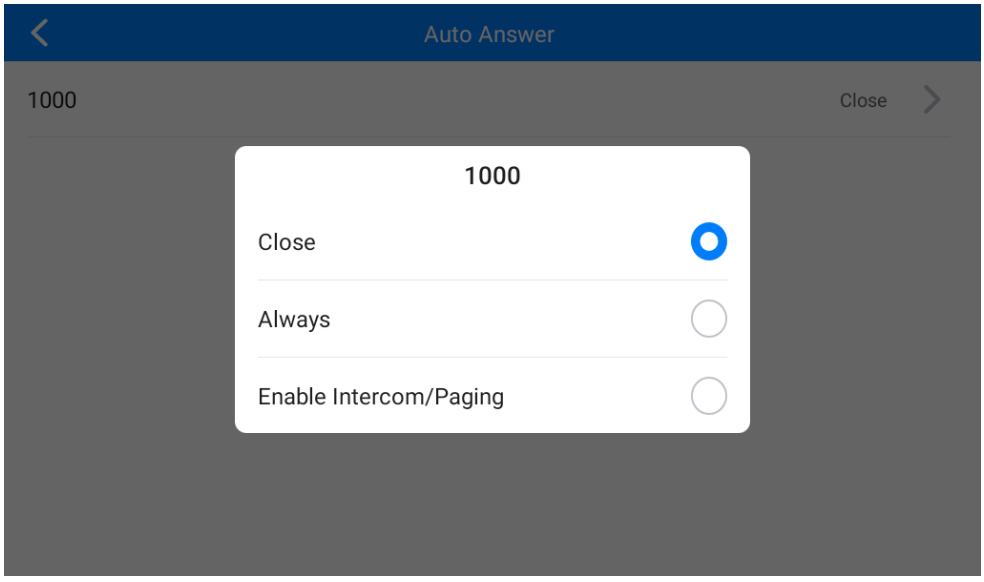


Features

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

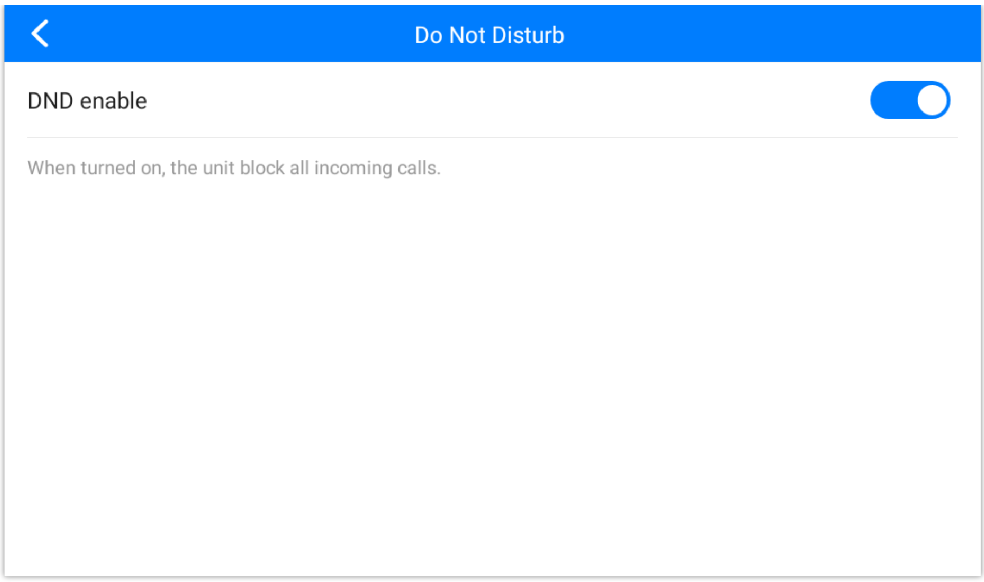
Auto-Answer

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



Do Not Disturb

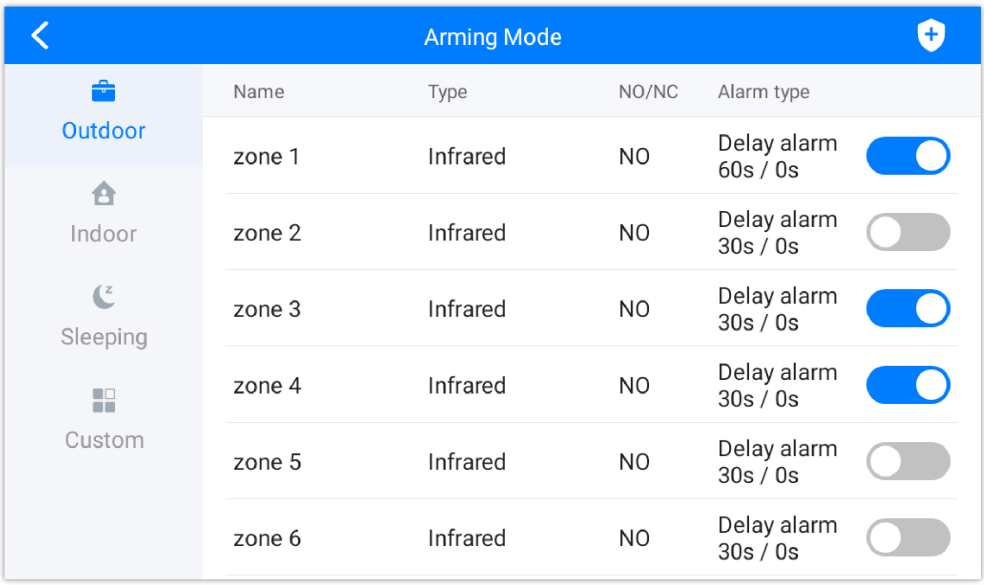
Enable/Disable the DND mode. When enabled, all incoming calls are rejected.



Arming mode

Enable/Disable the Arming mode on configured zones (Zone 1-8) per status (Outdoor, Indoor, Sleeping, or Custom.)

The zones are configured from the Web UI under **System Settings** → **Arming Settings**, or from the LCD settings under **Settings** → **Features** → **Zone Settings**.



Zone Settings

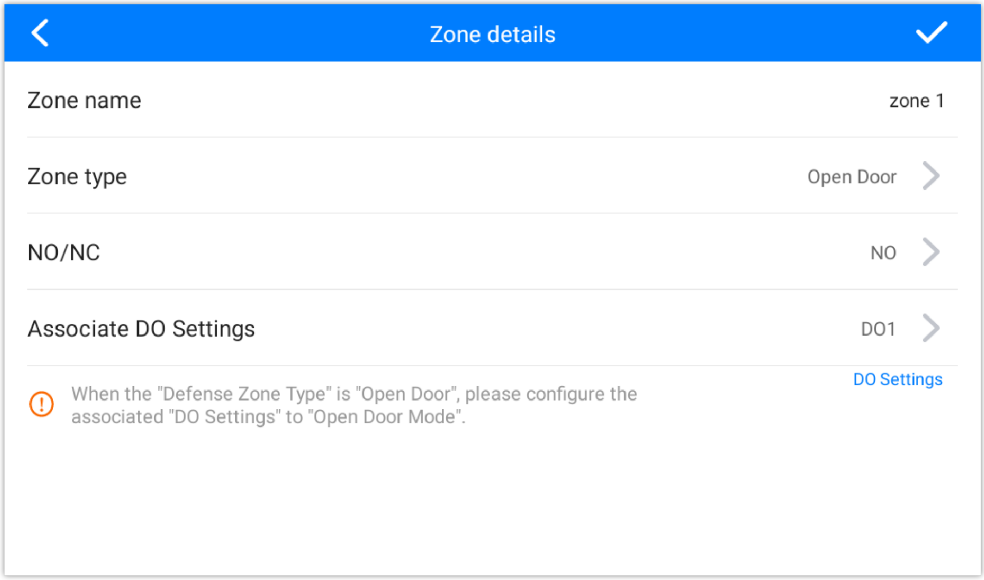
Tap the zone to be edited and set Zone Name, Zone Type, along with the alarm type...Etc.

- **Zone Name:** Enter the name of the zone.
- **Zone Type:** Select the **Type** of the Zone:
  - Infrared
  - Smoke
  - Gas
  - Drmagnets (door lock)
  - Urgency
  - DoorBell
  - Open Door
  - Others
- **NO/NC:** Match the alarm type:

- **NO:** Normally Open device
- **NC:** Normally Close device

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

- **Associate DO Settings:** when defining the zone type as an open door, you can define the associated door or doors to be opened, which is configured on the digital output (ALMOUT1, and ALMOUT2)



DO Settings

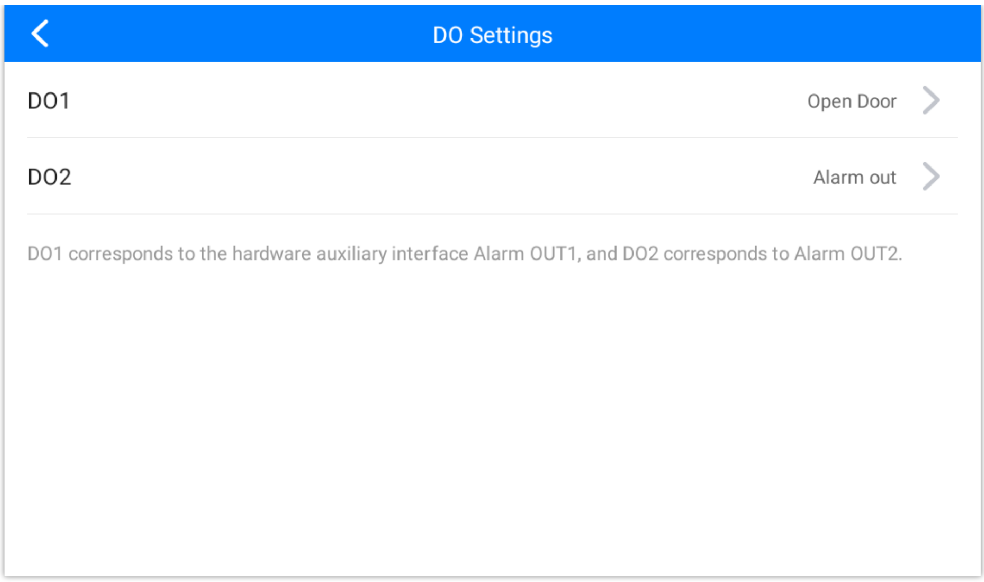
Configures the Digital Output settings on the GSC3574/75. You can choose to put the DO mode to :

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

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

- **Door unlock holding time (S):** Duration of time in seconds that the door remains open.
- **Door system SIP user ID:** Defines the SIP extension of the Door system used.
- **Door system IP Address:** Defines the IP Address of the Door system used.
- **Door Control SIP account:** Defines the Account used on the door system side for the GSC3574/75 Relay Mode
- **Door Control Password:** Defines the Account used on the door system side for the GSC3574/75 Relay Mode
- **Display open door** icon on the desktop: Enables the option to display the open door icon on the home screen. This Open Door Button has a higher priority than the GDS device in Monitor → Door System.

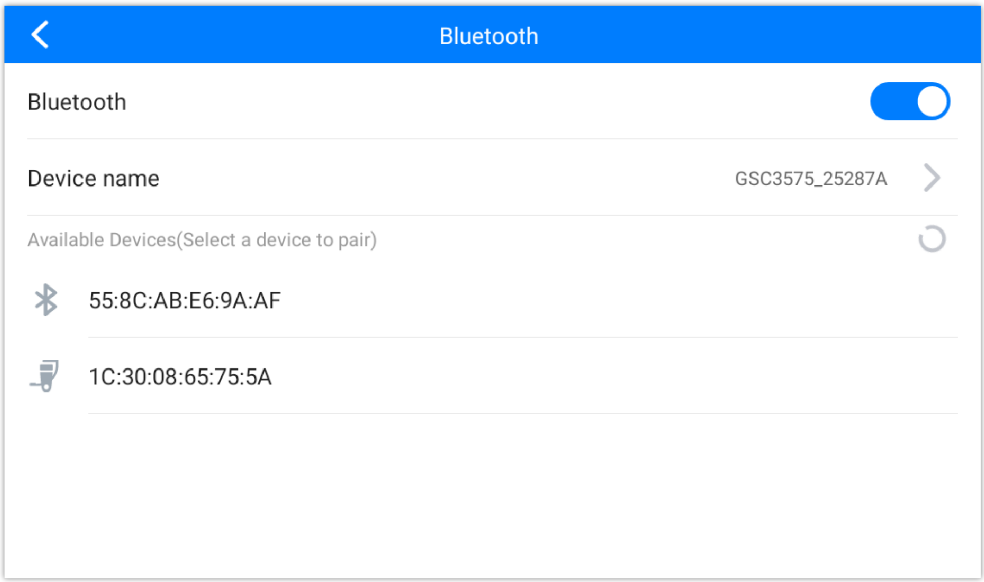
The Door Open feature is disabled by default.



Bluetooth

This option helps to connect additional gadgets and devices to the GSC3574/75 via Bluetooth:

- You can enable the Bluetooth feature by toggling the highlighted button
- Specify the device name
- A list of available devices will be displayed for pairing



Bluetooth Settings

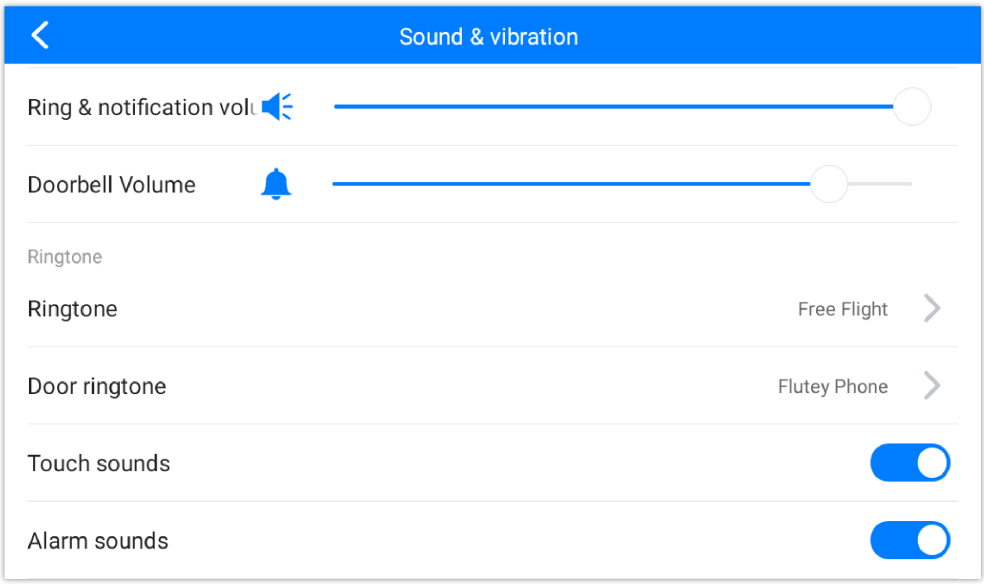
Basic

Sound & Vibration

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

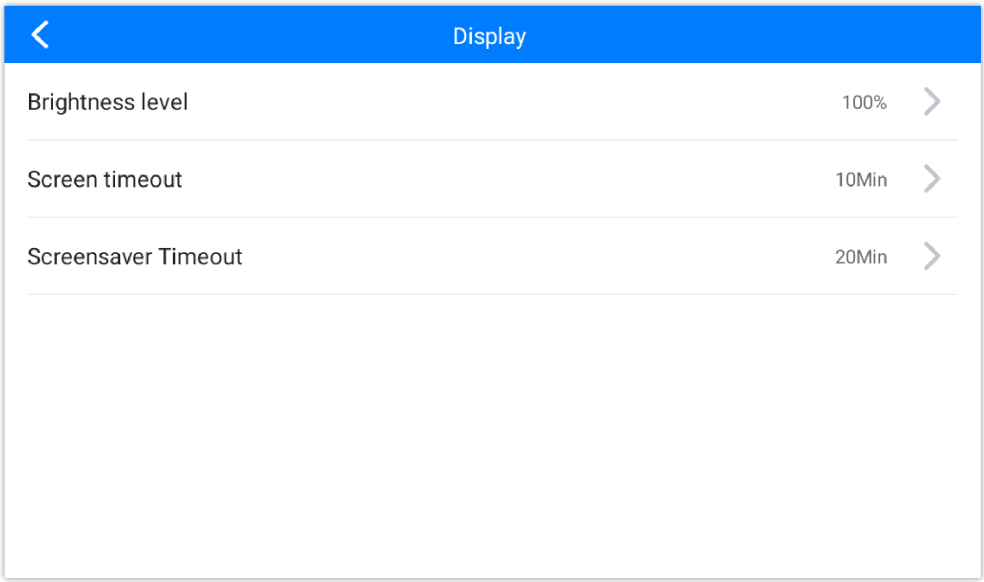
- **Media Volume**: Adjust the sound volume for media audio.
- **Ring & Notification Volume**: Adjust the phone's ringing volume.
- **Doorbell volume:** Adjust the Doorbell volume.
- **Ringtone**: Select the phone's ringtone for an incoming call.
- **Door Ringtone:** Select the Door ringtone when a call arrives from GDS37XX.
- **Touch Sounds:** Enable/disable Touch sounds.

- **Alarm Sounds:** Enable/Disable Alarm sounds.



Display

- **Brightness**: Tap on **Brightness** and scroll left/right to adjust the LCD brightness.
- **Screen timeout**: Tap to open the dialog to set the screen timeout interval.
- **Screensaver timeout**: Tap to set the screensaver timeout interval.

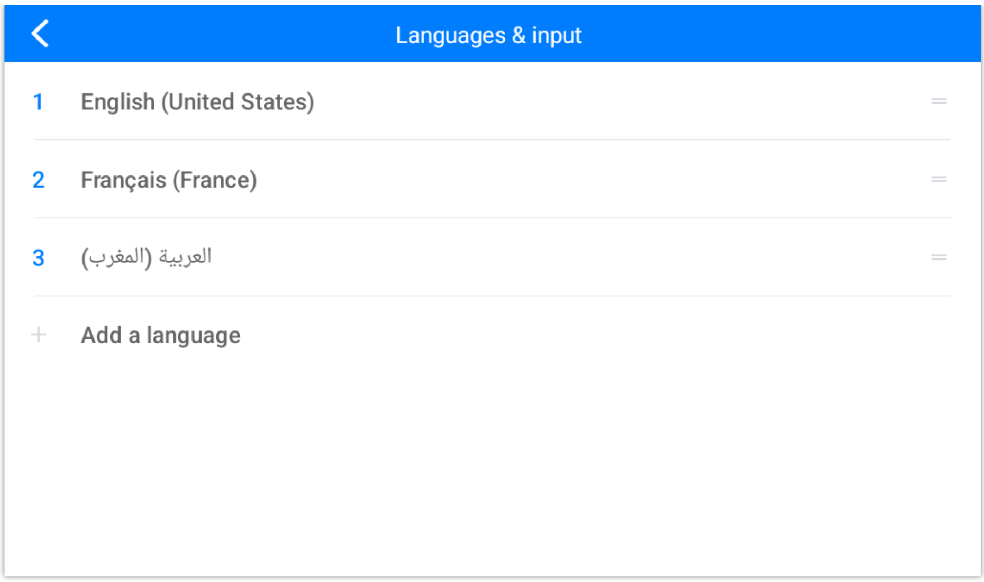


Note

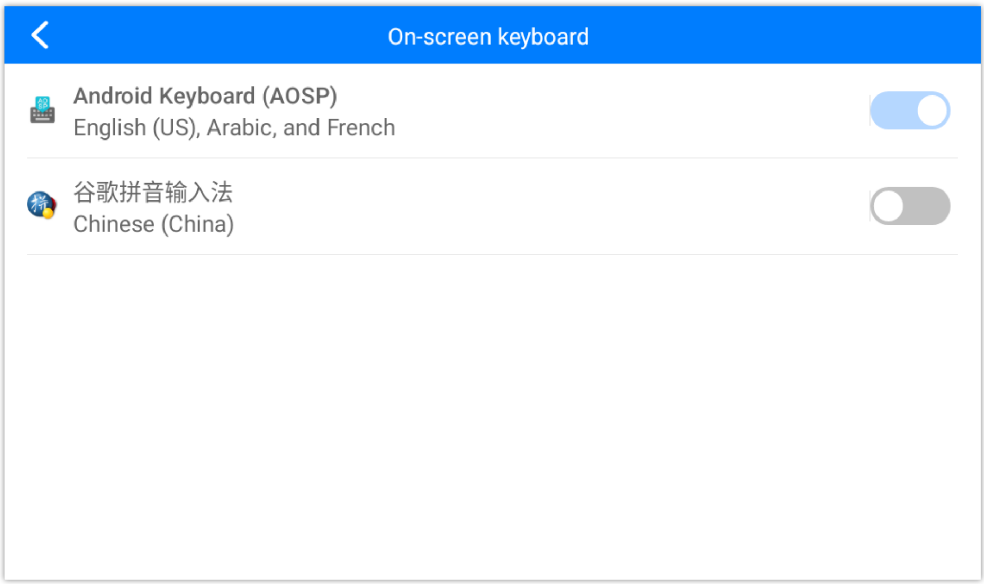
You can adjust the screen brightness from the notification bar as well.

Language & Keyboard

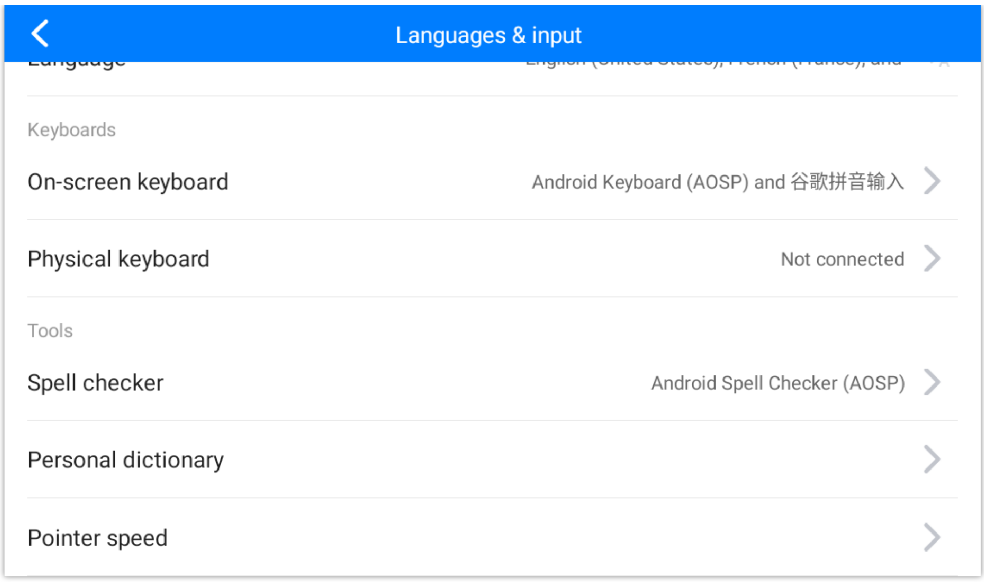
- **Language**: Tap to open the list of downloaded languages. Select Add language to select the language that you would like to add to the list of languages defined.



- **On-screen keyboard:** Defines the keyboard format that will be displayed.
- **Physical keyboard:** Refers to configurations for external keyboards connected to the GSC3574/75 via Bluetooth or a wired connection, offering customization options for key mappings, shortcuts, and typing behavior.

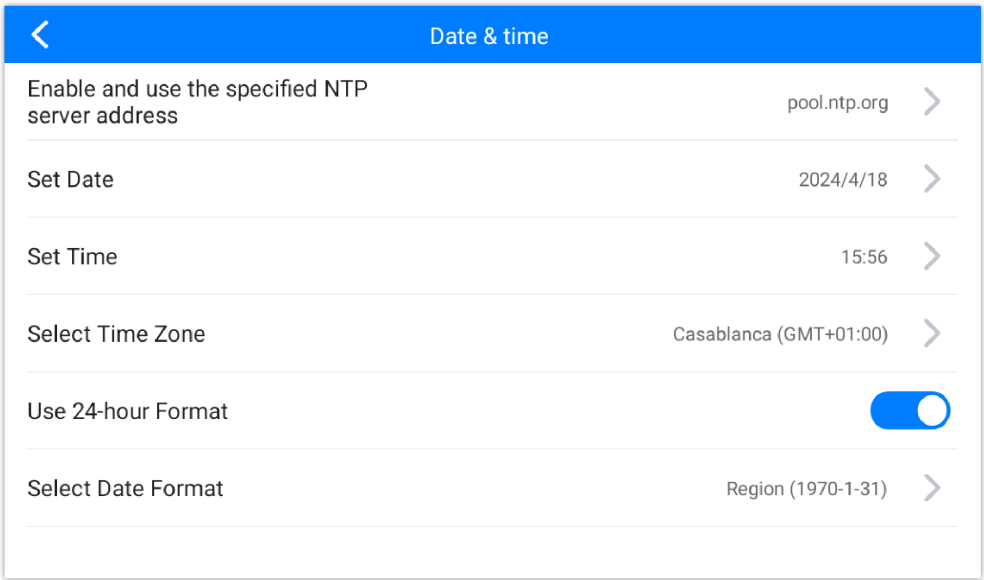


- **Spell checker:** enables automatic detection and correction of spelling errors as you type, enhancing text accuracy and readability across various applications and interfaces.
- **Personal dictionary:** allows users to add custom words or phrases, ensuring they're not flagged as misspellings and enhancing the device's ability to recognize and accommodate personalized language preferences.
- **Pointer Speed:** controls the sensitivity and responsiveness of the on-screen cursor or pointer, allowing users to adjust it to their preferred level of precision and speed for smoother navigation and interaction with the device.



Date & Time

- **Enable and use the specified NTP server address:** Assign the URL or IP Address of the NTP Server. The default NTP Server used is pool.ntp.org
- **Set date**: Set the current date for the GSC3574/75.
- **Set time**: Set the time on the GSC3574/75 manually.
- **Select time zone**: Select the time zone for the GSC3574/75.
- **Date format**. Select the format of year, month, and day for the date to be displayed. The default is "yyyy-mm-dd". Available options are:
  - *yyyy-mm-dd*
  - *mm-dd-yyyy*
  - *dd-mm-yyyy*
- **Use 24-hour format**. Check/uncheck whether to display the time using the 24-hour time format or not. For example, in 24-hour format, 13:00 will be displayed instead of 1:00 p.m.



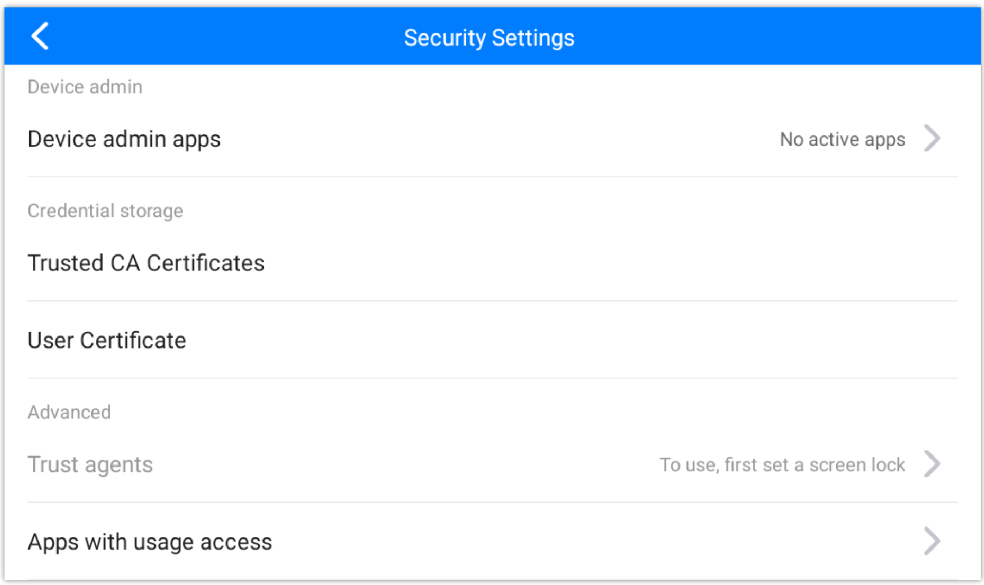
Security Settings

For enhanced security, the following configuration sets security protocols for the GSC3574/75 device

The following configurations are defined :

- **Screen lock:** Enables the Screen lock using Pattern or PIN. Disabled by Default

- **Show Password:** Displays the password when it's being typed.
- **Device Admin apps:** Grant certain applications elevated privileges to perform system-level actions such as locking the device, wiping data remotely, or enforcing security policies, often used by enterprise IT departments for device management and security enforcement.
- **Credential storage:** contains both Trusted CA Certificates and User Certificates.
- **Trust Agents:** Enables additional authentication methods such as fingerprint or face recognition to unlock the device or access secure features, enhancing security by providing alternative verification options beyond traditional passwords or PINs.
- **Apps with usage access:** allow certain applications to monitor and collect data on the GSC3574/75 usage patterns, including which apps you use most frequently and for how long.



Desktop Shortcut Settings

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

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

Speed dial

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

- **Shortcut name:** Defines the shortcut name
- **Number:** the phone number to be dialed

RTSP

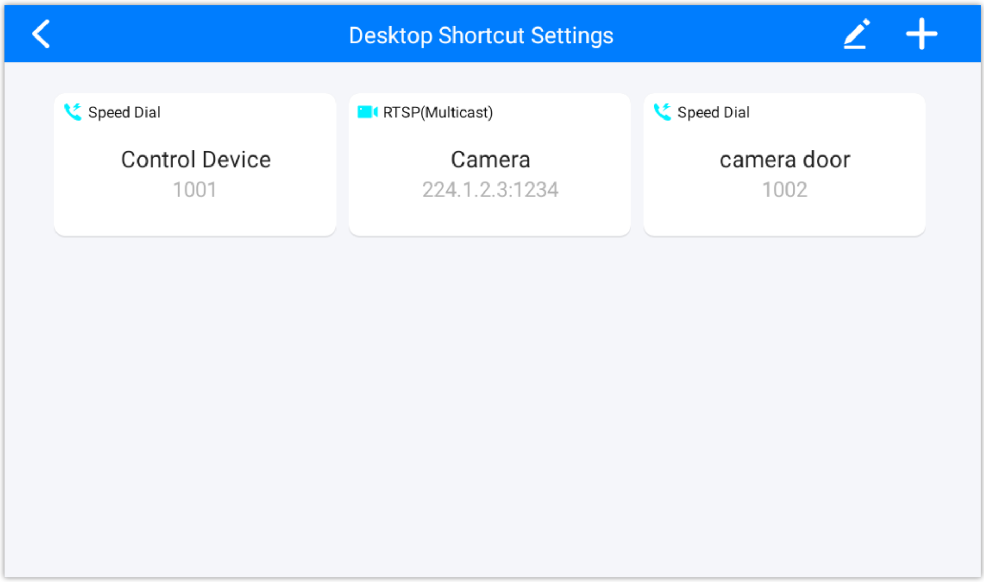
This option sets the RTSP streaming configuration by defining the following attributes :

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

Send HTTP URL

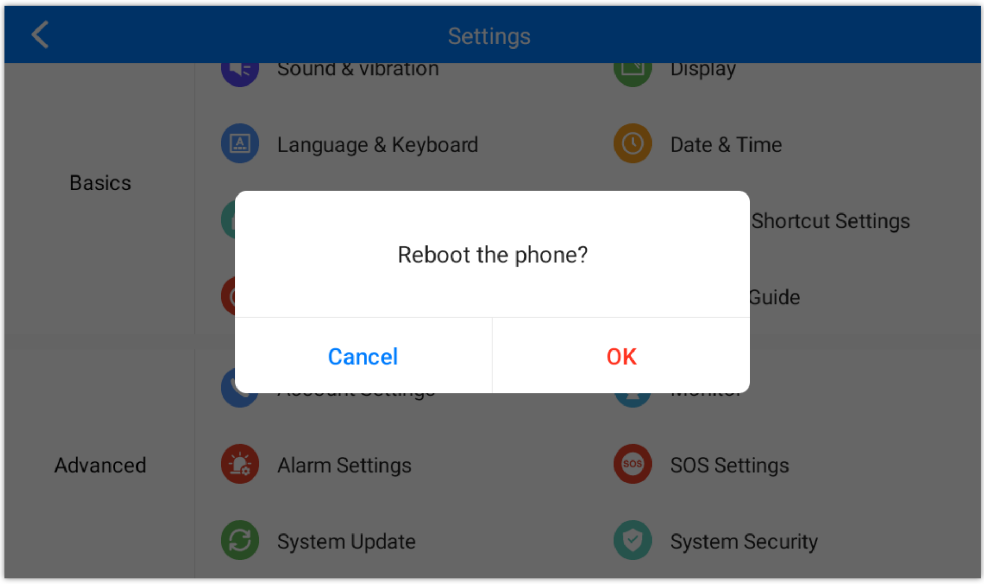
This option sets the HTTP URL configuration by defining the following attributes :

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



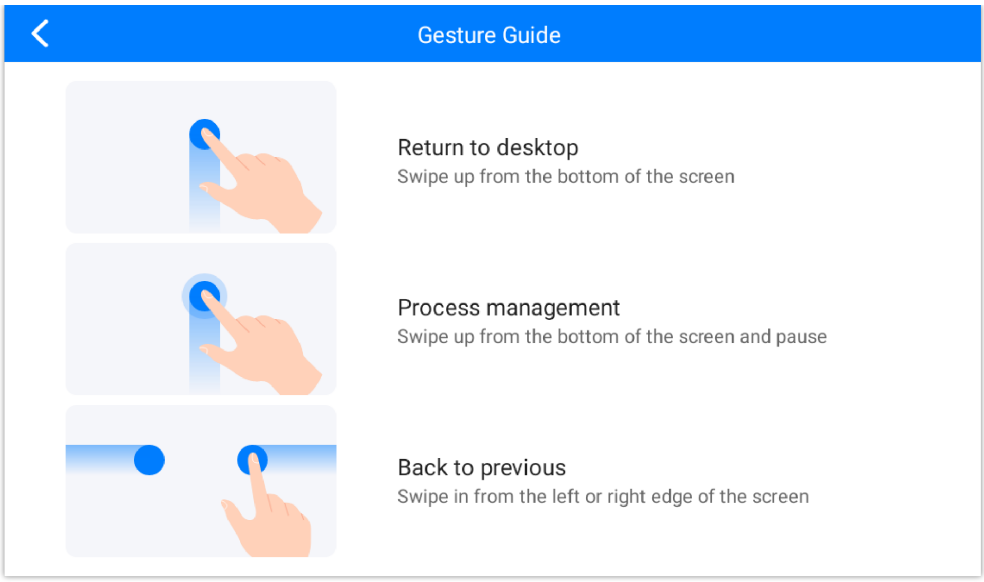
Reboot the Phone

- Reboot the GSC3574/75 after confirming the reboot pop-up.



Gesture Guide

This section displays the different gestures supported to navigate through the GSC3574/75, it also shows the steps needed to perform different actions such as accessing the opened tabs section, and returning to the desktop…



Note:

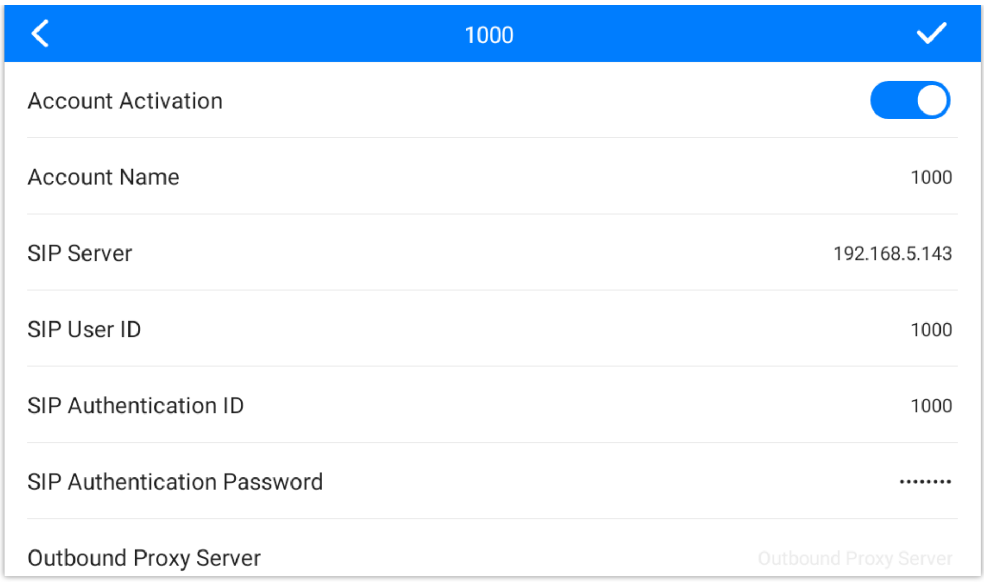
When the "Return to Desktop" gesture is performed, the screen navigates back to the default homepage, as defined in the **Homepage Setting** on the Web UI under **System Settings** → **Preferences**. This may be either the Main Menu Page or the Desktop Shortcut Page, depending on the configuration.

Advanced

Accounts

Set up to 6 SIP accounts. The Account Settings page allows you to configure SIP settings for each account. Tap on Account# to access the settings. When configured, press the ✔ sign (on the top right corner) to confirm the changes, or press the back button to cancel them. Users can press Empty Configuration at the bottom of the page to clear all the settings. The following settings can be configured for each account. Refer to [Account Settings Page Definitions] for a description of each option.

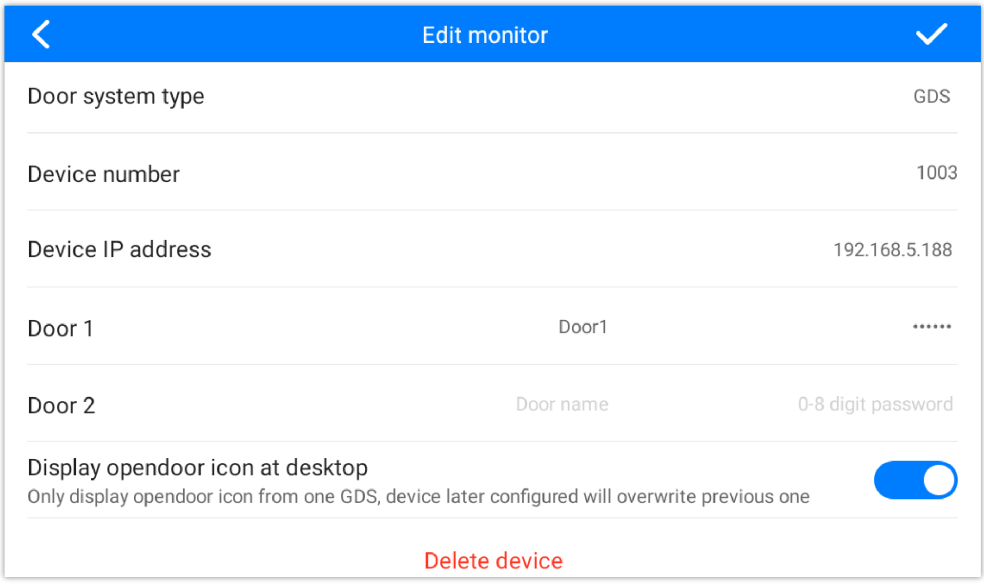
- **Account Activation**: activate/deactivate the current SIP account.
- **SIP Server**: Enter the SIP server FQDN or IP.
- **SIP User ID**: Set the SIP Account User ID.
- **SIP Authentication ID**: Set the SIP Account Authentication ID.
- **SIP Authentication Password**: Set the SIP Account Authentication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



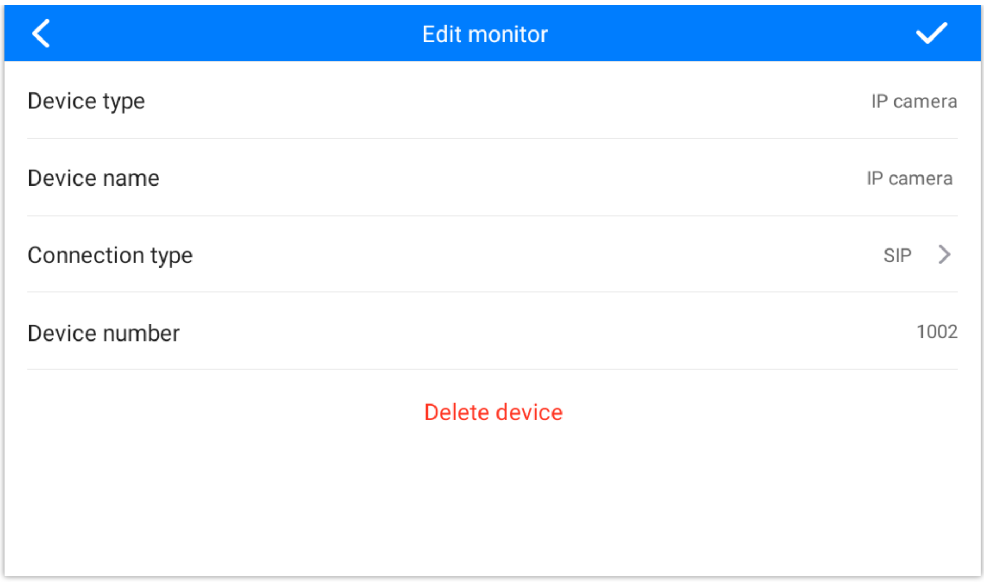
Monitor

The monitor section allows the user to monitor up to 50 door systems and up to 32 IP cameras:

- **Door System**: Add/Edit or delete the GDS37xx's configuration. Make Call to GDS37xx.
- **Door System Type**: Select either **GDS**, **HTTP**, or **OTHER** for other door control vendors.
- **Device Name**: Set the device name.
- **Connection type:** Select the signaling protocol to be used, SIP, RTSP(TCP), RTSP(UDP), RTSP(Multicast). The default is SIP, this option is for IP cameras only.
- **Device Number**: Set the SIP extension or the IP address of the Door System.
- **Door 1/2**: Enter the DTMF PIN to open the door remotely.
- **IP Camera**: Add/Edit or delete the IP Camera's configuration. Make a Call to the IP Camera.
- **Device Name**: Set the device name.
- **Device Number**: Set the SIP extension or the IP address of the IP Camera.
- **Display open door icon at desktop:** Displays the open door icon at the desktop. It only displays the open door icon from one GDS; a device later configured will overwrite the previous one.



Door System Settings

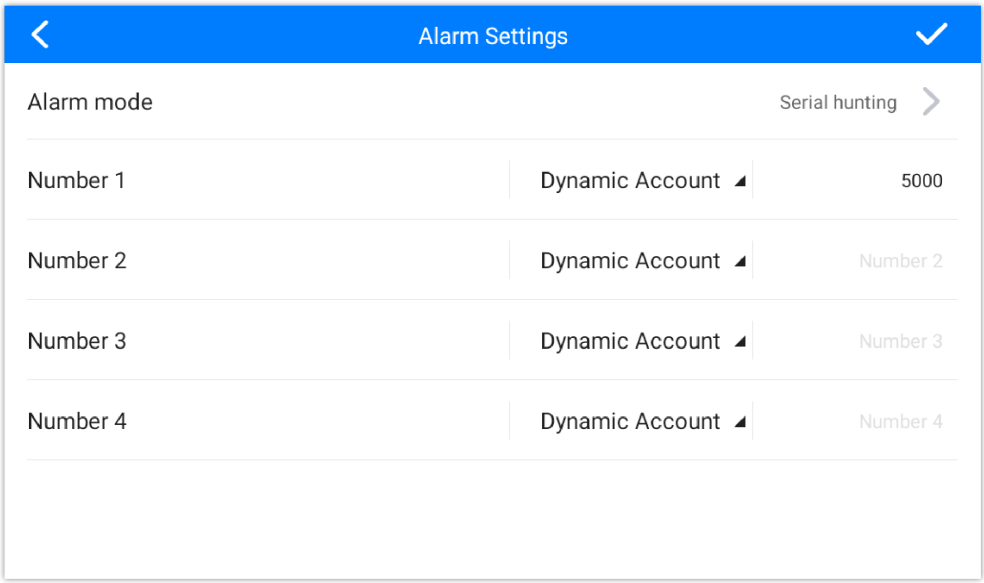


IP camera settings

Alarm Settings

Select the Alarm Mode and configure from which account to make calls when an alarm is triggered as well as the receiving numbers.

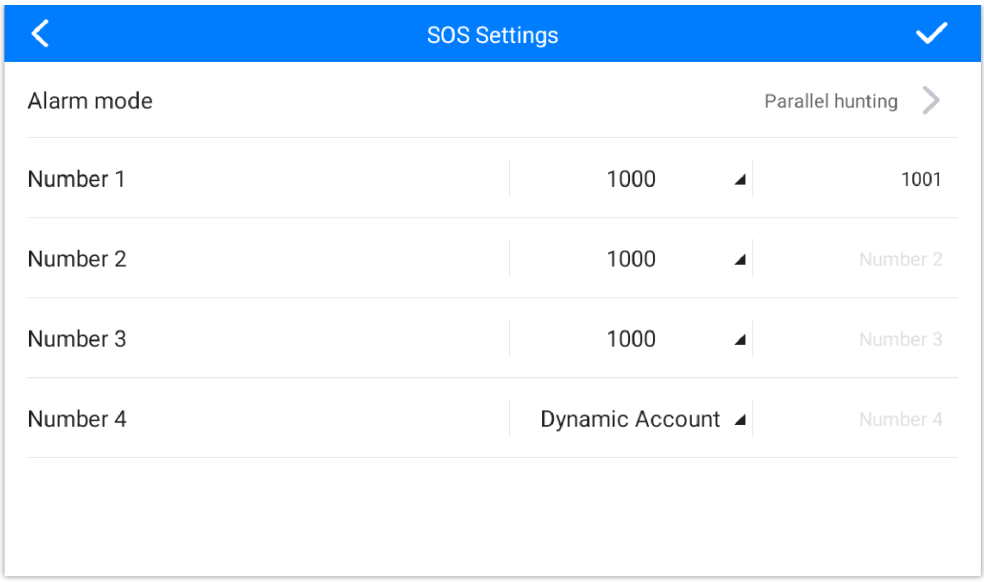
- **Alarm Mode**: Select between Serial or Parallel Hunting.
- **Number 1-4**: Set the Account from which the outgoing call will be made and towards which Number.



SOS Settings

Select the Alarm Mode and configure from which account to make calls when the SOS key is pressed, as well as the receiving numbers.

- **Alarm Mode**: Select between Serial or Parallel Hunting.
- **Number 1-4**: Set the Account from which the outgoing call will be made and towards which Number.



Note

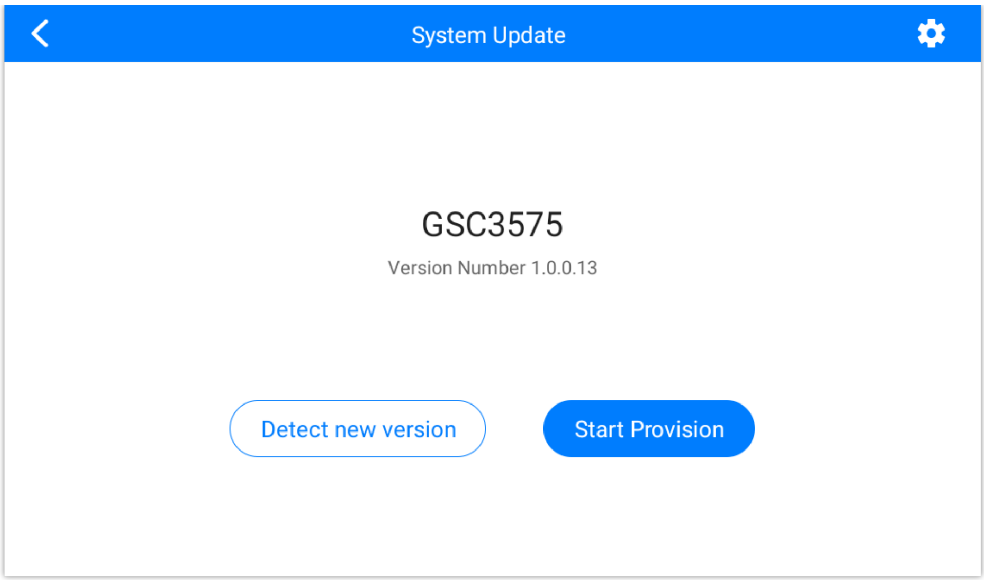
Long-press the SOS icon to trigger the SOS alarm to the configured numbers.

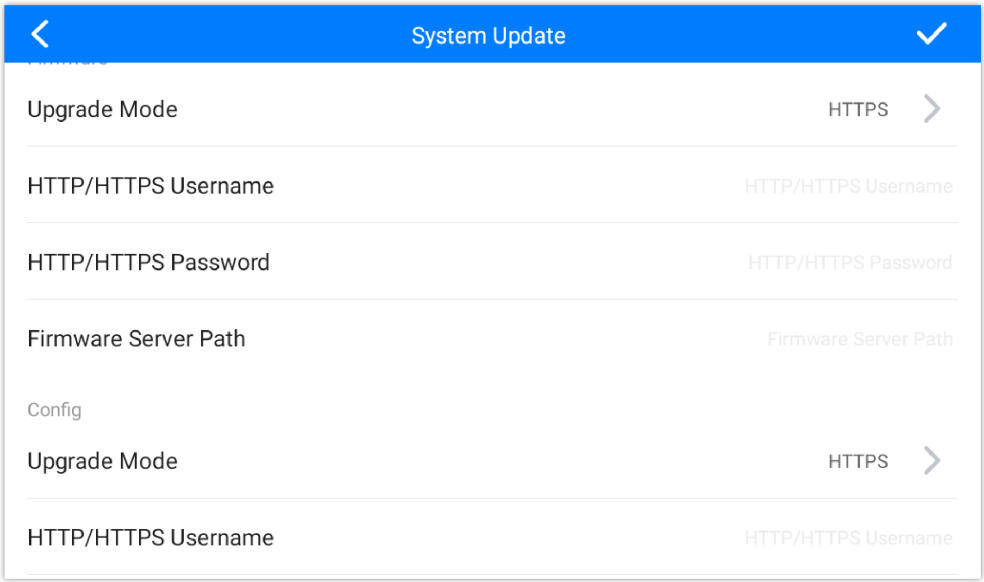
System Update

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

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

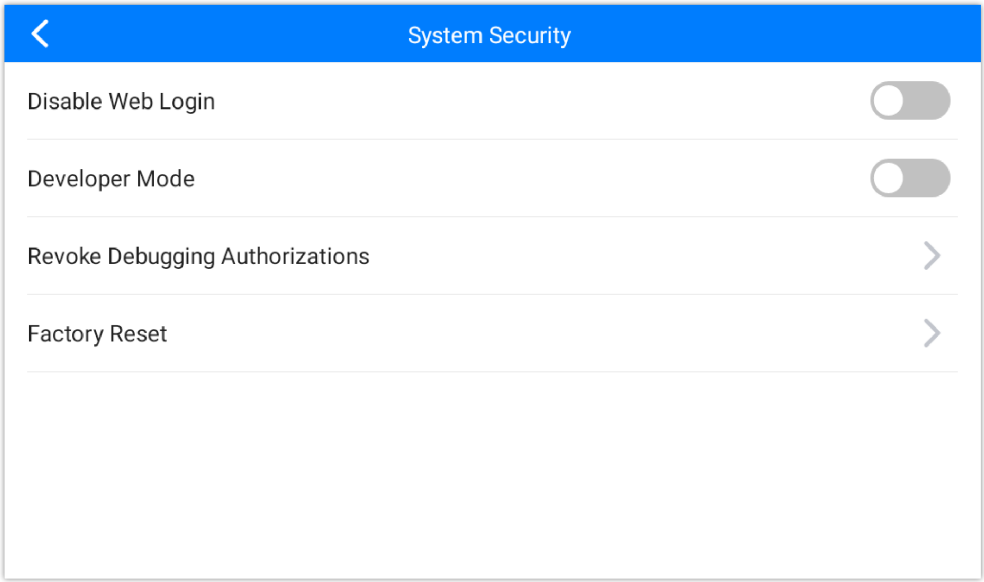




System Security

The system security settings contain the configuration parameters:

- **Disabling Web Login**
- **Enabling Developer Mode**
- **Revoking Debugging Authorizations**
- **Performing a Factory Reset**



CONFIGURATION VIA WEB BROWSER

The GSC3574/75 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the GSC3574/75 through a Web browser such as Google Chrome, Mozilla Firefox, and Microsoft Edge.

To access the Web GUI:

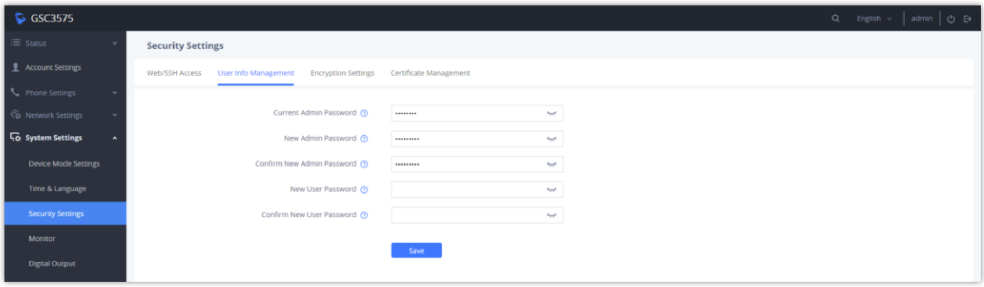
1. Connect the computer to the same network as the GSC3574/75.
2. Make sure the GSC3574/75 is turned on and shows its IP address. You may check the IP from the LCD **Settings→Status→Network Status**
3. Open a Web browser on your computer.
4. Enter the GSC3574/75's IP address in the address bar of the browser.
5. Enter the administrator's login and password available on the MAC sticker to access the Web Configuration Menu.

Notes:

- The computer must be connected to the same sub-network as the GSC3574/75. This can be easily done by connecting the computer to the same hub or switch as the GSC3574/75 is connected to.
- If the GSC3574/75 is properly connected to a working Internet connection, the IP address of the GSC3574/75 will display in **Settings** → **Status** → **Network Status**. This address has the format: xxx.xxx.xxx.xxx, where xxx stands for a number from 0-255. Users will need this number to access the Web GUI. For example, if the GSC3574/75 has IP address 192.168.40.154, please enter "https://192.168.40.154" in the address bar of the browser.
- There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed
End User Level	user	123	Browse the following pages: ● Status ● Phone settings(Only Multicast Paging, ● Network Settings ● System Settings ● Maintenance ● Contacts and LDAP Phonebook
Administrator Level	admin	Random Password (on the back of the unit)	Browse all pages

- When accessing the GSC3574/75, the user can then change the default administrator password immediately after providing the initial random password on the back of the unit. The user can also change the admin password from **System Settings** → **Security Settings** → User Info Management
- The new password field is case-sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits, and special characters is recommended for better security.



Change Password

Note

When changing any settings, always SUBMIT them by pressing the "Save" button on the bottom of the page. If the change is saved only but not applied, after making all the changes, click on the "APPLY" button on the top of the page to submit. After submitting the changes in all the Web GUI pages, reboot the GSC3574/75 to have the changes take effect if necessary (All the options under the "Accounts" page and "Phonebook" page do not require a reboot. Most of the options under "Settings" page do not require a reboot).

This section describes the options in the GSC3574/75's Web GUI. As mentioned, you can log in as an administrator or an end user.

- **Status:** Displays the Account status, Network status, and System Info of the GSC3574/75.
- **Account Settings:** To configure the SIP account settings and swap account settings.
- **Phone Settings:** To configure call features, ring tone, audio control, LCD display, multicast paging, etc.
- **Network Settings:** To configure network settings.
- **System Settings:** This section configures the features related to the device's main functionalities, such as the monitor feature, arming settings, alarm settings, and Desktop Shortcut Settings…
- **Maintenance:** To configure web access, upgrading and provisioning, syslog, security settings, etc.
- **App:** To manage contacts, LDAP directory, and contacts…

Status Page Definitions

Status – Account Status	
Account	Displays the list of accounts supported by the GSC3574/75, the device supports up to 6 accounts
SIP User ID	Displays the registered SIP user ID.
SIP Server	Displays the SIP server address
Status	Shows whether the device is registered or not.
Status – Network Status	
MAC Address	Displays the 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
NAT Type	Displays the type of NAT connection used by the device.
IPv4 Address Type	Displays The configured address type: DHCP, Static IP or PPPoE.
IPv4 Address	Displays The IP address of the device.
Subnet Mask	Displays Subnet mask of the device.
Gateway	Displays Default gateway of the device.
DNS Server 1	Displays DNS Server 1 of the device.
DNS Server 2	Displays DNS Server 2 of the device.

IPv6 Address Type	Displays The configured address type: DHCP, Static IP.
IPv6 Address	Displays The IPv6 address obtained on the device.
IPv6 Gateway	Displays IPv6 gateway of the device.
IPv6 DNS Server 1	Displays IPv6 DNS Server 1 of the device.
IPv6 DNS Server 2	Displays IPv6 DNS Server 2 of the device.
Status – System Info	
Product Model	Displays the Product model of the device.
Hardware Version	Displays the Hardware version number.
Part Number	Displays the Product part number.
Serial Number	Displays the Product Serial number.
System Version	Displays the Firmware version. This is the main software release version.
Boot Version	Displays the Booting code version.
Kernel Version	Displays the Kernel version
Android™ Version	Displays the Android OS version.
CPE Version	Displays the CPE version. The current version is 1.0.4.144.
Certificate Type	Displays the certificate type of the device.
System Up Time	Displays the total running time of the device since last reboot.

Status Page Definitions

Account Settings Page Definitions

Account x □ General Settings	
Account Registration	
Account Active	Indicates whether the account is active. The default setting is “No”.
Account Name	The name associated with each account to be displayed on the LCD. (e.g., MyCompany)
SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (e.g., sip.mycompany.com, or IP address)
SIP User ID	User account information, provided by your VoIP service provider.

SIP Authentication ID	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	The account password required for the phone to authenticate with the SIP server before the account can be registered. After it is saved, this will appear as hidden for security purpose.
Display Name	The SIP server subscriber's name (optional) that will be used for Caller ID display (e.g., John Doe).
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to "user=phone". A "user=phone" parameter will be attached to the Request-URI and "To" header in the SIP request to indicate the E.164 number. If set to "Enable", "tel:" will be used instead of "sip:" in the SIP request.
Voice Mail Access Number	Allows users to access voice messages by pressing the MESSAGE button on the phone. This value is usually the VM portal access number.
Network Settings	
Outbound Proxy	The IP address or domain name of the main outbound proxy, media gateway, or session border controller. This information is utilized by the device to navigate Firewall or NAT obstacles in various network settings. In the event of detecting a symmetric NAT, STUN becomes ineffective, leaving only an outbound proxy capable of resolving the issue.
Secondary Outbound Proxy	The IP address or domain name of the Secondary Outbound Proxy, Media Gateway, or Session Border Controller. This secondary outbound proxy comes into play when the primary one encounters a failure.
DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. ● A Record ● SRV ● NAPTR/SRV
Max Number Of Sip Request Retries	Sets the maximum number of retries for the device to send requests to the server. In DNS SRV configuration, if the destination address does not respond, all request messages are resent to the same address according to the configured retry times. Valid range: 1-10.

DNS SRV Failover Mode	Configures the preferred IP mode for DNS SRV. If set to “default”, the first IP from the query result will be applied. If set to “Saved one until DNS TTL”, previous IP will be applied before DNS timeout is reached. If set to “Saved one until no response”, previous IP will be applied even after DNS timeout until it cannot respond. ● Default If the option is set with “default”, it will again try to send register messages to one IP at a time, and the process repeats. ● Saved one until DNS TTL If the option is set with “Saved one until DNS TTL”, it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up. ● Saved one until no responses If the option is set with “Saved one until no responses”, it will send registered messages to the previously registered IP first, but this behavior will persist until the registered server does not respond. ● Failback follows failback expiration timer If “Failback follows failback expiration timer” is selected, the device will send all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires.
Failback Expiration (m)	Specifies the duration (in minutes) since failover to the current SIP server or Outbound Proxy before making failback attempts to the primary SIP server or Outbound Proxy.
Register Before DNS SRV Failover	Configures whether to send REGISTER requests to the failover SIP server or Outbound Proxy before sending INVITE requests in the event of a DNS SRV failover.
NAT Traversal	Configures whether NAT traversal mechanism is activated. Please refer to user manual for more details. If set to “STUN” and STUN server is configured, the phone will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the phone will try to use public IP addresses and port number in all the SIP&SDP messages. The phone will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be “Keep-alive”. Configure this to be “No” if an outbound proxy is used. “STUN” cannot be used if the detected NAT is symmetric NAT. Set this to “OpenVPN” if OpenVPN is used.
Proxy-Require	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall.
Account x □ SIP Settings	
Basic Settings	
SIP Registration	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is “Enabled”.
Unregister Before New Registration	● If set to “**No**”, the phone will not unregister the SIP user’s registration information before new registration. ● If set to “**All**”, the SIP Contact header will use “*” to clear all SIP user’s registration information. ● If set to “**Instance**”, the phone only needs to clear the current SIP user’s info.
REGISTER Expiration (m)	Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar. The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
SUBSCRIBE Expiration (m)	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar.

	The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
Re-Register before Expiration (s)	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default value is 0.
Registration Retry Wait Time (s)	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
Add Auth Header On Re-register	If enabled, the phone will add Authorization header in initial REGISTER request. Default is “Disabled”.
Enable SIP OPTIONS Keep Alive	Configures whether to enable SIP OPTIONS to track account registration status. If enabled, the phone will send periodic OPTIONS messages to server to track the connection status with the server. Default is “Disabled”.
SIP OPTIONS Keep Alive Interval	Configures the time interval the phone sends OPTIONS message to the server. If set to 30 seconds, it means the phone will send an OPTIONS message to the server every 30 seconds.
SIP OPTIONS Keep Alive Maximum Tries	Configures the maximum number of times the phone will try to send OPTIONS message consistently to server without receiving a response. If set to “3”, the phone will send OPTIONS message 3 times. If no response from the server, the phone will re-register.
SUBSCRIBE for MWI	When set to “Yes”, a SUBSCRIBE for Message Waiting Indication will be sent periodically. The default setting is “No”.
Use Privacy Header	Configures whether the “Privacy Header” is present in the SIP INVITE message. ● **Default**: the phone will add “Privacy Header” when special feature is not “Huawei IMS”. ● **Yes**: the phone will always add “Privacy Header”. ● **No**: the phone will not add “Privacy Header”. The default setting is “default”.
Use P-Preferred- Identity Header	Configures whether the “P-Preferred-Identity Header” is present in the SIP INVITE message. ● **Default**: the phone will add “P-Preferred-Identity header” when special feature is not “Huawei IMS”. ● **Yes**: the phone will always add “P-Preferred-Identity header”. ● **No**: the phone will not add “P-Preferred-Identity header”.
Use P-Access-Network-Info Header	Configures to use P-Access-Network-Info header in SIP request. Default setting is “Yes”.
Use P-Emergency-Info Header	Configures to use P-Emergency-Info header in SIP request. Default setting is “Yes”.
Use MAC Header	● If **Register Only**, all outgoing SIP message will include the MAC header. ● If **Yes to all SIP**, all outgoing SIP messages will include the MAC header. ● If **No**, the phone’s MAC header will not be included in any outgoing SIP messages. The default setting is “No”.

Add MAC in User-Agent	● If **Yes except REGISTER**, all outgoing SIP messages will include the phone's MAC address in the User-Agent header, except for REGISTER and UNREGISTER. ● If **Yes to All SIP**, all outgoing SIP messages will include the phone's MAC address in the User-Agent header. ● If **No**, the phone's MAC address will not be included in the User-Agent header in any outgoing SIP messages. The default setting is "No".
SIP Transport	Selects the network protocol used for the SIP transport. The default setting is "UDP".
Local SIP Port	Configures the local SIP port used to listen and transmit.
SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	Configures whether the actual ephemeral port in contact with TCP/TLS will be used when TLS/TCP is selected for SIP Transport. The default setting is "No".
Support SIP Instance ID	Configures whether SIP Instance ID is supported or not. The default setting is "Yes".
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
SIP Timer D Interval	Sets the time interval of SIP Timer D. This timer specifies the wait time of response retransmissions when the client receives 3xx ~ 6xx response to an INVITE. The valid range is 0-64 seconds. If set to 0, the parameter will not take effect. The true time interval is equal to T1*64.
Remove OBP From Route	Configures to remove outbound proxy from route. If set to "Enabled", the SIP account will notify the server to remove the proxy in NAT/Firewall environment. If set to "Always", the SIP account will notify the server to remove the proxy unconditionally.
Enable 100rel	The use of the PRACK (Provisional Acknowledgment) method enables reliability to SIP provisional responses (1xx series). This is very important in order to support PSTN internetworking. To invoke a reliable provisional response, the 100rel tag is appended to the value of the required header of the initial signaling messages. Disabled by Default
Session Timer	
Enable Session Timer	Configures whether to enable session timer function. 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. If set to "Yes", the phone will use the related parameters when sending session timer according to "Session Expiration". If set to "No", session timer will be disabled. The default setting is "No".
Session Expiration (s)	Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180. The valid range is from 90 to 64800.

Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
UAC Specify Refresher	As a caller, select UAC to use the phone as the refresher, or select UAS to use the callee or proxy server as the refresher. When set to “Omit”, the refresh object is not specified. The default setting is “UAC”.
UAS Specify Refresher	As a callee, select UAC to use caller or proxy server as the refresher, or select UAS to use the phone as the refresher. The default setting is “UAC”.
Caller Request Timer	If set to “Yes” and the remote party supports session timers, the phone will use a session timer when it makes outbound calls. The default setting is “No”.
Callee Request Timer	If set to “Yes” and the remote party supports session timers, the phone will use a session timer when it receives inbound calls. The default setting is “No”.
Force Timer	If set to “Yes”, the phone will use the Session Timer even if the remote party does not support this feature. Otherwise, Session Timer is enabled only when the remote party supports it. The default setting is “No”.
Force INVITE	Select “Yes” to force using the INVITE method to refresh the session timer. The default setting is “No”.
Account x □ Codec Settings	
Preferred Vocoder	
Preferred Vocoder (Choice 1 – 9)	Multiple vocoder types are supported on the phone, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message. The vocoders supported are: ● G.722.1 ● G729A/B ● G726-32 ● iLBC ● Opus ● G.722.1C ● G.722 ● PCMU ● PCMA
Codec Negotiation Priority	Configures the phone to use which codec sequence to negotiate as the callee. When set to “Caller”, the phone negotiates by SDP codec sequence from received SIP Invite. When set to “Callee”, the phone negotiates by audio codec sequence on the phone. The default setting is “Callee”.
Use First Matching Vocoder in 200OK SDP	When set to “Yes”, the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is “No”.
iLBC Frame Size	Selects iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is “30ms”.
G726-32 ITU Payload Type	Payload type for G726-32 in ITU packing mode. Payload 2 remains static, while payload dynamic varies dynamically.

G.726-32 Dynamic Payload Type	Specifies G726-32 payload type. Valid range is 96 to 126.
Opus Payload Type	Specifies Opus payload type. Valid range is 96 to 127. It cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
DTMF	Specifies the mechanism to transmit DTMF digits. There are 3 supported modes: 1. **In audio**: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs). 2. **RFC2833** sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. 3. **SIP INFO** uses SIP INFO to carry DTMF. Default setting is "RFC2833".
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call.
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 126. The default value is 121.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 126. The default value is 124.
Silence Suppression	If 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. For codec G.723 and G.729 only. Default setting is "No".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120 kbps. 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 in the codec table or negotiate the payload type during the actual call. For example, if set to 2 and the first code is G.729, G.711 or G.726, the "ptime" value in the SDP datagram of the INVITE request is 20 ms. If the "Voice Frame/TX" setting exceeds the maximum allowed value, the phone will use and save the maximum allowed value for the selected first codec. It is recommended to use the default setting provided, and incorrect setting may affect voice quality. The default setting is 2.
Preferred Video Codec	
Preferred Video Codec	This parameter allows user to select preferred video codec from the "available" list. The device supports H.264.
Enable Video FEC	If set to "Yes," FEC (Forward Error Correction) will be activated for the video call.
Enable RFC5168 Support	If set to "Yes", RFC5168 support will be enabled for video call.
FEC Payload Type	Configures FEC payload type. The valid range is from 96 to 126.

Packetization Mode	Sets the video packetization mode. If set to “Single NAL Unit Mode”, the packetization mode will be negotiated as single NAL unit mode for video calls and used for video encoding regardles if the other party support the negotiation. If set to “Non-Interleaved Mode”, the packetization mode will be negotiated as Non-interleaved mode for video calls and used for video encoding regardless if the other party supports the negotiation. If set to “Prefer Non-Interleaved Mode”, the packetization mode will prioritize Non-interleaved mode to be negotiated for video calls but if the other party does not support this， the device negotiate “Single NAL Unit Mode”.
H.264 Image Size	Select the H.264 image size from “720P” , “4CIF”, “VGA”, “CIF” , “QVGA” or “QCIF”.
Use H.264 Constrained Profiles	Configures whether to use H.264 CBP to establish video call with WebRTC. The function takes effect when H.264 profile setting includes BP type. It is recommended to set to “Yes” when establish video call with WebRTC.
H.264 Profile Type	Select the H.264 profile type from “Baseline Profile”, “Main Profile”, “High Profile” or “BP/MP/HP”. The lower profile type is easier to decode, while the higher level has high compression ratio. For device with low CPU, select “Baseline Profile” to play record; “Baseline Profile” is more likely to be used in a video conference that has high demandings for the video quality. Select among three types to achieve the best video effect.
Video Bit Rate	The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted than the video quality will decrease due to packet loss.
SDP Bandwidth Attribute	Select the SDP bandwidth attribute from “Standard” , “Media Level” , “Session Level” or “None”. **Standard:** Use AS at the session level and TIAS at the media level. **Media Level:** Use AS at the media level. Session Level: Use AS at the session level. **None:** Do not change the format. The default setting is “Media Level”. Please do not change the format or it may cause decode failure if unclear about what format the server supports.
H.264 Payload Type	Enter H.264 codec payload type. The valid range is from 96 to 127.
Packet Retransmission	If set to “NACK”, the signaling will carry NACK info. After negotiation, the media will use NACK to retransmit lost packets. If set to “NACK+RTX (SSRC-GROUP) “, the signaling will carry both NACK and RTX info. After negotiation, the media will use NACK+RTX (SSRC-GROUP) to achieve packet loss retransmission. If set to “Disabled”, packet loss retransmission cannot be used.
RTP Settings	
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu. ● No ● Enabled but Not forced ● Enabled and Forced ● Optional The default setting is “No”.
SRTP Key Length	Allows users to specify the length of the SRTP calls. Available options are: ● **AES 128&256 bit** ● **AES 128 bit** ● **AES 256 bit** Default setting is AES 128&256 bit

Enable SRTP Key Life Time	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. The default setting is “Yes”.
RTCP Keep-Alive Method	Configures the RTCP channel keep-alive packet type. ● **Receiver Report:** The RTCP channel will sends “receiver report+source description+RTCP extension” as keep-alive data. ● **Sender Report:** The RTCP channel will sends “Sender report+source description+ RTCP extension” as keep-alive data.
RTP Keep-Alive Method	Configures the RTP channel keep-alive packet type. ● **No:** No data will be sent ● **RTP Version 1**: The wrong version infor “1” will be carried when sending RTP data packets. ● **RTP Packet with Silent Payload:** If set to “RTP Packet with Silent Payload”, the silent payload will be carried when sending RTP format packets.
RTCP Destination	Configures the server address. When there is a call, the RTCP package sent from the device will also be sent to this address. Note: The address should contain port number.
Symmetric RTP	Configures whether Symmetric RTP is used or not. Symmetric RTP means that the UA uses the same socket/port for sending and receiving the RTP stream. The default setting is “No”.
RTP IP Filter	Configures whether to filter the received RTP. If set to “Disabled”, the device will receive RTP from any address. If set to “IP Only”, the device will receive RTP from certain IP address in SDP with no port limited. If set to “IP and Port”, the device will only receive RTP from IP address & port in SDP.
RTP Timeout (s)	Configures the RTP timeout of the phone. If the phone does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. The default range is 0 and 6-600. If set to 0, the phone will not hang up the call automatically.
Account x □ Call Settings	
Call Features	
Auto-answer	If set to “Yes”, the device will automatically answer incoming calls. If set to “Intercom/Paging Only”, it will answer the call based on the SIP Call-Info or Alert-Info header sent from the server/proxy.
Play Warning Tone for Auto Answer Intercom	Plays Warning Tone for Auto Answer Intercom
Send Anonymous	If set to “Yes”, the “From” header in outgoing INVITE messages will be set to anonymous. Default is “No”.
Reject Anonymous Call	If set to “Yes”, anonymous calls will be rejected. The default setting is “No”.
Call Log	Configures Call Log setting on the phone. ● **Log All Calls** ● **Log incoming/Outgoing Only (missed calls NOT recorded)** ● **Disable Call Log** The default setting is “Log All Calls”.
Enable Call Features	If set to “Yes”, call features (including anonymous call, DND and etc) will be supported locally instead of using the feature code supported on SIP server/proxy. Please refer to user

	manual for more details.
Enable Call Waiting	Configures the call waiting function for this account. If set to “Default”, it will be configured according to global call waiting function. Default value is “Default”.
Mute on Answer Intercom Call	When enabled, device will mute the incoming intercom call by Call-Info/Alert-Info.
Use # as Dial Key	Allows users to configure the “#” key as the “Send” key. If set to “Yes”, the “#” key will immediately dial out the input digits. In this case, this key is essentially equivalent to the “Send” key. If set to “No”, the “#” key is treated as part of the dialed string. Enabled by Default.
Use # as Redial Key	Allows users to configure the “#” key as the “Redial” key. If set to “Yes”, the “#” key will immediately redial the last call. In this case, this key is essentially equivalent to the “Redial” key. If set to “No”, the “#” key is treated as part of the dialed string.
DND Call Feature On	Configuring the DND feature code. When the DND turned on, the feature code will be sent to server, then the server synchronously enables the DND function.
DND Call Feature Off	Configuring the DND feature code. When the DND turned off, the feature code will be sent to server, then the server synchronously disables the DND function.
No Key Entry Timeout (s)	This is used to set the time length before dialing the entered digits automatically when no key operation is detected. The Default value is 4 seconds
Ring Timeout (s)	Defines the timeout (in seconds) for the rings on no answer. The default value is 60 seconds
RFC2543 Hold	If yes, c=0.0.0.0 will be used in INVITE SDP for hold.
Dial plan	
Dial Plan Prefix	Configures a prefix added to all numbers when making outbound calls.
Disable Dialplan	Defines whether to disable dial plan of the Dial Page, Contacts, Incoming Call History, Outgoing Call History, Programmable Key & Click2Dial functions. If set to “Yes”, the corresponding dial plan of the function will be disabled.
Dial Plan	Configures the dial plan rule. For syntax and examples, please refer to user manual for more details. Dial Plan Rules: 1. Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d; 2. Grammar: x – any digit from 0-9; 3. Grammar: X – any character from 0-9, a-z, A-Z. 4. xx+ – at least 2 digit numbers 5. xx – only 2 digit numbers 6. XX – two characters (AA, Ab, 1C, f5, 68,…) 7. test : only string “test” will pass the dial plan check 8. ^ – exclude 9. [3-5] – any digit of 3, 4, or 5 10. [147] – any digit of 1, 4, or 7 11. <2=011> – replace digit 2 with 011 when dialing 12. | – the OR operand ● Example 1: {[369]11 | 1617xxxxxxx} Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617; ● Example 2: {^1900x+ | <=1617>xxxxxxx}

	Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers; ● Example 3: {1xxx[2-9]xxxxxx | <2=011>x+} Allows 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 Allows any length of numbers with leading digit 2, replacing the 2 with 011 when dialed. ● 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 – allows dialing to local area code (617) numbers by dialing7 numbers and 1617 area code will be added automatically; ● 1[2-9]xx[2-9]xxxxxx |- allows dialing to any US/Canada Number with 11 digits length; ● 011[2-9]x – allows international calls starting with 011; ● [3469]11 – allows 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. Max length of dial plan is up to 1024 characters.
Caller IDs	
Caller ID Display	When set to “Auto”, the phone will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. When set to “Disabled”, all incoming calls are displayed with “Unavailable”.
Callee ID Display	When set to “Auto”, the phone will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in the 180 Ringing. When set to “Disabled”, callee id will be displayed as “Unavailable”. When set to “To Header”, caller id will not be updated and displayed as To Header.
Ringtones	
Account RingTone	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu. **Note**: User can also choose The DTMF System Ringtone
Ignore Alert-Info header	Configures to play default ringtone by ignoring Alert-Info header. The default setting is “No”.
Match Incoming Caller ID	Specifies matching rules with number, pattern, or Alert Info text (up to 10 matching rules). When the incoming caller ID or Alert Info matches the rule, the phone will ring with selected distinctive ringtone. Matching rules: ● Specific caller ID number. For example, 8321123. ● A defined pattern with certain length using x and + to specify, where x could be any digit from 0 to 9. Samples: **xx+** : at least 2-digit number. **xx** : only 2-digit number. **[345]xx**: 3-digit number with the leading digit of 3, 4 or 5. **[6-9]xx**: 3-digit number with the leading digit from 6 to 9. ● Alert Info text Users could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it. The custom ring tone will be used if the phone receives SIP INVITE with Alert-Info header in the following format: Alert-Info: <http://127.0.0.1>; info=priority When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone.

	Note: Beginning with firmware version 1.0.3.98, a new feature was introduced that enables the use of a ringtone stream via a remote URL. The functionality of this feature works as follows: the following audio file named **test.wav** is uploaded onto an HTTP server and the remote URL is "http://192.168.5.165:8080/test.wav;info=ring3", the IP phone then attempts to use the provided URL first to play the ringtone. If the URL is not functional for some reason, it will then use the info=ring3 parameter, as the default ringtone.
Account x □ Advanced Settings	
Security Settings	
Check Domain Certificates	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is "No".
Enabled Authentication Server Validation	Validates CA certification when TLS/TCP is configured for SIP.
SIP CA Certificate	Select the CA certificate for server verification.
SIP User Certificate	Select the user certificate to access SIP TLS authentication content required by some specific servers. If the private key is included, upload it with the user certificate.
Validate Incoming SIP Messages	Defines whether the incoming SIP messages will be validated or not.
Only Accept SIP Requests From Known Servers	When set to "Yes", the SIP address of the request URL in the incoming SIP message will be checked. If it doesn't match the SIP server address of the account, the request will be rejected.
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it doesn't match the device's SIP User ID, the call will be rejected.
Allow SIP Reset	Allow SIP Notification message to perform factory reset. The default setting is "No".
Authenticate Incoming INVITE	If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. The default setting is "No".
SIP Realm Used for Challenge INVITE & NOTIFY	Configure this option to set the SIP server used to validate incoming INVITE or NOTIFY (for check-sync, resync, reboot). Only takes effect when Authenticate Incoming INVITE or SIP NOTIFY Authentication is enabled.
MOH	
Upload Local MOH Audio File	Configures to play reminder tone when the call is on hold.
Enable Local MOH	If set to "Yes" , the local MOH will be enabled. Users need to upload local MOH audio file. Once enabled, users could play the file when holding the call.
Advanced Features	
Virtual Account Group	Configures the account into virtual account group. If the outgoing/incoming call fails when using one account, the device will try to use other accounts in the same group.
Special Feature	Different soft switch vendors have special requirements. Therefore users may need select special features to meet these requirements. Users can choose from Standard, CBCOM, RNK, China Mobile, ZTE IMS, Mobotix, ZTE NGN, or Huawei IMS depending on the server type.

Feature Key Synchronization	This feature is used for BroadSoft or Metaswitch call feature synchronization. When set to “BroadSoft/Metaswitch”, DND and Call Forward features can be synchronized with the server. The local call forward function are disabled when this feature is active.
Allow Sync Phonebook Via SIP Notify	If set to “Yes”, the device will allow SIP NOTIFY messages to sync local phonebook.

Account Page Definitions

Phone Settings Page Definitions

Phone Settings – General Settings	
Basic Settings	
Local RTP Port	Defines the Local RTP port used. Audio RTP port：Port_Value+10*N Audio RTCP port: Port_Value+10*N+1. Default Port is 50040
Use Random Port	When set to “Yes”, this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple devices are behind the same full cone NAT. (This parameter must be set to “No” for Direct IP incoming calls, but IP outgoing calls are not affected) Disabled by Default.
Hide User Info for Video Call	Configures whether to display user information in a video call. If enabled, user information will not be displayed in the upper left corner of the video area during a video call. Disabled by Default.
Enable In-call DTMF Display	Enables DTMF display when in-call. Enabled by Default.
Enable LDAP Timeout Auto Search	Configures whether to display the matched content automatically in LDAP search when timeout. If set to “No”, users need to click the Search button to search the matched contacts mentioned above. Enabled by Default
Keep-alive Interval (s)	Specifies how often the device sends a blank UDP packet to the SIP server in order to keep the “pin hole” on the NAT router to open. Default value is 20 seconds
STUN Server	The IP address or domain name of the STUN server. STUN resolution results are displayed in the STATUS page of the device Web GUI. Only non-symmetric NAT routers work with STUN.
Use NAT IP	The NAT IP address in SIP/SDP messages. This field is blank by default settings. You should ONLY use it when required by your ITSP.
Phone Settings – Call Settings	
Basic Settings	
Enable Video Call	Enables the video call feature. Enabled by Default
Enable Direct IP Call Mode	Configures enable/disable direct IP call mode of the device. If set to “Yes”, the feature of direct IP call will be enabled. Disabled by default

Enable Quick IP-call Mode	This feature allows users to make a direct IP call by dialing the last octet of the IP address (3 digits instead of 12 digits IP address) if the devices are on the same LAN/VPN. No SIP server is required so the field should be left blank. When set to “Yes”, if XXX is dialed, where X is 0-9 and XXX <=255, the device will make a direct IP call to aaa.bbb.ccc.XXX where aaa.bbb.ccc comes from the LAN/VPN IP address REGARDLESS of the subnet mask. XX or X is also valid so a leading 0 is not required (but OK). See Quick IP Call Mode for details. The default value is “Disabled”
Enable Paging Call Mode	Configures enable/disable paging call mode of the device. If set to “Yes”, the feature of paging call will be enabled. Disabled by default
Enable Call Waiting	Enables the call waiting feature. Enabled by Default
Enable Call Waiting Tone	Enables the call waiting tone when call waiting is on. Enabled by default
Enable DND Reminder Ring	Enables the DND reminder ring. If set to “Yes”, a ring splash will play for incoming calls when DND is active. Enabled by default
Auto Mute on Entry	Configures whether to mute the call on entry automatically. If set to “Disabled”, then do not use auto mute function. If set to “Auto Mute on Outgoing Call”, then mute automatically when the other party answers the outgoing call. If set to “Auto Mute on Incoming Call”, then mute automatically when answering the incoming call. If set to “Mute on Incoming & Outgoing Call”, then mute automatically when the call is established. **Note:** this function only takes effect when the device is changed from the idle status to call status. Users could click the Mute button on call interface to cancel the current mute status.
Virtual Account Group Avaya Mode	If set to “Yes”, when processing SIP Register 3XX Response, if there exists a virtual group, it will parse the address site in 3XX, modify the account server info “SIP Server: port” & “SIP Transaction” in virtual account group and initiate registration again.
Number of Concurrent Registration for Virtual Account Group	Configures the amount of concurrent accounts in virtual account group. If the total amount of virtual group accounts is “N”, the number of accounts the user sets is “n”, then the device will register the first n accounts; If registration for all of these accounts failed, then register the last N-n accounts.
Filter Characters	Filter Characters are used to filter the specific separator characters for Click2Dial or contacts imported from other devices. These specific characters are not part of the actual phone number and needed to filter out. Users could set up multiple characters. For example, if set to “[()-]”, when dialing (0571)-8800-8888, the character “()-” will be automatically filtered and dial 057188008888 directly. Initiate calls from other places except dial screen, such as call history and contacts, will automatically filter the characters. Dialing out from Dial screen will not filter any characters.
Escape ‘#’ as %23 in SIP URI	Replaces ‘#’ by ‘%23’ in some special situations. The option is enabled by default.
Record Storage Path	Configure the recording storage path.
Record Mode	Configures recording mode. If set to “Record locally”, the device will use the local recorder for call recording, and the audio file will be saved according to the recorder setup. If set to “Record on UCM”, the device will send the recording feature code to the UCM server to request for recording, and the recording function will be executed by the server.
Enable Auto Record When Call Established	Configures whether to auto record when a call is established. If set to “Yes”, the call recording will start automatically when the call is established. Disabled by default

Rejected Call Notification	Specify whether to enable rejected call notification. Once enabled, a missed call will prompt on LCD when reject the incoming call.
Return Code When Refusing Incoming Call	When refusing the incoming call, the device will send the selected type of SIP message of the call.
Return Code When Enable DND	When DND is enabled, the device will send the selected type of SIP message.
Default Video Stream	Defines the stream that will be automatically enabled when a video call starts. Users can choose a preferred video source from a predefined list of available streams. The default option is "**Call Video**" which refers to the live video feed from the ongoing video call. Users can also select an RTSP stream from a camera monitored by the GSC3574/75 control station. **Notes:** ● Selecting a monitored RTSP stream will cause that external video feed to appear automatically at the start of each video call. ● To control the default video stream from the LCD, make sure to check the option "**Set as default call video source**" from the monitored camera settings.
Call Function Buttons	
Call Function Button Display Timeout (s)	Sets the display timeout (in seconds) for call function buttons display. A value of "0" keeps the buttons always visible. Valid range: 0–30 seconds. The default setting is 5 seconds.
Call Function Buttons	Sets the buttons displayed below the call screen and on the side bar. Users can choose up to 4 buttons. The options are: ● **Bottom Bar:** Mute, Keyboard, Hold, More, Record, Screenshot, Video, Call details. ● **Side Bar:** Video Source, Speaker. **Note:** Changes will not take effect during an active call.
Phone Settings – Ringtone	
Auto Config CPT 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 manually configure CPT parameters.
● Dial Tone ● Second Dial Tone ● Ringback Tone ● Busy Tone ● Reorder Tone ● Confirmation Tone ● Call Waiting Tone ● Call Waiting Tone Gain ● Default Ring Cadence	Configures tone frequencies based on parameters from the local telecom provider. By default, they are set to the North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val, f2=val [, c=on1/off1[-on2/off2[-on3/off3]]];(Frequencies are in Hz and cadence on and off are in 10ms)ON is the period of ringing ('On time' in 'ms') while OFF is the period of silence. 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 repeat the pattern. Up to three cadences are supported.
Phone Settings – Video Settings	
Video Display Mode	Sets the video display mode to "Original proportion", "Equal proportional cutting" or "Proportional add black edge".

	● **Original proportion:** the device displays video in its original proportion that received from remote party, if the remote video display proportion is different from the device, the device will stretch or compress video to display it ● **Equal proportional cutting:** the device will cut video to meet its own display proportion ● **Proportional add black edge:** the device will display video in its original proportion, if still exists spare space, the device will add black edge on it The default setting is “Equal proportional cutting”.
Enable Frame Skipping In Video Decoder	If set to default setting “Yes”, the device will skip the P frame in lost video packet to decode the I frame in the next video packet. This setting helps to reduce video distortion.
Phone Settings – Multicast Paging	
Multicast Paging	
Paging Barge	During active call, if incoming multicast paging has higher priority (Disable being the highest, 1 being the second), then the call will be put on hold and multicast paging will be played, the priority range is 1-10
Paging Priority Active	If enabled, during a multicast paging, if another multicast is received with higher priority (1 being the highest), then the new multicast call will be played instead.
Multicast Listening	
Multicast Listening	Defines multicast listening addresses and labels. For example: ● “Listening Address” should match the sender’s Value such as “237.11.10.11:6767” ● “Label” could be the description you want to use.

Settings Page Definitions

Network Settings Page Definitions

Network Settings – Ethernet Settings	
IP Mode	Selects which Internet protocol to use. When both IPv4 and IPv6 are enabled, device attempts to use preferred protocol first and switches to the other choice if it fails.
IPv4 Address Type	Users could select “DHCP”, “Static IP” or “PPPoE”. • DHCP: 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.) • PPPoE: Configures PPPoE account/password. Obtain the IP address from the PPPoE server via dialing. • Static IP: Manual configures IP Address, Subnet Mask, Default Router’s IP Address, DNS Server 1, DNS Server 2.
DHCP VLAN Override	Selects the DHCP Option VLAN mode. When setting to “DHCP Option 132 and DHCP option 133”, the device will get DHCP option 132 and 133 as VLAN ID and VLAN priority. When setting to “Encapsulated in DHCP Option 43”, the device will get values from Option 43 which has VLAN ID and VLAN priority encapsulated. Note: Please make sure the “Allow DHCP Option 43, 160 and 66 Override Server” setting under maintenance->upgrade is checked.
Host Name (Option 12)	Specifies the name of the client hostname. This field is optional but may be required by some Internet Service Providers.
Vendor Class ID (Option 60)	Specifies the name of the client Vendor Class ID. This field is optional but may be required by some Internet Service Providers.

Layer 2 QoS 802.1Q/VLAN Tag (Ethernet)	Assigns the VLAN Tag of the Layer 2 QoS packets for LAN port. The default value is 0. Note: Please do not change the setting before understanding the VLAN's settings. Otherwise, the device might not be able to get the correct IP address.
Layer 2 QoS 802.1p Priority Value (Ethernet)	Assigns the priority value of the Layer 2 QoS packets. The Default value is 0.
IPv6 Address	Defines how the IPv6 address will be obtained on the device. The options are: Auto-configured, or statically configured
Static IPv6 Address	Enter the static IPv6 address in "Statically configured" IPv6 address type.
IPv6 Gateway	The static gateway when static IPv6 is used.
IPv6 Prefix Length	Enter the IPv6 prefix length in "Statically configured" IPv6 address type.
DNS Server 1	Enter the DNS Server 2 when static IP is used.
DNS Server 2	Enter the DNS Server 2 when static IP is used.
Preferred DNS Server	Defines the preferred DNS server.
802.1X Mode	Allows the user to enable/disable 802.1X mode on the device, the supported 802.1X Modes are: ● **EAP-MD5** ● **EAP-TLS** ● **EAP-PEAP**
802.1X Identity	Enters the Identity information for the 802.1X mode.
802.1X Secret	Enters the secret for the 802.1X mode.
802.1X CA Certificate	Select the CA certificate for server verification.
802.1X User Certificate	Select the user certificate to be used for mutual server authentication. If the private key is included, upload it with the user certificate.
Network Settings – Wi-Fi Settings	
WI-FI Basics	
IP Mode	Selects which Internet protocol to use. When both IPv4 and IPv6 are enabled, device attempts to use preferred protocol first and switches to the other choice if it fails.
Wi-Fi Function	This parameter enables/disables the Wi-Fi function. The default setting is set to "No".
WiFi Band	Sets the type of WiFi Band. The default setting is 2.4G&5G.
ESSID	This parameter sets the ESSID for the Wireless network. Press "Scan" to scan for the available wireless network.
Add Network	
ESSID	Enter the name of hidden ESSID.

Security Mode for Hidden SSID	This parameter defines the security mode used for the wireless network when the SSID is hidden.
Password	Configures the hidden ESSID password.
Advanced Settings	
Country Code	Configure WiFi country code. The default value is “US”.
Network Settings – OpenVPN® Settings	
Enable OpenVPN®	This option enables/disables OpenVPN® functionality, and requires the user to have access to an OpenVPN® server. Disabled by Default. **NOTE:** To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key. Additionally, the user must also set the SIP account to use “OpenVPN” for the “Nat Traversal” (under Account-> Network Settings).
OpenVPN® Mode	Simple mode only supports some basic or common parameters configuration. Expert mode supports configuration file upload, which can be fully customized. Please refer to https://openvpn.net for more information.
Enable OpenVPN® Comp-lzo	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.
OpenVPN® Server Address	Configures the URL/IP address for the OpenVPN® server.
OpenVPN® Port	The network port for the OpenVPN® server.
OpenVPN® Server Secondary Address	Allows the user to configure a secondary OpenVPN® server as a backup in case the primary server is down. If “Randomly Select Server” is enabled, the server will randomly be chosen instead of starting with the primary server address.
OpenVPN® Secondary Port	Configure OpenVPN® Secondary Port.
Randomly Select Server	If enabled, a server will be randomly selected for OpenVPN® requests. If disabled, requests will be made in the order of the server configuration. This setting is disabled by default.
OpenVPN® Transport	Determines network protocol used for OpenVPN®.
OpenVPN® CA Certificate	Select the CA certificate for server verification.
OpenVPN® User Certificate	Select the user certificate to be used for mutual server authentication. If the private key is included, upload it with the user certificate.
OpenVPN® Cipher Method	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server.
OpenVPN® Username	OpenVPN® authentication username (optional).
OpenVPN® Password	OpenVPN® authentication password (optional).

Upload OpenVPN® Configuration	Upload configuration file to the device. The supported upload extension is .zip
Network Settings – Advanced Settings	
Preferred DNS 1	Configures the preferred DNS 1 address.
Preferred DNS 2	Configures the preferred DNS 2 address.
Enable LLDP	If enabled, the device will accept VLAN, QoS and other parameters sent in LLDP packet from the switch in the network.
LLDP TX Interval (s)	Configures the interval the device sends LLDP-MED packets.
Enable CDP	Configures whether to enable CDP to receive and/or transmit information from/to CDP-enabled devices.
Layer 3 QoS for SIP	Defines the Layer 3 QoS parameter for SIP packets. This value is used for IP Precedence, Diff-Serv or MPLS.
Layer 3 QoS for Audio	Defines the Layer 3 QoS parameter for audio packets. This value is used for IP Precedence, Diff-Serv or MPLS.
HTTP/HTTPS User-Agent	This sets the user-agent for HTTP/HTTPS request.
SIP User-Agent	This option sets the user-agent for SIP. If the value includes the word "$version", it will be replaced with the system version.
Maximum Transmission Unit (MTU)	Configures the MTU in bytes. Please set MTU reasonably according to your needs. **Note:** If MTU is set to less than 1280, IPv6 may not take effect.
HTTP/HTTPS Proxy Hostname	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.
HTTP/HTTPS Proxy Port	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.
Bypass Proxy For	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.

Network Page Definitions

System Settings Page Definitions

System Settings – Device Mode Settings	
Device Mode	Select the device mode of the GSC3574/75, two options are available: ● **Control Station Mode (Default):** In this mode, the GSC3574/75 functions as a normal control station of the on premise security control, where it is usually deployed with other IP surveillance cameras such as the GSC36xx devices, and Door systems, such as the GDS37xx device models, in this mode the main functionalities deployed are the open door features, the "Monitor" feature, used to display the video feed of the cameras, in addition to some functionalities related to alarm out/in settings, this mode is the default mode of the GSC3574/75. ● **Meeting Room Panel Mode:** In this mode, the GSC3574/75 works as an extension of the UCM63xx model, it is used to display the organized onsite meetings from the UCM

	platform, and it can also create immediate meetings based on the availability of the time slots, this feature is useful when the GSC3574/75 is deployed in a meeting room scenario where hosts will need to either create immediate meetings or join an already scheduled meeting.
Association Server	If "Association" is selected, the server's meeting data will overwrite and clear the local meeting data. If "Disassociation" is selected, the system will clear the current meeting data.
Meeting Server	Defines the Meeting server address, which can be the IP address of the UCM on which the onsite meetings will be configured, **Example:** http(s)://192.168.86.199:8089
Server Connection Status	Displays the connection status, whether it has been connected to the meeting server or not.
Meeting Room Name	Defines the meeting room name, when not connected to any SIP server, when it's connected to a SIP server it will display the name defined on the UCM63xx onsite meeting settings.
System Settings – Time & Language	
Time Settings	
NTP Server	Defines the URL or IP address of the NTP server. The device may obtain the date and time from the server.
Allow DHCP Option 42 to Override NTP Server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server to synchronize date and time on the device if it's set up on the LAN.
Allow DHCP Option 2 to Override Time Zone Setting	Allows device to get provisioned for Time Zone from DHCP Option 2 in the local server automatically.
Time Zone	Controls the date/time display according to the specified time zone.
Time Display Format	12-hour or 24-hour time display format.
Date Display Format	Configures date format displayed on the device.
Language	
Language Selection	Select the language displayed on the device.
Select Language File	Press "Browse" to bring up a file selection menu to select the local .txt file to upload to the device.
System Settings – Security Settings	
Web/SSH Access	
Enable SSH	If set to "Yes", the device will allow any SSH access to the device.
SSH Port	This field is for customizing the SSH port.
Access Method	Allows users to select HTTP or HTTPS for Web Access.

Web Port	By default, HTTP uses port 80 and HTTPS uses port 443. This field is for customizing the web port.
Web Access Control	Configures Web access control by using Whitelist or Blacklist on incoming IP addresses.
Web Access Control List	Configures the list of IP addresses as Whitelist or Blacklist to allow or restrict web access based on the “Web Access Control” settings, you can configure up to two IP addresses
WebServer User Certificate	Selects the user certificate as the web server certificate to encrypt web access.
Configuration Via Keypad Menu	Configures access control for keypad Menu settings on the Settings interface of the device. **Unrestricted:** Configure all settings on the Settings interface; **Basic Settings Only:** Network, Features and Advanced options will not be displayed; **Basic settings & Network settings:** Advanced and Features options will not be displayed; **Constraint Mode:** users need to input admin password to access Network, Features and Advanced options; **Strict Mode:** users need to input admin password to access all desktop Apps except for “Call”, “File Manager” and “Applications”
Permission to Install/Uninstall Apps	Configures the permissions for users to install/uninstall the applications. If set to “Allow”, the user is free to install/uninstall third-party apps; If set to “Require admin password”, the user needs to input the correct administrator password to install/uninstall third-party apps; If set to “Require admin password if the app source is unknown”, the user needs to input administrator password only when installing apps from unknown source, and administrator password authentication is required when the user uninstalls third-party apps. If set to “Not allow”, the user cannot install/uninstall third-party apps.
User Info Management	
Current Admin Password	Enter current login user password. This field is case sensitive.
New Admin Password	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.
Confirm New Admin Password	Enter the new Admin password again to confirm.
New User Password	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.
Confirm New User Password	Enter the new User password again to confirm.
Encryption Settings	
Minimum TLS Version	Configures the minimum TLS version supported by the device.
Maximum TLS Version	Configures the maximum TLS version supported by the device.
Enable Weak TLS Cipher Suites	Defines the function for weak TLS cipher suites. If set to “Enable Weak TLS Cipher Suites”, allow users to encypt data by weak TLS cipher suites. If set to “Disable Symmetric Encryption RC4/DES/3DES”, allow users to disable weak cipher DES/3DES and RC4.
Certificate Management	
Trusted CA Certificates	Tusted CA certificates ensure secure communication by verifying the authenticity of SSL/TLS connections. They validate the identity of parties involved, safeguarding against unauthorized access or data breaches. Properly configured, they establish a foundation of trust for encrypted

	communication, enhancing overall system security, the GSC3574/75 supports contains two types of CA certificates: ● **Custom CA:** These are Certificate Authorities (CAs) that organizations can upload and configure themselves. They offer flexibility and control over the certificate hierarchy, allowing tailored security setups to be implemented, to add the CA certificate, Click on "Add", then select the file in PEM, DER, CRT, or CER format, then give it a label or name. ● **Phone CA:** Predefined by the system, Phone CAs are used in VoIP environments where devices like IP GSC3574/75 act as CAs. They streamline certificate management.
User Certificates	User certificates serve as digital credentials verifying user identities, granting access based on permissions, and facilitating secure interactions with the panel's functionalities, bolstering overall system security, you can add a user certificate in PEM, PFX, or P12 format, by clicking the icon "Add", then defining a label, and an optional password.
System Settings – Monitor	
Door System	The GSC3574/75 supports adding up to 50 door control devices, including GDS37xx Door control models and third-party variants. To add a door control device, simply click the "add" icon and proceed to specify the following fields: ● **Door system type:** Select access control mode. A GDS can support up to two access controls, you can choose between GDS when integrating a GDS device, HTTP request with an HTTP URL, or "OTHER", when wanting to integrate device of other vendors. ● **Door system number:** Enables open door button display when caller numbermatches this setting. e.g:"36311″. ● **Account:** Defines the Account used to perform the call. ● **Device IP:** Enables open door button display when IP address matches this setting. e.g:"192.168.124.81″ ● **Related Display Name 1:** Configures the display name of the door system. When the call matches the configured system number, the name will be displayed on LCD. ● **Access password 1:** Configures the access password of the door system. This password corresponds to the system number. When a call comes from the door system, tap on the open button on LCD to send the password to the corresponding door system. ● **Related Display Name 2:** Configures the display name of the door system 2. When the call matches the configured system number, the name will be displayed on LCD. ● **Access password 2:** Configures the access password of the door system 2. This password corresponds to the system number. When a call comes from the door system, tap on the open button on LCD to send the password to the corresponding door system. ● **URL:** When defining HTTP as the Door system type, you can then configure the URL responsible performing the open door action
IPC	The GSC3574/75 supports the management of up to 32 IP Cameras, to add an IP camera to to be managed, Click on "Add", the define the following fields: ● **Device Name:** Enter the camera name, which will be displayed in the preview. ● **Connection Type:** Select the connection type for the device, the options are : SIP, RTSP(TCP), RTSP(UDP), RTSP(Multicast) ● **Number:** Enter the Camera SIP extension ● **RTSP URL:** Enter the RTSP address of the camera. ● **RTSP Username:** Enter the RTSP username of the camera. ● **RTSP Password:** Enter the RTSP password of the camera.
System Settings – Digital Output	
Digital Output 1,2	
Digital Output	Defines the digital output action that is going to be performed when the ALMOUT1 or ALMOUT2 is triggered, the options are: ● **Disabled:** No action is taken when the alarm output is triggered. ● **To Alarm:** The triggered event activates the alarm system, signaling a security breach or emergency.

	● **To Door:** The triggered event controls the door, unlocking it or performing a related action. ● **Ring for Incoming Call:** The event prompts a ringing signal, indicating an incoming call or communication request.
Door Control SIP Account	Defines the Door Control SIP Account
Door System SIP User ID	Defines the door system SIP User ID
Door System IP Address	Defines the door system IP Address
Door System Display Name	Defines the Door System Display Name
Door System Password	Defines the Door System Password
Door Unlock Holding Time	Defines the time in seconds of holding the door unlocked.
System Settings – Arming Settings	
Arming Mode	Selects the Arming Mode of the device, depending on the state you want the GSC3574/75 to be in, the options available are: ● Outdoor ● Indoor ● Sleeping ● Custom ● Disarm The default value is "Disarm"
Zone Settings	Defines the zone settings based on the below parameters: ● **Zone Name:** Specifies the Zone name. ● **Zone Type:** Select the Zone type, this can be: Doorbell, open door, infrared, smoke sensor, Gas, Drmagnet, Urgency, and Others. ● **NO/NC:** Defines the door reaction on the selected zone to be either: Normal Open, or Normal Close. ● **Alarm Type:** Defines the alarm type to either, a delay alarm, instant alarm, or alarm in 24H. ● **Enter Delay(s):** defines the Enter delay in seconds, which is the period of time allowed for a person to enter a secured area after disarming the system. The default value is 30 seconds. ● **Exit Delay(s):** Defines Exit delay in seconds, which is the time provided for a person to leave a secured area after arming the system. The default value is 0 seconds. After defining the above values for each zone you can map the Arming Mode Settings for application to one or multiple zones. There are eight zones available (Zone1, Zone2, Zone3, Zone4, Zone5, Zone6, Zone7, and Zone8), and users can activate arming modes according to the specified zone. The available arming modes include Outdoor, Indoor, Sleeping, and Custom.
System Settings – Alarm Settings	
Enable Verification to Cancel Alarms	Enable/disable verification to cancel alarms. When enabled, password verification is required to manually cancel alarms triggered by events (e.g., zone breaches or abnormal sounds). This feature is disabled by default.
Cancel Alarm Password	Configures the verification password for cancelling alarms.
Call Mode	Allows user to select between "Serial Hunting" so call will be made towards all configured SIP Number by order of priority, and Parallel Hunting where all Configured SIP Numbers will receive the call simultaneously.

Order (1-4)	Displays the order of the service.
Account	When set to “Dynamic”, the GSC3574/75 will use the first available Account. User can specify from which account the call can be made for each destination. Default is Dynamic.
SIP Number	Enter the Number to receive the call. User can set up to 4 SIP Numbers.
System Settings – SOS	
Call Mode	Allows user to select between “Serial Hunting” so call will be made towards all configured SIP Number by order of priority, and Parallel Hunting where all Configured SIP Numbers will receive the call simultaneously.
Order (1-4)	Displays the order of the service.
Account	When set to “Dynamic”, the GSC3574/75 will use the first available Account. User can specify from which account the call can be made for each destination. Default is Dynamic.
SIP Number	Enter the Number to receive the call. User can set up to 4 SIP Numbers.
System Settings – Desktop Shortcut Settings	
Desktop Shortcut (3/9)	The user can add up to 9 Desktop dial shortcuts, to Configure a shortcut, Click on “Add”, then define the following parameters: ● **Type:** Selects the type of desktop shortcut call. ● **Name:** Enter the name of the Desktop Dial call. ● **Account:** Selects the account for speed dial. ● **Number:** Enter the number for speed dial.
System Settings – Preferences	
LCD & LED Management	
Enable Missed Call Backlight	If set to “Yes”, LCD backlight will be turned on when there is a missed call on the device. This action requires a reboot to be completed.
Enable Missed Call Indicator	If set to “Yes”, the LED indicator on the upper middle side of the device will light up when there is new missed call on the device.
Enable MWI Indicator	If set to “Yes”, the LED indicator on the upper middle side of the device will light up when there is new voicemail on the device.
Enable Contact Full Indicator	If set to “Yes”, the LED indicator on the upper right corner of the device will light up when the contact storage or message storage is full.
Enable Indicator When LCD is Off	If set to “Yes”, the LED indicator on the upper right corner of the device will light up when the LCD screen is off.
Screen Timeout	Defines the duration of inactivity in minutes after which the LCD backlight turns off. If set to “Never”, the screen will always remain on. The default setting is 3 minutes.
Screensaver Timeout	Specifies the period of inactivity in minutes before the screensaver activates. If set to “Never”, the screensaver will not appear.

	The default setting is 2 minute.
Homepage Setting	Determines the default page shown on the LCD when the device is idle, restarts, or when the “return to desktop” gesture is performed. The available options are: ● **Main Menu Page** ● **Desktop Shortcut Page** (If no shortcuts are configured, the Main Menu Page will be used instead.) The default setting is “Main Menu Page”.
Peripherals Interface Management	
USB Output Current	Configure the USB output current. If the device is powered by PoE, only USB output 0.46A power is supported. If the device is powered by a 12V/1.5A power supply, it can support USB output of 1A current for connecting to external devices for power supply.
System Settings – TR-069	
Enable TR-069	Enables TR-069 feature.
ACS URL	Defines the URL for TR-069 Auto Configuration Servers (ACS).
ACS Username	Defines the ACS username for TR-069.
ACS Password	Defines the ACS password for TR-069.
Enable Periodic Inform	Enables periodic inform. If set to “Yes”, device will send inform packets to the ACS.
Periodic Inform Interval (s)	Sets up the periodic inform interval in seconds to send the inform packets to the ACS.
Connection Request Username	The user name for the ACS to connect to the device. It should match the configuration in the ACS.
Connection Request Password	The password for the ACS to connect to the device. It should match the configuration in the ACS.
Connection Request Port	The port for the request sent from the ACS to the device. It should not be occupied by other protocol used on the device. For example, it cannot be 5060 or 5004 which are already used for SIP protocol.
CPE CA Certificate	Select the CA certificate for server verification.
CPE User Certificate	Select the user certificate to be used for mutual server authentication. If the private key is included, upload it with the user certificate.

System Settings Page Definitions

Maintenance Page Definitions

Maintenance – Upgrade
Upgarde
Firmware

Complete Upgrade	If enabled, all files will be replaced except user data. Disabled by Default
Upload Firmware File to Update	Allows users to load the local firmware to the device to update the firmware. This setting requires a reboot
Firmware Upgrade Mode	Allows users to choose the firmware upgrade method: TFTP, HTTP, HTTPS.
Firmware Server Path	Defines the server path for the firmware server. It could be different from the Config Server Path which is for provisioning.
HTTP/HTTPS Username	Defines the user name for the firmware HTTP/HTTPS server.
HTTP/HTTPS Password	Defines the password for the firmware HTTP/HTTPS server.
Firmware File Prefix	Enables your ITSP to lock firmware updates. Only matching encrypted postfix and(or) suffix, will the firmware be downloaded and flashed into the device.
Firmware File Postfix	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the device.
Firmware Upgrade	Firmware Updates: Click the “Update Detect” button to check whether the firmware in the firmware server has an updated version. If so, update immediately.
Config File	Click to download the device configuration file in .txt format.
Download Device Configuration	Click to download the device configuration file in .txt format.
Upload Device Configuration	Upload configuration file to the device.
Use Grandstream GAPS	It is used to configure the download path and update mode for the configuration file server. If set to “Yes”, 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; If set to “No”, users can manually configure the path and update mode for the configuration file server.
Config Upgrade Mode	Allows users to choose the config upgrade method: TFTP, HTTP or HTTPS.
Config Server Path	Defines the server path for provisioning. It could be different from the Firmware Server Path.
HTTP/HTTPS User Name	The user name for the config HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the config HTTP/HTTPS server.
Config File Prefix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the device.
Config File Postfix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the device.
Authenticate Conf File	Authenticate the configuration file before the device accepts the file.
XML Config File Password	The password for encrypting the XML configuration file using OpenSSL. This is required for the device to decrypt the encrypted XML configuration file.
Provision	

Automatic Upgrade	Set automatic upgrade every intervals/day/week. The device will send request to upgrade automatically according to the setup time.
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent.
Upgrade with Prompt	If set to “Yes”, the device will pop up a prompt after downloading the firmware files to confirm whether start upgrading . Otherwise, the device will automatically start upgrading process.
Allow DHCP Option 43, 160 and 66 Override Server	If set to “Yes”, 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 upgrade mode and server path of the configuration upgrade mode will be reset according to option 160 and 66 sent by the server. If set to “Prefer, fallback when failed”, the device can fallback to use the configured provisioning server under its Firmware and Config server path in case the server from DHCP Option fails.
DHCP Option 120 Override SIP Server	If set to “Yes”, the device will enable DHCP Option 120 from local server to override the SIP Server on the device.
Allow DHCP Option 242 (Avaya IP Phones)	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.
Download and Process All Available Config Files	By default, the device will provision the first available config in the order of 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.xml, cfgMODEL.xml, cfg.xml.
Config Provision	The device will download the configuration files and provision by the configured order.
Enable PNP Feature	Configures whether to enable PNP feature. This function offers automatic configuration. If set to “Yes”, users should set PNP(3CX) Auto Provision to “No” first. Meanwhile, the device will check the local SIP port in Account Settings. If the port is 5060, it would warn the users and set it to 0 automatically.
PNP URL	Configures the PNP file server URL. Users should input transport protocol in URL such as HTTP/HTTPS/TFTP. You could also set the device to be the file server. The format is http://192.168.121.111/pnp. In this case, you have to copy your cfg file to the device /sdcard/pnp directory.
PNP (3CX) Auto Provision	If enabled, the device will send SUBSCRIBE request for automatic assigned URL to the multicast address in LAN when bootup to accomplish automatic configuration of SIP account, It requires 3CX server support.
Advanced Settings	
Send HTTP Basic Authentication by Default	Determine whether to send basic HTTP authentication information to the server by default when using wget to download firmware or config file. If set to “Yes”, send HTTP/HTTPS user name and password no matter the server needs authentication or not. If set to “No”, only send HTTP/HTTPS user name and password when the server needs authentication.
Enable SIP NOTIFY Authentication	Device will challenge NOTIFY with 401 when set to “Yes”.
Enabled Authentication Server Validation	Configures whether to validate the server certificate when downloading the firmware/config file. If set to “Yes”, the device downloads firmware/configuration files only from servers validated by CA certificates.
CA Certificate	Select the CA certificate for server verification.
User Certificate	Select the user certificate to be used for mutual server authentication. If the private key is

	included, upload it with the user certificate.
Factory Reset	Restore to factory default settings. **Note:** Please backup the data to avoid data loss.
Safe Mode	Configures enable/disable safe mode. If enabled, the device will enter safe mode after rebooting, which will help remote troubleshooting when an abnormal situation occurs. Note: Once entering safe mode, only the system applications will be up and running, all widgets and 3rd party apps will be disabled.
Maintenance – System Diagnosis	
Syslog	
Syslog Protocol	Configure sending syslog through UDP or secured SSL/TLS protocol to syslog server.
Syslog Protocol	The IP address or URL for the System log server.
Syslog Level	Selects the level of logging for syslog. There are 4 levels: DEBUG, INFO, WARNING and ERROR. Please refer to the user manual for more details.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages.
Syslog Keyword Filter	Only send the syslog with keyword. Multiple keywords are separated by comma. E.g.: set the filter keyword to “SIP” to filter SIP log.
Logcat	
Clear Log	Click “CLEAR” button to delete the logs saved in the device.
Log Tag	Specifies the log tag to filter the log.
Log Priority	Selects the log priority. The log priority options are: Verbose/Debug/Info/Warn/Error/Fatal/Silent(suppress all output) The default value is Verbose
Debug	
One-click Debugging	Capture the checked items in the debugging list. If “Capture trace” is selected, click “Start” to start capture and click “Stop” to end. Otherwise, click “Capture” to download. All log files will be generated in a TAR package and the trace file as PCAP.
Debug Info Menu	Display a list of info items that can be debugged. Currently system logs, info log, capture trace, tombstones, ANR log are supported. The captured data can be viewed in “Debug information list”. By default all items are selected.
Debug Info List	Select an existing debug file and click the “Delete” button on the right to delete the file.
View Debug Info	Click “List” to view the existing debugging info package or trace file. The files are listed in chronological order. Click the file to download to computer.
Enable Core Dump Generation	Configures whether to generate and save the core dump file when the program crashes. The default setting is “No”.
Core Dump List	Select the existing core dump file in the drop-down box. Users could click the “Delete” button on the right to delete the file.

View Core Dump	Click “List” to view all existing core dump files. The files are listed in chronological order. Click the file to download to computer.
Record	Click “Start” to capture audio data and “Stop” to end. The audio record data is used to help troubleshoot audio issues. You can record up to 1 minute audio data.
Recording List	Choose the existing audio file. Click the “Delete” button on the right to delete this file.
View Recording	Click on the “List” button to view the audio records. The files are listed in chronological order. Click the file to download to computer. Note: The audio data file will be saved under FileManager -> Internal Storage -> Recfiles folder. The record files can also be deleted from this folder.
Screenshot	Click the screenshot to capture and save the current screen image.
Screenshot List	Select the existing screenshot file and click the “Delete” button on the right to delete the file.
View Screenshot	Click the “List” button to view the existing screenshot file. Click the file name to open or save the screenshot to the computer.
Traceroute	
Target Host	The IP address or URL for the Target Host of the Traceroute.
Ping	
Target Host	The IP address or URL for the Target Host of the Ping.
NSLookup	
Host Name	Enter a host name to look up the corresponding IP address. This feature can also do reverse name lookup and find the host name for the entered IP address.
Maintenance – Event Notification	
Bootup Completed ● **Bootup Completed** ● **Incoming Call** ● **Outgoing Call** ● **Missed Call** ● **Connected** ● **Disconnected** ● **DND On** ● **DND Off** ● **On Hold** ● **Unhold** ● **Log On** ● **Log Off** ● **Register** ● **Unregister**	Set the URL for events on device web GUI. 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. Here is an example: 192.168.40.207?mac=$mac&local=$local 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.
CA Certificate	Event Notification CA file (ca.crt) required by the Event Notification server for authentication purposes.
User Certificate	Selects the user certificate to be used for mutual server authentication.

Maintenance Page Definitions

Application Page Definitions

App – Contacts	
General Settings	
Sort Phonebook By	Sort phonebook based on the selection of first name or last name.
Default Contacts Tab	Configures the default display Contacts page after clicking Contacts application. If set to “Default”, display all contacts page of the device.
Import/Export Contacts	
Import	
Clear The Old List	If set to “Yes”, the device will clear the old list before importing the new file.
Clear Old History Mode	If set to “Clear all”, the device will delete all previous records before importing the new records. If set to “Keep Local Contacts”, the manually added local contacts will not be deleted when importing new records.
Replace Duplicate Items	If set to “Yes”, the device will replace any duplicate items in the device with the item in the new file.
Replace Duplicate Entries Mode	If set to “Replace by name”, records of the same name will be replaced automatically when importing new records. If set to “Replace by number”, records of the same number will be replaced automatically when importing new records.
File Encoding	Selects the file encoding for import/export.
File Type	Selects the file type for import/export.
Import Local files	Imports the contacts list in XML format.
Export	
File Encoding	Selects the file encoding for import/export.
File Type	Selects the file type for import/export.
Export	Exports the saved contacts.
Download Contacts	
Clear The Old List	If set to “Yes”, the device will clear the old list before downloading the new file.
Clear Old History Mode	If set to “Clear all”, the device will delete all previous records before importing the new records. If set to “Keep Local Contacts”, the manually added local contacts will not be deleted when importing new records.
Replace Duplicate Items	If enabled, the device will replace any duplicate items in the device with the item in the new file. Enabled by Default

Replace Duplicate Entries Mode	If set to “Replace by name”, records of the same name will be replaced automatically when importing new records. If set to “Replace by number”, records of the same number will be replaced automatically when importing new records.
Download Mode	Selects the file download mode for the download server. The options are: Download through TFTP, HTTP, or HTTPS Disabled by Default.
File Encoding	Selects the file encoding for download.
Download Server	The URL/IP address of the download server.
HTTP/HTTPS User Name	The user name for the config HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the config HTTP/HTTPS server.
Automatic Download Interval	The interval at which the phonebook will be downloaded from the download server (in hours).
Download Now	This allows the user to download the data file from the download server to the device. Press the “Download” button to trigger the file download.
App – LDAP Phonebook	
Connection Mode	Configures to use LDAP or LDAPS to connect.
Server Address	LDAP server address, the value can be IP or Domain name.
Port	LDAP server port.
Base DN	Searching root directory of the server.
User Name	User name to use when querying LDAP server.
Password	Password to use when querying LDAP server.
LDAP Name Attributes	This setting specifies the “name” attributes of each record which are returned in the LDAP search result. The setting allows the users to configure multiple space separated name attributes. Example: gn cn sn description
LDAP Number Attributes	Specifies the “number” attributes of each record which are returned in the LDAP search result. This field allows users to configure multiple space separated number attributes.Example: telephoneNumber telephoneNumber Mobile
LDAP Mail Attributes	Specifies the “mail“ attributes of each record which are returned in the LDAP search result. This field allows users to configure multiple space separated E-Mail attributes.Example: mail mail mailBox
LDAP Name Filter	Configures the filter used for name lookups. Examples: (|(cn=%)(sn=%)) returns all records which has the “cn“ or “sn“ field containing with the entered filter value;(!(sn=%)) returns all the records which do not have the “sn“ field containing with the entered filter value;(&(cn=%)(telephoneNumber=*)) returns all the records with the “cn“ field containing with the entered filter value and “telephoneNumber“ field set.
LDAP Number Filter	Configures the filter used for number lookups. Examples:(|(telephoneNumber=%)(Mobile=%) returns all records which has the “telephoneNumber“ or “Mobile“ field containing with the

	entered filter value;(&(telephoneNumber=%) (cn=*)) returns all the records with the “telephoneNumber“ field containing with the entered filter value and “cn“ field set.
LDAP Mail Filter	Configures the filter used for E-Mail lookups.Examples:(|(mail=%)(mailBox=%)) returns all records which has the “mail“ or “mailBox“ field containing with the entered filter value;(!(mail=%)) returns all the records which do not have the “mail“ field containing with the entered filter value;(&(mail=%) (cn=*)) returns all the records with the “mail“ field containing with the entered filter value and “cn“ field set.
Search Field Filter	Configures filters used upon LDAP search. The default settings is “All Filter”.
LDAP Displaying Name Attributes	Name attributes displayed in the main interface. Example: cn sn telephoneNumber.
Max Hits	The maximum query results.
Search Timeout (s)	Configures the search timeout value. If exceeds the value and the server does not response, then stop searching.
LDAP Lookup When Dialing	If set to “Yes”, the device will do LDAP search at the beginning of the outgoing call. The default setting is “Disable”.
Search LDAP for Incoming Call	If set to “Yes”, the device will do LDAP search when there is an incoming call. The default setting is “Disable”.
LDAP Dialing Default Account	Configures the default account used when dialing LDAP contact.
App – Account Sharing	
General Settings	
Enable Account Sharing	Select whether to enable Account Sharing.
Role in Account Sharing	Select the role that the current device will play in the network, the supported roles are : ● Host Device ● Guest Device the guest device role does not need to register an account on IPPBX, and can make calls in and out of the network through the account set by the host device role,
Group Name	Set the group name, in the host-guest mode, devices with the same group name can discover each other. Note: This item is mandatory if using Account Sharing. The verification format is domain type.
Group Password	In the host-guest mode, by setting the group password, the guest device with the same group password as the host device can successfully register an account on the host device. Note: This item is mandatory if using Account Sharing.
SIP Server Port	Set the SIP service port in Account Sharing, where 0 indicates using the random port, ranging from 0 to 65535.
Account Settings	
Account	For the host device role, this setting determines which host device account will be used as the guest device outgoing and incoming account for calls outside the Account Sharing. For the guest device role, this setting determines which account the guest device will use to register on the host device.

Ringing Tone Settings	
Sync Ringing In Group	Set whether to enable synchronization of all successfully registered guest device ringtones within the group.
Discovered Guest Device List	Displays the list of discovered guest devices

Application Page Definitions

NAT Settings

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

- **STUN Server**

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

- **Use Random Ports**

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

- **NAT Traversal**

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

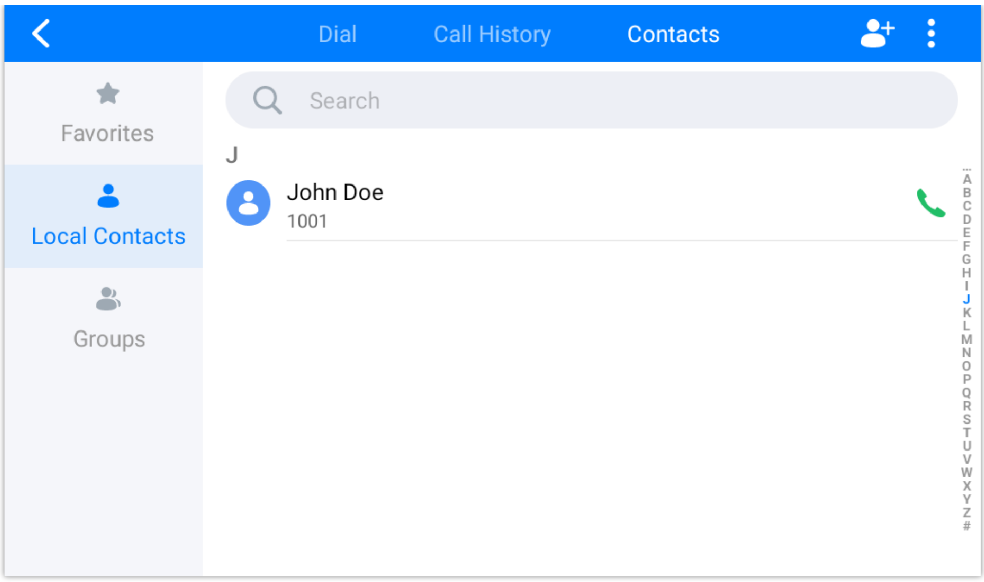
Contacts – Local Contacts

From the LCD settings, the user can create and add new contacts manually under **Call** → **Contacts**:

1. Click the icon to add a new contact

2. When Adding a new contact, the following fields can be defined:

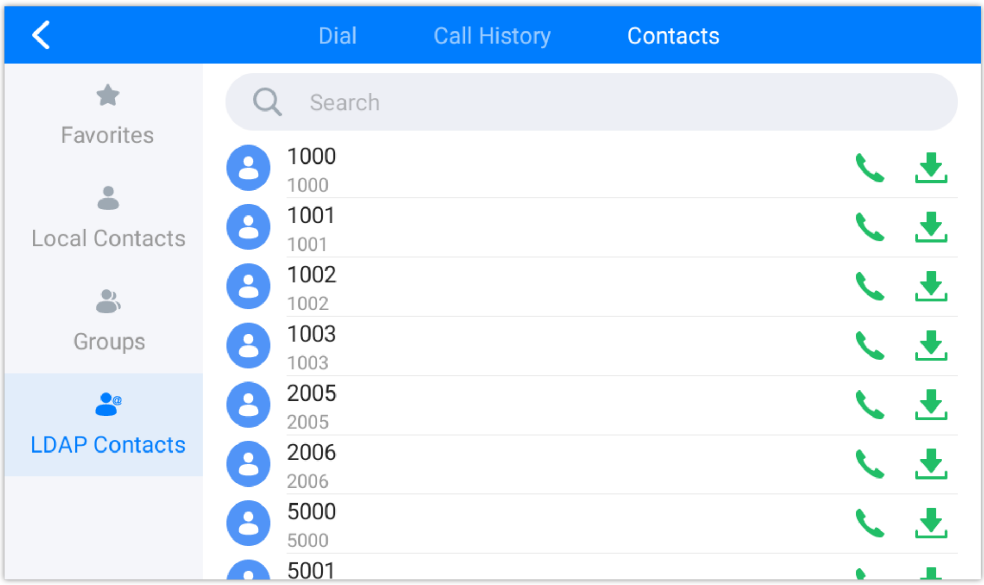
- **First Name**
- **Last Name**
- **Mobile, Home,** and **Work phone numbers**
- **Groups**
- **Ringtone**
- **Company**
- **Department**
- **Work**



Local Contacts

Contacts – LDAP Contacts

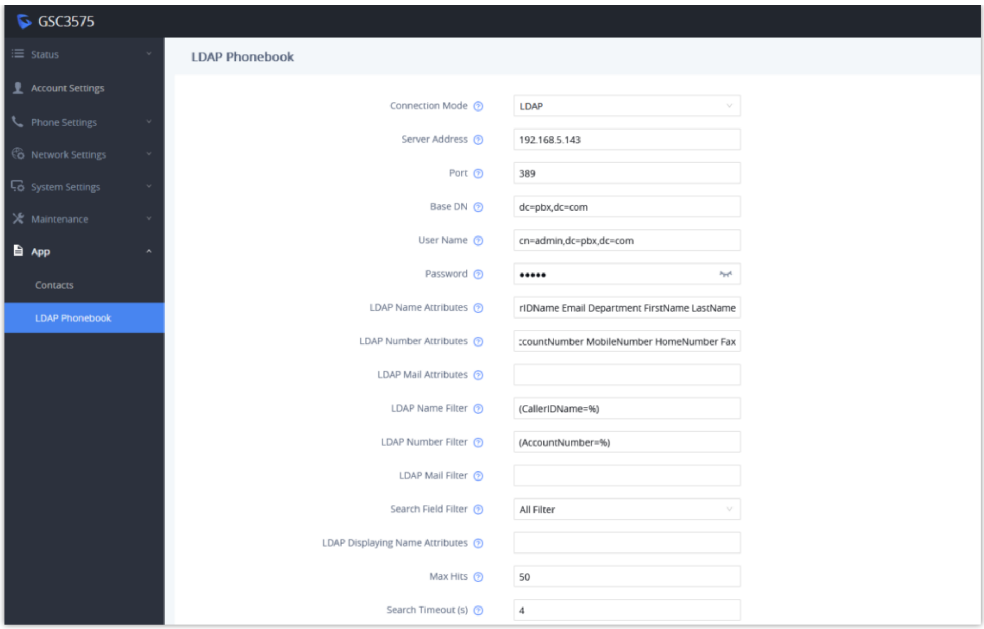
To view the imported LDAP Contacts on the LCD screen, From the Home screen, go to **Call** → **Contacts**, the list of imported LDAP Contacts will be displayed:



LDAP Contacts

The users can import contact information from the LDAP server. To do that, on the WebUI, go to **App** → **LDAP Phonebook**, then define the following fields for configuration (below is an example using the UCM63xx series) :

- **Server Address**: The IP address or domain name of the UCM63xx device.
- **Base DN**: dc=example (the same as the server base DN or a subset of the server base DN).
- **Username**: Username of the LDAP server.
- **Password**: The password of the LDAP server.
- **LDAP Name Attributes**: CallerIDName Email Department FirstName LastName
- **LDAP Number Attributes**: AccountNumber MobileNumber HomeNumber Fax
- **LDAP Number Filter**: (AccountNumber=%)
- **LDAP Name Filter**: (CallerIDName=%)
- **LDAP Display Name**: AccountNumber CallerIDName
- **LDAP Version**: If this option exists, please choose “version 3”.
- **Port**: 389



LDAP Phonebook Configuration

Saving Configuration Changes

After users make changes to the configuration, press the "Save" button to save the changes, followed by "Apply" in the top right corner of the screen, to apply the changes. Some configuration parameters with the icon ⓘ next to them will require the unit to be rebooted to take effect.

Rebooting The GSC3574/75

- **From The Web UI**

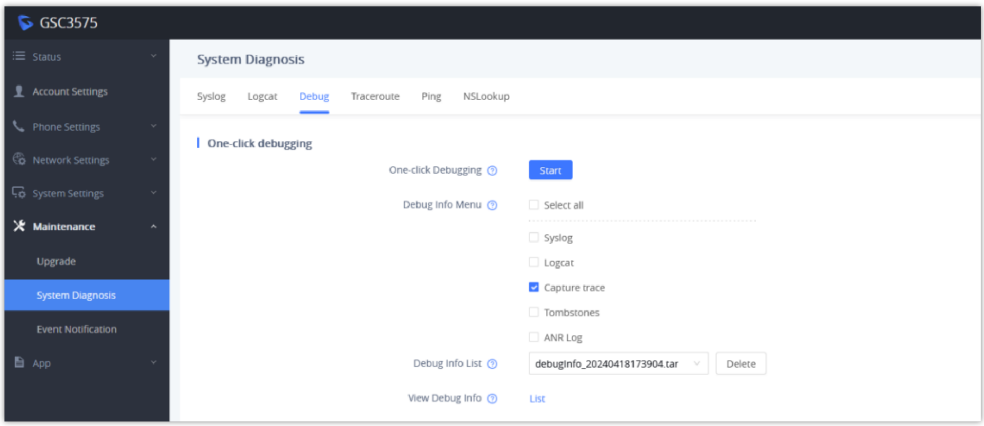
Press the "Reboot" button in the top right corner of the web GUI page to reboot the GSC3574/75 remotely. The web browser will then display a reboot message. Wait for about 1 minute to log in again.

- **From the LCD Settings**

Access **Settings** → **Basics**, then press the option "**Reboot the Device.**"

Packet Capture

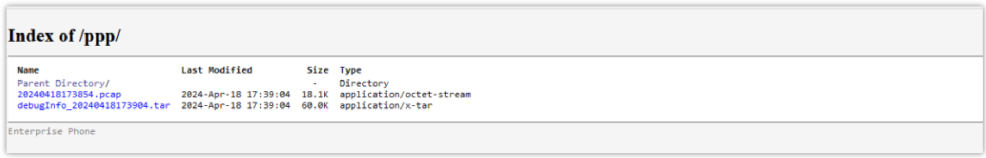
GSC3574/75 is embedded with a packet capture function. The related options are under **Maintenance→ System diagnosis → One-click debugging**, make sure you select only capture trace for a more narrow and accurate capture.



Packet Capture

When the capture configuration is set, press the **Start** button to start packet capture. Press the Stop button to end the capture.

Press the List button to display the list of captured files, The capture file is in .pcap format.

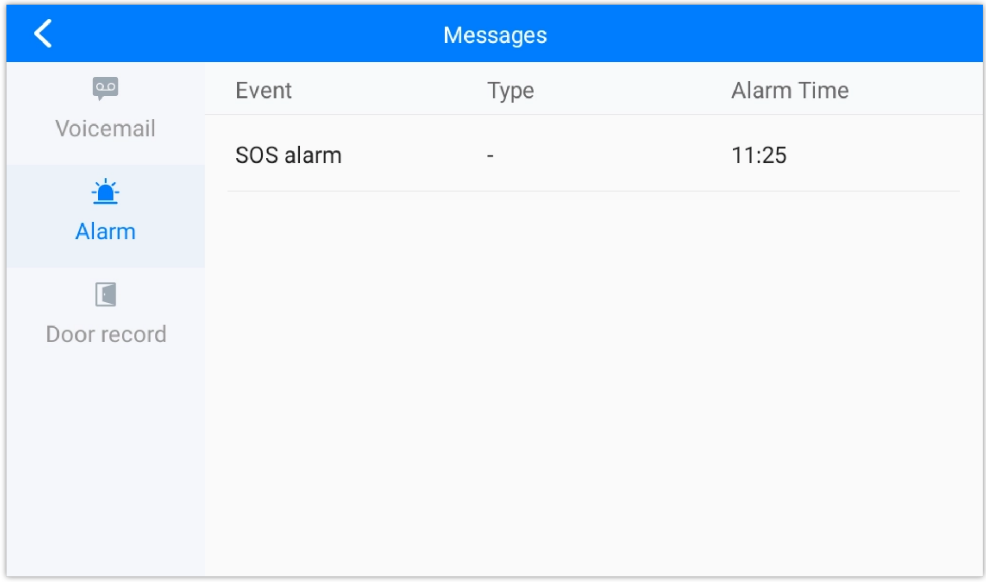


Captured PCAP file

ALARMS

The alarms tab on the LCD screen allows the users to view triggered alerts of all types, including SOS calls, Door opening actions, alarm triggering actions…

To view the alarm messages, from the home screen, go to **Messages → Alarm Messages**



ALARMS

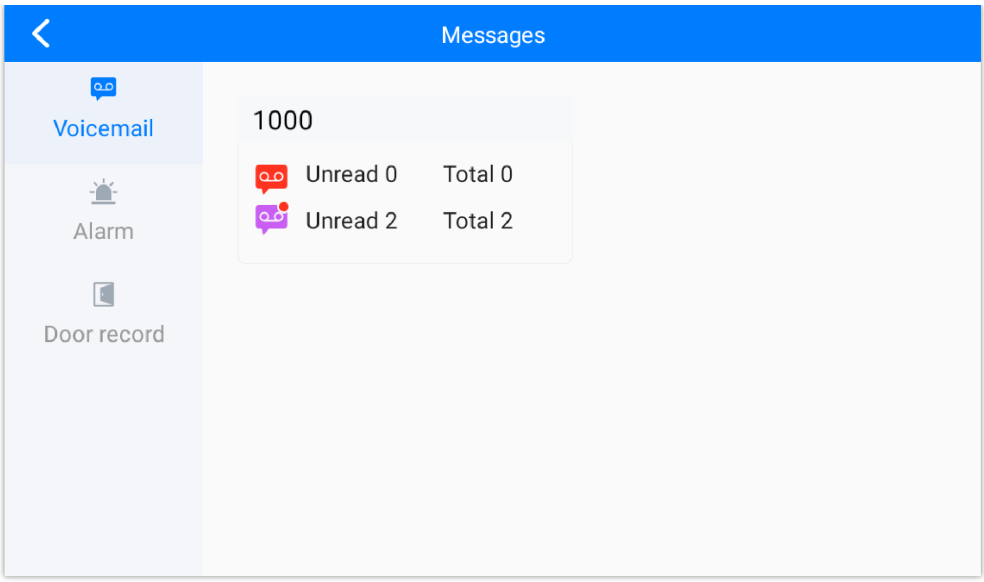
VOICEMAIL

To access voicemail messages received on the SIP account configured on your GSC3574/75 :

1. On your Home screen, click the icon

.

2. Select your account's voicemail, and provide the voicemail access password, to view the received voicemails.

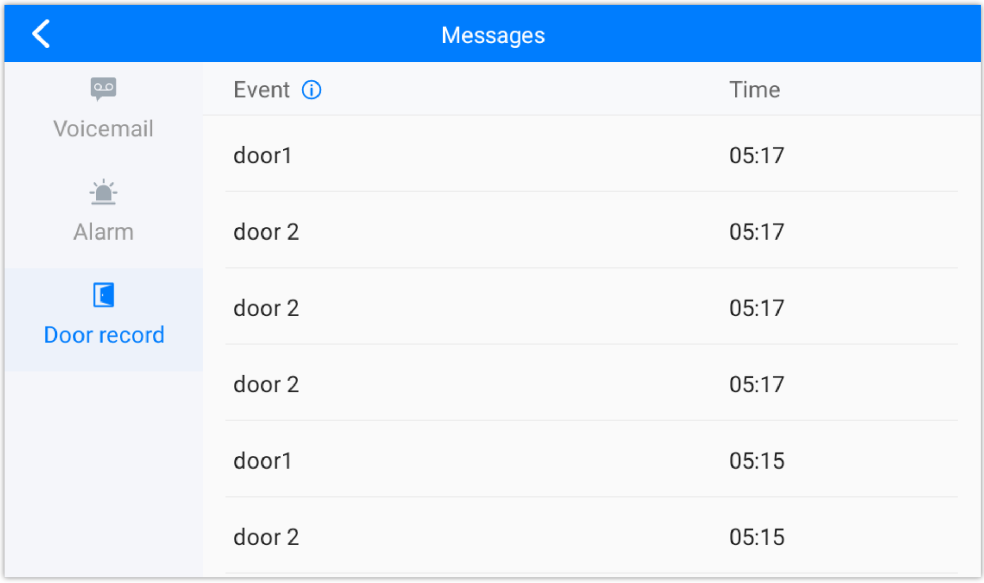


DOOR RECORD

The Door Record allows users to view a log of door opening actions for doors controlled by the GSC3574/75 control station and doors controlled by the connected door systems, such as the GDS device.

This feature provides a time-stamped list of door open events, showing when and which door was opened. To access the door record, please follow the steps below:

1. Open the **Voicemail/Messages** app from the home screen.
2. Tap the **Door Record** tab.
3. Review the list of recorded door openings. Each entry includes:
   - **Time**
   - **Door Name**

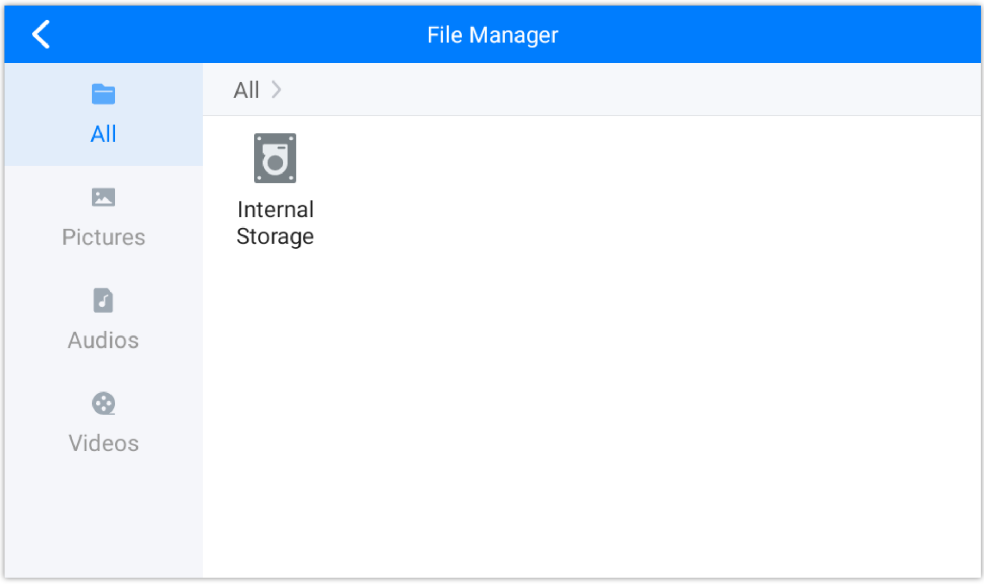


Notes:

- Door open events made during a call by sending a password via DTMF are not included.
- This log does not record door open events that are triggered from other devices, such as another IP phone.
- This feature only applies to doors actively monitored by the GSC3574/75.

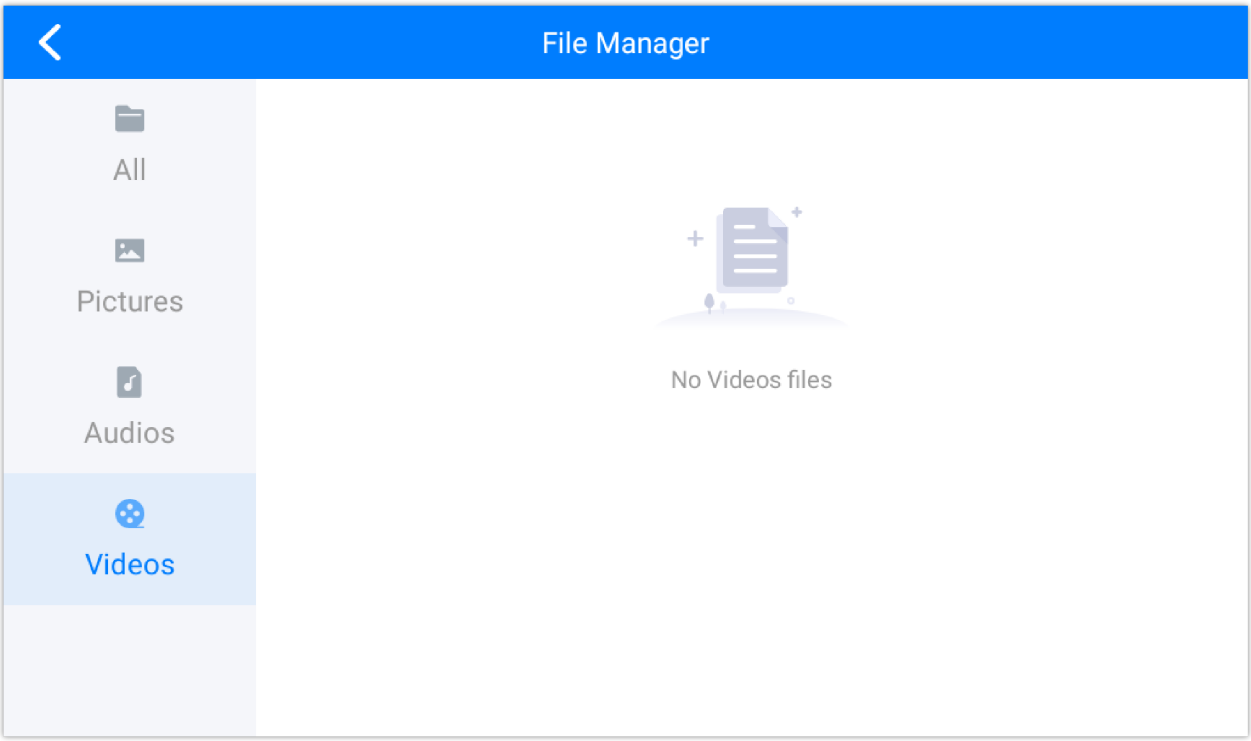
FILE MANAGER

The file manager is an embedded application within the GSC3574/75 device that allows users to view the content of their storage drives, for either internal or external drives. To access the file manager, on your home screen, click the icon , and you will be prompted with the following tab:



FILE MANAGER

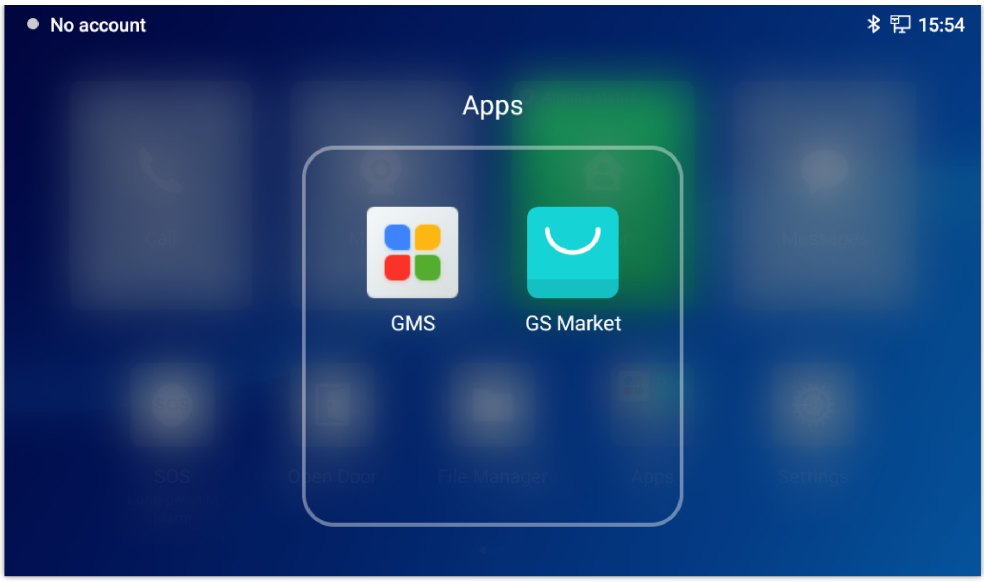
Click the Pictures tab, Audios tab, or Videos tab to display media from different folders and different storage drives



Video Lists

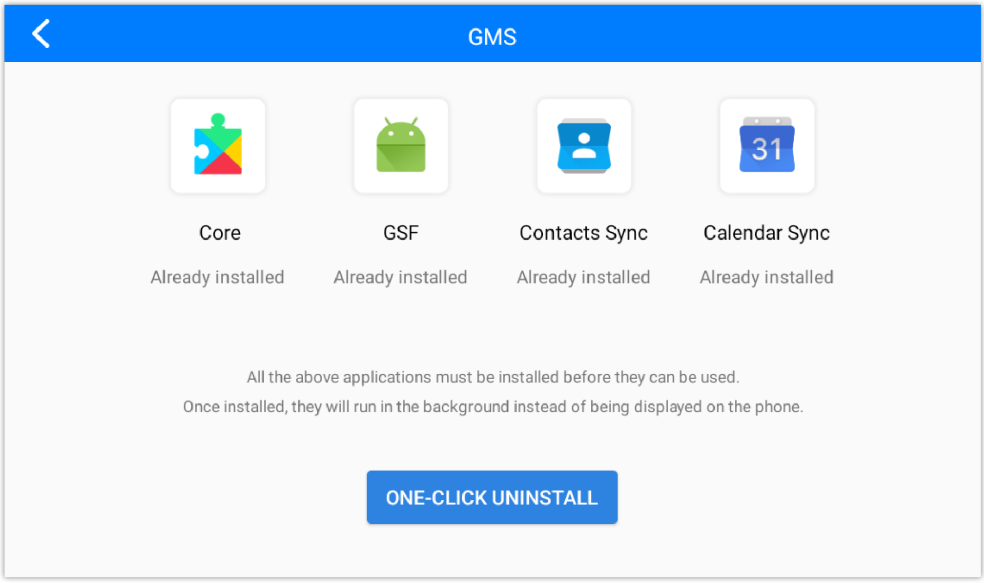
GS MARKET

The GSC3570 supports an extensive number of 3rd party Android applications that can be installed from the Google Play Store. To start installing applications from the store, the GMS application instance needs to be installed initially



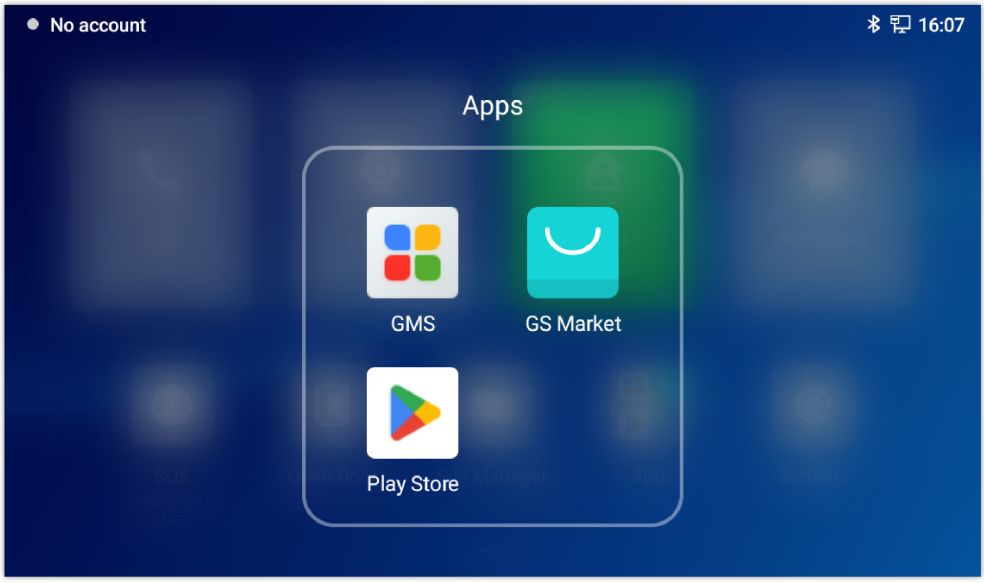
GS MARKET

Once installed with all its instances as shown below, the user will be able to install Google Play Store from the GS Market and start downloading applications.



GMS applications installed

The user will be able to view the Google Play icon after the software is installed



Play Store Installed

UPGRADING AND PROVISIONING

The GSC3574/75 can be upgraded via TFTP / HTTP / HTTPS by configuring the URL/IP Address for the TFTP / HTTP / HTTPS server and selecting a download method. Configure a valid URL for TFTP or HTTP/HTTPS; the server's name can be a FQDN or an IP address.

Examples of valid URLs:

- firmware.grandstream.com/BETA
- fw.mycompany.com

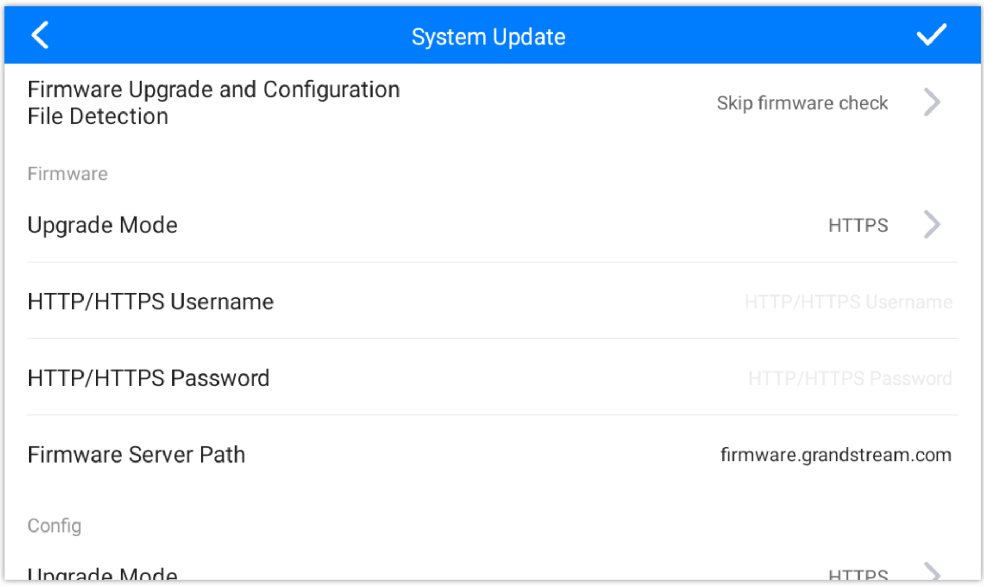
There are two ways to set up a software upgrade server: The LCD Menu or the Web Configuration Interface.

Upgrade via LCD Menu

Follow the steps below to upgrade the GSC3574/75 automatically using the configuration server path :

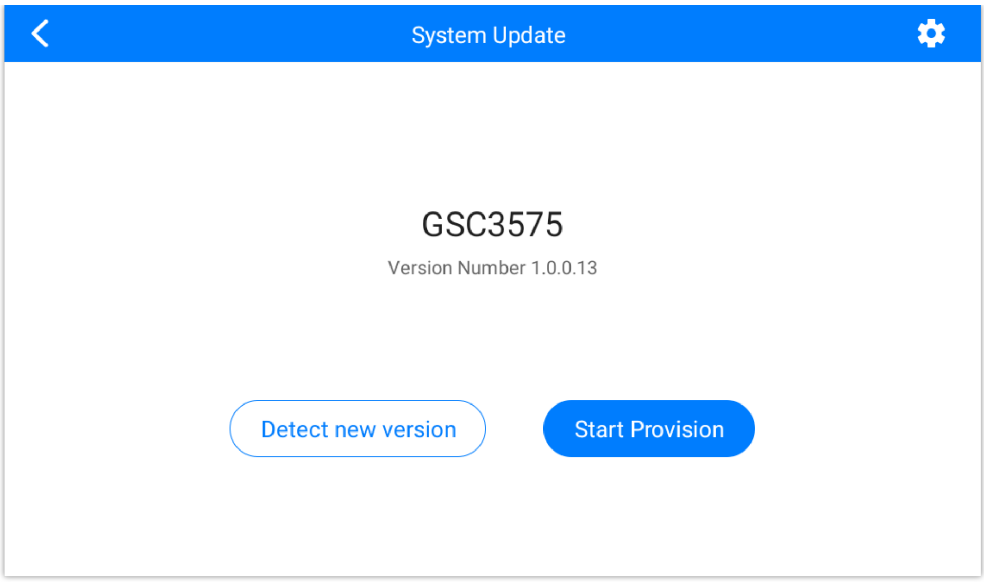
- Navigate to **Settings → Advanced → System Updates.**
- If not already configured, click the icon

  to define the firmware upgrade server path and protocol.



Define Firmware Server Path

- After the path is configured, click on "Detect new version" to automatically fetch a new firmware file from the provisioning server defined
- If the firmware file is detected, click on "**Start Provision**" to install the new firmware



LCD upgrade

Upgrade via Web GUI

Open a web browser on your PC and enter the IP address of the GSC3574/75. Then, log in with the administrator username and password. Go to the Maintenance → Upgrade → Firmware page, enter the IP address or the FQDN for the upgrade server in the "Firmware Server Path" field, and choose to upgrade via TFTP or HTTP/HTTPS. Update the change by clicking the "Save and Apply" button. Then, "Reboot" or power cycle the GSC3574/75 to update the new firmware.

When upgrading starts, the screen will show the upgrading progress. When done you will see the GSC3574/75 restart again. Please do not interrupt or power cycle the GSC3574/75 when the upgrading process is on.

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

For more information on the firmware upgrade methods, please check the Guide:

- **Firmware Upgrade Guide**

No Local TFTP/HTTP/HTTPS Servers

For users who would like to use remote upgrading without a local TFTP/HTTP/HTTPS server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for their GSC3574/75 via this server. Please refer to the webpage:

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

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

- http://www.solarwinds.com/products/freetools/free_tftp_server.aspx
- http://tftpd32.jounin.net/.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the GSC3574/75 to the same LAN segment.
3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade.
4. Start the TFTP server and configure the TFTP server in the GSC3574/75's web configuration interface.
5. Configure the Firmware Server Path to the IP address of the PC.
6. Update the changes and reboot the GSC3574/75.

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

Configuration File Download

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

A configuration parameter is associated with each field in the web configuration page. A parameter consists of a Capital letter P and 2 to 5-digit numbers. i.e., P36 is associated with the "SIP server" in the **Web GUI → Account Settings →Account 1 → General Settings**, or an alias. For a detailed parameter list, please refer to the corresponding configuration template.

When the GSC3574/75 boots up or reboots, it will issue a request to download a configuration file named "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the GSC3574/75, i.e., "cfgc074ad0102ab.xml". If the download of "cfgxxxxxxxxxxxx.xml" file is not successful, the GSC3574/75 will issue a request to download a specific model configuration file "cfg<model>.xml", where <model> is the GSC3574/75 model, i.e., "cfggsc3574.xml" for the GSC3574, "cfggsc3575.xml" for the GSC3575. If this file is not available, the GSC3574/75 will issue a request to download the generic "cfg.xml" file. The configuration file name should be in lowercase letters.

For more details on XML provisioning, please refer to:

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

No Touch Provisioning

After the GSC3574/75 sends the config file request to the provisioning server via HTTP/HTTPS. If the provisioning server responds "401 Unauthorized" asking for authentication, the GSC3574/75's LCD will prompt a window for the user to enter the username and password. Once the correct username and password are entered, the GSC3574/75 will send the config file request again with authentication. Then the GSC3574/75 will receive the config file to download and get provisioned automatically.

Besides manually entering the username and password in the LCD prompt, users can save the login credentials for the provisioning process as well. The username and password configuration are under GSC3574/75's web UI → Maintenance → Upgrade and provisioning page: "HTTP/HTTPS Username" and "HTTP/HTTPS Password". If the saved username and password are correct, the login window will be skipped. Otherwise, a login window will pop up to prompt users to enter the correct username and password again.

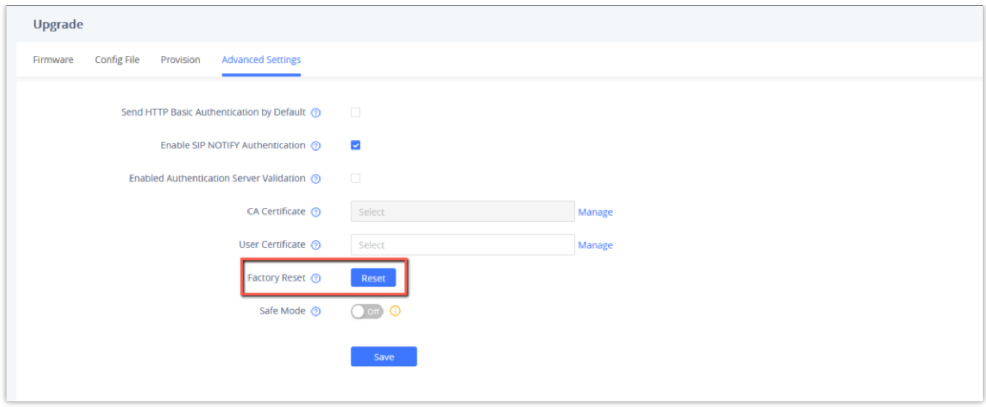
RESTORE FACTORY DEFAULT SETTINGS

> **Warning**
>
> Restoring the Factory Default Settings will delete all configuration information on the GSC3574/75. Please backup or print all the settings before you restore to the factory default settings. Grandstream is not responsible for restoring lost parameters and cannot connect your device to your VoIP service provider.

There are two methods to perform a factory reset on the GSC3574/75 IP Intercom series which are described below.

Restore to Factory using Web GUI

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

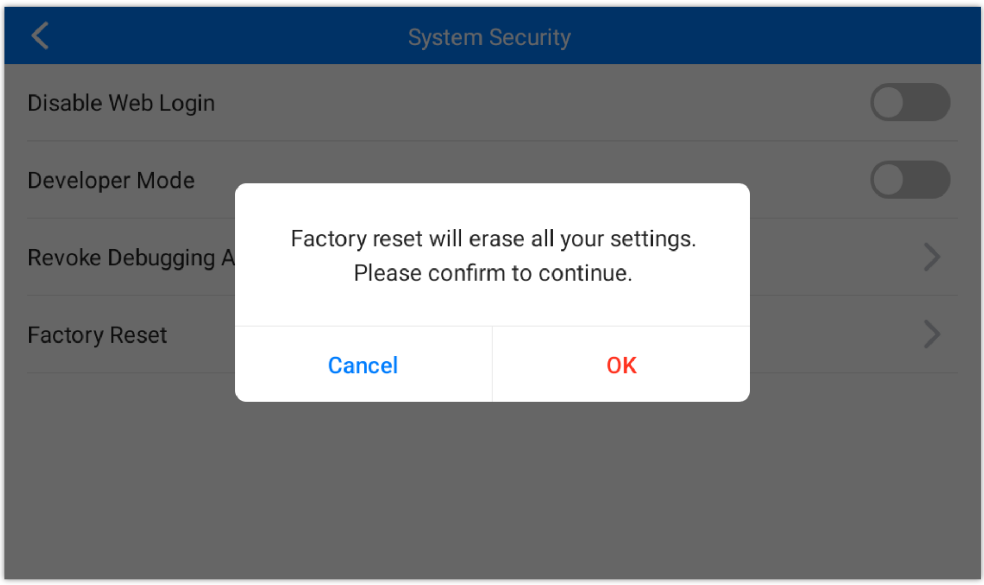


Factory Reset from web GUI

Restore to factory using LCD menu

Please follow the instructions below to reset the GSC3574/75:

- Press the MENU button, navigate to Settings Menu, then click **System Security** → **Factory Reset**.



Factory Reset from LCD

CHANGE LOG

This section documents significant changes from earlier versions of the user manual for GSC3574/75. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.1.13

- Added support for the door opening record. [Door Record]
- Added support to switch video stream. [Default Video Stream]
- Added automatic update of the thumbnail in the Monitor app. [Automatic Thumbnail Update]
- Added video resolution display in the right corner of the live stream in the Monitor application. [Live Stream Video Resolution Display]
- Added thumbnail support for SIP type in the Monitor application. [Automatic Thumbnail Update]
- Added support for homepage configuration. [Homepage Setting][Gesture Guide]
- Added support to cancel the alarm by password. [Enable Verification to Cancel Alarms][Cancel Alarm Password]
- Added support for one-way call function buttons. [Call Function Buttons]
- Added "Call Function Button Display Timeout (s)" under the Call Settings page. [Call Function Button Display Timeout (s)]
- Synchronized the name of Desktop Shortcut Settings in the web UI. [Desktop Shortcut Settings]

- Added support to configure the Screensaver Timeout in the web UI. [Screensaver Timeout]
- Added support for OpenVPN® failover. [OpenVPN® Server Secondary Address][OpenVPN® Secondary Port][Randomly Select Server]
- Updated CPE version to 1.0.4.144. [CPE Version]

Firmware Version 1.0.1.7

- This is the initial version for GSC3574/75.
