Grandstream Networks, Inc.

GXV3370

IP Multimedia Phone for Android^{TM}

Administration Guide

COPYRIGHT

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

https://www.grandstream.com/support

CAUTION

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

WARNING

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

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

The device complies with FCC radiation exposure limits set forth an uncontrolled environment and it also complies with Part 15 of the FCC RF Rules. This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and consider removing the no-collocation statement.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Caution

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

CE DECLARATION OF CONFORMITY

This transmitter complies with the essential requirements and provisions of directives 2014/53/EU, 2014/30/EU, 2015/35/EU, and subsequent amendments, according to standards
ETSI EN 300 328 V2.1.1 (2016-11); EN 301 893 V2.1.1 (2017-05)
ETSI EN 301 489-1 V2.1.1 (2017-02); ETSI EN 301 489-17 V3.1.1 (2017-02)
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013
EN 62311: 2008; EN62479: 2010

CE

Manufacturer:

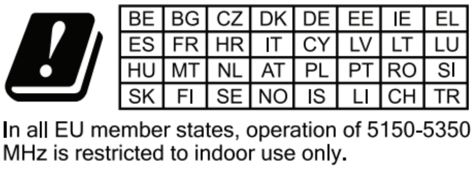
Grandstream Networks, Inc.
126 Brookline Ave, 3rd Floor Boston, MA 02215, USA

EUT Feature				
Tx/Rx Frequency Range	2402~2480 MHz	2402~2480 MHz	2412~2472 MHz	5150~5250 MHz 5250~5350 MHz 5470~5725 MHz
Number of Channels	79	40 (37 hopping + 3 advertising channels)	13	UNII Band I: 802.11a/n-HT20-VHT20: 4 channels 802.11n-HT40: 2 channels UNII Band II: 802.11a/n-HT20: 4 channels 802.11n-HT40: 2 channels UNII Band III: 802.11a/n-HT20: 11 channels 802.11n-HT40: 5 channels
Carrier Frequency of Each Channel	f=2402+k MHz (k=0,1,2….,78)	f=2402+k MHz (k=0,2,4…,39)	-	-
Antenna Type/Gain	Internal PCB Antenna / gain 3 dBi	Internal PCB Antenna / gain 3 dBi	Internal PCB Antenna / gain 3 dBi	Internal PCB Antenna / gain 4 dBi
Type of Modulation	Bluetooth BR 1Mbps: GFSK Bluetooth EDR 2Mbps: π/4-DQPSK Bluetooth EDR 3Mbps: 8DPSK	Bluetooth LE: GFSK	802.11b: DSSS (DBPSK / DQPSK / CCK) 802.11g/n: OFDM (BPSK / QPSK / 16QAM / 64 QAM)	802.11a/n: OFDM (BPSK / QPSK / 16QAM / 64QAM)
Operation temperature	0 °C ~ +40 °C			
Storage temperature	-10 °C ~ +60 °C			
Humidity	10 ~ 90% non-condensing			
Domestic use	Industrial use Class B			

Caution: Exposure to Radio Frequency Radiation

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

CE Authentication



BE	BG	CZ	DK	DE	EE	IE	EL
ES	FR	HR	IT	CY	LV	LT	LU
HU	MT	NL	AT	PL	PT	RO	SI
SK	FI	SE	NO	IS	LI	CH	TR

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

Hereby, Grandstream Networks, Inc. declares that the radio equipment GXV3370 is in compliance with Directive 2014/53/EU.
The full text of the EU declaration of conformity is available at the following internet address:
https://www.grandstream.com/support/resources/

GNU GPL INFORMATION

GXV3370 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:
https://www.grandstream.com/sites/default/files/Resources/gxv3370_gpl.zip

Table of Contents

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes how to configure the GXV3370 via phone's LCD menu and web UI menu to fully manipulate phone's features. The intended audiences of this document are VoIP administrators. To learn the basic functions of GXV3370, please visit https://www.grandstream.com/support to download the latest "GXV3370 User Guide".

This guide covers following topics:

- Product Overview
- Getting Started
- GXV3370 LCD Settings
- GXV3370 Web GUI Settings
- Upgrading and provisioning
- Restore factory default settings
- Safe Mode
- SDK Framework Service
- Experiencing the GXV3370 applications

CHANGE LOG

This section documents significant changes from previous versions of administration guide for GXV3370. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.3.36

- Added P22038 to restrict Wi-Fi settings on web UI. [Network Settings/Wi-Fi Settings]
- Supported GS Affinity. [Network Settings/Affinity Settings]

Firmware Version 1.0.3.30

- Added “Maximum Number of SIP Request Retries” option when DNS mode is set to SRV. [Account/General Settings]
- Added “Failback Expiration” settings when DNS SRV Failover Mode is Failback. [Account/General Settings]
- Added maximum transmission unit (MTU) settings. [Network Settings/Advanced Network Settings]
- Added "Screen Timeout" and "Screensaver Timeout" settings. [System Settings/Preferences]
- Added the option to upload GUI customization file from web UI. [Maintenance/Upgrade]
- Added Separate Ethernet and Wi-Fi traffic setting. [Network Settings/Advanced Network Settings]

Firmware Version 1.0.3.28

- Added 'Keep Associated Account' option under Contacts page. [Keep Associated Account][Keep Associated Account]

Firmware Version 1.0.3.27

- Improved Special Features settings layout on web UI. [Special Features]
- Added a “Mute” option to account ring tone list. [Account Ring Tone]
- Supported "Do not prompt Missed calls" for Ring Group missed call. [Call Log]

Firmware Version 1.0.3.25

- Added support for $variable in provisioning link (such as $MAC or $PN). [Firmware Server Path][Config Server Path]
- Added “Start provision” button to trigger the device to fetch configuration file from server on both web UI and LCD. [Start Provision]
- Differentiated rejected call logs from missed calls. [Rejected Call Notification]
- Added Lagos, Nigeria GMT+1:00 to time zone list. [Time Zone]

- Added file format verification when uploading OpenVPN® certificate files. [OpenVPN® CA][OpenVPN® Client Certificate][OpenVPN® Client Key]
- Added file format verification when uploading configuration files. [Upload Device Configuration]
- Added Call Function Button Display Timeout (s). [Call Function Button Display Timeout (s)]
- Added Self-defined time zone under web UI Time Settings. [Self-defined Time Zone]
- Supported Handsfree TX Gain settings. [Handsfree TX Gain]
- Added more Handset TX Gain (dB) options. [Handset TX Gain]
- Supported voice monitoring VQ RTCP-XR session report. [VQ RTCP-XR Collector Name][VQ RTCP-XR Collector Address][VQ RTCP-XR Collector Port]
- Supported web UI control list. [Web Access Control][Web Access Control List]
- Supported LCD to be turned on when BLF/SCA status updated. [Enable LCD Turn on Automatically when BLF/SCA status changes]
- Supported send URL via programmable key. [Send URL]

Firmware Version 1.0.3.19

- Implemented Slovak language to system. [GXV3370 Technical Specifications]
- Added reset button for each account to restore to default values.

Firmware Version 1.0.3.9

- Support Enable/Disable Call Waiting from each account. [Enable Call Waiting]
- Support Enable/Disable preview in Value-added Service. [Enable Preview]
- Enabled Offhook Auto Dial to be configured with special characters as ‘#’ or ‘*’ [Offhook Auto Dial]

Firmware Version 1.0.3.8

- Added Berlin, Dublin to Time Zone list. [Time Zone]
- Supported letters in dial plan, such as {\p\a\r\k\*x+}. [Dial Plan]
- Added display condition for DTMF button display during a call. [Display Condition]
- Supported each account can disable video call separately. [Enable Video Call]
- Added door button control in the incoming call interface. [Display Open Door Button]
- Supported volume adjustment on web UI. [Media volume]
- Supported callee ID display feature. [Callee ID Display]

Firmware Version 1.0.3.3

- Added support for guest login feature. [Phone Settings/General Settings]
- Added support for code selection for DND and rejecting calls. [Phone Settings/Call Settings]
- Added support for Group Listen with Speaker feature. [Phone Settings/Call Settings]
- Added support for Different Networks for Data and VoIP Calls configuration. [Network Settings/Ethernet Settings]
- Supported random upgrade check. [Maintenance/Upgrade]
- Supported video codec H.263. [Account/Codec Settings]

Firmware Version 1.0.1.55

- No major changes.

Firmware Version 1.0.1.54

- Added Support for configuring 2 Access Passwords to control the same GDS System. [Value-added Service Page Definitions]
- Added support for Zoom Mode feature. [Zoom mode]
- Added support for Wi-Fi band selection from web UI. [Wi-Fi]
- Added support for choosing "#" button as dial or redial function separately. [Use # as Dial Key]
- Added support for Broadsoft IM&P service. [Value-added Service/BroadSoft IM&P]
- Added support for MAC header in SIP REGISTER. [Use MAC Header]
- Added support for direct or quick IP call, and paging call mode selection in Dialpad. [Use Direct IP Call Mode] [Use Paging Call Mode] [Use Quick IP-Call mode]
- Added support for apply all available config files. [Download and Process All Available Config Files]
- Supported EEE (Energy-Efficient Ethernet) mode. [Enable EEE Mode]
- Supported HDMI audio enable/disable switch. [Sound]

Firmware Version 1.0.1.43

- Added option to disable recording during call. [Record Mode]
- Added support for Czech language [GXV3370 Technical Specifications]
- Added support to boot up in safe mode and option to boot the phone in safe mode from web GUI. [Safe Mode]
- Added RTP timeout support. [RTP Timeout Timer]
- Added mute support for paging/intercom. [Mute on Answer Intercom Call]
- Added SIP NOTIFY support to sync phone book [Allow Sync Phonebook via SIP Notify]
- Added support for second dial tone. [Call Progress Tones] [Dial Plan]
- Added option to support SUBSCRIBE expiration. [Subscribe Expiration]
- Added support for Baudisch Door System feature. [Door System Type]
- Added support for disabling handset. [Handset Option]
- Added ringtone selection support for door system settings. [Value-added Service Page Definitions]
- Added support to transfer a call via MPK BLF. [Enable transfer via non-Transfer Programmable Key]
- Removed codec Jitter Buffer Type settings from web UI account settings since GXV3370 is using a fixed value.
- Removed Hide Local Call History from web UI phone settings due to local Contacts app would not include Broadsoft contacts.

Firmware Version 1.0.1.33

- Supported TLS version 1.2. [GXV3370 Technical Specifications]
- Updated to SDK package version 1.1.5. [SDK FRAMEWORK SERVICE]
- Hide LCD/DDR/Factory Serial Number in the web UI under System Info. [System Info]

- Added more options in web UI Contacts Automatic Download Interval. [Automatic Download Interval]
- Supported choosing call function buttons for single call or conference. [Phone Settings/Call Settings].

Firmware Version 1.0.1.28

- Added different service type to web UI Value-added Service. [Value-added Service]
- Supported SDK. [SDK FRAMEWORK SERVICE]
- Added LDAP page configuration. [LDAP Phonebook]
- Added Wi-Fi country code configuration. [Country Code]
- Removed LDAP page temporarily. It will be added later.
- Added a new option “Basic settings & Network setting” for Configuration via Keypad Menu. [Configuration via Keypad Menu]
- Removed “Prefer Non-Interleaved Mode” in account code settings.
- Added “Speed conference” in MPK. [Applications/Programmable key]

Added LCD Settings → Network → VPN, to add or edit VPN profile. [Note: Since firmware version 1.0.3.36 this setting can be restricted from WEB UI as well as from LCD screen. This can only be configured via config template. When P22038=0, the Wi-Fi settings are neither accessible from web UI nor from LCD. To enable Wi-Fi on web UI and LCD screen, use P22038=1.

- VPN]

Firmware Version 1.0.1.12

- This is the initial version.

WELCOME

Thank you for purchasing Grandstream GXV3370 IP Multimedia Phone for Android^{TM}. The GXV3370 IP Video Phone for Android combines a 16-line IP video phone with a multi-platform video conferencing solution and the functionality of an Android tablet to offer an all-in-one communications solution. The phone features a 7” 1024x600 capacitive touch screen TFT LCD, Mega pixel camera, dual Gigabit ports with PoE/PoE+, HD audio and video, integrated Wi-Fi (802.11a/b/g/n) & Bluetooth, rich peripheral interfaces, and Android 7.0. By combining a state-of-the-art IP video phone, an advanced video conferencing solution, and the functionality of a tablet, businesses throughout the world can now use the GXV3370 for all communication and productivity needs.

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the GXV3370:

Table 1: GXV3370 Features in a Glance

 GXV3370	• 16 lines with up to 16 SIP, up to 7-way audio conference and 3-way 720p 30fps HD video conference, phonebook with up to 1000 contacts, call history with up to 1000 records • Dual switched 10/100/1000Mbps network ports, Dual band 2.4 & 5GHz Wi-Fi (802.11a/b/g/n), PoE/PoE+, Bluetooth 4.0+EDR, USB, SD, HDMI, EHS with Plantronics headsets support • 7” (1024x600) capacitive (5 points) touch screen TFT LCD, mega pixel CMOS sensor camera with privacy shutter • HD wideband audio, full-duplex Hands-free speakerphone with HD acoustic chamber, advanced acoustic echo cancellation and excellent double-talk performance • Runs the Android™ Operating System 7.0. • Built-in support for GXV series of video surveillance cameras, and GDS370x series of access control devices. • Create Android applications for any business need to run on GXV3370 using Google’s API and Grandstream’s SDK toolkit.

GXV3370 Technical Specifications

The following table resumes all the technical specifications including the protocols / standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings for the phone GXV3370.

Table 2: GXV3370 Technical Specifications

Protocols/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, OpenVPN®.
Network Interfaces	Dual switched 10/ 100/ 1000 Mbps ports with integrated PoE/PoE+
Graphic Display	7" 1024x600 capacitive touch screen (5 points) TFT LCD
Camera	Tiltable mega-pixel CMOS camera with privacy shutter, 720P@30fps
Bluetooth	Yes, integrated. Bluetooth 4.0 + EDR.
Wi-Fi	Yes, dual-band 2.4 & 5GHz with 802.11 a/b/g/n
Auxiliary Ports	RJ9 headset jack (allowing EHS with Plantronics headsets), 3.5mm stereo headset with microphone, USB port, SD, HDMI-out (1.4 up to 720p30fps)
Feature Keys	2 function touch keys VOLUME +/-, 3 dedicated Android touch keys HOME, MENU, and BACK
Voice Codec	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 Codec and Capabilities	H.263,H.264 BP/MP/HP, video resolution up to 720p, frame rate up to 30 fps, bit rate up to 2Mbps, 3-way video conference (720p@30fps), anti-flickering, auto focus and auto exposure
Telephony Features	Hold, transfer, forward (unconditional/no-answer/busy), call park/pickup, 7-way audio conference(including the host), shared-call-appearance (SCA) / bridged-line-appearance (BLA), virtual MPK, downloadable contacts (XML, LDAP, up to 1000 items), call record, call log (up to 1000 records), call waiting, auto answer, XML customization of screen, click-to-dial, flexible dial plan, hot desking, personalized music ringtones and music on hold, server redundancy & fail-over
Sample Applications	Local apps: Contacts, Call History, File Manager, MPK, Settings, Browser, Voicemail, Clock, Recorder, SMS, Backup and Restore, etc. Support 3rd party apps: Skype, Google Hangouts, Skype for Business, etc. API/SDK available for advanced custom application development.
Applications Deployment	Allow Android 7.0 compliant applications to be developed, downloaded, and run in the embedded device with provisioning control

HD Audio	Yes, HD handset and speakerphone with support for wideband audio
Base Stand	Yes, integrated stand with multiple adjustable angles. Wall mountable
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES encrypted configuration file, TLS, SRTP, HTTPS, 802.1x media access control
Multi-language	English, German, Italian, French, Spanish, Portuguese, Russian, Croatian, Chinese, Korean, Japanese, Czech, Slovak and more
Upgrade/ Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS or local HTTP upload, mass provisioning using TR-069 or AES encrypted XML configuration file
Power and Green Energy Efficiency	Universal power adapter included: Input: 100-240VAC 50-60Hz; Output 12VDC 1.5A Integrated PoE* 802.3af Class 3, PoE+ 802.3at, Class 4 **When using PoE to power up phone, the USB port will not work.*
Physical	**Dimension :** 252mm (W) x 211mm (L) x 84mm (H) **Unit weight:** 1.08kg **Package weight:** 1.77kg
Temperature and Humidity	Operation: 0^{o}C to 40^{o}C Storage: -10^{o}C to 60^{o}C Humidity: 10% to 90% Non-condensing
Package Content	GXV3370 phone, handset with cord, base stand, universal power supply, network cable, screen cleaning cloth, quick installation guide, brochure, GPL license
Compliance	**FCC:** Part 15 (CFR 47) Class B; UL 60950 (power adapter); Part68 (HAC) **CE :** EN55022 Class B, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, EN62479, RoHS **RCM:** AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950; AS/NZS 4268 **IC:** ICES 003, RSS 247, CS 03, RSS 102

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the GXV3370.

Equipment Packaging

Table 3: Equipment Packaging

GXV3370
• 1 x GXV3370 Main Case. • 1 x Handset. • 1 x Phone Cord. • 1 x Ethernet Cable. • 1 x 12V Power Adapter. • 1 x Wall Mount. • 1 x Screen Cleaning Cloth. • 1 x Quick Installation Guide. • 1 x GPL License.

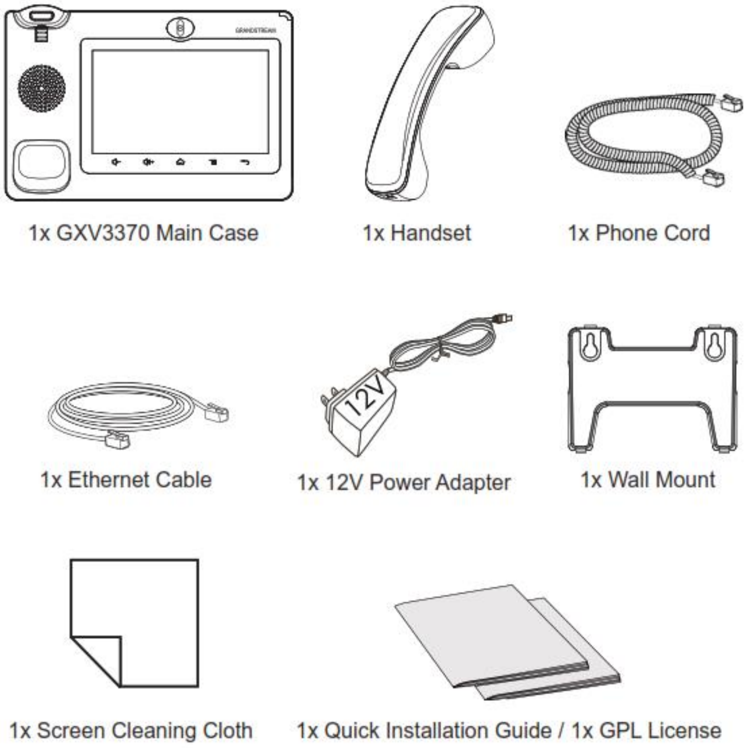


Figure 1: GXV3370 Package Content

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

GXV3370 Phone Setup

The GXV3370 can be installed on the desktop using the built-in stand or attached on the wall using the slots for wall mounting.

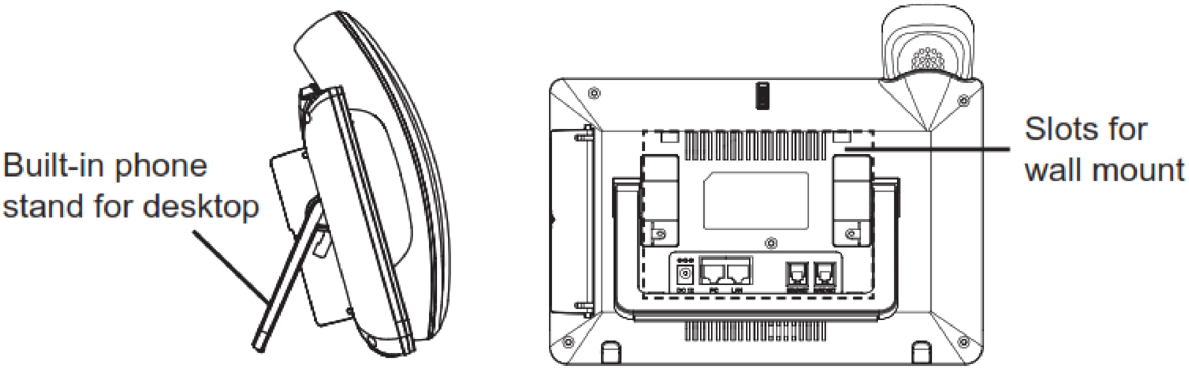


Figure 2: Built in Stand and Mounting Slots on The GXV3370.

Using the Phone Stand

The GXV3370 has a built-in phone stand. To use it, pull out the phone stand handle on the back of the phone. Adjust the angle as preferred and make sure the phone stands still on the desktop

Using the Slots for Wall Mounting

1. Attach the wall mount to the slots on the back of the phone;
2. Attach the phone to the wall via the wall mount hole;
3. Pull out the tab from the handset cradle (see figure below);
4. Rotate the tab and plug it back into the slot with the extension up to hold the handset while the phone is mounted on the wall.

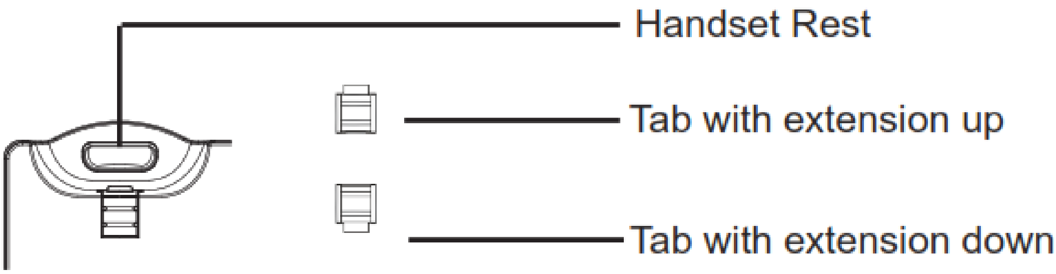


Figure 3: Tab on the Handset Cradle

Connecting the GXV3370

To setup your GXV3370, please follow the steps below:

1. Connect the handset and main phone case with the phone cord;
2. Connect the LAN port of the phone to the RJ-45 socket of a hub/switch or a router (LAN side of the router) using the Ethernet cable;
3. Connect the 12V DC output plug to the power jack on the phone; plug the power adapter into an electrical outlet. If PoE switch is used in step 2, this step could be skipped;
4. The LCD will display booting up or firmware upgrading information. Before continuing, please wait for the main screen display to show up;
5. Using the web configuration interface or from the menu of the touch screen, you can further configure network connection using static IP, DHCP etc.

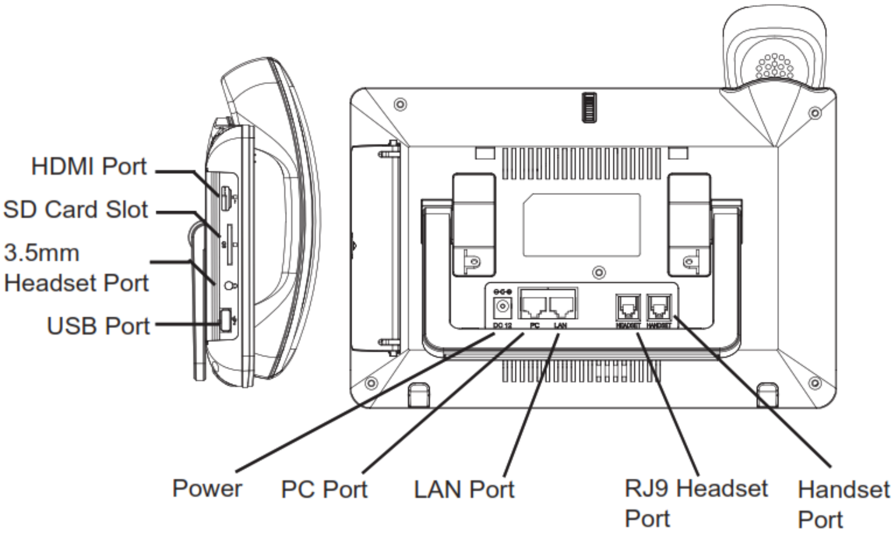


Figure 4: GXV3370 Back / Side View

Cleaning the Phone

For daily dust removal and fingerprint removal, please use the screen cleaning cloth in the factory package to wipe the phone. For some special cases like medical environment, you can use medical alcohol or isopropanol. The steps are as followed:

1. Before cleaning the phone, stop using it and disconnect it from the power supply.
2. Spray a small amount of disinfectant on screen, camera, handle, and other places that are easily touched by users.
3. Wipe the phone with screen cleaning cloth.
4. Power on until the disinfectant is completely volatilized.

Notes:

- Keep the power plug clean and dry or may lead to electric shock or other perils.
- DO NOT use disinfectant too frequently.
- DO NOT use high degree or even pure disinfectant. It could damage the phone.

GXV3370 LCD SETTINGS

The GXV3370 LCD MENU provides an easy access to the settings on the phone. Some of the settings from Web GUI could be configured via the LCD as well. The following table shows the LCD setting menu options.

Table 4: GXV3370 LCD Settings

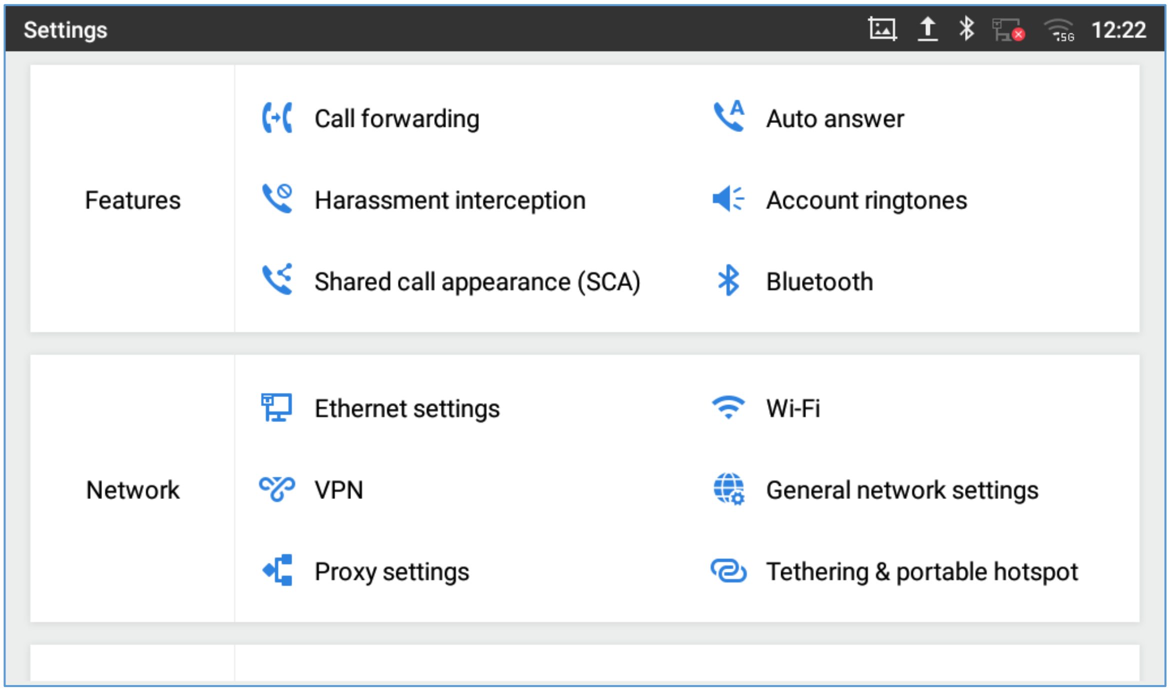
Features	• Call Forwarding • Auto-Answer • Harassment interception • Account Ringtones • Shared Call Appearance (SCA) • Bluetooth
Network	• Ethernet settings • Wi-Fi • General Network Settings • Proxy Settings • Tethering & Portable Hotspot
Basic	• Voice • Display • Language & Keyboard • Date & Time
System	• Security Settings • Peripherals • Accounts • Power Information • Reboot the Phone
Apps	• Application Management • Default Application • Notification Center
Advanced	• Account Settings • System Update • Syslog • System Security
About	• Account Status • Network Status • System Info • Storage Status

Access LCD Settings

To open the settings menu, you should:

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

- Swipe down from the top of the home screen to open the notifications panel and hit the ⚙ **Settings** icon in the top right corner.



Settings 12:22

Features	Call forwarding	Auto answer
	Harassment interception	Account ringtones
	Shared call appearance (SCA)	Bluetooth
Network	Ethernet settings	Wi-Fi
	VPN	General network settings
	Proxy settings	Tethering & portable hotspot

Figure 5: GXV3370 System Settings

Features

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

- **Call Forwarding**

  The incoming call to this SIP account can be forwarded to another account using different rules as configured here.

  - **Disabled**: Call forwarding feature is disabled. This is the default setting.
  - **Unconditional**: Forward all calls to a number.
  - **Time based**: Set the time range and number to be forwarded the calls to. In this time range, calls are forwarded to the number specified in "**In Time Forward To**"; out of this time range, calls are forwarded to the number specified in "**Out Time Forward To**".
  - **Others**: Configure Call forward when the phone is Busy or on DND or based on No Answer Out.

- **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.

- **Harassment interception**
  - **Blacklist**: This menu allows configuring a blacklist of number that will be blocked from calling the phone, users can either enter the numbers to block manually, from contacts or from call history
  - **Intercept anonymous calls:** when enabled the phone rejects all the anonymous calls, users can choose on which account this setting is to be applied

- **Account Ringtones**

  Select a ringtone for the incoming call to the SIP account chosen. The system ringtone is set by default.

- **Shared Call Appearance (SCA)**
  - **Shared Call Appearance (SCA)**: Enable or disable SCA on the account.
  - **Enable Barge-in**: If set to "Yes", the user could barge into an active call on a shared line.
  - **Auto Fill Call Park Code**: If set to "Yes", the configured "Call Park Service Code" will be automatically filled in on the phone's dial pad when picking up the parked call. This is used when "Special Mode" is set to "BroadSoft" (from web UI or provisioning) and "Enable SCA" is set to "Yes".
  - **Call Park Service Code**: Configure the retrieving feature code for call parking. If "Auto Fill Call Park Code" is set to "Yes", this call park service code will be automatically filled in on the phone's dial pad when picking up the parked call. This is used when "Special Mode" is set to "BroadSoft" (from web UI or provisioning) and "Enable SCA" is set to "Yes".
  - **Seize Line Timeout (s)**: Configure the time for the line can be seized (in seconds) when using shared line. The default setting is 15 seconds. For Shared Call Appearance, phone will send a SUBSCRIBE-request for the line-seize event package whenever a user attempts to take the shared line off hook. "Line Seize Timeout" is the line-seize event expiration timer.

- **Bluetooth**
  - **Bluetooth:** Tap on "**Bluetooth**" to turn on/off Bluetooth connection. By default, it is turned off.
  - **Enable handsfree mode:** Tap on "Enable handsfree mode" to activate it.

- **Show received files:** Shows the Transfer history of Bluetooth files
- **Additional Settings:** This menu is available only when the Bluetooth is enabled:
  - ❖ **Device Name**. Tap to change the name of the GXV3370, which is displayed on other Bluetooth devices when discovered. By default, it is "**GXV3370_XXXXXX**" Where XXXXXX are the last 6 digits of the phone's MAC address.
  - ❖ **Visibility timeout**. Tap to select the timeout interval among "2 minutes", "5 minutes", "1 hour" or "never". By default, the visibility timeout is 2 minutes.
  - ❖ **Visibility to nearby Bluetooth devices**. Sets the visibility of the phone to other Bluetooth devices. Normally this option is enabled during pairing process so that other Bluetooth devices can discover the GXV3370.
- **Available devices**: This section will show the available devices for pairing. Tap on ↻ to initiate scan process on the GXV3370 to discover the Bluetooth devices within the range.

Network

Users can configure Ethernet settings, Wi-Fi, VPN, PPPoE and other advanced network settings here.

Ethernet Settings

- **Preferred Internet Protocol:** Selects which Internet protocol to use. When both Ipv4 and Ipv6 are enabled, phone attempts to use preferred protocol first and switches to the other choice if it fails.

- **Ipv4 Settings**: Here user can configure the IPv4 address Type. 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. If **PPPoE** is selected, type PPPoE Account ID and PPPoE Password provided from the PPPoE server to get authenticated for network access.

- **Ipv6 Settings**: Here user can configure the Ipv6 address Type. 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, Prefix Length, DNS Server, and Alternative DNS server.

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

Wi-Fi

- Tap on “**Wi-Fi**” to turn on/off Wi-Fi connection. By default, it is turned off.

- Tap on **“Wi-Fi Band”** to set the type of Wi-Fi Band (“2.4G”, “5G” or “2.4G&5G”). The default setting is 2.4G&5G.

- Tap on “**Wi-Fi Settings**” to set up and manage wireless access points. This option is available only when Wi-Fi is turned on.

  - **Add Network**. If the Wi-Fi network SSID does not show up in the list, or users would like to set up advanced options for the Wi-Fi network, roll to the end of the Wi-Fi list and select “Add Network”. Then Enter SSID, Security type, password and set up address type (DHCP/Static IP/PPPoE) in the prompt dialog. The phone will reboot with Wi-Fi network connected.

  - **Refresh**. Press MENU button ≡ and select “Refresh” to initiate scan for the Wi-Fi network within the range.

  - **Advanced Settings**. Press MENU button ≡ and select “Advanced”.

    - **Install Certificates**. This is to install certificates (previously download/uploaded to the phone) when connecting to Wi-Fi network requesting SSL certificate.
    - **Wi-Fi Direct**. This is to set up peer-to-peer connection between two Wi-Fi Direct devices so that they can share data and sync files. Press MENU button ≡ and select “Advanced”. Then tap on “Wi-Fi Direct”, the Available devices will be displayed.

  - **Wi-Fi Configuration**

    - **Saved Networks:** this is to show all the Wi-Fi Networks that are registered on the phone.
    - **Network notification**: If enabled, the phone will show notification on the top status bar indicating an open network is available. By default, it is enabled.
    - **MAC address**: This shows the MAC address of the Wi-Fi.
    - **IP address**: This shows the IP address of the phone from Wi-Fi network.

**Note: Since firmware version 1.0.3.36 this setting can be restricted from WEB UI as well as from LCD screen. This can only be configured via config template. When P22038=0, the Wi-Fi settings are neither accessible from web UI nor from LCD. To enable Wi-Fi on web UI and LCD screen, use P22038=1.

VPN

Enable / Disable OpenVPN®

General Network Settings

- **LLDP**
  Turn on/off LLDP on the GXV3370. If turned on, the phone will be able to discover the LAN polices as set up in the switch side to obtain network settings such as VLAN tag, Layer 2 QoS 802.1p priority and Layer 3 QoS in a plug-and-play manner.
- **LLDP TX Interval**
  Specifies the time interval, in seconds, between successive LLDP-MED transmission cycles
- **Layer 3 SIP QoS**
  This field defines the layer 3 QoS parameter for SIP packets.
  This is the value used for IP Precedence, Diff-Serv or MPLS. The Default value is 26.
- **Layer 3 Audio QoS**
  This field defines the layer 3 QoS parameter for audio packets. This is the value used for IP Precedence, Diff-Serv or MPLS. The Default value is 46.
- **Layer 3 Video QoS**
  This field defines the layer 3 QoS parameter for video packets. This is the value used for IP Precedence, Diff-Serv or MPLS. The Default value is 34.
- **Second Layer QoS 802.1Q/VLAN tag (Ethernet)**
  This field contains the value used for layer 2 VLAN tagging for the Ethernet network.
  The Default value is 0.
- **Second Layer QoS 802.1p/Priority Value (Ethernet)**
  This assigns the priority value of the Layer 2 QoS packets on the Ethernet Network.
  The Default value is 0.
- **Layer 2 QoS 802.1p priority (Wi-Fi)**
  This assigns the priority value of the Layer 2 QoS packets on the Wi-Fi Network. Default value is 0.

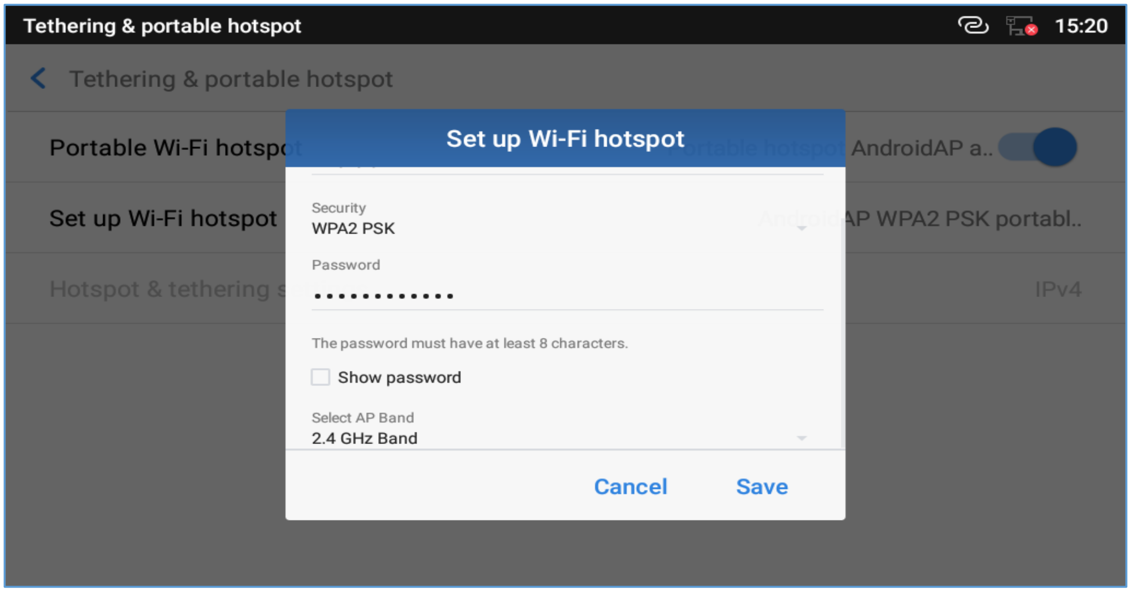
Proxy Settings

For some network setup, it is required to connect to the Internet via proxy server. Manually configure "Proxy hostname", "Proxy port" and "Bypass proxy for" in proxy settings for the phone to get Internet connection successfully.

Tethering & Portable Hotspot

The GXV3370 can serve as a Wi-Fi access point for other devices to provide wireless access to the network if the Portable Wi-Fi hotspot is turned on.

1. Turn on hotspot by tapping on “Portable Wi-Fi hotspot”. Icon will show on the top status bar.
2. Tap on “Set up Wi-Fi hotspot” to configure network SSID, security type and password. Please make sure the password has at least 8 characters. Otherwise, users will not be able to save the setting.
3. Tap on “Hotspot & tethering settings” and choose either to set up the hotspot for IPV4 only or for IPV4 & IPV6
4. On the other device that needs Wi-Fi access, turn on Wi-Fi, look for the SSID of the GXV3370 hotspot and enter authentication information to get connected.



Set up Wi-Fi hotspot

Security
WPA2 PSK

Password
••••••••••••

The password must have at least 8 characters.

□ Show password

Select AP Band
2.4 GHz Band

Cancel Save

Figure 6: GXV3370 Wi-Fi Hotspot

Basic

Sound

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

- **Silent mode**. Tap on it to turn on/off the sound from speaker when there is an incoming call.
- **HDMI**. Enable/disable audio switch between the phone and the HDMI output connected device (e.g. TV). When enabled, the TV will be used for audio output.
- **Media Volume**. Adjust the sound volume for media audio
- **Alarm Volume**. Adjust the alarm ring volume
- **Ring Volume**. Adjust the phone ringing volume
- **Notification Volume**. Adjust the notification sound volume
- **Ringtone**. Select phone’s ringtone for incoming call.
- **Default Notification Ringtone**. Select notification ringtone.
- **Default Alarm Ringtone.** Select the alarm ringtone

- **Other Sounds.** Enable/disable **Dial pad Tones**, **Screen locking sounds**, **Touch sounds** and **Button tones**.

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.
- **Screensaver.** Enable/disable the screensaver. Two options are available:
    - **Clock**: If the clock is set as screensaver, tap on ☰ and set the clock style and the Night Mode
    - **Screensaver**: If screensaver is set, please tap on ☰ to set use a network images or use local images as screensaver and set the Animation Interval between the images.
- **Font size.** Tap on it to adjust the font size for LCD screen.
- **Zoom mode.** Enable/Disable Zoom mode feature. If enabled, the font and icon become larger.

Language & keyboard

- **Language**. Tap to open the list of chosen languages, Language Number 1 is the language used on the phone. Tap on Add a Language to add more languages to the list.
- **Spell checker**. Configure whether to check spellings and select the language to check.
- **Personal dictionary**. Add new words to user’s dictionary so that they will not be displayed as error in the text.
- **Keyboard & input methods**
  Set up default input method for virtual and physical keyboard and the different parameters of the related to the Keyboard use. The default input method is Android Keyboard.
    - **Virtual Keyboard:**
        - **Android keyboard (AOSP)**: Set up the language used on Android keyboard and configure its different parameters including sound, auto-correction, word suggestion and so on.
        - **Manage Keyboards**. Tap on the + sign to choose which keyboard to use on the phone.
    - **Physical Keyboard**: When the physical keyboard is connected to the phone, users will have the possibility to choose a keyboard among the available ones on the virtual keyboard

  - **Show virtual Keyboard:** this option gives the possibility if keep showing the virtual keyboard even if the physical one is connected to the phone.
  - **Keyboard shortcuts helper:** Display available shortcuts.

- **Speech-Text to Speech Input.**
  - **Prefer engine.** Select the engine type. The default engine is Pico TTS.
  - **General:**
    - **Speech Rate**. Adjust the speech rate.
    - **Pitch:** Sets the speech pitch for the Text-To-Speech engine.
    - **Reset Speech Rate:** Reset the speed at which the text is spoken to normal.
    - **Reset speech pitch:** Reset the pitch at which the text is spoken to default.
    - **Listen to an example**: Play and listen the example of speech synthesis.
    - **Default Language Status:** Indicates if the language used is supported or not.
- **Pointer Speed**. Adjust the sensitivity of the mouse pointer.

Date & Time

- **Enable and use specified NTP server address**. Assign the URL or IP Address of NTP Server. The default NTP Server used is pool.ntp.org
- **Set date**. Set the current date for the GXV3370.
- **Set time**. Set the time on the GXV3370 manually.
- **Select time zone**. Select the time zone for the GXV3370.
- **Use 24-hour format**. Check/uncheck to display the time using 24-hour time format or not. For example, in 24-hour format, 13:00 will be displayed instead of 1:00 p.m.
- **Select date format**. Select the format of year, month, and day for the date to be displayed.

System

Security Settings

- **Device Security-Screen lock**. Set up pattern or password for screen lock. Wizard will be provided to set up the pattern. The screen will be locked after booting up or the screen is off (i.e., screensaver screen activated, or manually slide down **Status Bar→Screen Off** 🔒 to turn off LCD). Users will then be required to enter password or pattern to login. When the screen is locked, users can still be able to answer or reject incoming call.

- **Passwords-Make passwords visible**. Check/uncheck to show/hide letters when user's type screen lock password instantly.

- **Device Administration**
  - **Device administrators**. View or deactivate device administrators.
  - **Unknown sources**. Check/uncheck to enable/disable permission to install applications that you obtain from web sites and email.
- **Credentials Storage**
  - **Storage Type:** Shows the type of the storage which is **"Hardware-Backed** by default
  - **Trusted Credentials**. Display trusted CA certificates for system or user. Users can tap on the certificate to check the credential details or disable it.
  - **User Credentials**. View and modify stored credentials
  - **Install from SD card**. Install encrypted certificates from SD card.
  - **Clear credentials**. Clear credential storage of all contents and reset its password.

- **Advanced**
  - **Trust Agents**. View or deactivate trust agents
  - **Apps with usage access**. Manage what apps have access to app-usage data on your device.

Peripherals

Plug in RJ9/UHS Headset. Switch the media channel to RJ9 headset after plugging.

Accounts

Add a system account to synchronize contacts calendars and other information.

Power Information

PoE Power Supply notification. If enabled, the phone's system will display a notification of disabling USB socket when using PoE power supply. If disabled, the notification will not be shown.

Reboot the Phone

Press to reboot the phone. A confirmation window will pop up to Cancel or go on with the reboot.

Apps

Application Management

Tap on an application, process, or service to open it. The Application Info screen for each application lists its name, version, size, etc. Depending on the app, it may also include options for managing the application's data, forcing the application to stop, and disabling the application. Usually the options are:

- Tap the "**Force stop**" softkey to stop an application forcefully. This setting might not be valid for some applications.
- Tap the "**Stop**" softkey to stop an application gracefully. This setting might not be valid for some applications.
- Tap the "**Disable**" softkey to disable the application. Users could tap on "Enable" to turn it back on again. This usually applies to the built-in applications.
- Tap the "**Uninstall**" softkey to uninstall the applications.
- **Storage** provides storage information that an application uses on the phone. Tap "Clear data" to delete an application setting and other data. This setting might valid for some applications. If the application stores data in a temporary space of the phone's memory, "Cache" lists how much information is stored.
- Tap on "**Clear cache**" to clear the cache.
- "**Permissions**" lists information of the data that the app has access to. For example, the application might access the location information, storage, phone calls etc.
- "**Open by default**". If the application is configured to launch certain file type by default, tap on "Clear defaults" to reset this.
- If an application is misbehaving, tap on "**Report**" softkey (if available) to send the developer information for the application.
- **Memory** will show the memories used on the phone by the applications
- **Modify System settings** gives the application the permission to modify the system settings
- **Store** provides Information about the Install source of the App

⚠ **Note:**

Stopping a built-in application, operating system processes or services might disable one or more dependent functions on the phone. Users may need restart the phone to restore full functionality again.

Default Application

This page allows to set default applications to launch with certain actions. Default applications can be set for following actions:

- **Opening Links.** Select which application to use as default when clicking on a web link (browser); when opening a picture (gallery) or when opening a music file (music).
- **Assist & Voice Input.** Select a default application if previously installed.
- **Home app.** Select default launcher application if already installed.
- **Browser app.** Select default browser if more than one is installed.
- **Emergency app**. Select emergency default application if already installed.

Notification Center

Tap on an application, process, or service to open it. The notification Info screen for each application lists supported actions and allow user to activate/deactivate each notification. Following notifications can be configured (supported notifications depend on the applications):

- **Block all.**
- **Show silently.**

Advanced

Account Settings

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

- **Account Activation.**
- **Account Name.**
- **SIP Server.**
- **SIP User ID.**
- **SIP Authentication ID.**
- **SIP Authentication Password.**
- **Outgoing Proxy Server.**
- **Voicemail User ID.**
- **Display Name.**

System Update

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

- **Firmware upgrade and configuration file detection.** This will send a request to firmware and provisioning server to upgrade/provision the phone if the files are available on the servers.
- **Firmware:**
  - **Upgrade Mode:** This field allows the user to choose the firmware upgrade method: TFTP, HTTP or HTTPS.
  - **HTTP/HTTPS username:** The username for the HTTP/HTTPS server if set up on the server.
  - **HTTP/HTTPS password:** The password for the HTTP/HTTPS server if set up on the server.
  - **Firmware Server Path:** This defines the server path for the firmware server. It can be different from the configuration server for provisioning.
- **Config:**
  - **Upgrade mode:** This field allows the user to choose the provisioning method: TFTP, HTTP or HTTPS.
  - **HTTP/HTTPS username:** The username for the HTTP/HTTPS server if set up on the server.
  - **HTTP/HTTPS password:** The password for the HTTP/HTTPS server if set up on the server.
  - **Config Server Path:** This defines the server path for the provisioning server. It can be different from the firmware server.

Syslog

- **Syslog level:** Select the level of logging for syslog. The default setting is "None". There are 4 levels: DEBUG, INFO, WARNING and ERROR.
- **System log protocol:** Select the protocol of syslog (UDP or SSL/TLS).
- **Syslog server address:** The URL/IP address for the syslog server. If the GXV3370 has network connection, the phone will send the syslog packets to this server address.
- **System log keyword filtering:** Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to "SIP" to filter SIP log.

System Security

- **Disable Web Login**: This disables web GUI access.
- **Developer Mode**. To enable/disable developer mode.

- **Revoke debugging authorization**. To Revoke access to debugging from all computers previously authorized

- **Factory Reset**. Restore default settings.

Status

Account Status

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

Network Status

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

System Info

This page shows system info including Total Memory, Available Memory, Android Version, System Version, Hardware version, CPU temperature…

Storage Status

This page shows device storage status.

GXV3370 WEB GUI SETTINGS

The GXV3370 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow users to configure the application phone through a Web browser such as Microsoft's IE, Mozilla Firefox, Google Chrome and etc.

Status Page Definitions

Status/Account Status

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

Status/Network Status

MAC Address	Global unique ID of device, in HEX format. The MAC address will be used for provisioning and can be found on the label coming with original box and on the label located on the back of the device.
NAT Type	Type of NAT connection used by the phone.
Ipv4	
Address Type	Configured address type: DHCP, Static IP or PPPoE.
Ipv4 Address	IP address of the phone.
Subnet Mask	Subnet mask of the phone.
Default Gateway	Default gateway of the phone.
DNS Server 1	DNS Server 1 of the phone.
DNS Server 2	DNS Server 2 of the phone.
Ipv6	
Ipv6 Address Type	Configured address type: DHCP, Static IP or PPPoE.
Ipv6 Address	IPv6 address of the phone.
Ipv6 DNS Server 1	IPv6 DNS Server 1 of the phone.
Ipv6 DNS Server 2	IPv6 DNS Server 2 of the phone.

Status/System Info

Product Model	Product model of the phone: GXV3370.
Hardware Revision	Hardware version number.
Part Number	Product part number.
Serial Number	Product serial number.
System Version	Firmware version ID. This is the main software release version, which is used to identify the software system of the phone.
Recovery Version	Recovery image version.
Boot Version	Booting code version.
Kernel Version	The kernel version.
System Up Time	System up time since the last reboot.

Account Page Definitions

GXV3370 has 16 lines that can be configured to accommodate 16 independent SIP accounts. Each SIP account has an individual configuration page.

Account/General Settings

On Register	
Account Active	Indicates whether the account is active. The default value for the first account is “Yes”.
Account Name	Configures the name associated with each account to be displayed on the LCD.
SIP Server	Specifies the URL or IP address, and port of the SIP server. This should be provided by VoIP service provider (ITSP).
SIP User ID	Configures user account information provided by your VoIP service provider (ITSP). It is usually in the form of digits similar to phone number or actually a phone number.
SIP Authentication ID	Configures the SIP service subscriber’s Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	Configures the account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After saving, it will appear as hidden for security purpose.
Display Name	Specifies the SIP server subscriber’s name (optional) that will be used for Caller ID display. The configured content will be included in the From, Contact and P-Preferred-Identity headers of SIP INVITE message.

Tel URI	Indicates E.164 number in "From" header by adding "User=Phone" parameter or using "Tel:" in SIP packets, if the phone has an assigned PSTN Number. • **Disabled:** Will use "SIP User ID" information in the Request-Line and "From" header. • **User=Phone:** "User=Phone" parameter will be attached to the Request-Line and "From" header in the SIP request to indicate the E.164 number. If set to "Enable". • **Enabled:** "Tel:" will be used instead of "sip:" in the SIP request. Please consult your carrier before changing this parameter. Default is "Disabled".
Voice Mail Access Number	Sets if the phone system allows users to access the voice messages by pressing the MESSAGE key on the phone. This ID is usually the VM portal access number. For example, in UCM6xxx IPPBX, *97 could be used.
Network Settings	
Outbound Proxy	Configures the IP address or the domain name of the primary outbound proxy, media gateway or session border controller. It is used by the phone for firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and only an outbound proxy can provide a solution
Secondary Outbound Proxy	Sets IP address or domain name of the secondary outbound proxy, media gateway or session border controller. The phone system will try to connect the Secondary outbound proxy only if the primary outbound proxy fails.
DNS Mode	Defines which DNS service will be used to lookup IP address for SIP server's hostname. There are three modes: • A Record • SRV • NATPTR/SRV To locate the server by DNS SRV set this option to "SRV" or "NATPTR/SRV". Default setting is "A Record".
Maximum 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. The default setting is 4. The range is from 1 to 10.
DNS SRV Fail-over Mode	The option will decide which IP is going to be used in sending subsequent SIP packets (ex: Register refresh requests) after the list of Ips for SIP server host is resolved with DNS SRV.

	• **Default (prefer server with lowest SRV priority):** The phone will always prefer to send SIP requests to the available server having the lowest priority, and in case it's down it contacts the next one, but once the server having lowest priority is UP again, the phone will switch over to this one. • **Saved one until DNS TTL (Stay on responding IP until DNS timeout):** On this mode, the phone will resolve DNS SRV records and tries to send the request to the server having lowest priority and if it doesn't respond, it will move on to the next IP until one of the servers responds, once this happen the phone will keep contacting this responding IP until DNS timeout (30 minutes) before starting over. • **Saved one until no response (Stay on responding IP until its failure):** On this mode, the phone will send SIP requests to the last responding IP, and it does not failover/switchover to the next one until this responding server is down. • **Saved Failback follows failback expiration timer:** On this mode, the phone will send all SIP requests to the current failover SIP server or Outbound Proxy until the failback timer expires. Failback Expiration can specify 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. The default setting is 60. The range is from 1 to 64800.
NAT Traversal	Specifies which NAT traversal mechanism will be enabled on the phone system. It can be selected from the dropdown list: • NAT NO • STUN • Keep-alive • UPnP • Auto • VPN If the outbound proxy is configured and used, it can be set to "NAT NO". If set to "STUN" and STUN server is configured, the phone system will periodically send STUN message to the SUTN server to get the public IP address of its NAT environment and keep the NAT port open. STUN will not work if the NAT is symmetric type. If set to "Keep-alive", the phone system will send the STUN packets to

	maintain the connection that is first established during registration of the phone. The "Keep-alive" packets will fool the NAT device into keeping the connection open and this allows the host server to send SIP requests directly to the registered phone. If it needs to use OpenVPN to connect host server, it needs to set it to "VPN". If the firewall and the SIP device behind the firewall are both able to use UPNP, it can be set to "UPNP". Both parties will negotiate to use which port to allow SIP through. The default setting is "Keep-alive".
Proxy-Require	Adds the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server.

Account/SIP Settings

SIP Basic Settings	
SIP Registration	Allows the phone system to send SIP REGISTER messages to the proxy/server. The default setting is "Yes".
Unregister before New Registration	Controls whether to clear SIP user's information by sending un-register request to the proxy server. When set to "All", the un-registration is performed by sending a REGISTER message with "Contact" header set to * and Expires=0 parameters to the SIP server when the phone starts pre-registration after rebooting. If set to "Instance", the phone only cleans the current SIP user's info by sending REGISTER message with "Contact" header set to concerned SIP user's info and Expires=0 parameters to the SIP server. The default setting is "Instance".
Register Expiration (m)	Configures the time period (in minutes) in which the phone refreshes its registration with the specified registrar. The default setting is 60. The maximum value is 64800 (about 45 days).
Subscribe Expiration (m)	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar. The maximum value is 64800 (about 45 days). Default value is 60.
Re-register before Expiration (s)	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default setting is 0. The range is from 0 to 64,800.
Registration Retry Wait Time (s)	Configures the time period (in seconds) in which the phone will retry the registration process in the event that is failed. The default setting is 20. The maximum value is 3600 (1 hour).
Add Auth Header on RE-	Configure if the SIP account needs to add Auth header in RE-REGISTER.

SIP OPTIONS Keep Alive Maximum Tries	Configures the maximum times of sending OPTIONS message consistently from the phone to server. Phone will keep sending OPTIONS messages until it receives response from SIP server. The default setting is “3”, which means when the phone sends OPTIONS message for 3 times, and SIP server does not respond this message, the phone will send RE-REGISTER message to register again. The valid range is 3-10.
Subscribe for MWI	Configures the phone system to subscribe voice message service. If it is set to “Yes”, the phone system will periodically send SIP SUBSCRIBE message for Message Waiting Indication service. GXV3370 phone system supports both synchronized and non-synchronized MWI. Default is “No”.
Use Privacy Header	Determines if the Privacy header will be presented in the SIP INVITE message and if it includes the caller info in this header. If it is set to “Default”, the Privacy Header will be omitted in INVITE when “Huawei IMS” special feature is active. If set to “Yes”, it will always be presented. If set to “No”, it will always be omitted. The default setting is “Default”.
Use P-Preferred-Identity Header	Specifies if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to “default”, the P-Preferred-Identity Header will be omitted in SIP INVITE message when “Huawei IMS” special feature is active. If set to “Yes”, the P-Preferred-Identity Header will always be presented. If set to “No”, it will be omitted. The default setting is “Default”.
Use P-Access-Network-Info Header	Use P-Access-Network-Info header in SIP INVITE message. Default setting is Yes.
Use P-Emergency-Info Header	Use P-Emergency-Info header in SIP INVITE message. Default setting is Yes.
Use MAC Header	Use MAC Header in SIP register request and add MAC address in User-Agent header in SIP request. Default Setting is NO.
SIP Transport	Determines which network protocol will be used to transport the SIP message. It can be selected from TCP/UDP/TLS. Default setting is “UDP”.
Local SIP Port	Determines the local SIP port used to listen and transmit. The default setting is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4, 5068 for Account 5, and 5070 for Account 6. The valid range is from 5 to 65535.
SIP URI Scheme When Using TLS	Defines which SIP header, “sip” or “sips”, will be used if TLS is selected for SIP Transport. The default setting is “sip”.
Use Actual Ephemeral Port in Contact with TCP/TLS	Determines the port information in the Via header and Contact header of SIP message when the phone system use TCP or TLS. If set to No, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the particular connection. The default setting is “No”.

Support SIP Instance ID	Determines if the phone system will send SIP Instance ID. The SIP instance ID is used to uniquely identify the device. If set to “Yes”, the SIP Register message Contact header will include +sip.instance tag. The default setting is “Yes”.
SIP T1 Timeout	Defines an estimate of the round-trip time of transactions between a client and server. If no response is received in T1, the figure will increase to 2*T1 and then 4*T1. The request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 sec.
SIP T2 Interval	Specifies the maximum retransmit time of any SIP request messages (excluding the SIP INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. The default setting is 4 sec.
SIP Timer D Interval	Defines the amount of time that the server transaction can remain when unreliable response (3xx-6xx) received. The valid value is 0-64 seconds. The default value is 0.
Remove OBP from Route	Configures the phone system to remove the outbound proxy URI from the Route header. This is used for the SIP Extension to notify the SIP server that the device is behind a NAT/Firewall. If it is set to “Yes”, it will remove the Route header from SIP requests. The default setting is “No”.
Enable 100rel	Actives PRACK (Provisional Acknowledgment) method. PRACK improves the network reliability by adding an acknowledgement system to the provisional Responses (1xx). It is set to “Yes”, the phone system will response to the 1xx response from the remote party. The default setting is “No”.
Session Timing	
Enable Session Timer	Allows the phone system to use the session timer, when set to “Yes”, it will be added in the SIP INVITE message to notify the server.
Session Expiration (s)	Configures the phone system’s SIP session timer. It enables SIP sessions to be periodically “refreshed” via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180. The valid range is from 90 to 64800.
Min-SE (s)	Determines the minimum session expiration timer (in seconds) if the phone act as a timer refresher. The default setting is 90. The valid range is from 90 to 64800.
UAC Specify Refresher	Sets which party will refresh the active session if the phone makes outbound calls.

	If it is set to "UAC" and the remote party does not support Refresher feature, the phone system will refresh the active session. If it is set to "UAS", the remote party will refresh it. If it is set to "Omit", the header will be omitted so that it can be selected by the negotiation mechanism. The default setting is "Omit".
UAS Specify Refresher	Specifies which party will refresh the active session if the phone receives inbound calls. If it is set to "UAC", the remote party will refresh the active session. If it is set to "UAS" and the remote party does not support refresh feature, the phone system will refresh it. The default setting is "UAC".
Caller Request Timer	Sets the caller party to act as refresher by force. If set to "Yes" and both party support session timers, the phone will enable the session timer feature when it makes outbound calls. The SIP INVITE will include the content "refresher=uac". The default setting is "No".
Callee Request Timer	Sets the callee party to act as refresher by force. If set to "Yes" and both parties support session timers, the phone will enable the session timer feature when it receives inbound calls. The SIP 200 OK will include the content "refresher=uas". The default setting is "No".
Force Timer	Configures the session timer feature on the phone system by force. If it is set to "Yes", the phone will use the session timer even if the remote party does not support this feature. If set to "No", the phone will enable the session timer only when the remote party supports this feature. To turn off the session timer, select "No". The default setting is "No".
Force INVITE	Sets the SIP message type for refresh the session. If it is set to "Yes", the Session Timer will be refreshed by using the SIP INVITE message. Otherwise, the phone system will use the SIP UPDATE or SIP OPTIONS message. Default is "No".

Account/Codec Settings

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

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	Configures the phone to use the first matching codec in the 200OK message. The default value is 0.
ILBC Frame Size	Sets the ILBC (Internet Low Bitrate Codec) frame size if ILBC is used. Users can select it from 20ms or 30ms. The default setting is 30ms.
G726-32 ITU Payload	Configures G726-32 payload type for ITU packing mode. Payload 2 is static and payload dynamic is dynamic. The default setting is "2".
G726-32 Dynamic PT	Specifies the G726-32 payload type, and the valid range is 96 to 126. The default setting is "126".
Opus Payload Type	Defines the desired value (96-126) for the payload type of the Opus codec. The default value is 123.
DTMF	Specifies the mechanism to transmit DTMF (Dual Tone Multi-Frequency) signals. There are 3 supported modes: in audio, RFC2833, or SIP INFO. • **In audio**, which means DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs); • **RFC2833**, which means to specify DTMF with RTP packet. Users could know the packet is DTMF in the RTP header as well as the type of DTMF. • **SIP INFO**, which uses SIP INFO to carry DTMF. The defect of this mode is that it is easily to cause desynchronized of DTMF and media packet if the SIP and RTP messages are required to transmitted, respectively. The default setting is "RFC2833".
DTMF Payload Type	Configures the RTP payload type that indicates the transmitted packet contains DTMF digits. Valid range is from 96 to 126. Default value is 101.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call. The default setting is "No".
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	Enables the silence suppression/VAD feature. If it is set to "Yes", when silence is detected, a small quantity of VAD packets (instead of audio packets) will be sent during the period of no talking. If set to "No", this feature is disabled. The default setting is "No".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is 2.
Preferred Video Codec	
Preferred Video Codec	This parameter allows user to select preferred video codec from the "available" list. The phone supports H.264, H.263.This configuration will be included with the same preference order in the SIP SDP message.
Enable Video FEC	When enabled, the video sender will temporarily allocate part of the bandwidth to one data channel to send FEC data to system, thus, to improve the video quality the receiver gets. Enabling this function will take up part of bandwidth and reduce call rate. The default setting is "Yes".
Enable RFC5168 Support	Enables/disables RFC5168 mechanism for video calls. RFC5168 allows SIP party to request the sender to refresh its video frame in H.264 or refresh the full picture in VP8.The default setting is "Yes".
Video FEC Mode	If set to 0, FEC is not sent by separate port. If set 1, FEC is sent by separate port. Default setting is 0.
FEC Payload Type	Configures FEC payload type. The range is 96-127. Default setting is 120.
Packetization Mode	Configures video packetization mode. If set to "Single NAL Unit Mode", the packetization mode will be negotiated as single NAL unit mode when dial video calls, if the other party does not support the negotiation, then single NAL unit mode will be used for video encoding by default. If set to "Non-Interleaved Mode", the packetization mode will be negotiated as Non-interleaved mode when dial video calls, If the other party does not support negotiation, then the Non-interleaved mode will be used for video encoding by default. The default setting is "Non-Interleaved Mode".
H.264 Image Size	Sets the H.264 image size. It can be selected from the dropdown list. • **720P** • **4CIF** • **VGA** • **CIF** • **QVGA** • **QCIF**

	Note: For some network environment, the default setting “720P” might be too high that causes no video or video quality issue during video call. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower. The default setting is 720P.
Use H.264 Constrained Profiles	Configures that whether to set H.264 constrained profiles. The default setting is “No”.
H.264 Profile Type	Selects the H.264 profile type from the dropdown list. • **Baseline Profile** • **Main Profile** • **High Profile** • **BP/MP/HP** (Default Setting) **Note:** Lower levels are easier to decode, but higher levels offer better compression. Usually, for the best compression quality, choose “High Profile”; for playback on low-CPU machines or mobile devices, choose “Baseline Profile”. If “BP/MP/HP” is selected, all three profiles “Baseline Profile” “Main Profile” and “High Profile” will be used for negotiation during video decoding to achieve the best result. This is usually used in video conference when there is higher requirement on the video.
Video Bit Rate	Configures the bit rate for video call. It can be selected from the dropdown list. The default setting is 2048 kbps. The valid range is from 32 – 2048 kbps. **Note:** The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. For some network environment, the default setting “720P” might be too high that causes no video or video quality issue during video call. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower.
SDP Bandwidth Attribute	Sets the SDP bandwidth attribute. It can be selected from the drop-down list. The default setting is “Media Level”. • **Standard:** use AS format in session level; use TIAS format in media level • **Media Level:** use AS format in media level. • **Session Level:** use AS format in session level. • **None:** no modifications in the session format. **Note:** Please do not modify this setting without knowing the session format supported by the server. Otherwise, it might cause video decoding failure.
H.264 Payload Type	Specifies the H.264 codec message payload type format. The default setting is 99. The valid range is from 96 to 127.
H.263 Encoder Resolution	Selects the resolution (CIF/QCIF) used for H.263 codec.

Presentation Settings	
Enable BFCP	If set to “Yes”, the device will be able to receive the presentation stream in video calls and video meetings.
Initial INVITE with Media Info	Initial INVITE SDP contains presentation media.
Presentation H.264 Image Size	Selects the H.264 image size. Users can select 1080P or 720P.
Presentation H.264 Profile Type	Select the Presentation H.264 Profile Type from “Baseline Profile”, “Main Profile”, “High Profile” and “BP&MP&HP”. The default setting is “BP&MP&HP”. The lower the profile type is, the easier the packet can be decoded. However, 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 demanding for the video quality. Select among the three types to achieve best video effect.
Presentation Video Bit Rate	Configures the bit rate of the video. The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. Video Bit Rate can be set to integer value from 512kbps to 2048kbps.
Presentation Video Frame Rate	Configure the video frame rate for presentation.
BFCP Transport Protocol	Defines the transport protocol used for BFCP. Users can choose from Auto/UDP/TCP. The default setting is “UDP” first, if not supported, then choose “TCP”. If choose “Auto”, automatically switches between “UDP” and “TCP”.

Account/RTP Settings

SRTP Mode	Sets if the phone system will enable the SRTP (Secured RTP) mode. It can be selected from dropdown list: • **Disable** • **Enabled but not forced** • **Enabled and forced** SRTP uses encryption and authentication to minimize the risk of denial of service. (DoS). If the server allows to use both RTP and SRTP, it should be configured as “Enabled but not forced”. The default setting is “Disable”.
SRTP Key Length	Configures all the AES (Advanced Encryption Standard) key size within SRTP. It can be selected from dropdown list: • **AES128&256 bit** • **AES 128 bit**

	- **AES 256 bit** If it is set to "AES 128&256 bit", the phone system will provide both AES 128 and 256 cipher suite for SRTP. If set to "AES 128 bit", it only provides 128-bit cipher suite; if set to "AES 256 bit", it only provides 256-bit cipher suite. The default setting is "AES128&256 bit".
Enable SRTP Key Lifetime	Defines the SRTP key lifetime. When this option is set to be enabled, during the SRTP call, the SRTP key will be valid within 2^{31} SIP packets, and phone will renew the SRTP key after this limitation. Default is "Yes".
RTCP Destination	Configures a remote server URI where the RTCP messages will be sent to during an active call.
Symmetric RTP	Configures if the phone system enables the symmetric RTP mechanism. If it is set to "Yes", the phone system will use the same socket/port for sending and receiving the RTP messages. The default setting is "No".
RTP IP Filter	Receives the RTP packets from the specified IP address and Port by communication protocol. If it is set to "IP Only", the phone only receives the RTP packets from the specified IP address based on the communication protocol; If it is set to "IP and Port", the phone will receive the RTP packets from the specified IP address with the specified port based on the communication protocol. The default setting is "Disable".
RTP Timeout Timer (s)	Disconnects the call automatically when there is no RTP stream for a specific timeout. Default is 30 seconds.
VQ RTCP-XR Collector Name	Configures the host name of the RTCP server that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Address	Configures IP address of the RTCP server that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Port	Configures the port of the RTCP server that accepts voice quality reports contained in SIP PUBLISH messages.

Account/Call Settings

Call Features	
Enable Video Call	Configures the video call function for this account. If set to "Default", it will be configured according to global video call function.
Start Video Automatically	Permits the phone system to enable the video feature automatically when it makes an outbound call. If set to "Yes", the video codec attributes will be included in the SIP INVITE message. Or the attributes will not be included. The default setting is "Yes".
Remote Video Request	Configures the preference to handle video request from the remote party during an audio call. The default is "Prompt". - "**Prompt**": A message will be prompted if a video request is received.

	Users can select “Yes” to establish video or “No” to reject the request. • “**Accept**”: Video request will be accepted automatically, and video will be established. • “**Deny**”: Video request will be rejected automatically.
Video Layout	Defines whether to enter full screen when incoming video call is answered. • “**Fullscreen**”: GXV3370 will show the remote video feed in full screen. • “**Only display Remote Screen**”: GXV3370 only displays the remote screen in full screen mode. • “**Default**”: GXV3370 will show both remote and local video feed.
Auto Answer	Sets the phone system to allow to answer an incoming call automatically when idle. If it is set to “Yes”, the phone will automatically enable the speaker phone to answer all the incoming calls after a short reminding beep. If set to “Enable Intercom/Paging”, it will automatically answer the incoming calls whose SIP INVITE includes auto-answer tag in the info header. The default setting is “No”.
Play Warning Tone for Auto Answer Intercom	When this option is enabled, the phone will play a warning tone When auto-answering intercom. The default setting is “Yes”.
Intercom Barging	Configures whether to answer the incoming intercom call when there is already an active call on the phone. When” Intercom Barging” is enabled, and if the current active call is an intercom call, the incoming intercom call will be automatically rejected; otherwise if the current active call is not an intercom call, the current active call will be put on hold and the incoming intercom will be automatically answered. When “Intercom Barging” is disabled, a prompt will show up indicating the incoming intercom call without interrupting the current active call. Default setting is disabled.
Auto Preview	Configures whether to turn on video to preview the video of the caller. If set to “Yes”, the user can view the video and hear the caller on the incoming page when there is an incoming call. If set to “Yes with Ringing”, the caller can view the video of the caller and hear the ringtone on the incoming page but cannot hear the caller. **Note:** If Auto Answer function has been enabled, this function does not take effect. Default Value: “No”.
Send Anonymous	Sets the phone system to make an anonymous outgoing call. If set to “Yes”, the “From” header in the SIP INVITE messages will be set to anonymous, blocking the Caller ID to be displayed. Default is “No”.
Intercept Anonymous Calls	If set to “Yes”, anonymous calls will be automatically blocked. The default setting is “No”.
Call Log	Categorizes the call logs saved for this account. If it is set to “Log All”, all the call logs of this account will be saved. If set to “Log Incoming/Outgoing Calls (Missed Calls Not Record)”, the whole call history will be saved other than missed call. If it is set to “Disable Call All”, none of the call history will be saved.

	If it is set to “Don’t Prompt Missed Call”, the phone will log the missed call histories, but there is no prompt to indicate the missed calls on phone LCD. The default setting is “Log All”. **Note:** Call log will not show for Ring Group missed call if “Do not prompt Missed calls” is selected.
Enable Call Features	Configures the local start command feature. If it is set to “Yes”, the feature will be enabled to recognize the local star code command. Otherwise, it will be disabled. The default setting is “No”.
Enable Call Waiting	This feature allows user to set call waiting availability under each account rather than globally.
Mute on Answer Intercom Call	When enabled, phone will mute the incoming intercom call based on Call-Info/Alert Info Headers. Default is disabled.
Transfer on 3-way Conference Hang up	Transfers conference from hosted party when hang up, thus other parties can continue the conference without interruption. Default is unchecked.
Use # as Dial Key	Treats “#” as the “Send” (or “Dial”) key when set to “Yes”. If set to “No”, this “#” key can be included as part of the dialed number. Please make sure the dial plan is properly configured to allow dialing # out. Default is “Yes”.
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 equivalent to the "Redial" key. If set to "No", the "#" key is treated as part of the dialed string. Default is “Yes”.
DND Call Feature On	Configures the feature code to enable the DND (Do Not Disturb) feature for this account. If it is configured, the phone will dial the feature code automatically when the DND feature is enabled.
DND Call Feature Off	Configures the feature code to disable the DND (Do Not Disturb) feature for this account. If it is configured, the phone will dial the feature code automatically when the DND feature is disabled.
No Key Entry Timeout (s)	Determines the expiration timer (in seconds) for no key entry. The dialed digit will be sent out if no other digits entered within the set period. The default value is 4 seconds. The valid range is from 1 to 15. This feature does not work if the dialer page is entered via the Account Widget on the phone.
Ring Timeout (s)	Defines the expiration timer (in seconds) for the rings with no answer. The default setting is 60. The valid range is from 10 to 300.
Refer-To Use Target Contact	Sets the phone system to use the target’s Contact header tag to the Refer-To header in the SIP REFER message during an attended transfer. The default setting is “No”.
RFC2543 Hold	If yes, c=0.0.0.0 will be used in INVITE SDP for hold.
Call Forward	
Call Forward Type	Sets the Call Forwarding feature for this account.

	• **None:** Disable call forwarding feature. • **Unconditional:** Set to forward all calls to a specified account. • **Time based:** Set the call forwarding rule based on time. The system can forward incoming calls to the accounts of In Time Forward to and Out Time Forward to. • **Others**: Set the call forwarding rule based on following account status. ✓ **Forward when Busy:** the call will be forward to number set under "Busy To" when the account is busy. ✓ **Forward when No Answer**: The call will be forwarded to the number set under "No Answer To" after the configured timeout. (range 1- 120s) ✓ **Forward when DND:** When the phone is on DND mode the call will be forwarded to number configured under "DND To".
Dial Plan	
Dial Plan Prefix	Configures the digits prepended to the dialed number.
Disable Dial Plan	Enables/disables the Dial plan mechanism for different cases. If the specific case is checked, the Dial plan mechanism will be disabled. • **Dial Page:** It controls the pattern of dialing numbers from the keypad, phone app and account widget. • **Contact:** It controls the pattern of dialing numbers from local or LDAP. • **Incoming call history:** It controls the pattern of dialing numbers from inbound call logs. • **Outgoing Call History:** It controls the pattern of dialing numbers from outbound call logs. • **MPK&Click2Dial:** It controls the pattern of dialing numbers from MPK app and the link on the webpage. The default setting is unchecking all the cases.
Dial Plan	Configures the dial plan to establish the expected number and pattern of digits for a telephone number. This parameter configures the allowed dial-plan for the phone. 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; a) xx+ or xx. – at least 2-digit numbers b) xx – only 2-digit numbers c) ^ - exclude d) [3-5] – any digit of 3, 4, or 5 e) [147] – any digit of 1, 4, or 7

f) <2=011> - replace digit 2 with 011 when dialing

g) | - the OR operand

h) \+ - add + to the dialing number

i) , - play second dial tone.

j) Back slash "\"—can be used to escape specific letters. E.g. if { \p\a\r\k\+60 } dial plan is configured, park+60 should be able to pass dial plan check. This also can be used to escape Mark and User-unreserved characters.

- Example 1: {[369]11 | 1617xxxxxxx}

Allow 311, 611, and 911 or any 10-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+}

Allow any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR allow any length of numbers with leading digit 2, replacing the 2 with 011 when dialed.

- Example 4: {0,x+}

If user dials 0 second dial tone will be played, and users can continue entering digits. For instance, if pressing 01234, after pressing 0 second dial tone is played, full number is sent in INVITE.

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

Allow any number of digits, OR any number with a leading +, OR any number with a leading *, OR any number with a leading * followed by a 2 digits number and a *. To dial + from keypad, press on 0 until + appears on LCD.

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

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

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

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

	Note: In some cases, where the user wishes to dial strings such as *123 to activate voice mail or other applications provided by their service provider, the * should be predefined inside the dial plan feature. An example dial plan will be: {*x+} which allows the user to dial * followed by any length of numbers.
Caller IDs	
Caller ID Display	Specifies which header tag will be used from the SIP INVITE message for the Caller ID display. If it is set to Auto, the phone system will use the one of the available headers in the priority hierarchy of P-Asserted Identify Header, Remote-Party-ID Header and FROM Header. If it is set to “From Header”, it will use the FROM header information for the Caller ID. If it is set to “Disabled”, all the incoming calls Caller ID will be displayed with “Unavailable”. The default setting is “Auto”.
Callee ID Display	If 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. If set to "Disabled", the callee ID will be displayed as "Unavailable". If set to "To Header", the callee ID will not be updated and displayed as To Header. The default setting is “Auto”.
Ring Tones	
Account Ring Tone	Configures the ringtone for the account. Users can set ringtones from the dropdown list. User can also import customized ringtone from LCD Setting menu. The customized ringtone file name will also be showed up in the dropdown list that allows user to select. A “silent” option has been added to account ring tone list.
Ignore Alert-Info header	Configures the default ringtone. If set to “yes”, the incoming alert info header from the SIP server will be ignored and default configured ringtone will be played. The default setting is “No”.
Match Incoming Caller ID	Specifies the rules for the incoming calls. If the incoming caller ID or Alert Info matches the number, pattern or Alert Info text rules, the phone will play the selected distinctive ringtone. The rule policy: • 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
Distinctive Ring Tone	Selects the distinctive ring tone if the incoming caller ID matched the specified Match Incoming Caller ID rule. If so, the phone will play the selected ringtone.

Account/Advanced Settings

Security Settings	
Check Domain Certificate	Sets the phone system to check the domain certificates if TLS/TCP is used for SIP Transport. The default setting is "No".
Validate Certification Chain	Configures whether to validate certification chain when TLS/TCP is configured for SIP Transport. If this is set to “Yes”, phone will validate server against the new certificate list. The default setting is “No”.
Validate Incoming SIP Messages	Specifies if the phone system will check the incoming SIP messages caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
Allow Unsolicited REFER	It is used to configure whether to dial the number carried by Refer-to after receiving SIP REFER request actively. If it is set to "Disabled", the phone will send error warning and stop dialing. If it is set to "Enabled/Force Auth", the phone will dial the number after sending authentication, if the authentication failed, then the dialing will be stopped. If it is set to "Enabled", the phone will dial up all numbers carried by SIP REFER. The default is "Disabled".
Only Accept SIP Requests from Known Servers	Answers the SIP request from saved servers when set to “Yes”, only the SIP requests from saved servers will be accepted; and the SIP requests from the unregistered server will be rejected. The default setting is “No”.
Check SIP User ID for Incoming INVITE	Configures the phone system to check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is “No”.
Allow SIP Reset	It is used to configure whether to allow SIP Notification message to perform factory reset on the phone. The default setting is "No".
Authenticate Incoming INVITE	Configures the phone system to authenticate the SIP INVITE message from the remote party. 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 item to validate incoming INVITE, but you must enable authenticate incoming INVITE first to make it take effect. You can verify the NOTIFY information for the provision, including check- sync, resync and reboot, but only when SIP NOTIFY authentication enabled first to make it take effect.
MOH	
MOH Mode	Configures MOH mode. If set to "Local MOH", a local MOH audio file needs to be uploaded for this mode to work.
Upload Local MOH Audio File	Loads the MOH (Music on Hold) file to the phone. Click on “Browse” button to upload the music file from local PC. The MOH audio file has to be in .wav or .mp3 format. **Note**: Please be patient while the audio file is being uploaded. It could take more than 3 minutes to finish the uploading especially the file size is large. The button will show as “Processing” during the uploading. Once done, it will show as “Browse” again. Click on “Save” on the bottom of the web page and “Apply” on the top of the web page to save the change.
Advanced Features	
Virtual Account Group	It is used to set to categorize accounts in server mode groups, the accounts in the same group will be combined as one and the account widget will display the Caller ID in the account with lowest ID. The phone can answer any incoming calls to each account in groups. If user makes an outbound call, the phone system will use the lowest ID account by default. If the account fails or SIP INVITE message is timeout, the phone system will failover to the next account in the group with higher account ID. If all the accounts are not available in the group, the phone system will traverse all the accounts in the group and notify the end users the session is failed.
Allow Sync Phonebook via SIP Notify	Allows users to synchronize XML phonebook upon receiving SIP NOTIFY message with header ***Event: sync-contacts***. **Note:** Received SIP NOTIFY will be first challenged for authentication purpose before contacting configured server to download XML phonebook. The parameters used are the ones configured at [**Download Contacts**]. The authentication can be done either using admin credentials (if no SIP account is configured) or using SIP account credentials. The default setting is “Yes”.

Account/Special Features

Special Feature	Configures phone’s settings to meet different vendors’ server requirements.

	Users can choose from Standard, CBCOM, RNK, China Mobile, ZTE IMS, Mobotix, ZTE NGN, or Huawei IMS depending on the server type.
Call Settings	
Feature Key Synchronization	This feature is used for BroadSoft / Metaswitch call feature synchronization. When it's set to BroadSoft / Metaswitch, DND and Call Forward features can be synchronized with BroadSoft / Metaswitch server. The call forward function will take effect on the server side while the local call forward function is not effective.
Enable BroadSoft Call Park	If enabled, phone will send SUBSCRIBE to BroadSoft server to obtain Call Park notifications.
Conference URI	Configures the conference URI for BroadSoft Network Conference feature.
BroadSoft Call Center	Enables BroadSoft Call Center feature. When enabled, Feature Key Synchronization will be enabled regardless of web UI settings.
Hoteling Event	Enables BroadSoft Hoteling feature.
Call Center Status	When enabled", the phone will send SUBSCRIBE to the server to obtain call center status.
SCA	
Enable SCA (Shared Call Appearance)	If enabled, the Shared Call Appearance (BroadSoft Standard) feature will be applied for the registered account.
Enable Barge-in	If enabled, users can barge into an active call on a shared line.
Auto-filling Call Park Feature Code	If enabled, the Call Park feature code will be automatically filled in the dialing interface when the phone is in call pickup.
Call Park Feature Code	Configures the pickup feature code for Call Park.
Line-seize Timeout (s)	Configures the interval (in seconds) when the line seize is considered timed out when Shared Line feature is used. Valid range is 15-60.

Phone Settings Page Definitions

Phone Settings/General Settings

Basic Settings	
Local RTP Port	Defines the local RTP-RTCP port pair used to listen and transmit. (The default value is 50040, Max is 65000). The following rule is applied: N>=0, the default value of Port_Value is 5004. - Audio RTP port: Port_Value+10*N - Audio RTCP port: Port_Value+10*N+1 - Video RTP port: Port_Value+10*N+2 - Video RTCP port: Port_Value+10*N+3

	- FEC RTP port: Port_Value+10*N+4 - FEC RTCP port: Port_Value+10*N+5 - BFCP Protocol port: Port_Value+10*N+6 - BFCP RTP port: Port_Value+10*N+8 - BFCP RTCP port: Port_Value+10*N+9
Use Random Port	Forces the phone system to use random ports for both SIP and RTP messages. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is “No”. **Note:** This parameter must be set to “No” for Direct IP Calling to work.
Disable in-call DTMF display	Enables/disables the phone system to omit the DTMF digits displaying from the LCD screen. The default setting is “No”.
Enable Enterprise Contacts Timeout Auto Search	Configures whether to display the matched content automatically in search of the LDAP contacts when timeout. If set to “No”, users need to click the “Search” button to search the matched contacts mentioned above. The default setting is “Yes”.
Keep-alive Interval (s)	Specifies how the phone system will send a Binding Request packet to the SIP server in order to keep the “ping hole” on the NAT router to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN Server	Configures the URI of STUN (Simple Traversal of UDP for NAT) server. The phone system will send STUN Binding Request packet to the STUN server to learn the public IP address of its network. Only non-symmetric NAT routers work with STUN. The default setting is “stun.ipvideotalk.com”.
TURN Server Username	Fill in the username to validate TURN server.
TURN Server Password	Fill in the password to validate TURN server.
Use NAT IP	Configures the IP address for the Contact header and Connection Information in the SIP/SDP message. It should ONLY be used if it is required by your ITSP. The default setting is keep the box blank.
Guest Features	
Guest Settings	
Guest Login	Enable/disable guest login. Users should configure SIP domain name when using this function. Users should input SIP username and password on LCD after rebooting the phone. Setting is disabled by default and requires reboot to take effect.
Guest Login Timeout	Configures guest login timeout. If user have logged in as guest, the web page will log out and exit automatically if there is no operation upon timeout
Guest Login PIN Code	When set "Guest Login" option to "Yes" and "Guest Login Timeout" to "Never", users should input the PIN code to login.
SIP Domain	

Server Alias	The server alias is used to customize the server name.
Server List	This is the list of SIP domain names under the selected severs. The registration priority of addresses in the list is from top to bottom. Up to 16 SIP domains are supported.

Phone Settings/Call Settings

Call Settings	
Enable Video Call Feature	Enables the video call feature on the phone. The default setting is “Yes”.
Use Direct IP Call Mode	Configures enable/disable direct IP call mode of the phone. If set to "Yes", the feature of direct IP call will be enabled.
Use Paging Call Mode	Configures enable/disable paging call mode of the phone. If set to "Yes", the feature of paging call will be enabled.
Use Quick IP-Call mode	Sets the phone system to automatically fills in the first three octets to make an outbound IP call. If it is set to “Yes”, users can dial an IP address under the same LAN/VPN segment by entering the last octet in the IP address. To dial quick IP call, offhook the phone and dial XXX (X is 0-9 and XXX <=255), the phone will make direct IP call to aaa.bbb.ccc.XXX where aaa.bbb.ccc comes from the local IP address REGARDLESS of subnet mask. XX or X are also valid so leading 0 is not required (but OK). No SIP server is required to make quick IP call. This setting can be configured after enabling ‘**Use Direct IP Call Mode** option. The default setting is “No”.
Enable Call-Waiting	Enables the call waiting feature. If it is not checked, the phone system will reject the second incoming call during an active session without user’s knowledge. But this missed call record will be saved to remind users. The default setting is “Yes”.
Enable Call-Waiting Tone	Sets the phone system to play the call waiting tone if there is another incoming call. If it is set to “No”, the phone will only display the indicator on the LCD screen for another incoming call. The default setting is “Yes”.
Enable DND Reminder Ring	Enables the DND reminder ring. If set to "Yes", the ring splash that indicates an incoming call when DND is enabled will be played. Default setting is “Yes”
Enable Transfer	Enables the Transfer function. Default settings is “Yes”
Hold Call Before Completing Transfer	When set to "Yes" the phone holds the second call before completing the attended transfer (it sends the INVITE method to hold the call before sending the REFER method).
Default Transfer Mode	Sets the default transfer mode for the phone system. If the Blind Transfer or Attended Transfer mode is set, the phone system will use the specific mode to transfer an active call.

	The users still have privilege to switch the mode on the LCD screen when they tap the transfer key. The default setting is “Blind Transfer”.
Enable transfer via non-Transfer Programmable Key	Programmable Key with the type speed dial, BLF and speed dial via active account will perform as transfer programmable keys under active call. The transfer mode during the call depends on the “Default Transfer Mode” mentioned above. MPK can also be selected as forward/transfer destination on the ringing screen when [**Enable Function for Incoming Call**] is set to “Call Transfer”.
Enable Function for Incoming Call	Enables the preview feature for the incoming video calls. Defines the function for the incoming video call. • If it is set to “Preview”, the phone system will pop up the PREVIEW key on the LCD screen when there is an incoming video call, and users could tap on it to check video caller without answering the incoming video call (the call will keep playing ringback on the caller side). **Note**: By pressing the preview button, the phone will send the SIP 183 message to the caller’s camera, based on SIP RFC3261; the caller’s camera should start sending the stream to the phone upon receiving the SIP 183. At any time, the GXV3370 user can press the "Answer" button. If done, then the phone will send the SIP 200OK and call will be fully established. • If set to "Call Transfer", the phone system will pop up the "TRANSFER" key on the LCD screen when there is an incoming call, and users could tap on it to show up the dialer without answering the incoming call, then, users could transfer this incoming call to others. The default setting is “None”.
Enable Conference	Enables the conference. When set to “No”, the phone will block the conference application. The default setting is “Yes”.
Auto Conference	Allows the phone system to invite all call parties into a conference by pressing the Conf key. If it is disabled, the end user has to add each call party to conference manually. The default setting is “No”.
Auto Mute on Entry	Configures whether to mute the call on entry automatically. • If set to "**Disable**", 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 answers the incoming call; If set to "Mute on Incoming & Outgoing Call", then mute automatically when the call gets through.

	Note: This function only take effect when the phone is from the idle status to call status. Users could click the Mute button on call interface to cancel the current mute status.
Always Ring Speaker	Determines if the speaker will play the ringtone if the speaker channel is not set as default channel. If set to "Yes", the phone will force to play the ring speaker in speaker channel. The default setting is "No". End user might need this feature when the headset is connected.
Offhook Auto Dial	Configures the User ID/extension to dial automatically when the phone is off hook. The phone will use the first account to dial the configured numbers out. The default setting is "No".
Offhook Auto Dial Delay (s)	Defines the timer for warm line dialing. After the timer expires, the phone system will dial the configured number in Off-hook Auto Dial automatically. If it is not configured, the configured number will be dialed immediately.
Offhook/OnHook Timeout (s)	If configured, the phone will exit the dial-up screen when timeout after Offhook or Onhook. default is 30s. The valid range is 10-60s.
Handset Option	Configures the Handset options and can be set to: • If set to "**Enable**"**:** when off hook, the phone will enter into the dial screen, and the media channel will switch to the handset; no matter if any third app is opening. • If set to "**Disable**": The Handset will be disabled. • If set to "**Auto**": when the 3rd-party application is calling, only the media channel will switch to the handset when off hook; otherwise, the phone will enter into the dial screen, and the media channel will switch to the handset. Default setting is "Auto".
Auto UnHold When Press the Line Key	Configures when there are multiple lines, whether to UnHold the line automatically when click the line being held and hold the line in the primary call. **Note**: the hold situation which is set manually will not be put on hold automatically. The default setting is "No".
Virtual Account Group Avaya Mode	If set to "Yes", when processing SIP Register 3XX Response, it will parse the address site in 3XX, modify the account server info "SIP Server: port" & "SIP Transaction" in virtual account group and initiate registration again. This feature is designed for the Avaya customers.
Number of Accounts The Virtual Account Group Register	Configures the number of concurrent the main server and standby server register, each account supports 1 SIP main server and 4 standby server registration.

Filter Characters	Sets the characters for filter when dial out numbers. Users could set up multiple characters. For example, if set to “[()-]”, when dial (0571)-8800-8888, the character “()-“ will be automatically filtered and dial 057188008888 directly.
Escape # as %23 in SIP URI	Determines which characters will be included in the SIP INVITE URI if end users input #. If it is set to “Yes”, the phone system will replace the # by %23. Otherwise, it will include # in the SIP INVITE message. The default setting is “Yes”.
Use 3rd Party App as Basic Phone	Enter the package and activity of the 3rd party app that substitutes GS phone application, separated by "/". e.g.: *com.broadsoft.ucone.androidtablet/com.broadsoft.android.common.activity.LauncherActivity.* After input, when the user offhook or click the phone application, it will automatically enable the configured app to enter the corresponding interface. Default setting is blank, which means use GS phone application.
Record Mode	• Configures phone recording mode. • If set to "**Record locally**", then the phone will use the local tape recorder for call recording, and the audio file will be saved in accordance with the tape recorder setup. • If set to "**Record on PortaOne**", then will send the specified SIP messages to the corresponding server. • If set to "**Record on UCM**", then will send the recording feature code to the UCM server to request for recording, and the recording function will be executed by the server. • If set to "**Record on Broadsoft**", then will send the recording feature code to the Broadsoft server to request for recording, and the recording function will be executed by the server. • If set to “**Disable**”, recording functionality will be disabled during calls.
Enable Auto Record When Call Established	Configures whether to auto record a call. If enabled, all recordings will start automatically after the call is established.
Rejected Call Notification	Specifies whether to enable rejected call notification. Once enabled, a missed call will prompt on LCD when rejecting an incoming call, and the rejected call will be saved in Call History Missed numbers and missed call prompt will be displayed.
Return Code When Refusing Incoming Call	When refusing the incoming call, the phone will send the selected type of SIP message of the call.
Return Code When Enable DND	When DND is enabled, the phone will send the selected type of SIP message.

Group Listen with Speake	Configures whether to enable speaker sound when in a call with handset/headset. If set to "Yes", the speaker sound is enabled, but you cannot talk through the speaker.
One-way Call Function Buttons	Users can configure and customize the call functions in the call interface during a normal call. The available call functions are: Mute, Hold, Video, Record, Transfer, Call Details, New Call, Keyboard, Media Channel, Conference. **Note:** Users can choose only 3 of these functions to be shown on the call interface during a one-way call.
Conference Call Function Buttons	Users can configure and customize the call functions in the call interface during a conference. The available call functions are: Invite, Mute, Hold, Record, Call Details, New Call, Keyboard, Media Channel. **Note:** Users can choose only 3 of these functions to be shown on the call interface during a conference.
Call Function Button Display Timeout (s)	Configures the timeout period for call function buttons display. If set to "0", the buttons will be always displayed. The value range is 0-30 seconds.

Phone Settings/Ring Tone

Auto Config CPT by Region	Configures whether to choose Call Progress Tone automatically by region. If set to "Yes", the phone will configure CPT (Call Progress Tone) according to different regions automatically. If set to "No", you can manually configure CPT parameters. The default setting is "No".
Call Progress Tones: • **Dial Tone** • **Second Dial Tone** • **Ring Back Tone** • **Busy Tone** • **Reorder Tone** • **Confirmation Tone** • **Call-Waiting Tone**	Configures tone frequencies according to user preference. By default, the tones are set to North American frequencies. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. **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 repeats the pattern. Please refer to the document below to determine your local call progress tones: http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf
Call-Waiting Tone Gain	Adjusts the call waiting tone volume. Users can select "Low", "Medium" or "High". The default setting is "Low".
Default Ring Cadence	Defines the ring cadence for the phone. The default setting is c=2000/4000.

Phone Settings/Video Settings

Video Frame Rate	Configures video frame rate for SIP video call from “5 frames/second”, “15 frames/second”, “25 frames/second” and “30 frames/second”. The default setting is 15 frames/second. The video frame rate is adjustable based on network conditions. Increasing the frame rate will significantly increase the amount of data transmitted, therefore consuming more bandwidth. The video quality will be affected due to packet loss if extra bandwidth is not allocated.
Video Display Mode	Sets the video display mode to "Original proportion", "Cut proportionally" or "Add black margin proportionally”. • If set to "**Original proportion**", the phone displays video in its original proportion. If the video display proportion is different from the one of the phones, the phone will stretch or compress video to display it. • If set to "**Cut proportionally**” the phone will cut video to meet its own display proportion. • If set to "**Add black margin proportionally**", the phone will display video in its original proportion. If it still exists spare space, the phone will add black edge on it.
Enable Frame Skipping in Video Decoder	Enables the phone system for frame skipping in video decoder. If it is enabled, the video decoder will skip the P frame and start decoding from the next I frame. Enabling this option will help reduce flickering in the video when the bandwidth is limited in the network environment. The default setting is "Yes".

Phone Settings/Multicast Paging

Multicast Paging	
Paging Barge	Sets the threshold of paging calls. If the paging call’s priority is higher than the threshold, the existing call will be hold and the paging call will be answered. Otherwise, the existing call does not be affected. If it is set to Disable, any paging call will not be answered. The default setting is “Disable”.
Paging Priority Active	Determines if a new paging call whose priority is higher than the existing paging call will be answered. If it is checked, this feature will be enabled. The default setting is disabled.
Multicast Paging Codec	Selects the codec type for the multicast paging call. This list includes PCMU, PCMA, G726-32, G722, and G729A/B, iLBC, Opus.

Enable Multicast Paging Video	Enables the video feature to establish a multicast paging call. The default setting is disabled.
Multicast Paging Video Codec	Sets the video codec for the multicast paging call. The default setting is “H.264”.
Multicast Paging Image Size	Sets the video image size for the multicast paging call. This list includes 720P, 4CIF, VGA, CIF, QVGA, and QCIF. The default setting is “VGA”.
Multicast Paging Video Bit Rate	Determines the video bit rate for the multicast paging call. The default setting is “256 kbps”.
Multicast Paging Video Frame Rate	Configures the video frame rate for the multicast paging call. This list includes “15 frames/second”, “25 frames/second”, “30 frames/second”, and “Variable frames rate”.
Multicast Paging H.264 Profile Type	Specifies the H.264 codec profile type for the multicast paging call. This list includes “Baseline Profile”, “Main Profile”, and “High Profile”. **Note**: Lower profile is easier to decode, while higher profile has higher compress rate. Usually, use Baseline profile for low CPU Performance device, and choose high profile for video conference.
Multicast Paging H.264 Payload Type	Determines the H.264 codec payload type for the multicast paging call. The default setting is “99”.
Multicast Listening	
• **Priority** • **Listening Address** • **Label**	Configures the IP address and port number for monitoring multicast paging call. When the initiator initiates a call, answer the call, and display listening address and tag of the monitoring target. This feature supports Video Multicast, when the initiator initiates Video Multicast, it will automatically add the number 2 on the port of the listening address. Reboot the phone to make changes take effect. The valid IP address range is from 224.0.0.0 to 239.255.255.255. Users may also fill the label for each listening address corresponding to priority.

Network Settings Page Definitions

Network Settings/Ethernet Settings

Ethernet Settings	
Preferred Internet Protocol	If IPv4 is selected, the phone will be using IPv4 addressing, otherwise, it will be using IPv6 addressing. Default is Prefer IPv4.
Different Networks for Data and VoIP Calls	Configures whether to set up different networks for the phone data and the call. If set to "Yes", you need to configure the data network and VoIP network, respectively. **Note:** This setting needs reboot to take effect.

Network Configuration of Data	
IPv4	
IPv4 Address Type	Users could select "DHCP", "Static IP" or "PPPoE". • **DHCP**: Obtain IP address via a DHCP server in the LAN. All domain values for static IP/PPPoE are unavailable, even though the values have been saved in the flash. • **PPPoE:** Configures PPPoE account/password. Obtain the IP address from the PPPoE server via dialing. • **Static IP:** Manually configures IP Address, Subnet Mask, Default Router's IP Address, DNS Server 1, and DNS Server 2. By default, it is set to "DHCP".
DHCP VLAN Override	Selects the DHCP Option VLAN mode. When set to "DHCP Option 132 and DHCP option 133", the phone will get DHCP option 132 and 133 as VLAN ID and VLAN priority. When set to "Encapsulated in DHCP Option 43", the phone will get values from Option 43 which encapsulate VLAN ID and VLAN priority. **Note**: Please make sure the "Allow DHCP Option 43 and Option 66 to Override Server" setting under maintenance→upgrade is checked. The default setting is " DHCP Option 132 and DHCP option 133 ".
Host name (Option 12)	Sets the name of the client in the DHCP request. It is optional but may be required by some Internet Service Providers.
Vendor Class ID (Option 60)	Configures the vendor class ID header in the DHCP request. The default setting is Grandstream GXV3370.
IP Address	Defines the phone’s static IP address if the static IP is used.
Subnet Mask	Determines the network’s subnet mask if the static IP is used.
Default Gateway	Defines the network’s gateway address if the static IP is used.
DNS Server 1	Configures the primary DNS IP address if the static IP is used.
DNS Server 2	Configures the secondary DNS IP address if the static IP is used.
PPPoE Account ID	Configures the PPPoE account ID if the PPPoE is used.
PPPoE Password	Sets the PPPoE password if the PPPoE is used.
Layer 2 QoS 802.1Q/VLAN Tag (Ethernet)	Assigns the VLAN Tag of the Layer 2 QoS packets for Ethernet. The Default value is 0. **Note:** When **Different Networks for Data and VoIP Calls** set to Yes, then this option will be applied for Data.
Layer 2 QoS 802.1p Priority Value (Ethernet)	Assigns the priority value of the Layer 2 QoS packets for Ethernet. The Default value is 0. The setting needs reboot to take effect. **Note:** When **Different Networks for Data and VoIP Calls** set to Yes, then this option will be applied for Data.

IPv6	
IPv6 Address	Configures the appropriate network settings on the phone. Users could select from "Auto-configured" or “Statically configured”.
Static IPv6 Address	Enter the static IPv6 address in "Statically configured" IPv6 address type.
IPv6 Prefix Length	Enter the IPv6 prefix length in "Statically configured" IPv6 address type. Default is 64.
DNS Server 1	Enter DNS Server 1 when static IP is used.
DNS Server 2	Enter DNS Server 2 when static IP is used.
Preferred DNS Server	Enter the Preferred DNS server.
Network Configuration of VoIP Calls	
IPv4	
IPv4 Address Type	Users could select "DHCP" or "Static IP". • **DHCP**: Obtain IP address via a DHCP server in the LAN. All domain values for static IP/PPPoE are unavailable, even though the values have been saved in the flash. • **Static IP:** Manually configures IP Address, Subnet Mask, Default Router's IP Address, DNS Server 1 and DNS Server 2. By default, it is set to "DHCP".
IP Address	Defines the phone’s static IP address if the static IP is used.
Subnet Mask	Determines the network’s subnet mask if the static IP is used.
Default Gateway	Defines the network’s gateway address if the static IP is used.
DNS Server 1	Configures the primary DNS IP address if the static IP is used.
DNS Server 2	Configures the secondary DNS IP address if the static IP is used.
Layer 2 QoS 802.1Q/VLAN Tag (Ethernet) for VoIP Calls	Assigns VLAN Tag of Layer 2 QoS packets (Ethernet) for VoIP. The default value is 0.
Layer 2 QoS 802.1p Priority Value (Ethernet) for VoIP Calls	Assigns the priority value of Layer 2 QoS packets (Ethernet) for VoIP Calls. The default value is 0. The setting needs reboot to take effect.
802.1x Mode	
802.1x mode	Enables and selects the 802.1x mode for the phone system. The supported 802.1x modes are: **EAP-MD5, EAP-TLS, EAP-PEAP** The default setting is "Disable".
802.1x Identity	Enters the identity information for the selected 802.1x mode. (This setting will be displayed only if 802.1 X mode is enabled).
802.1x Secret	Enters the secret for the 802.1x mode. This option will appear when 802.1x mode is EAP-MD5 or EAP-PEAP.
CA Certificate	Uploads the CA Certificate file to the phone. (This setting will be displayed only if the 802.1 X mode is enabled)

Client Certificate	Loads the Client Certificate file to the phone. (This setting will be displayed only if the 802.1 X TLS mode is enabled)
Private Key	Loads the private key file to the phone. (This setting will be displayed only if the 802.1 X TLS mode is enabled)

Network Settings/Wi-Fi Settings

Wi-Fi Basics	
Wi-Fi Function	Enables/disables the Wi-Fi feature. The default setting is "Disable".
Wi-Fi Band	Configures the Wi-Fi frequency band from the list: • 2.4G • 5G • 2.4 G & 5G Default setting is 2.4G & 5G.
ESSID	Permits to scan and select the available Wi-Fi networks within the range if the Wi-Fi feature is enabled. Click on "Select" to select the Wi-Fi network to connect to. The ESSID will be auto filled in the ESSID filed.
Add Network	
ESSID	Configure the hidden ESSID name.
Security Mode for Hidden SSID	Defines the security mode used for the wireless network when the SSID is hidden. Default is “None”.
Password	Determines the password for the selected Wi-Fi network.
Advanced Settings	
Layer 2 QoS 802.1p Priority Value (Wi-Fi)	Assigns the priority value of the Layer 2 QoS packets for Wi-Fi. The Default value is 0.
Country Code	Configure Wi-Fi country code. The default value is "United States of America". **Note:** Reboot is required to take effect.

Note: Since firmware version 1.0.3.36, Wi-Fi settings can be restricted from WEB UI as well as from LCD screen. This can only be configured via config template. When P22038=0, the Wi-Fi settings are neither accessible from web UI nor from LCD. To enable Wi-Fi on web UI and LCD screen, use P22038=1.

Network Settings/OpenVPN® Settings

Enable OpenVPN®	This enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server. The default setting is No. NOTE: To use OpenVPN® functionalities, users must enable OpenVPN® and configure all 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 "VPN" for the "Nat Traversal" (under Account-> Network Settings).
Enable OpenVPN® Comp-lzo	Enables OpenVPN® 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	The URL/IP address for the OpenVPN® server.
OpenVPN® Port	The network port for the OpenVPN® server. By default, it is set to 1194.
OpenVPN® Transport	Determines network protocol (UDP or TCP) used for OpenVPN®. Default is UDP.
OpenVPN® CA	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device. The file will not be uploaded if it is not in the correct format.
OpenVPN® Client Certificate	OpenVPN® Client certificate file (*.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device. The file will not be uploaded if it is not in the correct format.
OpenVPN® Client Key	The OpenVPN® Client key (*.key) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device. The file will not be uploaded if it is not in the correct format.
OpenVPN® Cipher Method	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Available options are: “Blowfish”, “AES-128” or “AES-256”. Default is “Blowfish”.
OpenVPN® Username	OpenVPN® authentication username (optional).
OpenVPN® Password	OpenVPN® authentication username (optional).

Network Settings/Advanced Network Settings

Advanced Network Settings	
DNS Refresh Timer (m)	Configures the refresh time (in minutes) for DNS query. If set to "0", the phone will use the DNS query TTL from DNS server response. Default value is 0.
DNS Failure Cache Duration (m)	Configures the duration (in minutes) of previous DNS cache when DNS query fails. If set to "0", the feature will be disabled. Note: Only valid for SIP registration. Default value is 0.
IPv4 Preferred DNS1 Server	This fields sets the preferred DNS server for the user.

IPv4 Preferred DNS2 Server	This fields sets the second preferred DNS server for the user.
Enable LLDP	Enables the LLDP (Link Layer Discovery Protocol) feature on the phone system. If it is set to "Yes", the phone system will broadcast LLDP PDU to advertise its identity and capabilities and receive same from a physical adjacent layer 2 peer. The default setting is "Yes".
LLDP TX Interval (s)	Configures the interval the phone sends LLLD-MED packet. The default setting is 30s.
Enable CDP	Configures whether to enable CDP to receive and/or transmit information from/to CDP-enabled devices. The default setting is "Yes".
Layer 3 QoS for SIP	Defines the Layer 3 packet's QoS parameter for SIP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is 26 it is equivalent to the DSCP name constant AF31.
Layer 3 QoS for Audio	Defines the Layer 3 packet's QoS parameter for RTP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is 46 it is equivalent to the DSCP name constant EF.
Layer 3 QoS for Video	Defines the Layer 3 packet's QoS parameters for H.264 messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is 34 it is equivalent to the DSCP name constant AF41.
HTTP/HTTPS User-Agent	Sets the user-agent for phonebook and screen saver.
SIP User-Agent	Sets the user-agent for SIP.
Separate Ethernet & Wi-Fi Traffic	Configures whether to separate Ethernet & Wi-Fi traffic. If enabled, VoIP calls are forced to use Ethernet, and other application data preferentially use Wi-Fi.
Maximum Transmission Unit (MTU)	Configures the MTU in bytes. The MTU must be set according to the needs. The range is form 576 to 1500. **Note:** If MTU is set to less than 1280, IPv6 may not take effect.
PC Port Mode	
PC Port Mode	Enables and defines the PC port mode. If it is set to "Mirrored", the traffic in the LAN port will go through PC port as well and packets can be captured by connecting a PC to the PC port. The default setting is "Enabled".
PC Port VLAN Tag	Defines the VLAN Identifier of the Layer 2 frame for PC port. This adds the VLAN tag value on the target address received from the LAN port of the phone then sends the value to the device connected to the PC port. **Note**: VLAN tag value on the device connected to the PC port should be the same as the VLAN tag value assigned to the PC port here.
PC Port Priority Value	Determines the Priority Code Point within a Layer 2 frame header for PC

	port.
Proxy	
HTTP/HTTPS Proxy Hostname	Configures the HTTP/HTTPS proxy URI of the network. Some of networks requires going through a proxy to access to the Internet. The default setting is keeping this field blank.
HTTP/HTTPS Proxy Port	Configures the HTTP/HTTPS proxy port number of the network. Some of networks requires going through a proxy to access to the Internet. The default setting is keeping this field blank.
Bypass Proxy For	Defines the specific URI that the phone can directly access to without HTTP/HTTPS proxy. If it is filled, the phone will bypass the proxy to send the packets to the specific URI. The default setting is filed blank.

Network Settings/Affinity Settings

Affinity Support	Configures whether to enable the Affinity feature. Note: The Affinity CTI function can only be used when the phone has a registered account. This option is disabled by default.
Preferred Account	Selects SIP account for Affinity.

System Settings Page Definitions

System Settings/Time and Language

Time Settings	
Assign NTP Server Address	Defines the URL or IP address of the NTP server. The phone may obtain the current date and time information from the server. The default setting is “pool.ntp.org”.
DHCP Option 42 override NTP server	Obtains NTP server address from a DHCP server using DHCP Option 42; it will override configured NTP Server. If set to “No”, the phone will use configured NTP server to synchronize time and date even if an NTP server is provided by DHCP server. The default setting is "Yes".
DHCP Option 2 to override Time Zone setting	Obtains time zone setting (offset) from a DHCP server using DHCP Option 2; it will override selected time zone. If set to “No”, the phone will use selected time zone even if provided by DHCP server. The default setting is Yes.
Time Zone	Specifies the local time zone for the phone. It covers the global time zones and user can selected the specific one from the drop-down list.
Self-defined Time Zone	This parameter allows the users to define their own time zone. The syntax is: **std offset dst [offset], start [/time], end [/time]** Default is set to: **MTZ+6MDT+5,M4.1.0,M11.1.0** **MTZ+6MDT+5**

	This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east. **M4.1.0,M11.1.0** The 1st number indicates Month: 1,2,3.., 12 (for Jan, Feb, .., Dec) The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…) The 3rd number indicates weekday: 0,1,2,..,6(for Sun, Mon, Tues, … ,Sat) Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.
Time Display Format	Specifies which format will be used to display the time. It can be selected from 12-hour and 24-hour format.
Date Display Format	Determines which format will be used to display the date. It can be selected from the drop-down list. • Normal (M/DD/YYYY): 1/31/2012 • YYYY/MM/DD: 2012/01/31 • MM/DD/YYYY: 01/31/2012 • DD/MM/YYYY: 31/01/2012 The default setting is MM/DD/YYYY.
Language	
Language	Sets the language to display on the phone's LCD.

System Settings/Security Settings

Web/SSH Access	
Enable SSH	Enables SSH access to the phone. Default setting is “Yes”.
SSH Port	Customizes SSH port. Valid range: 1 – 65535. Default is 22.
Access Method	Determines which protocol will be used to access the phone ‘s Web GUI. It can be selected from HTTP and HTTPS. The default setting is HTTP.
Port	Specifies which port to use to access the phone ‘s Web UI. By default, if HTTP, the port number will be 80; if HTTPS is selected, the port number will be 443.
Web Access Control	Configures Web access control by using Whitelist or Blacklist on incoming IP addresses. Default setting is None.
Web Access Control List	Only allow the list of IP addresses as Whitelist, or restrict the list of IP addresses as Blacklist to access Web.
Configuration via Keypad Menu	Configures access control for keypad Menu settings on the Settings interface of the phone.

	• **Unrestricted**: configure all settings on the Settings interface; • **Basic Settings Only**: The Advanced Settings option will not be displayed; • **Basic Settings & Network Settings**: Only the Advanced Settings option will not be displayed • **Constraint Mode**: users need to input admin user password to configure Wireless & Network and Advanced Settings. **Note**: When access control for keypad is limited to “Basic Settings Only” or “Constraint Mode”, the Admin authentication will be mandatory to start Factory Reset process.
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 need 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 need to input admin password only when install apps from unknown source, administrator password authentication is required when the user uninstall third-party apps. If set to "**Not allow**", the user cannot install/uninstall third-party apps.
User Info Management	
Current Admin Password	Enter current logged-in user's password. This field is case sensitive. The default password is "admin".
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 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. The default password is “123”.
Confirm New User Password	Enter the new User password again to confirm.
TLS	
Minimum TLS Version	Configures the minimum TLS version supported by the phone.
Maximum TLS Version	Configures the maximum TLS version supported by the phone.
Enable Weak TLS Cipher Suite	Defines the function for weak TLS cipher suites. If set to "Enable Weak TLS Cipher Suites", allow users to encrypt 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.
SIP TLS	
SIP TLS Certificate	Defines the SSL certificate used for SIP over TLS.
SIP TLS Private Key	Defines the SSL Private key used for SIP over TLS.
SIP TLS Private Key Password	Defines the SSL Private key password used for SIP over TLS.
Certificate Management	
CA Certificate	
Import Trusted CA Certificates	Allows to upload the CA Certificate file to phone.
Trusted CA Certificates	Lists trusted CA certificates previously uploaded. Administrator can delete a certificate from here.
User Certificate	
Add Certificate	Allows to upload & Install User Certificate file to phone.
Custom Certificate	
Import Custom Certificate	Allows to upload a Custom Certificate file to phone.
Custom Certificate	Lists trusted Custom Certificate previously uploaded. Administrator can delete a certificate from here.

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 phone. The default setting is "Yes". **Note:** Reboot is required for the setting to take effect
Enable Missed Call Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is missed call on the phone. Default setting is "Yes".
Enable MWI Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is new voicemail on the phone. If it set to “No”, the LED indicator will keep off if the phone system receives SIP NOTIFY message about unread voice mail. The default setting is "Yes".
Enable New Message Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is new message on the phone. Default setting is "Yes".
Enable Contact Full Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when the contact storage or message storage is full. The default setting is "Yes".

Enable Indicator When LCD is Off	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when the LCD screen is off. If it set to “No”, the LED indicator will keep off when the LCD screen is off. The default setting is "Yes".
Screen Timeout	Configures the timeout interval of the LCD backlight. If set to "never", the screen will always stay on. The default value is 3 minutes.
Screensaver Timeout	Configures the screensaver timeout. The default value is 2 minutes
Audio Control	
RJ9 Headset TX Gain (dB)	Configures the Transmission Gain in RJ9 headset channel. It can be selected from the dropdown list. The default setting is 0dB: • -24 • -18 • -12 • -6 • 0 • +6 • +12 • +18 • +24
RJ9 Headset RX Gain (dB)	Configures the Receive Gain in RJ9 headset channel. It can be selected from the dropdown list. The default setting is 0dB: • -9 • -6 • 0 • +6 • +9
3.5mm Earphone TX Gain (dB)	Set the Transmission Gain in 3.5mm earphone headset channel. It can be selected from the dropdown list. The default setting is 0dB: • -24 • -18 • -12 • -6 • 0 • +6 • +12 • +18 • +24
Headset Type	Specifies which type of headset will be connected to the phone system. It can be selected from the dropdown list:

	• Normal Headset • Plantronics EHS If a normal RJ11 headset is connected, it should set to “Normal Headset”. If a Plantronics EHS headset is used, it should set to “Plantronics EHS”.
Enable 3.5mm Headset Control	If set to "Yes", the headset can control the Onhook and Offhook. The default setting is "No".
Handset TX Gain (dB)	Configures the transmission gain of the handset. Default setting is “0dB”. • 0 • -4 • -2 • +2 • +4 • +6
Handsfree TX Gain (dB)	This feature configures the transmission gain for handsfree mode. Default setting is “0dB”. • 0 • -16 • -12 • -8 • -6 • -4 • 0 • +4 • +6 • +8 • +12 • +16
Adjust volume	Configures the volume of ringtone.
Media volume	Configures the volume of media.
Alarm volume	Configures the volume of Alarm.

System Settings/TR-069

Enable TR-069	Sets the phone system to enable the “CPE WAN Management Protocol” (TR-069). The default setting is "No".
ACS URL	Specifies URL of TR-069 ACS (e.g., http://acs.mycompany.com), or IP address.
ACS Username	Enters username to authenticate to ACS.
ACS Password	Enters password to authenticate to ACS.

Periodic Inform Enable	Sends periodic inform packets to ACS. Default is “No”.
Periodic Inform Interval (s)	Configures to sends periodic “Inform” packets to ACS based on specified interval.
Connection Request Username	Enters username for the ACS to connect to the phone.
Connection Request Password	Enters password for the ACS to connect to the phone.
Connection Request Port	Enters the port for the ACS to connect to the phone.
CPE Cert File	Uploads Cert File for the phone to connect to the ACS via SSL.
CPE Cert Key	Uploads Cert Key for the phone to connect to the ACS via SSL.

Maintenance Page Definitions

Maintenance/Upgrade

Firmware	
Upgrade via Manual Upload	
Complete Upgrade	If enabled, all files will be replaced except user data. Default is disabled.
Upload Firmware File to Update	Allows users to load the local firmware to the phone to update the firmware.
Upgrade via Network	
Firmware Upgrade Mode	Allows users to choose the firmware upgrade method: TFTP, HTTP, HTTPS, or Manual Upload. The default setting is "HTTP".
Firmware Server Path	Sets IP address or domain name of firmware server. The URL of the server that hosts the firmware release. Default is "fm.grandstream.com/gs". Administrators are now able to configure variables in the provisioning server URL. Currently, the following variables are supported in the provisioning server URL: • **$PN:** is used to identify the directory name of the provisioning server directory where the corresponding boot files and configuration files are located. • **$MAC:** is used to identify the MAC address of the IP phone. Variables $PN and $MAC can be embedded in server URL setting in Web UI and in DHCP Option 66. **Example (Web UI):** 192.168.0.2/$PN/$MAC **Example (DHCP Option 66):** tftp://192.168.0.2/$PN/$MAC $PN will be replaced with phone model, e.g., GXV3370 $MAC will be replaced with phone's MAC address, e.g., 000b829a8ffe
HTTP/HTTPS Username	Enters the username for the firmware HTTP/HTTPS server.
HTTP/HTTPS Password	Enters the password for the firmware HTTP/HTTPS server.
Firmware File Prefix	Checks if firmware file is with matching prefix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
Firmware File Postfix	Checks if firmware file is with matching postfix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
Firmware Upgrade	Click the "**Update**" button to check whether the firmware in the firmware server has an updated version, if so, update immediately.
Config File	
Configure Manually	

Download Device Configuration	Click to download the device configuration file in .txt format.
Upload Device Configuration	Upload configuration file to the phone.
Configure via Network	
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**", then users can manually configure the path and update mode for the configuration file server.
Config Upgrade Via	Selects provisioning method: TFTP, HTTP or HTTPS. Default setting is "HTTPS".
Config Server Path	Sets IP address or domain name of configuration server. The server hosts a copy of the configuration file to be installed on the phone. Default is "fm.grandstream.com/gs". Administrators are now able to configure variables in the provisioning server URL. Currently, the following variables are supported in the provisioning server URL: • **$PN:** is used to identify the directory name of the provisioning server directory where the corresponding boot files and configuration files are located. • **$MAC:** is used to identify the MAC address of the IP phone. Variables $PN and $MAC can be embedded in server URL setting in Web UI and in DHCP Option 66. **Example (Web UI):** 192.168.0.2/$PN/$MAC **Example (DHCP Option 66):** tftp://192.168.0.2/$PN/$MAC $PN will be replaced with phone model, e.g., GXV3370 $MAC will be replaced with phone's MAC address, e.g., 000b829a8ffe
HTTP/HTTPS Username	Configures the username for the config HTTP/HTTPS server.
HTTP/HTTPS Password	Configures the password for the config HTTP/HTTPS server.
Always Perform HTTP Basic Authentication	Configures whether to send basic HTTP authentication information to the server when downloading firmware, config file or GUI customization file. If enabled, the phone will always send HTTP/HTTPS username and password even if the server didn't request authentication. If disabled, the phone will only send HTTP/HTTPS username and password when the server requires authentication. Default is No.

Config File Prefix	Checks if configuration files are with matching prefix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
Config File Postfix	Checks if configuration files are with matching postfix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
Authenticate Conf File	Sets the phone system to authenticate configuration file before applying it. When set to "Yes", the configuration file must include value P1 with phone system's administration password. If it is missed or does not match the password, the phone system will not apply it. The default setting is "No".
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file is using OpenSSL.
Download Device Configuration	Downloads the phone's configuration file in text format. The config file includes all the P value parameters for phone's current settings except password for security purpose. Users can use the Grandstream configuration file generator to generate binary config file from this text file.
Upload Device Configuration	Uploads configuration file to the phone. The file will not be uploaded if it is not in the correct format. **Note**: The GXV3370 supports only txt format for config file upload.
Start Provision	Press to trigger the device to fetch configuration file from server configured under the Config server Path. The same button is located on LCD screen under Settings → System Update.
GUI Customization File	
Configure Manually	
Upload GUI Customization File	Uploads GUI customization file from web UI manually.
Configure via Network	
GUI Customization File Download Mode	Selects download method: TFTP, HTTP or HTTPS. Default setting is "HTTPS".
GUI Customization File URL	Sets IP address or domain name of the GUI customization file server. The server hosts a copy of the file to be installed on the phone. The Default setting is **fm.grandstream.com/gs**.
GUI Customization File HTTP/HTTPS Username	Enters the username for the firmware HTTP/HTTPS server.
GUI Customization File HTTP/HTTPS Password	Enters the password for the firmware HTTP/HTTPS server.
Use Configurations of	Retrieve and download customization file with the configuration of the

Config File Server	config file.
Provision	
Automatic Upgrade	
Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options: • **No**: The phone will only do upgrade once at boot up. • **Check every day**: User needs to specify "Hour of the day (0-23)". • **Check every week**: User needs to specify "Hour of the day (0-23)" and "Day of the week (0-6)". • **Check at a period Time:** User needs to specify "Hour of the day (0-23)" **Note**: Day of week is starting from Sunday. The default setting is "No".
Enable Randomized Automatic Upgrade	Configures whether the phone will upgrade automatically at random time point within the configured period. This option is used for multiple phones upgrade at the same time.
Automatic Upgrade Check Interval (m)	Configures how the phone system will check the server for new firmware and configuration file downloading. It only valid if the user selects "Check at a period of time" in the "Automatic Upgrade". Default setting is 10080 (namely 7 days).
Starting – Ending Hour of the Day (0-23)	Defines at which hour of the day they phone system will check the HTTP/HTTPS/TFTP server for firmware upgrades or configuration files changes.
Day of the Week	Defines which day of the week the phone system will check the HTTP/HTTPS/TFTP server for firmware upgrades or configuration files changes.
Firmware Upgrade and Provisioning	Defines the phone system's rules for automatic upgrade. It can be selected from: • Always Check at bootup • Always Check at bootup, when F/W pre/suffix changes, • Skip the Firmware Check. The default setting "Always Check at bootup".
Upgrade with Prompt	If set to "No", the phone will automatically start upgrading after downloading the firmware file. Otherwise, users would need to confirm in the prompted message on the LCD screen to start upgrading process. The default setting is "Yes".
Config Provision	

Download and Process All Available Config Files	By default, the device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, and cfg.xml (corresponding to device specific, model specific, and global configs). If set to "Yes", the device will download and apply (override) all available configs in the order of cfgMAC, cfg.xml, cfgMODEL.xml, cfgMAC.xml. Default Setting is “No”.
Config Provision	Device will download the configuration files and provision by the configured order.
DHCP Option	
Allow DHCP Option 43, 160 and 66 Override Server	If DHCP option 43, 160 and 66 is enabled on the LAN side, the device will reset the CPE, upgrade, network VLAN tag, and priority configuration according to option 43 sent by the server. At the same time, the update mode and server path of the configuration upgrade mode will be reset according to the option 160 and 66 sent by the server. Default is "Yes".
DHCP Option 120 Override SIP Server	Configures the phone system to allow the DHCP offer message to override the Config Server Path via the Option 120 header. Default setting is "Yes".
Allow DHCP Option 242 (Avaya IP Phones)	Enables DHCP Option 242. Once enabled, the phone will use the configuration info issued by the local DHCP in Option 242 to configure proxy, transport protocol and server path. The default setting is “Yes”.
PNP Feature	
Enable PNP Feature	Enables the PNP (Plug and Play) feature on the device. If it is enabled, the device will be set as a provision server to send SIP NOTIFY message including the provision URL to response the client phone’s SIP SUBSCRIBE request. This feature will be enabled if the PNP URL is configured. If this setting is enabled, the 3CX Auto provision will be disabled automatically.
PNP URL	Configures the URL to provision another client phone’s config server path. The URL will be included in the SIP NOTIFY message.
PnP(3CX) Auto Provision	Sets the phone system to broadcast the SIP SUBSCRIBE message during booting up to allow itself to be discovered and be configured by the SIP platform. The default setting is "Yes".
Advanced Settings	
Enable SIP NOTIFY Authentication	Enables the phone to challenge SIP NOTIFY with 401. The default setting is “Yes”.
Validate Certification Chain	Configures whether to validate the server certificate when download the firmware/config file. If it is set to "Yes", the phone will download the firmware/config file only from the legitimate server. Default setting is "No".

Enable EEE Mode	Enable/disable EEE mode. If set to "Yes", the phone will turn on the EEE mode. Note: Regardless of whether the EEE mode is turned on or off, the network will reconnect.
mDNS Override Server	Sets the phone system to broadcast the Multicast DNS (mDNS) message during booting up to allow itself to be discovered and be configured by the SIP platform. If it is set to “User Type A’, the phone system will broadcast the MDNS message “A_grandstream-cfg.local”; if it is set to “Use Type SRV”, the MDNS message will be “SRV_grandstream-cfg.local”. The default setting is “Use Type A”.
Factory Reset	Resets the phone system to the default factory setting mode. If the “Clear the SD card” is checked, the SD card storage mounted on the phone will be format as well.
Safe Mode	Configures enable/disable safe mode. If enabled, the phone 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 applications will be disabled

Maintenance/System Diagnosis

Syslog	
Syslog Protocol	Select the transport protocol over which log messages will be carried. • **UDP:** Syslog messages will be sent over UDP. • **SSL/TLS:** Syslog messages will be sent securely over TLS connection. To upload server CA certificate, follow below steps: ✓ Copy CA file in SD card and plug it to the phone. ✓ Go to LCD menu **Settings→Security Settings→Install from SD card** to install the CA file.
Syslog Server	Configures the URI which the phone system will send the syslog messages to. The default setting is "log.ipvideotalk.com".

Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet: • **DEBUG** (Sent or received SIP messages). • **INFO** (Product model/version on boot up, NAT related info, SIP message summary, Inbound and outbound calls, Registration status change, negotiated codec, Ethernet link up). • **WARNING** (SLIC chip exception). • **ERROR** (SLIC chip exception, Memory exception). **Note**: Changing syslog level does not require a reboot to take effect.
Syslog Keyword Filter	Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to “SIP” to filter SIP log.
Logcat	
Clear Log	Clears the log files saved in the phone system.
Log Tag	Configures the filter to display the specified process log file.
Log Priority	Selects the log priority to display. It can be selected from list below: • Verbose (Default Setting) • Debug • Info • Warning • Error • Fatal • Silent (suppress all output)
Get Log	Displays the log file on the web page.
Debug	
One-click Debugging	
One-click Debugging	Capture the checked info in the debugging list, click "Start" to debug if including "Capture trace" item and click "Stop" to end. Click "Capture" in another situation. All retrieved files will be generated to a package, and the last package will be overwritten, while the trace file will stay remain.
Debug Info Menu	Display a list of info items that can be debugged, currently supports system logs, info log, capture package, tombstones and ANR log. The captured data can be viewed in "Debug information list". The default is all selected.
Debug Info List	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.

View Debug Info	You can select the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
Core Dump	
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	Selects the existing core dump file in the drop-down box. Users could delete the file by pressing on “Delete” button.
View Core Dump	Press “List” button to view all existing core dump files. The files are listed in chronological order, users could click the file name to download the file to the local computer.
Record	
Record	Click to start capturing audio data, click the "Stop" button to end. To capture the audio data of the device can help to locate audio issues. The default is not enabled. You can record up to 1-minute audio data.
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 captured audio data will be sorted by time. Click to download the data to the computer for analysis. Note: The audio data file will be saved under FileManager → Internal Storage → Recfiles folder. Users can also delete files under this folder.
Traceroute	
Target Host	The IP address or URL for the Target Host of the Traceroute. Press **Start** to send traceroute request to configured target host. Press **Stop** to end traceroute running process.

Maintenance/Event Notification

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

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

Bootup Completed	Configures the event URL when phone boots up.
Incoming Call	Configures the event URL when phone has an incoming call.
Outgoing Call	Configures the event URL when phone has an outgoing call.
Offhook	Configures the event URL when the phone is off hook.
Onhook	Configures the event URL when the phone is on-hook.
Missed Call	Configures the event URL when the phone has new a missed call.
Connected	Configures the event URL when a call is established.
Disconnected	Configures the event URL when a call is disconnected.
DND On	Configures the event URL when DND is enabled.
DND Off	Configures the event URL when DND is disabled.
Forward On	Configures the event URL when the forward feature is enabled on the phone.
Forward Off	Configures the event URL when the forward feature is disabled on the phone.
Blind Transfer	Configures the event URL when users transfer a call with blind transfer on the phone.
Attended Transfer	Configures the event URL when users transfer a call with attended transfer on the phone.
On Hold	Configures the event URL when users hold a call on the phone.
UnHold	Configures the event URL when users resume a call on the phone.
Log On	Configures the event URL when users log on the phone successfully.
Log Off	Configures the event URL when users log off the phone.
Register	Configures the event URL when an account in the phone is registered successfully.
Unregister	Configures the event URL when an account in the phone is unregistered.

Application Page Definitions

Applications/Programmable key

Programmable key	
Format	
Display Format	Configures the display format for the MPK. Users could select "Name", "User ID" or "Name(User ID)". "Name" is the one saved in phone contacts. The default setting is "Name, User ID, Key mode”.
Show Display Name from Server	If selected, the display name on the server will replace the name users configured.
BLF	

Key Mode	The key modes are: • **Speed Dial**: Press to dial the UserID when the accounts being configured as VPK. • **Busy Lamp Field**: Monitor the UserID status when the accounts being configured as VPK. • **Call Transfer**: Transfer the current active call to UserID when the accounts being configured as VPK. • **Call Intercom**: Intercom/paging to the UserID when the accounts being configured as VPK. • **Speed Dial via Active Account**: Similar to Speed Dial but it will dial based on the current active account. For example, if the phone is offhook and account 2 is active, it will call the UserID when the accounts being configured as VPK. • **Dial DTMF**: Dial the DTMF digits of the UserID when the accounts being configured as VPK during the call. • **Call Park**: Configure the call park feature code to park or retrieve the call. • **Multicast Paging**: For multicast sending, please fill in the display name in the Settings and fill in the sending address in the multicast address. • **Speed Conference**: Quickly dial up multiple numbers to set up a meeting. • **Dial Prefix:** After configured, once pressed this key, all numbers use this account will automatically add the prefix promptly • **Send URL:** After configured and click on the button, the device will send the entered URL automatically.
Account	Configures the SIP account when the accounts being configured as VPK.
Display Name	Configures the display name when the accounts being configured as VPK.
User ID	Configures the UserID for the corresponding VPK mode when the accounts being configured as VPK.
DTMF Content	When key mode is set to **Dial DTMF** it configures the dialed DTMF content.
Address	When key mode is set to **Multicast Paging**, it configures the multiple broadcast address.
Conference name	Set the name of speed meeting when the key mode is set to **Quick Conference.**
Mute all members	Enable or disable mute all meeting members when key mode is set to

	Quick Conference.
Configure	Configures the Number list when key mode is set to **Quick Conference.**
Programmable key → General Settings	
Enable LCD Turn on Automatically when BLF/SCA status changes	Configures whether to enable LCD turn on automatically when BLF/SCA status changes.
Account	Displays account name if configured, otherwise, displays "Account X" where X is the account number.
BLF Call-pick Prefix	Configures the prefix prepended to the BLF extension if the phone answers a call to the monitored party by the BLF key. Default setting is ** for each account.
Event List URI	Determines the event list BLF URI on the phone to monitor the extensions in the list with MPK keys. This feature is based on BroadSoft standard. It requires filling in the BLF ID to the box. For example, if the server provides the URI: BLF123@myserver.com, this field should be filled with BLF123. Then the monitored extensions will be populated in the MPK app or Extension Board (if supported).
Force BLF Call-pickup by Prefix	Uses the prefix for BLF Call-pickup. The default setting is "No".

System Application/Contacts

General Settings	
Sort Phonebook by	Sets which part of name, first name or last name, will be sorted in alphabetical order to display.
Default Contacts Tab	Controls the behaviors of the phonebook key. It could be set to: • Default • LDAP Search • Local Phonebook • Local Group • Broadsoft Phonebook • Favorites. The default setting is "Default", which set the phonebook key to the Contacts menu.
Emergency Call Numbers	Configures the emergency contact in logout mode. If the system is logout, guest users can dial the configured emergency contacts. Input the number in the input box and click "Add" to add the number to the contacts list. To delete the existing ICE number, select the number in the contacts list

	and click "Delete".
Import/Export Contacts	
Import	
Clear The Old List	Determines if the phone system will delete the previous contacts when a new contact file is imported. If set to "Yes", the previous contacts will be removed. The default setting is "No".
Clear Old History Mode	• If set to "Clear all", the phone will delete all previous records before importing the new records. • If set to "Keep Local Contacts", the new-added local new contacts will not be deleted when importing new records.
Replace Duplicate Items	Configures the phone system to keep the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the phone will replace the original entries to the new one. Otherwise, the phone system will save both contact entries. The default setting is "No".
Replace Duplicate Entries Mode	• If set to "Replace by name", replace the records of the same name automatically when importing new records. • If set to "Replace by number", replace the records of the same number automatically when importing new records.
Keep Associated Account	The feature configures whether to keep the associated account when importing contacts. If enabled, the associated account information in the contact file will be synchronized to the phone
File Encoding	Specifies the encoding format for phonebook file importing. The default setting is UTF-8. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR
File Type	Sets the type format for phonebook file importing. It can be selected from the dropdown list. The default setting is "XML". • XML • vCard
Import Local File	Uploads the contact file from PC to the phone.
Export	

File Encoding	Specifies the encoding format for phonebook file exporting. The default setting is UTF-8. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR
File Type	Sets the type format for phonebook file importing. It can be selected from the dropdown list. • XML • VCard The default setting is "XML".
Export	Downloads the phonebook file from the phone to PC.
Download Contacts	
Clear The Old List	Sets the phone system to delete the previous contacts when a new contact file is downloaded. If "Yes", the previous contacts will be removed. The default setting is "No".
Clear Old History Mode	• If set to "Clear all", the phone will delete all previous records before downloading the new records. • If set to "Keep Local Contacts", the new-added local new contacts will not be deleted when downloading new records.
Replace Duplicate Items	Keeps the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the phone will replace the original entries to the new one. Otherwise, the phone system will save both contact entries. The default setting is "Yes".
Replace Duplicate Entries Mode	• If set to "Replace by name", replace the records of the same name automatically when importing new records. • If set to "Replace by number", replace the records of the same number automatically when importing new records.
Download Mode	Enables the phone system to download phonebook file and select the server and protocol to download the phonebook file. It can be selected from TFTP, HTTP, and HTTPS. The default setting is “OFF”.

Keep Associated Account	The feature configures whether to keep the associated account when importing contacts. If enabled, the associated account information in the contact file will be synchronized to the phone
File Encoding	Selects the encoding format for phonebook file download. The default setting is UTF-8. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR
Download Server	Configures the server URL to download the phonebook file. The phone system will send a request to the server to download the phonebook file with filename ***phonebook.xml***.
HTTP/HTTPS Username	Configures username for HTTP/HTTPS server to download the phonebook file.
HTTP/HTTPS Password	Specifies password for HTTP/HTTPS server to download phonebook file.
Automatic Download Interval	Determines how the phone system to send the request to the server to download the phonebook file. It can be selected from the dropdown list: • None • 5 Minutes • 30 Minutes • 1 Hour • 2 Hour • 4 Hour • 6 Hour • 8 Hour 12 Hour
Download Now	Starts downloading the XML phonebook to the phone immediately.

System Application/LDAP Phonebook

Connection Mode	Selects which protocol will be used for LDAP searching, LDAP or LDAPS.
Server Address	Configures the URI of the LDAP (Lightweight Directory Access Protocol)

	server.
Port	Configures the LDAP server port. The default LDAP port number is 389.

Base DN	Determines the LDAP search base. This is the location in the directory where the search is requested to begin.
	Example:
	dc=grandstream, dc=com
	ou=Boston, dc=grandstream, dc=com

Username	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	Specifies the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
LDAP Name Attributes	Configures the "name" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes. Example: cn sn description
LDAP Number Attributes	Configures the "number" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated number attributes. Example: telephoneNumber telephoneNumber Mobile
LDAP Mail Attributes	Determines the "mail" attributes of each record which are returned in the LDAP search result. Example: mail
LDAP Name Filter	Configures the filter used for name lookups. Examples: (|(cn=%)(sn=%)) returns all records which has the "cn" or "sn" field starting with the entered prefix; (!(sn=%)) returns all the records which do not have the "sn" field starting with the entered prefix; (&(cn=%) (telephoneNumber=*)) returns all the records with the "cn" field starting with the entered prefix and "telephoneNumber" field set.
LDAP Number Filter	Defines the filter used for number lookups. Examples: (|(telephoneNumber=%)(Mobile=%) returns all records which has the "telephoneNumber" or "Mobile" field starting with the entered prefix; (&(telephoneNumber=%) (cn=*)) returns all the records with the "telephoneNumber" field starting with the entered prefix and "cn" field set.
LDAP Mail Filter	Determines the filter used for mail lookups. Example: (mail=%)

Search Field Filter	Configures to filter according to which fields when searching on LDAP. Users can choose between 'Name Filter', 'Number Filter', 'Mail Filter' or 'All Filter'. The default setting is "All Filter".
LDAP Displaying Name Attributes	Configures the entry information to be shown on phone's LCD. Up to 3 fields can be displayed. Example: %cn %sn %telephoneNumber
Max Hits	Specifies the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. Default setting is 50.
Search Timeout (s)	Configures the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 4 seconds.
LDAP Lookup For Dial	Sets the phone system to do the LDAP number searching when making outgoing calls. The default setting is "No".
LDAP Lookup For Incoming Call	Sets the phone system to do LDAP number searching for incoming calls. The default setting is "No".
LDAP Dialing Default Account	Configures the default account that being used when dialing LDAP contact. Users may choose the Account 1-6; the default setting is "Default".

System Application/Recording

File name	Displays the name of the recording file
Duration	Displays the duration of the phone call
Date	Displays the date the call was recorded on
Operation	Delete, Modify, or download the recording file

Value-added Service Page Definitions

Value-added Service/Value-added Service (0/10)

Service Type	Users can set the service type to "Door System" to configure the door system options, or to "DTMF" to set DTMF content to send it during calls.
Door System Type	Set the door system type to "GDS" if the GDS door system is used or set it to "Baudisch" if another door system brand is used. **Note:** Each GDS door system has 2 different access passwords to control 2 doors separately named as [**Related Display Name1**] **&** [**Related Display Name2**] below for door 1 and 2 respectively.
System Number	Specifies the door system number which is the SIP user ID configured on door system or its IP address, if the door system is using IP call. It enables to show open door button when caller number or IP address matches with this setting. e.g:"36311" or "192.168.124.81". **Note:** When set "Door System Type" to "Baudisch" a "configure" button will appear to allow user to configure groups of door system URL and User ID

	for 100 entries. • **System Number:** This is used to configure the User ID of door system. Once configured, only the call from this User ID would use door system while other calls use the default mode. • **System Address:** This is used to input the IP address or URL of the system to identify the call from door system. Users can set HTTP authentication credentials on the URL for Door Systems that require authentication to send HTTP stream. The URL format will be similar to the following: http://username:password@192.168.1.150/goform/stream?cmd=get&channel=4
Display Name	Configures the display name of the door system. When the call matches the configured system number, the name will be displayed on LCD.
Related Display Name1	Configures the name that will be displayed on LCD for door 1 when the call matches the configured **GDS** door system number.
Access password	Determines the door system password which should match the one configured on the used door system settings. In case the GDS is set as 'Door System type' parameter, the password should match the one configured on the **GDS** to open door 1.
Related Display Name2	Indicates the name that will be displayed on LCD for door 2 when the call matches the configured system number.
Access password	The configured password should match the one configured on the GDS to open door 2.
System Ringtone	Allows users to configure the ringtone for the door System. Users can choose different ringtones from the dropdown list.
DTMF Content	Set the DTMF content that is going to be sent when the DTMF button is pressed under Call screen→"Keypad".
Display Condition	Configures whether the DTMF button display on incoming call interface or outgoing call interface.

Value-added Service/General Settings

Display Open Door Button when Calling	Configures whether display Open Door button when there is an incoming call.
Enable Preview	This feature allows user to enable/disable video preview but keep the ringing.

Value-added Service/Broadsoft Settings

Broadsoft Call Features	
Feature Key Synchronization	Synchronizes the BroadSoft standard call feature. If it is enabled, the phone will send SIP SUBSCRIBE message to the

	server and receive SIP NOTIFY message from the server to synchronize the DND, Call Forwarding and Call Center features. The default setting is “Disable”.
Enable BroadSoft Call Park	Configures whether to send SUBSRCIRBE message to BroadSoft server to obtain Call Park notifications. The default setting is “No”.
Conference URI	Configures the network-based conference URI (the BroadSoft Standard). If it is configured, end user needs to tap the N-way key during the conference to transfer the host to the remote media server.
Broadsoft Call Center	When enabled, Feature Key Synchronization will be enabled regardless of web settings. Default is Disabled.
Hoteling Event	Enables BroadSoft Hoteling Event feature. Default is Disabled.
Call Center Status	When set to "Yes", the phone will send SUBSCRIBE to the server to obtain call center status. Default is Disabled.
SCA	
Enable SCA (Shared Call Appearance)	Enables/disables the Shared Call Appearance (the Broadsoft Standard) feature for this account. If it is set to “Yes”, the phone system can update and share account status with another device. The default setting is "No".
Enable Barge-In	Enables/disables the Barge-In feature. If it is set to "Yes", the user could tap the SCA account to barge into an active session with another shared line. The default setting is "No".
Auto-filling CallPark Feature Code	If it is set to "Yes", the configured "Call Park Service Code" will be automatically filled in on the phone's dial pad when picking up the parked call. This option will be active only if "Special Mode" is set to "Broadsoft" and "Enable SCA" is set to "Yes". The default setting is "Yes".
CallPark Feature Code	Configures the pickup feature code for call park. If " Auto-filling CallPark Feature Code " is set to "Yes", this call park service code will be automatically filled in on the phone's dial pad when picking up the parked call. This is used when "Special Mode" is set to "BroadSoft" (from web UI or provisioning) and "Enable SCA" is set to "Yes"
Line Seize Timeout (s)	Defines line-seize expiration timer. For Shared Call Appearance, the phone must send a SUBSCRIBE request for the line-seize event package whenever a user attempts to take the shared line off hook. The default value is 15 seconds. The valid range is from 15 to 60.

Value-added Service/Broadsoft Directories

XSI Service Settings	
Authentication Type	Defines the authentication type in way of login or use SIP. If set to "Login Credentials", please fill in Username and Password in the following options; if set to "SIP Credentials", please fill in Username, User ID, and Password. The default setting is "SIP Credentials".
Server	Configures the BroadWorks XSI server URI. If the server uses HTTPS, please add the header "HTTPS" ahead of the Server URI. For instance, "https://SERVER_URI".
Port	Configures the BroadWorks XSI server port. The default port is 80. If the server uses HTTPS, set to 443.
Action Path	Configures Action path for BroadSoft XSI server.
BroadWorks User ID	Determines the User ID for Broadsoft XSI server.
SIP Authentication ID	Determines username for Broadsoft XSI server.
SIP Authentication Password	Determines password for Broadsoft XSI server.
Login Password	Specifies the password for the BroadWorks XSI query.
BroadSoft Directory & Call Logs Update Interval (s)	Configures the interval to obtain BroadSoft call log and directory data thus to update the matching number data on the dialing interface. Default is 1800 seconds.
BroadSoft Directory Hits	Configures the maximum hits returned from the BroadSoft XSI server directory. The valid range is from 1 to 1000. If set to blank, server's default value will be used.
BroadSoft Directory Order	Defines the BroadSoft directory order displayed on LCD. Select one item and click the Up/Down arrow on the right to adjust the order.
Network Directories	
Group Directory	Enables/disables the BroadWorks XSI Group Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Group" for it
Enterprise Directory	Enables/disables the BroadWorks XSI Enterprise Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Enterprise" for it.
Group Common	Enables/disables the BroadWorks XSI Group Common features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Group Common" for it.

Enterprise Common	Enables/disables the BroadWorks XSI Enterprise Common features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Enterprise Common" for it.
Personal Directory	Enables/disables the BroadWorks XSI Personal Directory features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Personal Directory" for it.
Polycom Phonebook	Enables/disables the BroadWorks XSI Polycom Phonebook features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Polycom Phonebook" for it
Missed Call Log	Enables/disables the BroadWorks XSI Missed Call Log features on the phone. The name filed is used to name the directory. If it keeps blank, the phone system will use the default name "Missed" for it.
Placed Call Log	Enables/disables the BroadWorks XSI Placed Call Log features on the phone. The name filed used to name the directory. If it keeps blank, the phone system will use the default name "Outgoing" for it.
Received Call Log	Enables/disables the BroadWorks XSI Received Call Log features on the phone. The name filed used to name the directory. If it keeps blank, the phone system will use the default name "Incoming" for it.

Value-added Service/BroadSoft IM&P

Login Credentials	
Server	BroadSoft IM&P server address. Usually it is not necessary to configure, and it can already be found in the BroadSoft IM&P username
Port	Specifies the BroadSoft IM&P server port. The default port is 5222.
Username	Determines the Username for the BroadSoft IM&P query. This is usually not the same as BroadSoft account username.
Password	Determines the password for the BroadSoft IM&P query. This is usually not the same as BroadSoft account password.
IM&P Settings	
Enable BroadSoft IM&P	Enables the BroadSoft XMPP feature.
Associated BroadSoft Account	Binds the SIP account for dialing the XMPP client contacts.
Auto Login	Sets the client to be logged automatically if the application is started.
Display Non XMPP Contacts	Determines if the client app will show the non-XMPP contacts.

UPGRADING AND PROVISIONING

The GXV3370 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, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:
firmware.grandstream.com/BETA
fw.mycompany.com

Upgrade and Provisioning Configuration

There are two ways to setup upgrade and provisioning on GXV3370. They are Keypad Menu and Web GUI.

- **Configure via keypad Menu**

  In GXV3370 Settings, select **Advanced → System Update**.

  1. Press **Detect New Version** to initiate upgrade process.

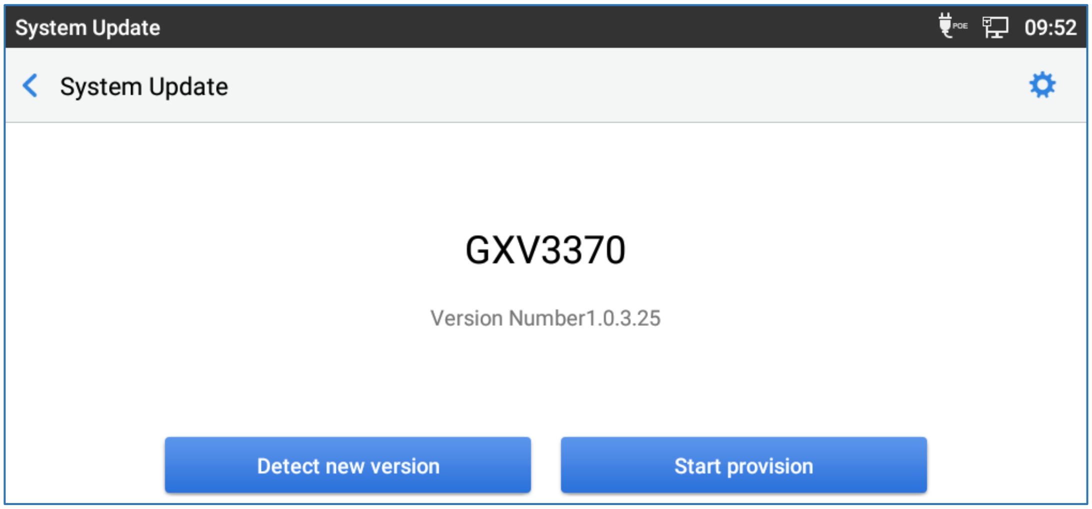
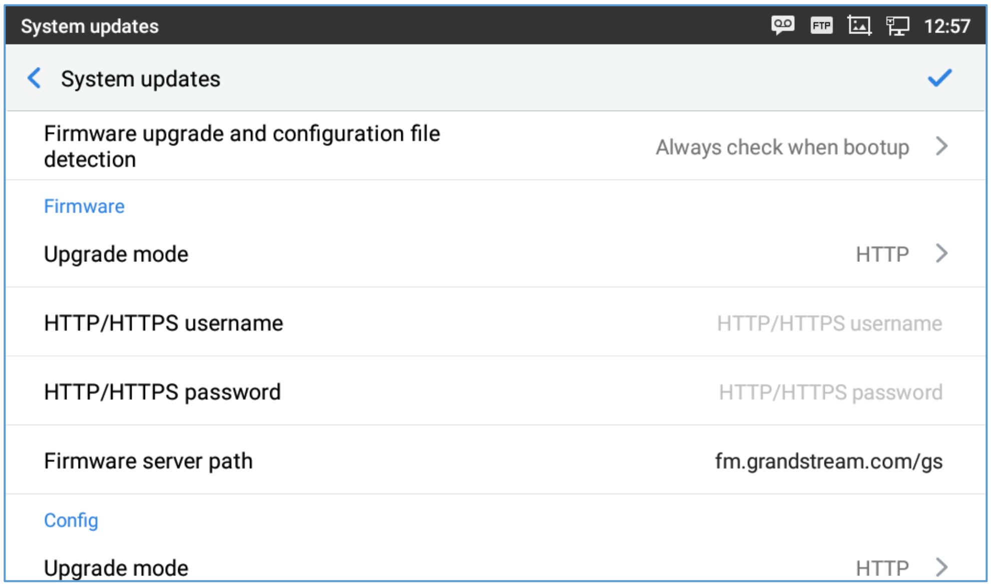


Figure 7: GXV3370 Upgrade – Detect New Version – Start Provision

  2. Press settings icon ⚙ to configure upgrade settings. Users may then select the upgrade mode and enter the IP address or FQDN for the Firmware server and the Config server. After making the changes, tap **Save** button to save the change. Then reboot the phone or go back and press **Detect New Version**.



System updates

Firmware upgrade and configuration file detection: Always check when bootup

Firmware

Upgrade mode: HTTP

HTTP/HTTPS username: HTTP/HTTPS username

HTTP/HTTPS password: HTTP/HTTPS password

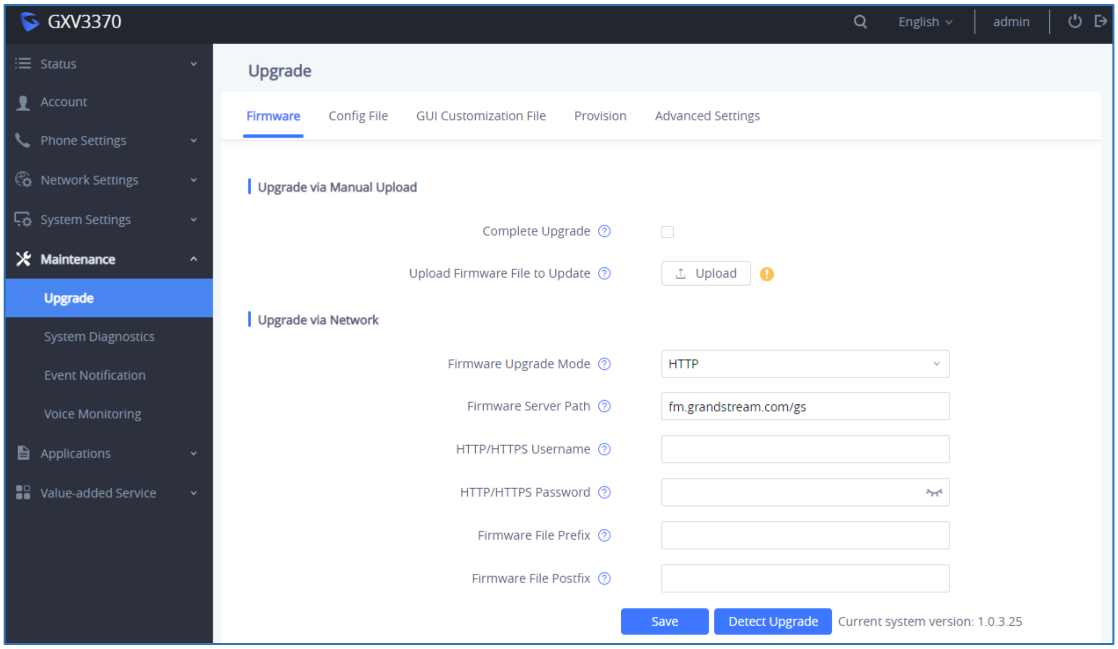
Firmware server path: fm.grandstream.com/gs

Config

Upgrade mode: HTTP

Figure 8: GXV3370 Upgrade Configuration via LCD

- **Configure via Web GUI**
  Open a web browser on PC and enter the IP address for the GXV3370. Then login with the administrator username and password (that needs to be at least 6 characters). Go to **Maintenance → Upgrade**. In the Upgrade web page, enter the IP address or the FQDN for the upgrade server and choose to upgrade via TFTP, HTTP or HTTPS (The default setting is HTTPS). Save and apply the changes, press **Upgrade** button, or reboot the phone to initiate firmware upgrade process.



Upgrade

Upgrade via Manual Upload

Complete Upgrade: □

Upload Firmware File to Update

Upgrade via Network

Firmware Upgrade Mode: HTTP

Firmware Server Path: fm.grandstream.com/gs

HTTP/HTTPS Username:

HTTP/HTTPS Password:

Firmware File Prefix:

Firmware File Postfix:

Current system version: 1.0.3.25

Figure 9: GXV3370 Upgrade Configuration via Web GUI

⚠ **Note:** Please do not power off or unplug the GXV3370 when the upgrading process is on.

Upload Firmware Locally

If there is no HTTP/TFTP server, users could also upload the firmware to the GXV3370 directly via Web GUI. Please follow the steps below to upload firmware to GXV3370 locally.

1. Download the latest GXV3370 firmware file from the following link and save it in your PC.

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

2. Log in the Web GUI as administrator in the PC.
3. Go to Web GUI→**Maintenance→Upgrade**.
4. Click the "Upload" button, a window will be prompted to select firmware file to upload.
5. Select the firmware file from your PC. Then uploading progress will show at the button where it was "Upload" in the above step.
6. When uploading is done, users can see the upgrading process starts on the GXV3370 LCD.
7. The phone will reboot again with the new firmware version upgraded.

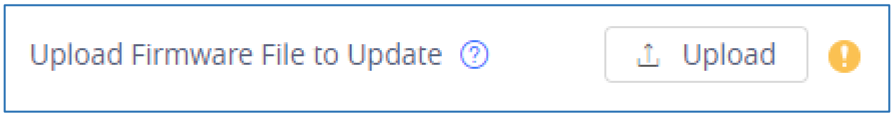


Figure 10: Upload Firmware File to Update

Upgrade via SD Card

For users that could not use remote upgrade or could not access the phone's Web GUI to upload firmware, upgrading via external SD card is an alternative. Follow the steps below to upgrade GXV3370 via SD card.

1. Download the firmware file to PC and save it in SD card.
2. Insert the SD card to GXV3370.
3. Power cycle the GXV3370.
4. Wait for the LED in the upper right of the phone to light up in Green, then about 2 seconds later press the both keys 🔉 (the first LCD key from the left : Volume Down) and ⌂ (the third LCD key from the left : Home) at the same time, it will go into the upgrading process.
5. The GXV3370 will start upgrading and display the upgrading process in the screen.
6. Wait until the upgrading is done.
7. The GXV3370 will reboot itself.
8. Check the firmware status and remove the SD card.

⚠ **Note:** Upgrading via USB storage device is not supported on the GXV3370.

No Local Firmware Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have a TFTP/HTTP/HTTPS server, some free Windows version TFTP servers are available for download from: http://www.solarwinds.com/free-tools/free-tftp-server and http://tftpd32.jounin.net/.
Please check our web site at https://www.grandstream.com/support/firmware for latest firmware.

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 GXV3370 device 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 phone's web configuration interface;
5. Configure the Firmware Server Path to the IP address of the PC;
6. Update the changes and reboot the GXV3370.

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

Provisioning and Configuration File Download

Grandstream SIP Devices can be configured via the Web Interface as well as via a Configuration File (binary or XML) through TFTP or HTTP/HTTPS. The "Config Server Path" is the TFTP, HTTP or 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 particular field in the web configuration page. A parameter consists of a Capital letter P and 2 to 3 (Could be extended to 4 in the future) digit numeric numbers. i.e., P2 is associated with the "Admin Password" in the Web GUI→**System Settings→Security Settings→User Info Management** page. For a detailed parameter list, please refer to the corresponding firmware release configuration template in the following link:
https://www.grandstream.com/support/tools

When the GXV3370 boots up, it will issue TFTP or HTTP request to download a configuration XML file named "cfgxxxxxxxxxxxx" followed by "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If downloading "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file. The configuration file name should be in lower case letters.
For more details on XML provisioning, please refer to the following document:
https://www.grandstream.com/sites/default/files/Resources/gs_provisioning_guide.pdf

Note:

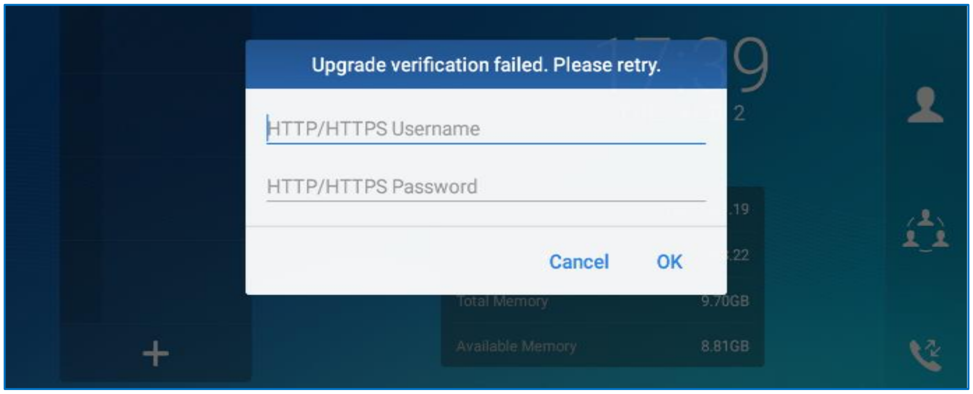
When the prompt in the figure below shows up, it means the firmware/config authentication failed. So the user will be required to check the username/password on device web UI → Maintenance →Upgrade:

Firmware HTTP/HTTPS username

Firmware HTTP/HTTPS password

Config HTTP/HTTPS username

Config HTTP/HTTPS password



Upgrade verification failed. Please retry.

HTTP/HTTPS Username

HTTP/HTTPS Password

Figure 11: Config File Upgrade Verification

FACTORY RESET

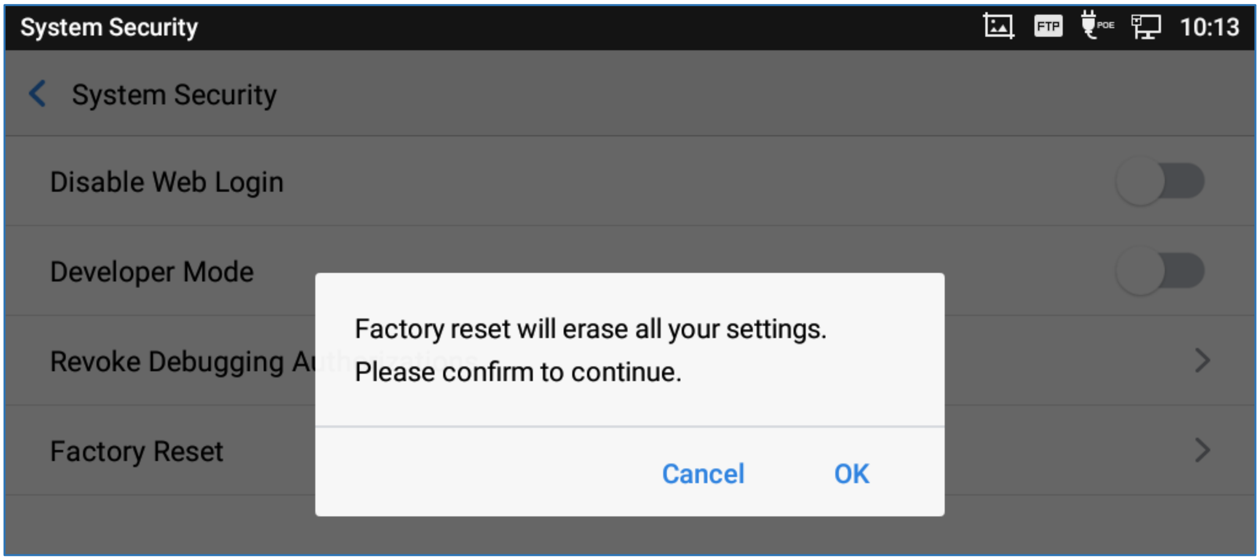
Restore to Factory Default via LCD Menu

⚠ **Warning**:

Restoring the Factory Default Settings will delete all configuration information on the phone. 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.

In order to restore the GXV3370 unit to factory reset via the LCD Menu, please, refer to the following steps:

1. On GXV3370 idle screen, go to **Settings → Advanced → System Security → Factory reset**.
2. Tap on Ok to confirm.



Factory reset will erase all your settings.
Please confirm to continue.

Figure 12: GXV3370 LCD - Confirm Factory Reset

Restore to Factory Default via the Web GUI

1. Login GXV3370 Web GUI and go to **Maintenance → Upgrade → Advanced Settings.**
2. At the bottom of the page, click on the **Reset** button for Factory reset.

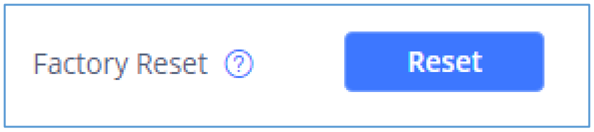
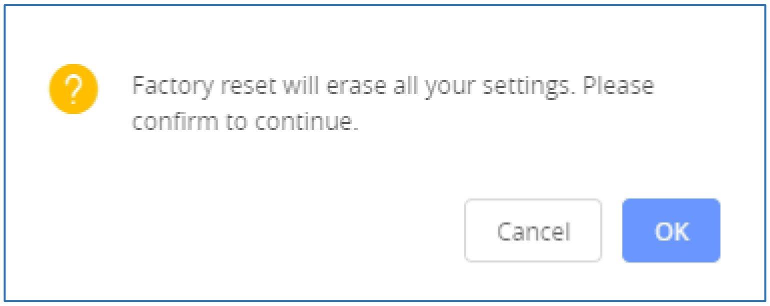


Figure 13: GXV3370 Web GUI - Factory Reset

3. A dialog box will pop up to confirm factory reset.

4. Click OK to restore the phone to factory settings.



Factory reset will erase all your settings. Please confirm to continue.

Figure 14: GXV3370 Web GUI - Confirm Factory Reset

Restore to Factory Default via Hard Keys

For users that could not restore the GXV3370 to factory reset via LCD Menu or the Web GUI, restoring the unit via Hard keys is an alternative. Please, follow the steps below to restore the GXV3370 via Hard Keys:

1. Power cycle the GXV3370.
2. Wait for the LED in the upper right of the phone to light up in Green, then about 2 seconds, press the both keys 🔊+ (the second LCD key from the left: Volume Up) and ☰ (the 4th LCD key from the left : Menu) at the same time, it will go into the factory reset process.
3. The LCD screen will display “Factory reset, please wait”.
4. The GXV3370 will reboot with factory default settings.

SAFE MODE

The GXV3370 allows users to enter safe mode by enabling safe mode option from WEB UI under **Maintenance→Upgrade/Advanced Settings→safe mode**. If enabled, the phone will enter safe mode after rebooting. Users can alternatively enter safe mode by pressing the Menu button ≡ during bootup. Before entering the safe mode, please power cycle the phone and when the plain text "GRANDSTREAM" shows up, immediately press, and hold the Menu button ≡ when the five buttons light up again after the top right LED flash ends. Users will see the phone boot up in safe mode.

Under safe mode, only the system applications will be up and running. Normally safe mode is not needed unless the phone cannot function anymore caused by incompatible 3rd party applications. For example, if a 3rd party application is downloaded and installed on the phone that cause the phone keep crashing or freezing and users cannot operate on the phone's settings, users can enter safe mode to remove the 3rd party application and boot up in normal mode again.

SDK FRAMEWORK SERVICE

The GXV3370 Software Development Kit (SDK) is making it possible for developers and system administrators to run and use API to manage the LCD screen display of the phone and its configuration.

Besides inheriting the Android interface functions, it has added other interfaces according to user's requirements for developing customized services and bring them into effective action on the GXV3370.

Note: SDK framework service is supported starting from firmware 1.0.1.21.

For more information about "SDK Framework Service", please refer to the documentation included in the following SDK package:

https://www.grandstream.com/sites/default/files/Resources/GXV33xx_WP820_SDK_Framework_Service_Guide.zip

EXPERIENCING THE GXV3370 APPLICATION PHONE

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

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

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

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