

Grandstream Networks, Inc.

GRP260x Series - Administration Guide



GRP260x Series - Administration Guide

Thank you for purchasing Grandstream GRP260X Essential IP Phones.

The GRP Series of Essential IP Phones provides simple, easy-to-use devices with zero-touch provisioning for mass deployment and easy management. The four devices in the Essential series are designed to offer simple-to-use, affordable desktop IP Phones with a sleek design and next-generation features. Built for the needs of on-site and remote workers and designed for easy deployment by enterprises, service providers, and other high-volume markets, these essential IP phones offer an easy-to-use and easy-to-deploy voice endpoint.

The following hardware versions do not support firmware downgrade after upgrading to version 1.0.5.37:

- GRP2601(P) hardware version 1.9A
- GRP2602(P) hardware version 1.9A
- GRP2604(P) hardware version 1.7A
- GRP2603P / GRP2604P hardware version 1.5A
- GRP2603P hardware version 1.5B
- GRP2603 / GRP2604 hardware version 1.6B

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the GRP260X phones:

 GRP2601GRP2601PGRP2601W	2 SIP account keys with dual-color LED 4 programmable context-sensitive soft keys. 10/100M network ports. Integrated PoE (for GRP2601P only). 5-way conference. Electronic Hook Switch (EHS) support for Plantronics & Jabra & Sennheiser. Wi-Fi support (GRP2601W only).
--	--



GRP2602GRP2602PGRP2602WGRP2602G

2 SIP account keys with dual-color LED 4 programmable context-sensitive soft keys. 10/100M network ports. (1000M for GRP2602G) Integrated PoE (for GRP2602P/GRP2602G only). 5-way conference. Electronic Hook Switch (EHS) support for Plantronics & Jabra & Sennheiser. Wi-Fi support (GRP2602W only).



GRP2603GRP2603P

3 SIP account keys with dual-color LED. 4 XML programmable context sensitive soft keys 132 x 64 backlit graphical LCD display 10/100/1000 Mbps Ethernet ports. Integrated PoE (GRP2603P only). 5-way conference. Electronic Hook Switch (EHS) support for Plantronics & Jabra & Sennheiser.



GRP2604GRP2604P

3 SIP account keys with dual-color LED. 4 XML programmable context sensitive soft keys 132 x 64 backlit graphical LCD display 10/100/1000 Mbps Ethernet ports. Integrated PoE (GRP2604P only). 5-way conference. Electronic Hook Switch (EHS) support for Plantronics & Jabra & Sennheiser.

GRP260x Features at a glance

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 GRP260X series.

- GRP2601/GRP2601P/GRP2601W Technical Specifications

Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTCP-XR, HTTP/HTTPS, ARP, ICMP, DNS(A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, SNMP, 802.1x, TLS, SRTP, IPV6
Network Interfaces	Dual switched auto-sensing 10/100 Mbps Ethernet ports, integrated PoE (GRP2601P only)
Graphic Display	132 x 48 (2.21") LCD display

Wi-Fi	GRP2601W, Single frequency, 2.4 GHz, 802.11 b/g/n/ax (2.4G only)
Feature Keys	4 XML programmable context sensitive soft keys, 5 (navigation, menu) keys. 8 dedicated function keys for: MESSAGE (with LED indicator), TRANSFER, HEADSET, MUTE, SEND/REDIAL, SPEAKERPHONE, VOL+, VOL
Voice Codec	Support for G.729A/B, G.711?/a-law, G.726, G.722(wide-band), G.723.1 ,iLBC, Opus, in- band and out-of-band DTMF(in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC, AJB
Auxiliary Ports	RJ9 headset jack (allowing EHS with Plantronics & Jabra & Sennheiser headsets)
Telephony Features	Hold, transfer, forward, 5-way conference, call park, call pickup, downloadable phonebook (XML, LDAP, up to 2000 items), call waiting, call log (up to 800 records), off-hook auto dial, auto answer, click-to-dial, flexible dial plan, hot-desking, personalized music ringtones and music on hold, server redundancy and fail-over
Base Stand	Yes, 1 angle positions available
Wall Mountable	Yes, (*wall mount sold separately)
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, SRTP, TLS, 802.1x media access control, secure boot.
Multi-language	LCD Language: English ???? (Simplified Chinese) ?????? (Arabic) Catala (Catalan) Cestina (Czech) Deutsch (German) ???????? (Greek) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ???????? (Korean) Latviesu valoda (Latvian) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Svenska (Swedish) Slovenscina (Slovenian) Slovencina (Slovak) Turkce (Turkish) ?????????? (Ukrainian) ???? (Traditional Chinese) ????? (Marathi) ????? (Hindi) WebUI Language: English ???? (Simplified Chinese) ???????? (Arabic) Cestina (Czech) Deutsch (German) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ???????? (Korean) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Slovenscina (Slovenian) Turkce (Turkish) ???? (Traditional Chinese)
Upgrade/Provisioning	Firmware upgrade via FTP/TFTP / HTTP / HTTPS, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal Power Supply Input 100-240VAC 50-60Hz; Output +5VDC, 600mA; PoE: IEEE802.3af Class 1, 3.84W; IEEE802.3az (EEE) (GRP2601P Only)
Physical	Dimension: 208mm (L) x 180mm (W) x 63.4mm (H) (with handset)Unit weight:650g; Package weight:810g (860g for GRP2601)
Temperature and Humidity	Operation: 0°C to 40°CStorage: -10°C to 60°CHumidity: 10% to 90% Non-condensing
Package Content	GRP2601/2601P phone, handset with cord, base stand, universal power supply (GRP2601 only), network cable, Quick Installation Guide
Compliance	FCC: Part 15 Class B; FCC Part 68 HAC;CE: EN 55032; EN 55035; EN 61000-3-2; EN 61000-3-3; EN 62368-1;RCM: AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004;IC: ICES-003; CS-03;

GRP2601/GRP2601P/GRP2601W Technical Specifications

- GRP2602/GRP2602P/GRP2602W/GRP2602G Technical Specifications

Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTCP-XR, HTTP/HTTPS, ARP, ICMP, DNS(A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE,LLDP, LDAP, TR-069, SNMP, 802.1x, TLS, SRTP, IPV6
---------------------	---

Network Interfaces	Dual switched auto-sensing 10/100 Mbps (1000 Mbps for GRP2602G) Ethernet ports, integrated PoE (GRP2602P/GRP2602G only)
Graphic Display	132 x 48 (2.21") backlit graphical LCD display
Wi-Fi	Yes, Dual band support (GRP2602W only)
Feature Keys	2 SIP account keys with dual-color LED, 4 XML programmable context sensitive soft keys, 5 (navigation, menu) keys. 8 dedicated function keys for: MESSAGE (with LED indicator), TRANSFER, HEADSET, MUTE, SEND/REDIAL, SPEAKERPHONE, VOL+, VOL-
Voice Codec	Support for G.729A/B, G.711u/a-law, G.726, G.722(wide-band), G.723, iLBC, OPUS, in-band, and out-of-band DTMF(in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC
Auxiliary Ports	RJ9 headset jack (allowing EHS with Plantronics & Jabra & Sennheiser headsets)
Telephony Features	Hold, transfer, forward, 5-way conference, call park, call pickup, shared-call-appearance (SCA)/bridged-line-appearance (BLA), downloadable phonebook (XML, LDAP, up to 2000 items), call waiting, call log (up to 800 records), off-hook auto dial, auto answer, click-to-dial, flexible dial plan, hot-desking, personalized music ringtones and music on hold, server redundancy and fail-over
HD audio	Yes, HD handset and speakerphone with support for wideband audio
Base Stand	Yes, 1 angle positions available
Wall Mountable	Yes, (*wall mount sold separately)
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	User and administrator level passwords, MD5 and MD5-session based authentication, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x media access control, secure boot
Multi-language	LCD Language: English (Simplified Chinese) (Arabic) Catala (Catalan) Cestina (Czech) Deutsch (German) (Greek) Espanol (Spanish) Francais (French) (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) (Japanese) (Korean) Latviesu valoda (Latvian) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) (Russian) Svenska (Swedish) Slovenscina (Slovenian) Slovencina (Slovak) Turkce (Turkish) (Ukrainian) (Traditional Chinese) (Marathi) (Hindi) WebUI Language: English (Simplified Chinese) (Arabic) Cestina (Czech) Deutsch (German) Espanol (Spanish) Francais (French) (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) (Japanese) (Korean) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) (Russian) Slovenscina (Slovenian) Turkce (Turkish) (Traditional Chinese)
Upgrade/Provisioning	Firmware upgrade via FTP/TFTP / HTTP / HTTPS, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal Power Supply Input 100-240VAC 50-60Hz; Output +5VDC, 600mA;PoE: IEEE802.3af Class 1, 3.84W; IEEE802.3az (EEE) (GRP2602P Only)
Physical	Dimension: 208mm (L) x 180mm (W) x 63.4mm (H) (with handset)Unit weight: 670g; Package weight:830g (880g for GRP2602)
Temperature and Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Package Content	GRP2602 phone, handset with cord, base stand, universal power supply (GRP2602/GRP2602W only), network cable, Quick Installation Guide
Compliance	FCC: Part 15 Class B; FCC Part 68 HAC;CE: EN 55032; EN 55035; EN 61000-3-2; EN 61000-3-3; EN 62368-1;RCM: AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004;IC: ICES-003; CS-03;

- GRP2603/GRP2603P Technical Specifications

Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTCP-XR, HTTP/HTTPS, ARP, ICMP, DNS(A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, SNMP, 802.1x, TLS, SRTP, IPV6
Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Ethernet ports, integrated PoE (GRP2603P only)
Graphic Display	132 x 64 backlit graphical LCD display
Feature Keys	3 SIP account keys with dual-color LED, 4 XML programmable context sensitive soft keys, 5 (navigation, menu) keys. 9 dedicated function keys for: MESSAGE(with LED indicator), TRANSFER, HOLD, HEADSET, MUTE, SEND/REDIAL, SPEAKERPHONE, VOL+, VOL-
Voice Codec	Support for G7.29A/B, G.711u/a-law, G.726, G.722(wide-band),G723,iLBC, OPUS, in-band, and out-of-band DTMF(in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC
Auxiliary Ports	RJ9 headset jack (allowing EHS with Plantronics & Jabra &Sennheiser headsets)
Telephony Features	Hold, transfer, forward, 5-way conference, call park, call pickup, shared-call-appearance(SCA)/bridged-line-appearance(BLA), downloadable phonebook (XML, LDAP, up to 2000 items), call waiting, call log (up to 800 records), off-hook auto dial, auto answer, click-to-dial, flexible dial plan, hot-desking, personalized music ringtones and music on hold, server redundancy and fail-over
HD audio	Yes, HD handset and speakerphone with support for wideband audio
Base Stand	Yes, 2 angle positions available
Wall Mountable	Yes, (*wall mount sold separately)
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, SRTP, TLS, 802.1x media access control, secure boot
Multi-language	LCD Language: English ???? (Simplified Chinese) ?????? (Arabic) Catala (Catalan) Cestina (Czech) Deutsch (German) ???????? (Greek) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ???????? (Korean) Latviesu valoda (Latvian) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Svenska (Swedish) Slovenscina (Slovenian) Slovencina (Slovak) Turkce (Turkish) ?????????? (Ukrainian) ????? (Traditional Chinese) ?????? (Marathi) ????? (Hindi) WebUI Language: English ???? (Simplified Chinese) ???????? (Arabic) Cestina (Czech) Deutsch (German) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ?????????? (Korean) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Slovenscina (Slovenian) Turkce (Turkish) ????? (Traditional Chinese)
Upgrade/Provisioning	Firmware upgrade via FTP/TFTP / HTTP / HTTPS, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal Power Supply Input 100-240VAC 50-60Hz; Output +5VDC, 600mA;PoE: IEEE802.3af Class 1, 3.84W; IEEE802.3az (EEE) (GRP2603P Only)
Physical	Dimension: 214mm (L) x 206mm (W) x 68mm (H) (with handset)Unit weight: 780g; Package weight: 1090g for GRP2603P &1140g for GRP2603
Temperature and Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Package Content	GRP2603 phone, handset with cord, base stand, universal power supply (GRP2603 only), network cable, Quick Installation Guide

Compliance	FCC: Part 15 Class B; FCC Part 68 HAC;CE: EN 55032; EN 55035; EN 61000-3-2; EN 61000-3-3; EN 62368-1;RCM: AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004;IC: ICES-003; CS-03;
------------	---

GRP2603/GRP2603P Technical Specifications

- GRP2604/GRP2604P Technical Specifications

Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTCP-XR, HTTP/HTTPS, ARP, ICMP, DNS(A record, SRV, NAPTR), DHCP, PPPoE, SSH, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, SNMP, 802.1x, TLS, SRTP, IPV6
Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Ethernet ports, integrated PoE (GRP2603P only)
Graphic Display	132 x 64 backlit graphical LCD display
Feature Keys	3 SIP account keys with dual-color LED, 4 XML programmable context sensitive soft keys, 5 (navigation, menu) keys. 9 dedicated function keys for: MESSAGE(with LED indicator), TRANSFER, HOLD, HEADSET, MUTE, SEND/REDIAL, SPEAKERPHONE, VOL+, VOL-
Voice Codec	Support for G.729A/B, G.711u/a-law, G.726, G.722(wide-band),G723,iLBC, OPUS, in-band, and out-of-band DTMF(in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC
Auxiliary Ports	RJ9 headset jack (allowing EHS with Plantronics & Jabra & Sennheiser headsets)
Telephony Features	Hold, transfer, forward, 5-way conference, call park, call pickup, shared-call-appearance(SCA)/bridged-line-appearance(BLA), downloadable phonebook (XML, LDAP, up to 2000 items), call waiting, call log (up to 800 records), off-hook auto dial, auto answer, click-to-dial, flexible dial plan, hot-desking, personalized music ringtones and music on hold, server redundancy and fail-over
HD audio	Yes, HD handset and speakerphone with support for wideband audio
Base Stand	Yes, 2 angle positions available
Wall Mountable	Yes, (*wall mount sold separately)
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, SRTP, TLS, 802.1x media access control, secure boot
Multi-language	LCD Language: English ???? (Simplified Chinese) ?????? (Arabic) Catala (Catalan) Cestina (Czech) Deutsch (German) ???????? (Greek) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ???????? (Korean) Latviesu valoda (Latvian) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Svenska (Swedish) Slovenscina (Slovenian) Slovencina (Slovak) Turkce (Turkish) ?????????? (Ukrainian) ???? (Traditional Chinese) ????? (Marathi) ????? (Hindi) WebUI Language: English ???? (Simplified Chinese) ???????? (Arabic) Cestina (Czech) Deutsch (German) Espanol (Spanish) Francais (French) ????? (Hebrew) Hrvatski (Croatian) Magyar (Hungarian) Italiano (Italian) ??? (Japanese) ???????? (Korean) Nederlands (Dutch) Polski (Polish) Portugues (Portuguese) ???????? (Russian) Slovenscina (Slovenian) Turkce (Turkish) ???? (Traditional Chinese)
Upgrade/Provisioning	Firmware upgrade via FTP/TFTP / HTTP / HTTPS, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal Power Supply Input 100-240VAC 50-60Hz; Output +5VDC, 600mA;PoE: IEEE802.3af Class 2, 3.84W-6.49W; IEEE802.3az (EEE) (GRP2604P Only)
Physical	Dimension: 208mm (L) x 180mm (W) x 63.4mm (H) (with handset)Unit weight: 670g; Package weight:830g (880g for GRP2602)

Temperature and Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Package Content	GRP2604 phone, handset with cord, base stand, universal power supply (GRP2604 only), network cable, Quick Installation Guide
Compliance	FCC: Part 15 Class B; FCC Part 68 HAC;CE: EN 55032; EN 55035; EN 61000-3-2; EN 61000-3-3; EN 62368-1;RCM: AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004;IC: ICES-003; CS-03;

GRP2604/GRP2604P Technical Specifications

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and information for obtaining the best performance with the GRP260X phone.

Equipment Packaging

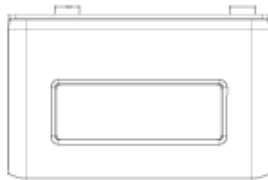
GRP260X
1 x GRP260X Main Case. 1 x Handset. 1 x Phone Stand. 1 x Ethernet Cable. 1 x Power Adapter (Except for GRP260xP). 1 x Phone cord. 1 x Quick Installation Guide.



1x Phone Main Case



1x Handset



1x Phone Stand



1x Ethernet Cable



1x 5V Power adapter
(With GRP260x Only)



1x Phone Cord



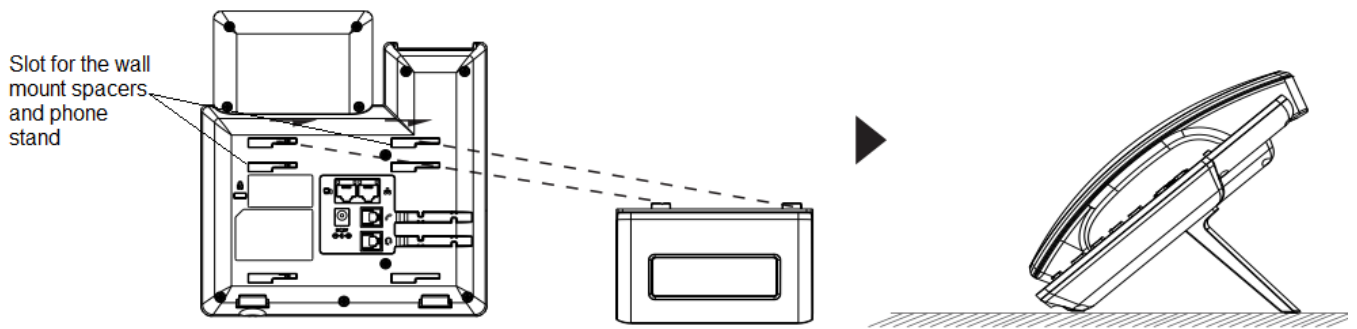
1x Quick Installation Guide

GRP260X Package Content

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

GRP260X Phone Setup

The GRP260X phones can be installed on the desktop using the phone stand or attached to the wall using the slots for wall mounting.



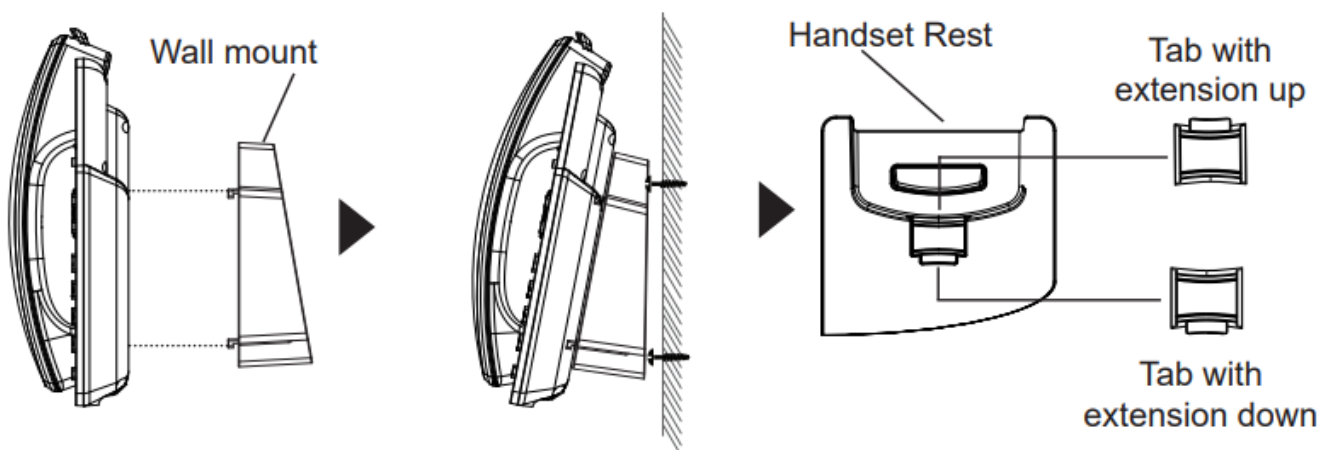
Phone Stand and Mounting Slots on the GRP260X

Using the Phone Stand

For installing the phone on the table with the phone stand, attach the phone stand to the bottom of the phone where there is a slot for the phone stand. (Upper half, bottom part).

Using the Slots for Wall Mounting

1. Attach the wall mount spacers to the slot for wall mount spacers 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 (see figure below).



Tab on the Handset Cradle

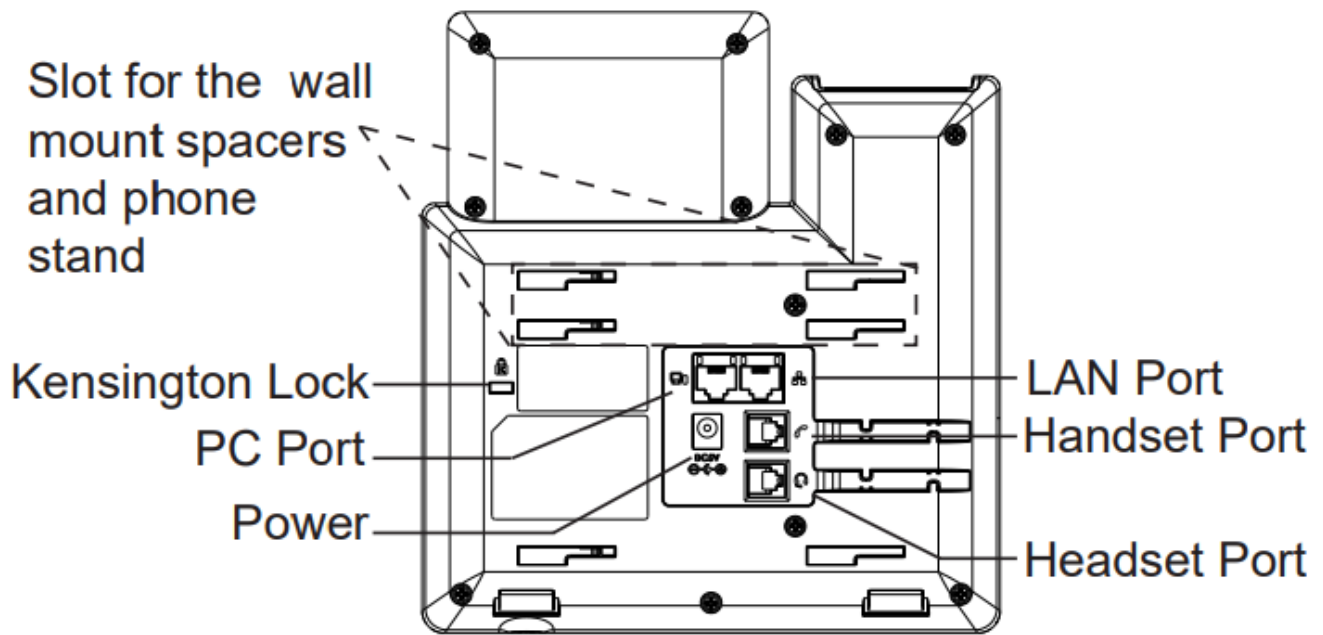
Connecting the GRP260X

To set up the GRP260X, 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 5V DC output plug to the power jack on the phone; plug the power adapter into an electrical outlet. If a PoE switch is used in step 3, this step could be skipped (For GRP260xP/G).
4. The LCD will display the Grandstream logo. Before continuing, please wait for the date/time display to show up.
5. Using the phone-embedded web server or keypad configuration menu, you can further configure the phone using either a static IP or DHCP.

Using Wi-Fi (GRP2602W only):

- On the LCD menu, navigate to "Settings -> Wi-Fi settings" and enable Wi-Fi.
- Select "Wi-Fi Network" and GRP2602W will automatically start scanning within the range.
- A list of Wi-Fi networks will be displayed. Select the desired network, and if required, enter the correct password to connect.
- Users can add and connect to a hidden network by accessing "Wi-Fi" Network" and then pressing on Add softkey softkey_add_blacklist . Then enter the Network's information.
- When the GPR2602W is not connected to any network (including Ethernet and Wi-Fi), a prompt interface will pop up to notify users about it. Users can quickly enter the "Wi-Fi Network" page by pressing on the Wi-Fi softkey.
- For easy deployment, The GRP2602W is preconfigured out of the box to connect to a default SSID named **wp_master** with a password (WPA/WPA2PSK) equal to **wp!987@DMIN**, users can adapt these settings from the web UI as well to make it easier for deployment on customer site.
- The QR code of SSID can be displayed to share with cellphones and other devices.



GRP260X Back Side View

Configuration via Keypad

To configure the LCD menu using the phone's keypad, follow the instructions below:

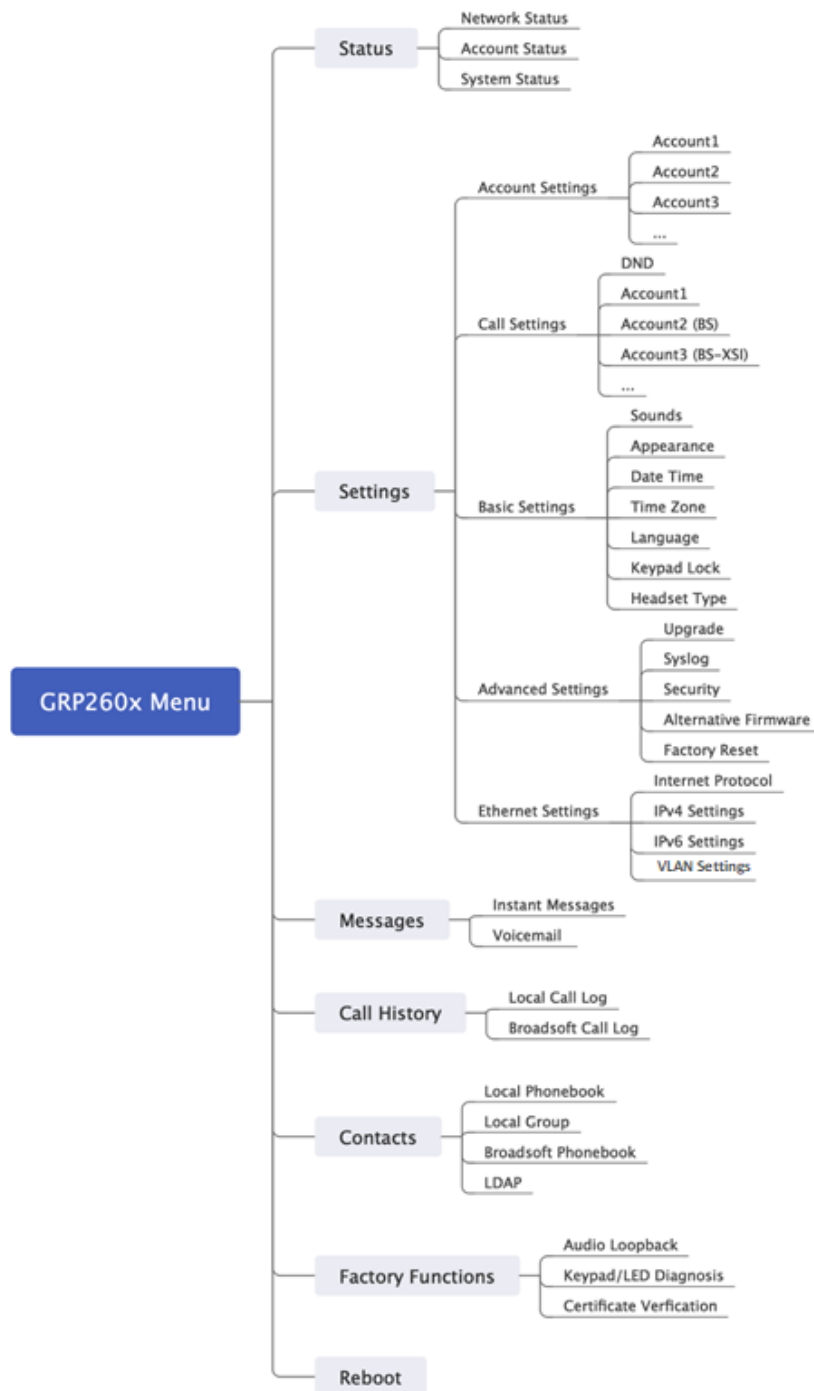
- **Enter MENU options.** When the phone is idle, press the round MENU button or Menu Softkey `idle_softkey_menu` to enter the configuration menu.
- **Navigate to the menu options.** Press the arrow keys UP/DOWN keys to navigate in the menu options.
- **Enter/Confirm selection.** Press the round MENU to enter the selected option.
- **Exit.** Press Return Softkey `softkey_back` to exit to the previous menu.
- **Return to the Home page.**

The MENU options are listed in the following table.

Status	Displays account status, network status, software version number and Hardware: Network status: Press to enter the sub menu for IP setting information (DHCP/Static IP/PPPoE), IPv4 address, IPv6 address, MAC address, Subnet Mask, Gateway, DNS and NTP servers. Account status: Shows Account registration status. System Status: Press to enter the sub menu for Hardware Information, Software version and IP Geographic Information.
--------	---

Settings	Settings sub menu contains the following options: - Account Settings: Enable/Disable SIP account, Configures Account Name, SIP server's address, SIP User ID, SIP Auth ID, SIP Password, Outbound Proxy, and Voice Mail Access Number. - Call Settings: Enable/Disable DND, Enable Disable Auto Answer for SIP account, Enable/Disable Call Forward (Forward All/Busy/No Answer). - Basic Settings: Sounds: Configures account ringtone and adjusts volume settings by pressing left/right arrow key. Appearance: Configures the idle and active LCD brightness. Date and Time: Adjusts Time and Date displaying format. Time Zone: Choose your Time Zone from the list by scrolling with UP/DOWN keys. Language: Selects the language to be displayed on the phone's LCD. Users could select Automatic for local language based on IP location if available. By default, it is Auto. Keypad Lock: Enables/Disables Keypad lock. Users can choose the Keypad Lock type (All Keys/Functional keys) and set up the lock password. If users enabled Keypad lock without configuring a password; They can unlock the phone by pressing on the unlock softkey. Headset Type: Choose the headset type of the headset connect to the phone. Users could choose Normal, Plantronics EHS, Jabra EHS, VBeT EHS, Sennheiser EHS. Softkey bar style: Chooses the corresponding style to show icons , you can choose from four different styles. Input Method: Chooses to set the input method to be one of the following options: 123, abc, ABC, Ab2, and Q9 for both the contact input method and LDAP input method, you can define the input language too. Key Customization: In this option you can set the hotkey settings to be configured for short press setting, long press setting, or reset the hotkey settings, you can also customize the VPKs by choosing the mode of each VPK to be set to Intercom, conference , call park , speed dial, Transfer... - Advanced Settings: Upgrade: Check for upgrade by contacting the firmware upgrade server. Sys Log: Configures Syslog level, Transport protocol and Syslog Server's address. Security: Enables disables Web and SSH access. Alternative Firmware: Press Switch/Convert softkey to switch between the dual firmware versions loaded to the phone. The phone will reboot with the chosen version. Language Download?: Gives you the option to download the chosen language files or restore them from previous firmware versions, you can also set the update to be either manual or automatic , it manual by default. - Ethernet Settings: Internet Protocol: Selects Prefer IPv4 / Prefer IPv6 / IPv4 only or IPv6 only. The default setting is "IPv4 only". IPv4 Settings: Selects IP mode (DHCP/Static IP/PPPoE); Configures PPPoE account ID and password; Configures static IP address, Netmask, Gateway, Preferred DNS server IPv6 Settings: Selects IP mode (DHCP/Static IP); Configures static IP address, IPv6 Prefix (64 bits), IPv6 Preferred DNS server. VLAN Settings: Enables CDP/LLDP, Configures LLDP TX interval, Enables Manual VLAN Configuration, Configures Layer 2 QoS 802.1q (VLAN ID/Priority). Reset Network settings: Resets the network configuration - Wi-Fi Settings (GRP2602W only): Wi-Fi: Enables/disables Wi-Fi. Wi-Fi Band: Choose Wi-Fi band (2G , 5G or 2G&5G). Wi-Fi Network: Scans and displays available Wi-Fi networks.
Messages	Instant Messages: Displays received instant messages Voicemail: Displays voicemail message information in the following format: Normal/Urgent
Call History	Displays Local Call Logs: "All" Calls / "Missed" Calls/ "Dialed" Calls/ "Answered" Calls.
Contacts	Contacts sub menu includes the following options: Local Phonebook Local Group LDAP User could configure phonebooks/groups options here, download phonebook XML to the phone and search and dial from the local phonebook and search and dial from LDAP phonebook.
Factory Functions	Factory Functions sub menu includes the following options: Audio Loopback: Speak to the phone using speaker/handset/headset. If you can hear your voice, your audio is working fine. Press Return Softkey to exit audio loopback mode. Keypad/Led Diagnosis: All LEDs will light up Press all the available keys on the phone. The LCD will display the name for the keys to be pressed to finish the keyboard diagnostic mode. Press Hook button to exit. Certification Verification: Verify the certificate loaded on the phone.
UCM Detect	Configures the IP address and port of the UCM on which the IP phone can be registered.
Factory reset	Performs a Factory reset on the phone.
Reboot	Reboots the phone.

The following picture shows the keypad MENU configuration flow:



GRP260x LCD settings

Users can also leverage the **numeric keys** and assign them different functions by pressing the key for **3 seconds** and selecting the **Mode** and **Value**. The **supported modes** are: Speed Dial, Speed Dial via Active Account, Dial DTMF, Voicemail, Call Return, LDAP Search, Call History, INFO, Messages, DND, Redial, Open Door, Provision, and HTTP Command.

Configuration via Web Browser

The GRP260X embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the IP phone through a Web browser such as Google Chrome, Mozilla Firefox, and Microsoft's IE. To access the Web GUI:

1. Connect the computer to the same network as the phone.
2. Make sure the phone is turned on and shows its IP address. You may check the IP address by pressing the Up-arrow button when the phone is in an idle state.
3. Open a Web browser on your computer.
4. Enter the phone's IP address in the address bar of the browser.
5. Enter the administrator's login and password to access the Web Configuration Menu.

The computer must be connected to the same sub-network as the phone. This can be easily done by connecting the computer to the same hub or switch as the phone is connected. In the absence of a hub/switch (or free ports on the hub/switch), please connect the computer directly to the PC port on the back of the phone.

If the phone is properly connected to a working Internet connection, the IP address of the phone will display in MENU→Status→Network Status. This address has the format: xxx.xxx.xxx.xxx, where xxx stands for a number from 0-255. Users will need this number to access the Web GUI. For example, if the phone has an IP address of 192.168.40.154, please enter "http://192.168.40.154" in the address bar of the browser.

There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed
End User Level	user	123 or unit label password	Only Status and Basic Settings
Administrator Level	admin	admin or unit label password	Browse all pages

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

Saving Configuration Changes

After users make changes to the configuration, pressing the "Save" button will save but not apply the changes until the "Apply" button on the top of the web GUI page is clicked. Or users could directly press the "Save and Apply" button.

Rebooting from Remote Locations

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

ADVANCED FEATURES

When **Special Feature** is set to **Zoom** under **Accounts -> Accounts -> Advanced Settings -> Advanced Features**, the phone supports a variety of Zoom Phone features that enhance call handling, collaboration,

and user flexibility. These features enable advanced call management capabilities such as shared lines, call monitoring, call parking, and hot desking, allowing organizations to streamline communications and improve productivity. The following sections provide an overview of the Zoom Phone features supported on Zoom-enabled phones.

SLA/SLG on Zoom Phones

Zoom Phones support **SLA** (Shared Line Appearance) and **SLG** (Shared Line Group) features, enabling users and administrators to share calling responsibilities, phone numbers, and voicemail access across multiple extensions and devices.

Shared Line Appearance (also known as Call Delegation) provides an easy way for phone users to assign others to handle calls on their behalf. For example, an executive can assign calling privileges to an assistant, allowing the assistant to make and receive calls on the executive's behalf.

Shared Line Group allows Zoom Phone administrators to share a phone number and extension with a group of phone users or common area phones. All members of the shared line group have access to the group's direct phone number and voicemail. Administrators can also apply business, closed, and holiday hours, as well as configure call routing rules for the group.

This feature is only available on Zoom-enabled phones. For details, please refer to the Zoom SLA and SLG Configuration Guide.

Call Monitoring and Privacy Mode on Zoom Phones

Zoom Phones support **BMWT** (Barge-In/Listen/Whisper/Takeover), a call monitoring and intervention feature that allows authorized users to supervise active calls and, when necessary, participate in or take control of them. Additionally, authorized users can monitor or intervene in active calls through configured softkeys.

In addition, Privacy Mode can be enabled to prevent unauthorized monitoring or intervention from other members in the call group while the call is in progress.

The following BMWT options are supported:

- **Barge-in:** Join an active call as an additional participant.
- **Listen:** Listen to an active call without any parties being aware.
- **Whisper:** Speak privately to the monitored extension without other parties being aware.
- **Takeover:** Replace the monitored extension and take full control of the active call.

This feature is only available on Zoom-enabled phones. For details, please refer to the Zoom BMWT and Privacy Mode Configuration Guide.

Call Park on Zoom Phones

Zoom Phones support **Call Park**, allowing users to place calls on hold and retrieve them from another phone or Zoom client using a retrieval code.

When a call is parked, Zoom Phone generates a retrieval code that can be used by another phone user to resume the call. Administrators can configure routing rules for unanswered parked calls. Public call park locations are accessible to all users, while private call park locations can be restricted based on administrator-defined permissions.

This feature is only available on Zoom-enabled phones. For details, please refer to the Zoom Call Park Configuration Guide

Hot Desking on Zoom Phones

Zoom Phones support **Hot Desking**, allowing users to temporarily sign in to a provisioned desk phone using

their extension number and PIN.

This feature enables users to access their phone number, extension, and voicemail from different desk phones without requiring a dedicated device. It is particularly useful in shared workspaces, rotating shifts, multi-office deployments, and other environments where users frequently change work locations.

Use case examples:

- **Out-of-office or traveling employees:** Users can enable Hot Desking on their desk phone, allowing other users to temporarily sign in and use the device.
- **Shared office or co-working space:** Users can share the same phone hardware while retaining access to their own extension, phone number, and voicemail.
- **Traveling sales or field teams:** Users can sign in to any Hot Desk phone at different office locations while maintaining a single phone number and extension.
- **24/7 call centers:** Shift workers can share the same desk phone while keeping separate extensions, phone numbers, and voicemail boxes.

This feature is only available on Zoom-enabled phones. For details, please refer to the Zoom Hot Desking Configuration Guide.

CONFIGURATION GUIDE

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

- **Status:** Displays the Account status, Network status, and System Info of the phone.
- **Account:** To configure the SIP account.
- **Phone Settings:** To configure phone general settings, Call Settings, Ringtone, and Multicast Paging.
- **Network Settings:** To configure network settings.
- **Programmable keys:** Configures idle and call screen softkeys And the Multi-purpose keys settings for the GRP2604 only.
- **System Settings:** Configures Time and Language settings, Security Settings, Preferences, TR-069.
- **Maintenance:** To configure upgrading and provisioning, System Diagnostics, Outbound Notifications, and Voice monitoring.
- **Application:** Configures Web Service settings, Contacts, LDAP, and Call History.
- **External Service:** Configures GDS Settings, Call Center, BroadSoft XSI.

Status Page Definitions

Status -> Account Status	
Account	Displays the account index. For GRP2601/GRP2601P: 2 SIP accounts For GRP2602/GRP2602P/GRP2602W: 4 SIP accounts For GRP2603/GRP2603P: 6 SIP accounts For GRP2604/GRP2604P: 6 SIP accounts
SIP User ID	Displays the configured SIP User ID for the account.
SIP Server	Displays the configured SIP Server address, URL or IP address, and port of the SIP server.
SIP Registration	Displays SIP registration status for the SIP account.
Status -> Network Status	
Ethernet	
LAN Port	Displays the LAN port connection status and link speed.
PC Port	Displays the PC port connection status.

MAC Address	Displays the device's unique hardware identifier in hexadecimal format. The MAC address is used for provisioning and is printed on the label inside the original box and on the back of the device.
PPPoE Link Up	Displays the PPPoE connection status.
IPv4	
IPv4 Address Type	Displays the configured address type, such as DHCP, Static IP or PPPoE.
IPv4 Address	Displays the IPv4 address obtained on the phone.
Gateway	Displays the gateway address obtained on the phone.
IPv4 NAT Type	Displays the IPv4 NAT type.
IPv6	
IPv6 Address Type	Displays the configured IPv6 address type, such as Auto-configured or Statically configured.
Global Unicast Address	Displays the global unicast IPv6 address assigned to the phone.
Link-Local Address	Displays the IPv6 link-local address assigned to the phone.
IPv6 Static Gateway	Displays the static IPv6 gateway address.
IPv6 DUID	Displays the DHCP Unique Identifier (DUID) used to identify the phone for DHCPv6.
IPv6 NAT Type	Displays the IPv6 NAT type.
DNS & NAT	
DNS Server	Displays the DNS server addresses configured or obtained by the phone.
DNS Mode	Displays the DNS Mode configured for each account.
NAT Traversal	Displays the type of NAT connection configured for each account.
Status -> System Info	
Information	
Product Model	Displays the product model of the phone.
Part Number	Displays the product part number.
Serial Number	Displays the serial number of the phone.
Certificate Type	Displays the encryption and hashing protocols used in the certificates.
Security Version	Displays the version of the security software.
Software Version	Displays the software version numbers for the following components: Boot: Boot version number. Core: Core version number. Base: Base version number. Prog: Program version number. This is the main firmware release number, which is always used for identifying the software system of the phone. Locale: Locale version number.
IP Geographic Information	Displays the following information determined based on the phone's IP address: Language: Language determined based on the phone's IP address. Recommend Time Zone: Recommended time zone detected based on the IP address.
System Time	Displays the following system time information: System Up Time: Time elapsed since the last reboot. System Time: Current system time. System Time Zone: Configured time zone.
System Information	Downloads the system information file.
Status	
Service Status	Displays memory information for gui, phone, cpe, and avs services.
User Space	Displays the percentage of User Space Used and the Database Status.

Core Dump	Provides options to manually generate GUI, AVS, CPE, and Phone core dump files and displays the Core Dump status.
Special Feature	OpenVPN(R) Support: Indicates whether the phone supports OpenVPN(R).
Status -> Call Status	
Record x	Displays the call status and call quality information for each record. To enable this page, navigate to Maintenance -> Voice Monitoring -> Display Report and enable Display Report on Web UI. This setting is enabled by default. The page provides the following information: Start Time: Start time of the call. End Time: End time of the call. Basic Info: Caller, callee and their extension numbers, IP addresses, ports, and codecs. Overview: Graphical representations of call quality and network quality. Quality: Graphical representations of audio quality metrics, including jitter, delay, and packet loss, along with the MOS-LQ (Listening Quality Mean Opinion Score) and MOS-CQ (Conversational Quality Mean Opinion Score) ratings.
Status -> Call Feature Status	
Call Feature Status	Displays the status of call features for each account and provides access to the configuration page for each feature by clicking the arrow icon next to it. The page provides the following information: Accounts: Account index. DND: Indicates whether Do Not Disturb is enabled or disabled. Auto Answer: Indicates whether automatic call answering is enabled or disabled. Forward All: Extension number configured to receive all forwarded calls. Busy Forward: Extension number configured to receive calls when the account is busy. Delay Forward: Extension number configured to receive calls when they are not answered within the specified time.

Account Page Definitions

Accounts -> Account x	
General Settings	
Account Register	
Account Active	Enables or disables the account.Disabled by default.
Account Name	Configures the account name displayed on the LCD (e.g., MyCompany).
SIP Server	Configures the URL or IP address and port of the SIP server provided by the VoIP service provider (e.g., sip.mycompany.com).
Secondary SIP Server	Configures the URL or IP address and port of the secondary SIP server, which is used when the primary SIP server fails.
Tertiary SIP Server	Configures the URL or IP address and port of the tertiary SIP server, which is used when both the primary and secondary SIP servers fail.
Outbound Proxy	Configures the IP address or domain name of the primary outbound proxy, media gateway, or Session Border Controller (SBC). The outbound proxy is used for firewall or NAT traversal in different network environments. If symmetric NAT is detected, STUN will not work, and an outbound proxy is required.
Secondary Outbound Proxy	Configures the IP address or domain name of the secondary outbound proxy, which is used when the primary outbound proxy cannot be reached.
SIP User ID	Configures the user account information, provided by your VoIP service provider.
SIP Authentication ID	Configures the SIP authentication ID used to authenticate the subscriber. It can be identical to or different from the SIP User ID.
SIP Authentication Password	Configures the password used to authenticate the account with the SIP server before registration. After saving, the password is hidden for security purposes.

Name	Configures the SIP subscriber name displayed as the Caller ID (e.g., John Doe). This setting optional.
TEL URI	Configures the use of the tel: URI scheme in SIP requests. The available options are: User=Phone: Attaches the "user=phone" parameter to the Request-URI and To header to indicate an E.164 number. Used when the phone has an assigned PSTN telephone number. Enabled: Uses "tel:" instead of "sip:" in SIP requests. Disabled: The default setting is "Disabled"
Voicemail Access Number	Configures the access code (e.g., *97) dialed to access voicemail by pressing the MESSAGE button. This is usually the voicemail portal access number.
Monitored Voicemail Access Number	Configures the access code (e.g., *98) used to access the voicemail box of a monitored extension. When a Voicemail VPK/MPK is configured with a target extension, the phone dials this access code followed by the target extension number (e.g., *981001).
BLF Server	Configures the optional BLF server used for SUBSCRIBE requests. This setting optional.
Account Display	Selects the account information displayed on the LCD. When set to "Username", the LCD displays the Username if it is not empty. When set to "User ID", the LCD displays the User ID if it is not empty. The default setting is "Account Name".
UCM User Password	Configures the UCM user password used to login to UCM and allow the user to access the UCM User Portal directly through the phone's Web UI under Accounts -> UCM.
Network Settings	
DNS Mode	Defines how the phone resolves the IP addresses of server hostnames. The available options are: A Record SRV NAPTR/SRV Use Configured IP The default setting is "A Record".Note: If "Use Configured IP" is selected, configure Primary IP, Backup IP 1, and Backup IP 2.
DNS SRV Failover Mode	Configures the preferred IP mode for DNS SRV when DNS Mode is set to "SRV" or "NAPTR/SRV". The available options are: Default: The phone will try to send REGISTER messages to one IP address at a time, and the process will repeat. Use current server until DNS TTL: The phone will send REGISTER messages to the previously registered IP address first. If there is no response, it will try each IP address one at a time. This behavior continues until the DNS TTL (time-to-live) expires. Use current server until no responses: The phone will send REGISTER messages to the previously registered IP address first. This behavior continues until the registered server does not respond. Use current server until failback timer expires: The phone will send all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires. The default setting is "Default".
Failback Timer (m)	Specifies the duration, in minutes, after failover to the current SIP server or Outbound Proxy before attempting to fail back to the primary SIP server or Outbound Proxy. This parameter applies when DNS Mode is set to "SRV" or "NAPTR/SRV" and DNS SRV Failover Mode is set to "Use current server until failback timer expires".The default setting is "60".
Register Before DNS SRV Failover	Enables or disables sending REGISTER requests to the failover SIP server or Outbound Proxy before sending INVITE requests in the event of a DNS SRV failover.Disabled by default.
Primary IP	Configures the primary IP address to which the phone sends DNS queries when "Use Configured IP" is selected for DNS Mode.
Backup IP 1	Configures the first backup IP address to which the phone sends DNS queries when "Use Configured IP" is selected for DNS Mode.
Backup IP 2	Configures the second backup IP address to which the phone sends DNS queries when "Use Configured IP" is selected for DNS Mode.

Maximum Number of SIP Request Retries	Specifies the maximum number of times the phone retries sending SIP requests to the server. In DNS SRV configuration, if the destination does not respond, requests are resent to the same address according to the configured retry count. The default setting is "2". The valid range is 1 to 10.
NAT Traversal	Configures whether the NAT traversal mechanism is activated. The available options are: Set to "No" if an Outbound Proxy is used. Set to "Auto" to automatically determine the NAT traversal method. Set to "STUN" if a STUN server is configured. The phone will route according to the STUN server. If the NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the phone will try to use public IP addresses and port numbers in all SIP and SDP messages. "STUN" cannot be used if the detected NAT type is Symmetric NAT. Set to "Keep-alive" to periodically send empty SDP packets to the SIP server to keep the NAT port open. Set to "UPnP" to use UPnP for NAT traversal. Set to "VPN" if OpenVPN is used. The default setting is "Auto".
Media NAT Traversal	Selects the method of NAT traversal for media packets. The available options are: No: NAT media traversal will not be used. Auto: The NAT media traversal method will follow the "NAT traversal (STUN)" logic. STUN: The phone will use the STUN protocol to discover the public IP address and port through a remote STUN server. TURN: The data stream will be forwarded using a TURN relay. ICE: The phone will collect local IP addresses, STUN-reflected addresses and TURN relay addresses to dynamically select the optimal connection path. The default setting is "Auto".
Candidate Type	Configures the ICE candidate type when Media NAT Traversal is set to "ICE". The available options are: All: All address types will be selected. Relay Candidates Only: The candidate addresses will be obtained through a TURN server, which will act as a relay for the media stream. The default setting is "All".
STUN/TURN Server	Configures the STUN/TURN server settings. This option appears when "ICE", "STUN" or "TURN" is selected in Media NAT Traversal.
Support rport (RFC3581)	Enables or disables using symmetric response routing. If enabled, the "rport" field will be added to the Via header field in SIP requests. The phone will extract the information from the SIP 200 OK response to a SIP REGISTER request to rewrite the SIP Contact information and apply it to subsequent SIP requests. Enabled by default.
Proxy-Require	Specifies a SIP extension used to notify the SIP server that the phone is behind a NAT/Firewall.
Use SBC	Enables or disables using a SBC server. If enabled, ensure that an Outbound Proxy is configured. Disabled by default.
SIP Settings	
Basic Settings	
SIP Registration	Enables or disables sending SIP Register messages to the proxy/server. Enabled by default.
UNREGISTER on Reboot	If set to "No", the phone will not unregister the SIP user's registration information before new registration. If set to "All", the SIP Contact header will use "*" to clear all SIP user's registration information. If set to "Instance", the phone only needs to clear the current SIP user's info. The default setting is "No".
REGISTER Expiration	Specifies the frequency, in minutes, in which the phone refreshes its registration with the specified registrar. The default value is "60". The maximum value is 64800 minutes (about 45 days).
SUBSCRIBE Expiration	Specifies the frequency, in minutes, in which the phone refreshes its subscription with the specified registrar. The default value is "60". The maximum value is 64800 minutes (about 45 days).
Re-Register before Expiration	Specifies the time frequency, in seconds, that the phone sends re-registration request before the Register Expiration. The default value is "0". The valid range is 0-64800.
Registration Retry Wait Time	Specifies the interval to retry registration if the process is failed. The default value is 20 seconds. The valid range is 1-3600.

Registration Retry Wait Time(s) upon 403 Forbidden	Specifies the interval, in seconds, to retry registration if the process is failed due to 403 Forbidden. If set to 0, registration retry is disabled. The default setting is "1200". The valid range is 0-3600 in second.
Add Auth Header on Initial REGISTER	Enables or disables adding the Authorization header in initial REGISTER request. Disabled by default.
Add Auth Header on RE-REGISTER	Enables or disables adding the Authorization header in RE-REGISTER request. Enabled by default.
Enable OPTIONS Keep-Alive	Enables or disables sending SIP OPTIONS to track account registration status. If enabled, the phone will send periodic OPTIONS messages to server to track the connection status with the server. Disabled by default.
OPTIONS Keep-Alive Interval	Configures the time interval, in seconds, in which the phone sends OPTIONS message to the server. The default setting is "30" seconds.
OPTIONS Keep-Alive Max Retries	Configures the maximum number of times the phone will try to send OPTIONS message consistently to server without receiving a response. If set to "3", the phone will send OPTIONS message 3 times. If no response from the server, the phone will re-register. The default setting is "3".
SUBSCRIBE for MWI	Enables or disables periodically sending a SUBSCRIBE for Message Waiting Indication. Disabled by default.
SUBSCRIBE for Registration	Enables or disables periodically sending a SUBSCRIBE for Registration. Disabled by default.
Use Privacy Header	Configures whether the "Privacy Header" is present in the SIP INVITE message. The available options are: Default: the phone will add "Privacy Header" when special feature is not "Huawei IMS". Yes: the phone will always add "Privacy Header". No: the phone will not add "Privacy Header". The default setting is "Default".
Use P-Preferred- Identity Header	Configures whether the "P-Preferred-Identity Header" is present in the SIP INVITE message. The available options are: Default: the phone will add "P-Preferred-Identity header" when special feature is not "Huawei IMS". Yes: the phone will always add "P-Preferred-Identity header". No: the phone will not add "P-Preferred-Identity header". The default setting is "Default".
Use X-Grandstream-PBX Header	Enables or disables using X-Grandstream-PBX header in the SIP request. Enabled by default.
Use P-Access-Network-Info Header	Enables or disables using P-Access-Network-Info header in the SIP request. Enabled by default.
Use P-Emergency-Info Header	Enables or disables using P-Emergency-Info header in the SIP request. Enabled by default.
Use P-Asserted-Identity Header	Enables or disables using P-Asserted-Identity Header in the SIP request. Disabled by default.
Use P-Early-Media Header	Enables or disables using P-Early-Media Header in the SIP request. Disabled by default.
Use Zoom E911 X-switch-info SIP Header	Enables or disables using Zoom E911 X-switch-info SIP Header in the SIP request. Disabled by default.
Use Accept-Language Header	Determines whether to include the Accept-Language header field in SIP REGISTER messages and SIP responses to SIP INVITE requests. If set to Disabled, the header field is not included. If set to Auto, the language configured under System Settings -> Time and Language -> Language -> Display Language is used. If set to a specific language, the Accept-Language header field is set to the selected language. The default setting is "Disabled".
Use MAC Header	If Register Only, all outgoing SIP message will include the MAC header. If Yes to all SIP, all outgoing SIP messages will include the MAC header. If No, the phone's MAC header will not be included in any outgoing SIP messages. The default setting is "No".

Add MAC in User-Agent	If Yes except REGISTER, all outgoing SIP messages will include the phone's MAC address in the User-Agent header, except for REGISTER and UNREGISTER. If Yes to All SIP, all outgoing SIP messages will include the phone's MAC address in the User-Agent header. If No, the phone's MAC address will not be included in the User-Agent header in any outgoing SIP messages. The default setting is "No".
SIP Transport	Selects the network protocol used for the SIP transport. The supported protocols are: UDP: A connectionless protocol with no error recovery, used for faster communication. It's commonly used for real-time SIP traffic (e.g., VoIP calls) where low latency is preferred. TCP: A connection-oriented protocol that ensures reliable communication with error-checking and retransmission of lost packets. It's used in environments where message delivery reliability is crucial. TLS/TCP: Combines TCP with encryption for secure SIP communication, ensuring confidentiality and integrity of the messages. It's used for SIP signaling over a secure channel, typically on port 5061. The default setting is "UDP".
Enable TCP Keep-alive	Enables or disables TCP Keep-alive for the TCP connection between the terminal and the SIP server.Enabled by default.
SIP Listening Mode	Configures whether the phone listens to multiple SIP protocols. The available options are: If set to Transport Only, the phone will only listen to the SIP transport protocol selected in SIP Transport. If set to Dual, the phone will listen to TCP when UDP is selected. If set to Dual (Secured), the phone will listen to TLS/TCP when UDP is selected. If "TCP" or "TLS/TCP" is selected, UDP will be listened too. If set to Dual (BLF Enforced), the phone will try to enforce BLF subscriptions to use TCP protocol by adding 'transport=tcp' to the Contact header. The default setting is "Transport Only".
Local SIP Port	Configures the local SIP port used to listen and transmit.The default setting is "5060".
SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport.The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	Enables or disables using the actual ephemeral port in contact with TCP/TLS when TLS/TCP is selected for SIP Transport.Disabled by default.
Support SIP Instance ID	Enables or disables support for SIP Instance ID.Enabled by default.
SIP T1 Timeout	Configures an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2.The default setting is "0.5" seconds.
SIP T2 Timeout	Configures the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value.The default setting is "4" seconds.
Outbound Proxy Mode	Configures whether to put the Outbound Proxy in the Route header, or if SIP messages should always be sent to Outbound Proxy. The available options are: In route Not in route Always send to The default setting is "In route".
Enable 100rel	Enables or disables appending the 100rel tag to the value of the Supported header in initial SIP signaling messages.Disabled by default.
Use Route Set in Notify (Follow RFC 6665)	Enables or disables using route set in NOTIFY (follow RFC 6665). If enabled, the Request URI of the refresh subscription will use the URI in the received NOTIFY Contact (RFC 6665). If disabled, the URI in the previously subscribed 200 OK Contact will be used. Enabled by default.
Session Timer	

Enable Session Timer	Enables or disables the session timer function. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. If enabled, the phone will use the related parameters when sending session timer according to "Session Expiration". If set disabled, session timer will be disabled.Disabled by default.
Session Expiration	Specifies the time, in seconds, after which the session is considered timed out if no successful session refresh transaction occurs.The default setting is "180". The valid range is from 90 to 64800.
Min-SE	Specifies the minimum session expiration time, in seconds.The default value is "90". The valid range is 90 to 64800.
Caller Request Timer	Enables or disables the use of a session timer for outbound calls when the remote party supports session timers.Disabled by default.
Callee Request Timer	Enables or disables the use of a session timer for inbound calls when the remote party supports session timers.Disabled by default.
Force Timer	Enables or disables the use of the session timer when the remote party does not support this feature. If enabled, the phone will use the session timer even if the remote party does not support it. Otherwise, the session timer is enabled only when the remote party supports it.Disabled by default.
UAC Specify Refresher	Configures which party refreshes the session when the phone acts as the caller. Set to "UAC" to use the phone as the refresher. Set to "UAS" to use the callee or proxy server as the refresher. Set to "Omit" to leave the refresher unspecified. The default setting is "UAC".
UAS Specify Refresher	Configures which party refreshes the session when the phone acts as the callee. Set to "UAC" to use the caller or proxy server as the refresher. Set to "UAS" to use the phone as the refresher. The default setting is "UAC".
Force INVITE	Enables or disables the use of the INVITE method to refresh the session timer. Disabled by default.
Codec Settings	
Audio	
Preferred Vocoder(Choice 1 - 8)	Multiple vocoder types are supported on the phone, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message. The vocoders supported are: OPUS PCMU PCMA G.723.1 G.722 (wide band) G.729A/B iLBC G.726-32 G.726-16 G.726-24 G.726-40
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	Enables or disables using the first matching vocoder in the received 200OK SDP as the codec.Disabled by default.
iLBC Frame Size	Selects iLBC packet frame size. The available options are 20ms and 30ms.The default setting is "30ms".
iLBC Payload Type	Specifies iLBC payload type. it cannot be the same as Opus or DTMF payload type.The default setting is "97". The valid range is 96 to 127.
G.726-32 Packing Mode	Selects the G726-32 packing mode. The available options are "ITU" and "IETF".The default setting is "ITU"
G.726-32 Dynamic Payload Type	Specifies G.726-32 payload type.The default setting is "127". Valid range is 96 to 127.
Opus Payload Type	Specifies Opus payload type. It cannot be the same as iLBC or DTMF Payload Type.The default setting is "123". The valid range is 96 to 127

Send DTMF	Specifies the mechanism to transmit DTMF digits. There are 3 supported modes: in-audio sends DTMF in the audio signal (not very reliable with low-bit-rate codecs). via RTP (RFC2833): sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. via SIP INFO uses SIP INFO to carry DTMF. The default setting is "via RTP (RFC2833)".
DTMF Payload Type	Specifies the payload type for DTMF using RFC2833. It cannot be the same as iLBC or OPUS payload type. The default setting is "101". The valid range is 96 to 127
Inbound DTMF Volume	Sets the volume size when using in-audio DTMF transmission mode. The default setting is "18". The valid range is 0-32.
Enable Audio RED with FEC	Enables or disables FEC for audio calls. Enabled by default.
Audio FEC Payload Type	Configures audio FEC payload type. The default setting is "121". The valid range is from 96 to 126.
Audio RED Payload Type	Configures audio RED payload type. The default setting is "124". The valid range is from 96 to 126.
Silence Suppression	Enables or disables sending a small quantity of VAD packets (instead of audio packets) will be sent during the period when silence is detected. For codec G.723 and G.729 only. Disabled by default.
Jitter Buffer Type	Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is "Adaptive".
Jitter Buffer Length	Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is "300ms".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120 kbps. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used in the codec table or negotiate the payload type during the actual call. For example, if set to 2 and the first code is G.729, G.711 or G.726, the "ptime" value in the SDP datagram of the INVITE request is 20 ms. If the "Voice Frame/TX" setting exceeds the maximum allowed value, the phone will use and save the maximum allowed value for the selected first codec. It is recommended to use the default setting provided, and incorrect setting may affect voice quality. The default setting is "2".
G.723 Rate	Selects encoding rate for G723 codec. The default setting is "5.3kbps encoding rate".
RTP Settings	
SRTP Mode	Configures the SRTP mode. The available options are: No Enabled but Not forced Enabled and Forced Optional The default setting is "No".
SRTP Key Exchange	Select SRTP key exchange method. The available options are: SDES DTLS The default setting is "SDES".
SRTP Key Length	Specifies the length of the SRTP calls. The available options are: AES 128&256 bit AES 128 bit AES 256 bit The default setting is "AES 128&256 bit".
Crypto Life Time	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. Enabled by default.
RTCP Mode	Configure RTCP port negotiation rules. The available options are: Default: Use the traditional RTCP port, which is "RTP port+1". Negotiate RTCP Port: Use attribute RTCP to negotiate. RTCP Mux: The caller actively negotiates the RTCP port and indicates RTCP Mux at the same time. RTCP Mux Only: The caller forces RTCP Mux, generated by the local media port only apply for RTP port. The default setting is "Default".
RTCP Keep-Alive Method	Configures the RTCP channel keep-alive packet type. The available options are: Receiver Report: The RTCP channel will send "receiver report+source description+RTCP extension" as keep-alive data. Sender Report: The RTCP channel will send "Sender report+source description+ RTCP extension" as keep-alive data. The default setting is "Receiver Report".

RTP Keep-Alive Method	Configures the RTP channel keep-alive packet type. The available options are: No: No data will be sent RTP Version 1: The wrong version info "1" will be carried when sending RTP data packets. RTP Packet with Silent Payload: The silent payload will be carried when sending RTP format packets. The default setting is "RTP Version 1".
VQ RTCP-XR Collector Address Selection	Configures the method for VQ RTCP-XR collector address selection. There are two supported methods: Manual: use the manually configured collector address with server/port in order to process XR reports. Auto: VQ collector address and port are not required to be filled in order to send XR reports. If the collector address is manually filled in, the same address will be used. If not filled in, the same server/port that is used for SIP registration will be used to process XR reports. The default setting for this parameter is "Manual".
VQ RTCP-XR Collector Name	Configure the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Address	Configures the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Port	Configure the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages. The default setting is "5060".
Symmetric RTP	Enables or disables whether Symmetric RTP is used or not. Symmetric RTP means that the UA uses the same socket/port for sending and receiving the RTP stream. Disabled by default.
RTP IP Filter	Configures whether to filter the received RTP. The available options are: Disable: The device receives RTP from any address. IP Only: The device receives RTP only from the IP address specified in the SDP, with no port restriction. IP and Port: The device receives RTP only from the IP address and port specified in the SDP. The default setting is "Disable".
RTP Timeout (s)	Configures the RTP timeout of the phone. If the phone does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. If set to 0, the phone will not hang up the call automatically. The default setting is "0". The valid range is 0 and 6-600.
Call Settings	
General	
Key as Send	Configures the send key. Pressing the selected key will immediately dial out. The default setting is "Pound (#)".
No Key Entry Timeout	Configures the timeout (in seconds) for no key entry. If no key has been pressed after the timeout, the collected digits will be sent out. The default setting is "4". The valid range is 1 to 15.
Send Anonymous	Enables or disables allowing the "From" header in outgoing INVITE messages to be set to anonymous. Disabled by default.
Anonymous Call Rejection	Enables or disables anonymous call rejection. Disabled by default.
Enable Call Waiting	Enables or disables the Call Waiting feature. If disabled, new incoming calls will be rejected after the call is established. The default setting is "Default".
RFC2543 Hold	Enables or disables RFC2543 Hold. If enabled, c=0.0.0.0 will be used in INVITE SDP for hold. Disabled by default.
Ring Timeout	Configures the timeout, in seconds, for the phone to ring when an incoming call is not answered. The default setting is "60". The valid range is 30-3600.
Call Log	Configures Call Log setting on the phone. The available options are: Log All Calls Log incoming/Outgoing Only (missed calls NOT recorded) Disable Call Log The default setting is "Log All Calls".
Auto Answer	
Auto Answer	Enables or disables the Auto Answer feature. If enabled, the phone will automatically answer incoming calls through the speakerphone after a short beep. Disabled by default.

Auto Answer Numbers	Configures up to 10 numbers for Auto Answer. If no numbers are configured, calls from all numbers will be automatically answered when Auto Answer is enabled.
Intercom	
Play warning tone for Auto Answer Intercom	Enables or disables playing a warning tone when auto answering intercom.Enabled by default.
Custom Alert-Info for Auto Answer	Used exclusively to match the contents of the Alert-Info header for auto answer. The default auto answer headers will not be matched if this is defined.
Allow Auto Answer by Call-Info/Alert-Info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info/Alert-Info header sent from the server/proxy.Enabled by default.
Allow Barging by Call-Info/Alert-Info	Enables or disables automatically putting the current call on hold and answer the incoming call based on the SIP Call-Info/Alert-Info header sent from the server/proxy. However, if the current call was answered based on the SIP Call-Info/Alert-Info header, then all other incoming calls with SIP Call-Info/Alert-Info headers will be rejected automatically.Disabled by default.
Mute on Intercom Answer	Enables or disables muting the microphone after answering an intercom call via Call-Info/Alert-Info.Disabled by default.
Record	
Record Key Default Function	Configures whether call recording is turned on or off when the Record key is pressed for the first time during a call using this account. For example, if the SIP server is configured to record calls automatically, set this parameter to "Record off".The default setting is "Record on".
Call Recording On	Configures the DTMF sequence sent when the Record key is pressed during a call on this account to turn call recording on. The phone toggles between this value and the off code if possible; otherwise, it always sends this code.
Call Recording Off	Configures the DTMF sequence sent when the Record key is pressed during a call on this account to turn call recording off.
Transfer	
Transfer on Conference Hangup	Enables or disables whether the call is transferred to the other party if the conference initiator hangs up.Disabled by default.
Transfer to VM feature code	Configures the transfer to voicemail feature code, which will be used as an extension prefix and called into the server to complete the transfer to voicemail when pressing the voicemail softkey or hardkey during a call.
Enable Recovery on Blind Transfer	Enables or disables call recovery to the transferee on failing blind transfer to the target.Enabled by default. Notes: This feature only applies to blind transfer. This feature depends on how server handles transfer. If there is any NOTIFY from server, this feature will not take effect. If server responds 4xx, phone should try to recover regardless of this option. During blind transfer, after transferor received 200/202 for REFER, but there is no NOTIFY from server after 7 seconds, transferor will decide to recover the call with transferee or not depending on the options. This is the only case that this option will be applied.
Blind Transfer Wait Timeout	Defines the timeout, in seconds, for waiting SIP frag response in blind transfer. The default setting is "30s". The valid range is 30 to 300.
Refer-To Use Target Contact	Enables or disables using the transferred target's Contact header information in the "Refer-to" header for attended transfers.Disabled by default.
Call Forward	
Enable Forward All	Enables or disables forwarding all incoming calls to the specified number.Disabled by default.
All To	Specifies the number to be forwarded to when Forward all is enabled.

Enable Busy Forward	Enables or disables forwarding incoming calls to the specified number when the phone is busy.Disabled by default.
Busy To	Specifies the number to be forwarded to for Call Forward On Busy.
Enable No Answer Forward	Enables or disables forwarding incoming calls to the specified number when the call is not answered.Disabled by default.
No Answer To	Specifies the number to be forwarded to for Call Forward On Busy.
No Answer Timeout (s)	Defines the timeout, in seconds, before the call is forwarded on no answer.The default setting is "12".
Enable Override Forward	Enables or disables allowing the numbers configured under Override Forward Numbers to override the local call forwarding configuration.Disabled by default.
Override Forward Numbers	Configures up to 10 numbers that can override the local call forwarding configuration when Enable Override Forward is enabled.
Dial Plan	
Dial Plan Prefix	Configures a prefix added to all numbers when making outbound calls.
Bypass Dial Plan	Enable or disable the dial plan bypass while dialing through: Contact Call History Incoming Call Call History Outgoing Call Dialing Page Multi-Purpose Keys Virtual Multi-Purpose Keys API
Dial Plan	Configures the dial plan that establishes the expected number and pattern of digits for a telephone number. This parameter configures the allowed dial plan for the phone. Dial Plan Rules: Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d; Grammar: x - any digit from 0-9; Grammar: X - any character from 0-9, a-z, A-Z. xx+ - at least 2 digit numbers xx - only 2 digit numbers XX - two characters (AA, Ab, 1C, f5, 68,...) test : only string "test" will pass the dial plan check ^ - exclude [3-5] - any digit of 3, 4, or 5 [147] - any digit of 1, 4, or 7 <2=011> - replace digit 2 with 011 when dialing - the OR operand x - uses the x character literally and escapes its representation Example 1: {[369]11 1617xxxxxx} Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617; Example 2: {^1900x+ <=1617>xxxxxx} Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers; Example 3: {1xxx[2-9]xxxxx <2=011>x+} Allows any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR Allows any length of numbers with leading digit 2, replacing the 2 with 011 when dialed. Example 4: [x-X*]+ Allows any number starting with any digit from "0-9" followed by a hyphen "-" and any character from "0-9, a-z, A-Z" then an asterisk "*". Example of a simple dial plan used in a Home/Office in the US: { ^1900x. <=1617>[2-9]xxxxx 1[2-9]xx[2-9]xxxxx 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]xxxxx - allows 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]xxxxx - allows dialing to any US/Canada Number with 11 digits length; 011[2-9]x - allows international calls starting with 011; [3469]11 - allows dialing special and emergency numbers 311, 411, 611 and 911. Note: In some cases, where the user wishes to dial strings such as *123 to activate voice mail or other applications provided by their service provider, the * should be predefined inside the dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers. The default setting is "{ x+ +x+ *x+ *xx*x+ }". The maximum length of dial plan is 1024 characters.
Call Display	
Caller ID Display	Determines where to locate the caller ID to display or not on the phone. The available options are: Auto: The phone will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header, and From Header in the incoming SIP INVITE. Disabled: All incoming calls are displayed with "Unavailable". From Header: the phone will display the caller ID based on the From Header in the incoming SIP INVITE. The default setting is "Auto".

Callee ID Display	Determines where to locate the callee ID to display or not on the phone. The available options are: 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 Disabled: Callee ID will be displayed as "Unavailable". To Header: Callee ID will not be updated and displayed as To Header. The default setting is "Auto".
Ringtone	
Ringback Tone at No Early Media	Enables or disables playing the ringback tone to the caller even if no early media RTP packets are received. Use P-Early-Media Header must be enabled under Accounts -> Accounts -> SIP Settings. When both settings are enabled, the phone will play a ringback tone when the RTP packets of early media audio arrive after receiving an 183 response on SDP. Disabled by default.
Account Ringtone	Selects the account ringtone. The default setting is "System Ringtone". Note: "Silent" and "Doorbell" ringtones are also available for selection. Press Upload a new ringtone to upload a custom ringtone.
Ignore Alert-Info header	Enables or disables playing the default ringtone by ignoring Alert-Info header. Disabled by default.
Enable Alert-Info Bellcore Mapping	Enables or disables the mapping of keywords in the Alert-Info header to predefined Bellcore ring tones. When an Alert-Info header containing "Bellcore-dr%N" is received where N is a value between 1 and 5, the corresponding Bellcore ring tone will be played if the option is enabled. If the option is disabled, a corresponding custom ring tone will be played instead. When N is 0, a silent ringtone will be used. When N is 6, a corresponding custom ringtone will always be played, regardless of the option setting. If N is outside the valid range (i.e., less than 0 or greater than 6), the default ring tone will be used. Enabled by default.
Match Incoming Caller ID	Specifies matching rules with number, pattern, or Alert Info text (up to 10 matching rules). When the incoming caller ID or Alert Info matches the rule, the phone will ring with selected distinctive ringtone. Matching rules: Specific caller ID number. For example, 8321123. A defined pattern with certain length using x and + to specify, where x could be any digit from 0 to 9. Samples: xx+ : at least 2-digit number. xx : only 2-digit number. [345]xx: 3-digit number with the leading digit of 3, 4 or 5. [6-9]xx: 3-digit number with the leading digit from 6 to 9. Alert Info text Users could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it. The custom ring tone will be used if the phone receives SIP INVITE with Alert-Info header in the following format: Alert-Info: <http://127.0.0.1>; info=priority When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone. Note: Beginning with firmware version 1.0.3.98, a new feature was introduced that enables the use of a ringtone stream via a remote URL. The functionality of this feature works as follows: the following audio file named test.wav is uploaded onto an HTTP server and the remote URL is "http://192.168.5.165:8080/test.wav;info=ring3", the IP phone then attempts to use the provided URL first to play the ringtone. If the URL is not functional for some reason, it will then use the info=ring3 parameter, as the default ringtone.
Advanced Settings	
Security Settings	
Check Domain Certificates	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. Disabled by default.
Trusted Domain Name List	Configure the list of up to 10 trusted domain names, which supports filling in the SAN list used only for domain name verification in TLS to obtain certificates. If it matches any item in the trusted domain name list, the certificate is trusted. By default, the remote proxy domain name and SIP server domain name are trusted. This field allows numbers/letters/-/./*. It supports wildcard domain names, such as "*.mycompany.com", and trusts any domains ending with ".mycompany.com".
Validate Certificate Chain	Validates certification chain when TCP/TLS is configured. Disabled by default.
Validate Incoming SIP Messages	Specifies if the phone will check the incoming SIP messages Caller ID and CSeq headers. If the message does not include the headers, it will be rejected. Disabled by default.

Omit charset=UTF-8 in MESSAGE	Omits charset=UTF-8 in MESSAGE content-type.Disabled by default.
Allow Unsolicited REFER	Configures whether to dial the number carried by Refer-to header after receiving out-of-dialog SIP REFER request actively. The available options are: If set to "Disabled", the phone will send error warning and stop dialing. If set to "Enabled/Force Auth", the phone will dial the number after sending authentication. If the authentication fails, it will stop dialing. If set to "Enabled", the phone will dial all numbers carried by SIP REFER. The default setting is "Disabled".
Accept Incoming SIP from Proxy Only	Enables or disables checking the SIP address in the Request URL of incoming SIP messages. If enabled, the phone will reject calls when the address does not match the SIP server address of the account.Disabled by default.
Check SIP User ID for Incoming INVITE	Enables or disables checking the SIP User ID in the Request-URI of incoming INVITE messages. If enabled, the phone will reject calls when the SIP User ID does not match the phone's SIP User ID.Disabled by default.
Allow SIP Reset	Enables or disables performing a factory reset through SIP NOTIFY. Disabled by default.
Authenticate Incoming INVITE	Enables or disables authentication for incoming INVITE messages. If enabled, the phone will challenge the incoming INVITE with a SIP 401 Unauthorized response.Disabled by default.
MOH	
On Hold Reminder Tone	Enables or disables playing a reminder tone when the call is on hold.Enabled by default.
Music On Hold URI	Specifies the URI used to request music on hold from the server when a call is placed on hold, if the server supports this feature.
Advanced Features	
Special Feature	Selects the special features to meet the requirements of other soft switch vendors. The available options are Standard, Nortel MCS, Broadsoft, CBCOM, RNK, Sylantro, Huawei IMS, PhonePower, UCM Call Center, and Zoom depending on the server type.The default setting is "Standard".
Feature Key Synchronization	Enables or disables synchronization of DND, Call Forward and Call Center Agent status between the Broadsoft server and the phone.Disabled by default.
Conference URI	Configures the conference URI when using Broadsoft N-way calling feature.
Reboot on check-sync event without "reboot="	Enables or disables whether the phone will reboot or provision when receiving SIP NOTIFY check-sync event without "reboot=" header. When enabled, the phone will reboot, otherwise it will provision.Enabled by default.
BroadSoft Call Center	Enables or disables Feature Key Synchronization when Special Features is set to BroadSoft, regardless of the web UI settings.Disabled by default.
Hoteling Event	Enables or disables the Hoteling Event feature when Special Features is set to BroadSoft.Disabled by default.
Call Center Status	Enables or disables the Call Center Status feature when Special Features is set to BroadSoft. If enabled, the phone sends a SUBSCRIBE request to the server to retrieve call center status.Disabled by default.
BroadSoft Executive Assistant	Enables or disables the Executive Assistant feature when Special Features is set to BroadSoft.Disabled by default.
BroadSoft Call Park	Enables or disables the BroadSoft Call Park feature when Special Features is set to BroadSoft. If enabled, the phone sends a SUBSCRIBE request to the BroadSoft server to receive Call Park notifications.Disabled by default.
Enable Call Monitor Function	Enables or disables the Call Monitor function when Special Features is set to Zoom.Enabled by default.

Support Call Monitor Privacy Mode	Enables or disables privacy mode for Call Monitor when Special Features is set to Zoom. This mode can be toggled directly from the phone's LCD.Enabled by default.
Barge-in Feature Code	Specifies the feature code used for barge-in when Special Features is set to Zoom (e.g., *123).
Listen Feature Code	Specifies the feature code used to silently monitor an active call when Special Features is set to Zoom.
Whisper Feature Code	Specifies the feature code used to whisper during a monitored call, allowing private guidance without being audible to the other call participants, when Special Features is set to Zoom.
Takeover Feature Code	Specifies the feature code used to take over an active monitored call when Special Features is set to Zoom.
BLF (Busy Lamp Field)	
Presence Eventlist URI	Configures the Presence Eventlist URI to monitor the extensions on Multi-Purpose Keys.If the server supports this feature, users need to configure a Presence Eventlist URI on the service side first (i.e., presence@myserver.com) with a list of extensions included. On the phone, in this "Presence Eventlist URI" field, fill in the URI without the domain (i.e., presence). To monitor the extensions in the list, under Web GUI Programmable Keys, please select "Presence Watcher" in the key mode, choose the account, and enter the value of each extension in the list.
Eventlist BLF URI	Configures the Eventlist BLF URI on the phone to monitor the extensions in the list with the Multi-Purpose Key. If the server supports this feature, users need to configure an Eventlist BLF URI on the service side first (i.e., BLF1006@myserver.com) with a list of extensions included. On the phone, in this "Eventlist BLF URI" field, fill in the URI without the domain (i.e., BLF1006). To monitor the extensions in the list, under Web GUI Programmable Keys, please select "Eventlist BLF" in the key mode, choose the account, and enter the value of each extension in the list.
Auto Provision Eventlists	Select the type of Eventlist used to automatically provision monitored extensions onto the available MPKs. The available options are: Disabled BLF Eventlist Presence Eventlist The default setting is "Disabled".
BLF Call-pickup	Configures BLF Call-pickup method. The available options are: Auto: The phone will do either Prefix or barge in code for BLF pickup depend on which on is set. Force BLF Call-pickup by prefix: The phone will ignore both BLF pickup method, now the monitored VPK will only dial the extension if pressed Disabled: The phone will ignore both BLF pickup method, now the monitored VPK will only dial the extension if pressed The default setting is "Auto".
BLF Call-pickup Prefix	Configures the prefix prepended to the BLF extension when the phone picks up a call with BLF key.The default setting is ""**".
Call Pickup Barge-In Code	Configures feature access code of Call Pickup with Barge-in feature.
PUBLISH for Presence	Enables presence feature on the phone.Disabled by default.
SCA	
Line-Seize Timeout	Configures the interval, in seconds, when the line-seize is considered timed out when Shared Call Appearance feature is used. The default value is "15s". The valid range is from 15 to 60.
Call Park	
Call Park Feature Code	Configure the feature access code for parking current call to a parking lot or another extension.
Call Park Retrieve Feature Code	Configure the feature access code for retrieving the parked call on accounts or BLF keys.
Dial Plan	
Name	Specifies the name for the configured rules.
Rule	Configures the rule settings (number pattern, prefix to add ...etc.).

Type	Selects the rule type. The available options are: Pattern: The phone will dial the number matching the entered pattern. Block: The phone will block the number/pattern matching the rule. Dial now: The phone will dial immediately the number once the DTMF matches the dial plan. Prefix: Specify the "Replaced" field to replace by the "Used" field to dial. Second tone: The phone plays the second dial tone when the entered "Trigger" digit is dialed.
Hidden Number Plan	
Hidden Number Features	Configure one of the following options for the hidden number features: Disabled: No number hiding applied. Incoming Calls Only: Hides caller ID for received calls. Outgoing Calls Only: Masks the caller's number when making calls. Both Direction Calls: Applies number hiding to incoming and outgoing calls. The default setting is "Disabled".
Hidden Number Plan List	Configure the hidden number rules, matching their syntax rules from top to bottom as follows: Expression: element(element)element (element)element element(element) (element) Element Rules: x:any digit number from 0-9 x+:substring with only digits (length>=1) [-+.*,#;]:possible special symbols in number ():the substring that needs to be hidden, there can be multiple hidden parts in a rule Examples: x+(xxxx)xxxx: 13705806547 -> 137****6547 xxx(x+)xxxx: 07113705806547 -> 071137****6547 071-x+(xxxx)xxxx: 071-13705806547 -> 071-137****6547
Hidden Number Plan Test	Tests a phone number against the configured hidden number rules.
Feature Codes	
Local Call Features Mode	Configures whether call features are handled locally on the phone using user feature codes or through feature codes provisioned by the server. The available options are: Disabled: The provisioned feature codes from the server will be used. User-configured feature codes are used only if server-provisioned feature codes are not provided. Enabled: The device performs Do Not Disturb, Call Forwarding, and other call features locally using its locally configured feature codes. Call Forwarding & DND Only: The device performs only Do Not Disturb and Call Forwarding locally. Enabled without Feature Codes: The device performs local call features, but does not support local feature codes. Note: If the device is registered with Broadsoft account, it does not matter if local call features are enabled or disabled, once the Broadsoft account is set, special feature to Broadsoft and Feature Key Synchronization is enabled, the call feature will be handled by Broadsoft server, not by the phone.
DND	
DND Call Feature On	Configures DND feature code to turn on DND.
DND Call Feature Off	Configures DND feature code to turn off DND.
Call Forward Always	
On	Configures Call Forward Always feature code to activate unconditional call forwarding.
Off	Configures Call Forward Always feature code to deactivate unconditional call forwarding.
Target	Configures the extension for the call to be forwarded to.
Call Forward Busy	
On	Configures the Call Forward Busy feature code to activate busy call forwarding.
Off	Configures the Call Forward Busy feature code to deactivate busy call forwarding.
Target	Configures the extension for the call to be forwarded to.
Call Forward No Answer	
On	Configures the Call Forward No Answer feature code to activate no-answer call forwarding.

Off	Configures the Call Forward Busy feature code to deactivate busy call forwarding.
Target	Configures the extension for the call to be forwarded to.
Call Forward No Answer Timeout (s)	Configures the timeout, in seconds, before the call is forwarded when there is no answer. The default setting is "12". The valid range is 1 to 120.
Accounts -> Account Swap	
Swap Account Settings	Allows users to swap the two accounts that they have configured. This will increase the flexibility of account management. Note: Press "Start" to complete the process.
Accounts -> UCM	
Account Tabs	Select the target SIP account tab corresponding to the extension registered on the UCM IP-PBX.
Extension	Displays the extension number associated with the selected SIP account.
UCM Password	Enter the user portal login password assigned to the corresponding extension on the UCM IP-PBX.
Verification Code	Enter the CAPTCHA characters displayed in the adjacent image box to authenticate the login attempt and prevent automated logins.
Login	Click the button to initiate authentication with the UCM server.

Account settings definitions

Phone Settings Page Definitions

Phone Settings -> General settings	
Basic Settings	
Local RTP Port	Defines the local RTP port used to listen and transmit. It is the base RTP port for channel 0. When configured, channel 0 will use this port _value for RTP; channel 1 will use port _value+2 for RTP. The default setting is "5004". The valid range is 1024 to 65400 .
Local RTP Port Range	Configures the range of local RTP port. The default setting is "200". The valid range is 24 to 10000.
Use Random Port	Enables or disables using random ports of the local SIP and RTP ports. Necessary when multiple phones are behind the same full cone NAT. Enabled by default. Note: Disable this setting in order to use Direct IP Calling.
Keep-Alive Interval	Specifies how often the phone sends a blank UDP packet to the SIP server to keep the "ping hole" on the NAT router open. The default setting is "20" seconds. The valid range is 10 to 160.
STUN Server	Specifies the IP address or domain name of the STUN server. STUN resolution results are displayed on the STATUS page of the Web GUI. STUN works only with non-symmetric NAT routers.
Use NAT IP	Specifies the NAT IP address to be used in SIP/SDP messages. This field is blank by default and should only be configured if required by the ITSP.
Delay Registration	Configures the time, in seconds, before the account is registered after bootup. The default setting is "0".
Enable Outbound Notification	Enables or disables outbound notifications, such as Action URL. Enabled by default.
Clear User Data On Log out	Enables or disables clearing the account's contacts and call history when the account is logged out. Disabled by default.
Public Mode	

Enable Public Mode	Enables or disables Public Mode for the hot desking feature. Disabled by default.
Public Mode Username Prefix	Configures the prefix of the username for public mode login.
Public Mode Username Suffix	Configures the suffix of the username for public mode login.
Allow Multiple Accounts	Enables or disables the use of other configured SIP accounts to make and receive calls while a user is logged in to a Public Mode account. When disabled, only the Public Mode account can be used after the user logs in to the Public Mode account on the LCD, even if other SIP accounts are configured on the phone. When enabled, Other configured SIP accounts can also be used after the user logs in to the Public Mode account on the LCD. Note: This option takes effect only when Public Mode is enabled. Disabled by default. Note: This option takes effect only when Public Mode is enabled.
Enable Remote Synchronization	Enables or disables automatically downloading the current account's settings from the remote server and uploading them to the server. Disabled by default.
Server Type	Configures the server type and protocol used to send requests to the Remote Synchronization Server. The available options are TFTP, FTP, and HTTP. The default setting is "TFTP".
Server Path	Configures the server path for the Remote Synchronization feature.
FTP/HTTP Username	Specifies the username for the FTP/HTTP server.
FTP/HTTP Password	Specifies the password for the FTP/HTTP server.
Public Mode Timeout	Configures the Public Mode timeout, in minutes, measured from the phone's last idle state. The default setting is "10". The valid range is 10 to 1440.
Pop-up Hidden Settings	
Hide Pop-up Options	Selects the types of pop-ups to hide on the LCD. The available options are: Disable All Info All Alarm & All Info All Custom The default setting is "Disable".
Custom Mode	Specifies the pop-ups to hide when Hide Pop-up Options is set to "Custom". The selected pop-ups will be hidden on the LCD. When configuring this setting in the configuration file, use the following values for the corresponding pop-ups, separated by commas ",": Conference Members Joining and Leaving Information: call.conf.member Missed Calls/New Messages: call.message_tips CTI Authcode: cti.auth_code Prompt for web modify configuration: sys.config.modified_by_web Saving: sys.config.saving Database corrupt: sys.db Network warning information: sys.net.warn_info Reboot confirmation countdown: sys.reboot_timming Remote control confirmation countdown: sys.remote_control_permission Firmware server auth failed: sys.upgrade.auth_fw Config server auth failed: sys.upgrade.auth_cfg Upgrade certificate failed: sys.upgrade.cert Failed to download config file: sys.upgrade.cfg Firmware upgrade reboot confirmation countdown: sys.upgrade.confirm Failed to download firmware: sys.upgrade.fw Firmware upgrade confirmation countdown: sys.upgrade.reboot_confirm Current firmware version: sys.upgrade.version User storage space is full: sys.user_space Please use the provided 5V power adapter!: sys.voltage Receive new voice mail: vm.new Default Admin Password: sys.default_pwd Example: To hide Failed to download firmware and Upgrade certificate failed, set the configuration file value to sys.upgrade.fw,sys.upgrade.cert.
Phone Settings -> Call Settings	
General	
Key Mode	Configures the line key mode. The available settings are: Account Mode: In Calling State, each key displays the call status of the corresponding account. Pressing the key switches to the first line under that account or selects the account to initiate a new call. Line Mode: In Calling State, each key controls a line. Pressing the key switches the call line. The default setting is "Line Mode".
Preferred Default Account	Selects the preferred default account for on-hook or off-hook dialing. When the selected account is unavailable, the system uses the first available account to dial out. The default setting is "Account 1".

Mute Key Functions While Idle	Selects the Mute key function while the phone is idle. The available settings are: DND: Pressing the Mute key while the phone is idle enables DND. Idle Mute: Pressing the Mute key while the phone is idle mutes the phone when answering incoming calls. Disabled The default setting is "DND".
Last Call Forward Always	Enables or disables storing the number entered for the ForwardAll feature for the next time the ForwardAll softkey is used.Disabled by default.Note: The ForwardAll softkey is currently only used for Account 1.
Show SIP Error Response	Enables or disables the display of SIP error response information on the LCD.Enabled by default.
Escape '#' as %23 in SIP URI	Enables or disables replacing # with %23 in the SIP URI for special situations.Enabled by default.
User-Agent Prefix	Configures the prefix in the User-Agent header.
Call-ID Domain Mode	<pre> > To: <sip:1003@192.168.6.208> Call-ID: 1459611249-24657-4@BJC.BGI.G.BIE [Generated Call-ID: 1459611249-24657-4@BJC.BGI.G.BIE] > To: <sip:1003@192.168.6.208> Call-ID: 70313272-24657-3@192.168.6.184 [Generated Call-ID: 70313272-24657-3@192.168.6.184] </pre> Selects the Call-ID domain format. The available settings are: Masked Info: The host IP address will be transformed according to the built-in rules, and the resulting value will be used in the Call-ID Domain. Masking the Call-ID domain reinforces the security by protecting the identity of the device in the network. See the screenshot below. Plaintext Host IP Address: The Call-ID Domain will use the host IP address in plain text. See the screenshot below. The default setting is "Masked Info".
Enable Hook Switch	Enables or disables the hook switch. The available options are: No: Disables the hook switch completely. Yes, except answering call: Disables the hook switch for answering calls. Yes: Enables the hook switch. The default setting is "Yes".
Speaker Key Mode	Enables or disables the speaker key. The available options are: Default: The speaker key can be used to make calls, end calls, and switch channels. Always Disable: Disables the speaker key completely. For Switching Channels: The speaker key cannot be used to hang up calls. The default setting is "Default".
Voicemail Key Mode	Enables or disables the voicemail key. The available options are: Default: The voicemail key functions normally, directing users to voicemail. Disabled: Disables the voicemail key. The default setting is "Default".
In-call Contact Info Display	Configures the contact information displayed during a call, up to 5 lines to display. The following labels and their combinations are supported: {number}? {name}? {title}? {company}? {department}? {email}? {firstName}? {lastName}? Examples: Line 1: {name} Line 2: {title}-{company} Line 3: {number} / {email} After configuration, the screen scrolls vertically according to the specified sequence.
Contact Source Priority	Configures the priority order of the caller ID sources displayed on the phone for incoming and outgoing calls. Select an ID source and click the Up/Down arrows on the right to adjust the order. Note: If Caller ID Display under Accounts -> Accounts -> Call Settings -> Call Display is set to "Disabled", the caller number cannot be obtained, and the phone displays "Unavailable".
Outgoing	
Click-To-Dial Feature	Enables or disables the Click-To-Dial feature. When enabled, users can click the green dial button in the upper-left corner of the phone's Web UI, select an account, and dial the target number. When the call is connected, the Click-To-Dial icon changes to red. Users can then hold, resume, or hang up the call using the call control icons displayed for the active call. Disabled by default. Note: Users can use the Click2Dial browser extension to share their screens during calls for remote presentations and to share files directly from their computers.
Enable Direct IP Call	Enables or disables direct IP calling. Enabled by default but will be disabled after a factory reset.

Use Quick IP Call Mode	Enables or disables dialing IP addresses under the same LAN/VPN segment by entering the last octet of the IP address.Disabled by default.
Enable Paging Call Mode	Enables or disables paging call mode. Enabled by default.
Predictive Dialing Feature	Enables or disables the predictive dialing feature on the call screen.Enabled by default.
Predictive Dialing Source	Selects the sources the predictive dialing feature will sequentially search the number based on.
Enable Local Dialing DTMF Tone in Speaker Mode	Enables or disables playing the local DTMF tone during dialing in speaker mode. When set to "Yes", the normal DTMF tone plays. When set to "Specific Tone", a specific tone plays instead.The default setting is "Yes".
Account Selection Mode for Dialing	Selects the account selection mode when placing a call from the dialing interface. The available options are: Auto: Calls placed to a number selected from the call history use the account previously used to call that number or the account configured for that contact. Current Account: Calls placed to a number selected from the call history or contacts use the account currently displayed or selected in the dialing interface. The default setting is "Auto".
Onhook Dial Barging	Enables or disables on-hook dialing barging. When disabled, on-hook dialing is not interrupted by an incoming call.Enabled by default.
Off-hook Auto Dial	Configures the digits to be dialed through the first account when the phone goes off-hook.
Off-hook Auto Dial Delay	Configures the delay, in seconds, before off-hook auto dialing. If set to "0", the number is dialed immediately. Otherwise, the number is dialed after the configured delay.The default setting is "4". The valid range is 0 to 10.
Off-hook/On-hook Timeout (s)	Configures the timeout, in seconds, before the phone returns to idle in an off-hook or on-hook dialing state.The default setting is "30". The valid range is 10 to 60.
Enable Live Keypad	Enables or disables live keypad dialing. When enabled, the phone automatically dials out and activates hands-free mode when a keypad key or softkey is pressed.Disabled by default.
Live Keypad Expiration	Configures the expiration time, in seconds, for live keypad.The default setting is "5". The valid range is 2 to 15.
Enable Auto Redial	Enables or disables automatically redialing a number at a later time when the called number is busy.Disabled by default.
Auto Redial Times	Configures the total times to redial if "Auto Redial" is enabled.The default setting is "10".
Auto Redial Interval	Configures the interval between each redial if "Auto Redial" is enabled.The default setting is "10".
Bypass Dial Plan Through Call History and Directories	Enables or disables dial plan checking when dialing from call history and phonebook directories.Disabled by default.
Enable Call Completion Service	Enables or disables automatically redialing a previously failed call when the remote party becomes available.Disabled by default.
Incoming	
Enable Incoming Call Popup	Enables or disables the incoming call pop-up window on the phone.Enabled by default.
Enable Missed Call Notification	Enables or disables missed call notifications on the phone.Enabled by default.Note: users can still initiate calls directly when a missed call notification is displayed.
Return Code When Refusing Incoming Call	Configures the return code sent by the phone when refusing an incoming call.The default setting is "Busy (486)".
Allow Incoming Call before Ringing	Enables or disables receiving incoming calls after dialing but before ringing. This setting can be used for custom configurations as needed.Disabled by default.

Enable Call Waiting	Enables or disables the call waiting feature.Enabled by default.
Enable Call Waiting Tone	Enables or disables Call Waiting alert tone when another incoming call is received while a call is in progress.Enabled by default.
Ring for Call Waiting	Enables or disables ringing instead of playing the call waiting tone when using the handset or headset.Disabled by default.
Auto Answer Delay	Configures the delay, in seconds, before automatically answering an incoming call.The default setting is "0". The valid range is 0-10 seconds.
In Call	
Enable In-call DTMF Display	Enables or disables displaying DTMF digits entered during a call on the LCD. Enabled by default.
Enable Local In-call DTMF Tone in Speaker Mode	Enables or disables playing local DTMF tones through the device's speaker during a call in speaker mode.Enabled by default.
Enable Sending DTMF via specific MPKs	Enables or disables sending DTMF during a call using specific MPKs. This setting does not affect Dial DTMF. Disabled by default.
Show on Hold Duration	Enables or disables displaying the call hold duration on the LCD. Enabled by default.
Enable Auto Unmute	Enables or disables automatically unmuting the phone when a user resumes a held call or establishes a new call. Enabled by default.
In-call Dial Number on Pressing Transfer Key	Configures the number to be dialed as DTMF when pressing the TRANSFER key.
Enable Busy Tone on Remote Disconnect	Enables or disables playing a busy tone when the remote party disconnects the call. Enabled by default.
Enable Mute Key In Call	Enables or disables the Mute key during a call.Enabled by default.
Phonebook Matching	
Filter Characters	Configures separator characters to filter from phone numbers used with Click2Dial or contacts imported from other devices. These characters are not part of the actual phone number and must be removed. Multiple characters can be configured.Example: if set to "[()-]", when dialing (0571)-8800-8888, the characters ()- are automatically filtered, and 057188008888 is dialed directly. When initiating calls from places other than the Dial screen, such as call history and contacts, the configured characters are automatically filtered. Characters are not filtered when dialing from the Dial screen.The default setting is "[()-]".
Enable Phonebook Matching Rules	Enables or disables phonebook matching rules. The following options are available: Dial Number: Processes the dialing number. Query Number: Processes the number used to query contacts. Display Number: Processes the number displayed for the receiver. All options are disabled by default.
Phonebook Matching Rules	Configures rules to match and modify phone numbers based on their length and digit patterns. The rules are checked from top to bottom and can be applied to numbers containing 4, 7, or 9 digits. Each rule specifies which numbers to match and what changes to make, such as adding a prefix or leaving the number unchanged. The matching rule specifies the phone number pattern to match, and the replacement rule specifies how to modify the matched number.Rule Format=Matching rule/Replacement rule Rule examples:? 9XXXXXXXX: Matches a nine-digit number starting with 9 and leaves it unmodified.Result: 9XXXXXXXX: 958242234 -> 958242234 ? (6XXXXXX)/95: Matches a seven-digit number starting with 6 and adds 95 as a prefix.Result: 6242234 -> 956242234 ? ([1235678] XXX) / 95612: Matches a four-digit number that starts with 1, 2, 3, 5, 6, 7, or 8, and adds 95612 as a prefix.Result: 2234 -> 956122234 Combining all three rules, the configuration value is: {9XXXXXXXX}(6XXXXXX)/95 ([1235678]XXX)/95612} Note: X represents any digit. represents all content matched by the matching rule. 1 represents the content matched by the first pair of parentheses () in the preceding matching rule.
Phonebook Matching Rules Test	Tests a phone number against the configured rules.

Transfer	
Enable Transfer	Enables or disables the call transfer feature.Enabled by default.
Hold Call Before Completing Transfer	Enables or disables putting the current call on hold before completing an attended transfer. When disabled, the phone does not put the current call or the transfer target on hold.Enabled by default.
Attended Transfer Mode	Selects the attended transfer mode. The available options are: Static: Attended transfers can only be performed with established calls. Dynamic: Attended transfers can be performed with established calls or initiated during the transfer process. This option does not affect blind transfers. The default setting is "Dynamic".
Call Park	
Enable Call Park Softkey	Enables or disables the call park feature for using call park-related softkeys.Enabled by default.
Call Park Softkey Feature Code	Configures the feature access code for parking the current call in a parking lot or at another extension.
Call Park Retrieve Softkey Feature Code	Configures the feature access code for retrieving a parked call from an account or parking lot.
Group Call Park Softkey Feature Code	Configures the feature access code for parking the current call in the group the user belongs to.
DND	
Enable DND Feature	Enables or disables the Do Not Disturb (DND) feature. When enabled, DND can be activated using the MUTE key, an MPK, the LCD menu or pressing the toggle under the setting.Enabled by default.
Return Code Upon DND	Configures the return code sent by the phone when DND is enabled.The default setting is "Temporarily Unavailable (480)".
Override DND	Configures whether and how the local DND function can be overridden. The available options are: Off: The local DND function operates normally. Allow All: The local DND function is overridden for all callers. Allow Only Contacts: When DND is enabled, only local contacts and configured override numbers can call in. Allow Override Numbers: When DND is enabled, only configured override numbers can call in. The default setting is "Off".
Override DND Numbers	Configures the numbers that can override the local DND function.
Conference	
Enable Conference	Enables or disables the conference feature.Enabled by default.
Hold Call before Adding Conferee	Enables or disables putting the current call on hold when adding new participants to a conference. When set to enabled, the current call is put on hold when the host presses the Conference or Add key to invite new participants. After the invited participant answers and agrees to join, the host must manually resume the conference. When set to disabled, the current call is not put on hold, and the invited participant automatically joins the conference after answering.Disabled by default.
BLF	
Enable BLF Pickup Screen	Enables or disables displaying a softkey that opens the monitoring screen when a monitored BLF line is ringing.Disabled by default.
Enable BLF Pickup Sound	Enables or disables playing a sound when a monitored BLF line is ringing.Disabled by default.
Hide BLF Remote Status	Enables or disables displaying status information for the monitored line.Disabled by default.
IM	
Enable IM Popup	Enables or disables displaying a pop-up when the phone receives an instant message (IM).Enabled by default.
Instant Message Popup Timeout	Configures how long, in seconds, the instant message pop-up remains on screen.The default setting is "10".

Play Tone on Receiving IM	Enables or disables playing a short tone when the phone receives an instant message while idle.Disabled by default.
Record	
Enable the Indicator in Recording	Enables or disables displaying the recording indicator on the LCD during call recording.Enabled by default.
Phone settings -> Ringtone	
Call Progresses Tones: System Ring Tone Dial Tone Second Dial Tone Message Waiting Ring Back Tone Call Waiting Tone Call Waiting Tone Gain Auto-Answer Tone Gain Busy Tone Reorder Tone	Configures ring and tone frequencies according to parameters from the local telecom provider. The default value is "North American Standard". Frequencies should be configured with known values to prevent uncomfortable high-pitched sounds.Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]];Frequencies are in Hz and cadence on/off periods are 10msON specifies the ringing duration ("On time" in ms), while OFF specifies the silence duration. To configure a continuous ring, set OFF to zero. Otherwise, the phone rings for the configured ON duration, pauses for the configured OFF duration, and repeats the pattern. Up to three cadences are supported.Call Waiting Tone Gain can be set to either: Low, Medium, or High. The default setting is "Low".Auto-Answer Tone Gain can be set to either: Low, Medium, or High. The default setting is "Medium".
Provision	
Total Number of Custom Ringtone Update	Configures the number of custom ringtones to update in the provisioning process.The default setting is "6".
Phone settings -> Multicast Paging	
Multicast Paging Function	Enables or disables multicast paging.Disabled by default.
Allowed In DND Mode	Enables or disables receiving multicast pages when DND mode is enabled.Disabled by default.
Paging Barge	Configures the priority threshold for multicast paging during an active call. If an incoming multicast page has a higher priority (1 being the highest and 10 being the lowest) than this value, the active call is put on hold and the multicast page is played.The default setting is "Disabled".
Paging Priority Active	Enables or disables playing an incoming multicast page with a higher priority (1 being the highest) than the currently playing page.Enabled by default.
Multicast Channel Number	Configures the multicast channel number. 0 is for normal RTP packets, and 1 to 50 are for Polycom multicast format packets.The default setting is "0". The valid range is 0 to 50.
Multicast Paging Codec	Selects the codec for sending multicast pages. The available codecs are: G.723.1 G.729A/B PCMU PCMA G.726-32 G722 The default setting is "G722".
Multicast Sender ID	Configures the outgoing caller ID displayed to recipients of multicast pages on channels 1-50.
Multicast Call Timeout (s)	Configures the timeout, in seconds, for multicast calls. When a multicast call exceeds the configured time, it automatically ends. Setting this value to 0 disables the multicast call timeout. The default setting is "0".
Multicast Tone	Enables or disables playing a prompt tone at the beginning and end of a received multicast page. Enabled by default.
Multicast Listening	Configures up to 10 multicast listening addresses and their corresponding labels. Listening Address: Must match the sender's address, such as 237.11.10.11:6767. Label: Specifies a description for the address. For details, refer to the Multicast Paging User Guide on the Grandstream website.
Phone settings -> Local Feature Codes	
Normal Call	
IP Call Feature Code	Configures the feature code for initiating an IP call.The default setting is *47.

Preferred Codec Feature Code	Configures the feature code that prefers a specific codec when initiating a call. The codes for different codecs are as follows: PCMU: 7110 PCMA: 7111 G723: 723 G726-32: 72632 G729A/B: 729 G722: 722 iLBC: 7201 OPUS: 7205 Example: To use PCMU when initiating a call dial: Feature Code + 7110 + Extension. The default setting is *01.
Force Codec Code Feature Code	Configures the feature code that forces the use of a specific codec when initiating a call. The codec codes and dialing is similar to Preferred Codec Feature Code. The default setting is *02.
Paging Call Feature Code	Configures the feature code for initiating a paging call. The default setting is *74.
SRTP	
Enable SRTP Feature Code	Configures the feature code for enabling SRTP. The default setting is *16.
Disable SRTP Feature Code	Configures the feature code for disabling SRTP. The default setting is *17.
Force Use SRTP Call Feature Code	Configures the feature code that forces enabling SRTP when initiating a call. The default setting is *18.
Force Not Use SRTP Call Feature Code	Configures the feature code that forces disabling SRTP when initiating a call. The default setting is *19.
Anonymous	
Enable Global Anonymous Call Feature Code	Configures the feature code for enabling global anonymous calling. The default setting is *30.
Disable Global Anonymous Call Feature Code	Configures the feature code for disabling global anonymous calling. The default setting is *31.
Anonymous Call Feature Code	Configures the feature code for initiating an anonymous call. The default setting is *67.
Non-Anonymous Call Feature Code	Configures the feature code for initiating a non-anonymous call. The default setting is *82.
Hide Callee-ID Call Feature Code	Configures the feature code for hiding the Callee-ID when initiating a call. The default setting is *68.
Call Waiting	
Enable Call Waiting Feature Code	Configures the feature code for enabling call waiting. The default setting is *51.
Disable Call Waiting Feature Code	Configures the feature code for disabling call waiting. The default setting is *50.
Initiate Call Waiting Call Feature Code	Configures the feature code for placing a call with call waiting enabled. The default setting is *71.
Initiate Non Call Waiting Call Feature Code	Configures the feature code for placing a call with call waiting disabled. The default setting is *70.
Forward	
Enable Forward All Feature Code	Configures the feature code for enabling unconditional call forwarding. The default setting is *72.
Disable Forward All Feature Code	Configures the feature code for disabling unconditional call forwarding. The default setting is *73.
Enable Busy Forward Feature Code	Configures the feature code for enabling call forwarding when the phone is busy. The default setting is *90.
Disable Busy Forward Feature Code	Configures the feature code for disabling call forwarding when the phone is busy. The default setting is *91.
Enable No Answer Forward Feature Code	Configures the feature code for enabling call forwarding when incoming calls are not answered. The default setting is *92.
Disable No Answer Forward Feature Code	Configures the feature code for disabling call forwarding when incoming calls are not answered. The default setting is *93.

Network Settings Page Definitions

Network Settings -> Ethernet Settings	
Internet Protocol	Selects the IP protocol mode used by the phone. Available options are IPv4 Only, IPv6 Only, Both, Prefer IPv4, and Both, Prefer IPv6. The default setting is "IPv4 Only".
IPv4 Address	
IPv4 Address	Configures the phone's IPv4 network settings. Available options are DHCP, Static IP, and PPPoE. The default setting is "DHCP".
Host name (Option 12)	Specifies the client name. This field is optional but may be required by some Internet Service Providers.
Vendor Class ID (Option 60)	Allows clients and servers to exchange the Vendor Class ID.
IPv4 Address	Specifies the IPv4 address when Static IP is selected.
Subnet Mask	Specifies the subnet mask when a static IP is selected for IPv4.
Gateway	Specifies the default gateway when a static IP is selected for IPv4.
PPPoE Account ID	Specifies the PPPoE account ID.
PPPoE Password	Specifies the PPPoE password.
PPPoE Service Name	Specifies the PPPoE service name.
DNS Server 1	Specifies the primary DNS server when Static IP is selected for IPv4.
DNS Server 2	Specifies the secondary DNS server when Static IP is selected for IPv4.
Preferred DNS Server	Specifies the preferred DNS server for IPv4.
IPv6 Address	
IPv6 Address	Configures the phone's IPv6 network settings. Available options are Auto-configured and Statically Configured. The default setting is "Auto-configured".
Static IPv6 Address	Specifies the static IPv6 address when Full Static is selected under Statically Configured IPv6 address type.
IPv6 Prefix Length	Specifies the IPv6 prefix length when Full Static is selected under Statically Configured IPv6 address type.
IPv6 Prefix (64 bits)	Specifies the IPv6 prefix (64 bits) when Prefix Static is selected under Statically Configured IPv6 address type.
DNS Server 1	Specifies the primary DNS server for IPv6.
DNS Server 2	Specifies the secondary DNS server for IPv6.
Preferred DNS server	Specifies the preferred DNS server for IPv6.
802.1X	
802.1X Mode	Configures the 802.1X authentication method. The available authentication methods include EAP-MD5, EAP-TLS, and EAP-PEAPv0/MSCHAPv2. The default setting is "Disabled".
802.1X Identity	Specifies the identity information used for 802.1X authentication. Note: Letters, digits, and special characters, including @ and ", are supported.
Password	Specifies the password used for 802.1X MD5 authentication. Note: Letters, digits, and special characters, including @ and ", are supported.
802.1X CA Certificate	Uploads or deletes the 802.1X CA certificate stored on the phone.
802.1X Client Certificate	Uploads or deletes the 802.1X client certificate stored on the phone.

Network Settings -> Wi-Fi Settings (GRP2601W/GRP2602W Only)	
Wi-Fi Function	Enables or disables the Wi-Fi feature on the phone. The available options are: Enable: Enables Wi-Fi to connect to Wi-Fi network. Disable: Disables Wi-Fi. User has ability to enable Wi-Fi from LCD Menu. Disable & Hide Menu from LCD: Disables Wi-Fi and hides "Wi-Fi Settings" menu from phone LCD. The default setting is "Enable".
Wi-Fi Band	Specifies the Wi-Fi frequency band used by the phone. The available options are: 5G & 2.4G, 5G, and 2.4G. The default setting is "5G & 2.4G".
Country Code	Configures Wi-Fi country code.
ESSID	
ESSID	Scans the available Wi-Fi networks and allows connecting to them or manually configuring a network by entering the SSID name, password, and security mode.
Security Mode	Specifies the encryption type used to secure the Wi-Fi connection. The security protocols supported are: WEP: Outdated and insecure Wi-Fi encryption protocol using RC4, easily compromised. WPA/WPA2: Improved Wi-Fi security using PSK, with WPA2 utilizing AES encryption. WPA-Enterprise(802.1x): Enterprise Wi-Fi security with 802.1X authentication and RADIUS server. WPA3-SAE: Latest Wi-Fi security with enhanced protections against brute-force attacks. WPA3-Enterprise(802.1x): Stronger encryption and security for enterprise networks using 802.1X authentication.
Password	Specifies the Wi-Fi authentication password for the selected Wi-Fi network.
Advanced	Configures advanced Wi-Fi network settings, regarding IPv4 and IPv6 modes.
Network Settings -> OpenVPN(R) Settings	
OpenVPN(R) Enable	Enables or disables the OpenVPN(R) feature. Disabled by default.
Manual Import	
Import OpenVPN(R) Configuration	Imports the configuration file from the current computer. After importing the .ovpn file, the local configuration will be overwritten and OpenVPN(R) function is automatically enabled.
Local Configuration	
OpenVPN(R) Server Address	Specifies the IP address or FQDN of the OpenVPN(R) server.
OpenVPN(R) Port	Specifies the listening port of the OpenVPN(R) server. The default setting is "1194". The valid range is 1 to 65535.
OpenVPN(R) Server Secondary Address	Configures a secondary OpenVPN(R) server address as a backup if the primary server is unavailable. When Randomly Select Server is enabled, the phone randomly selects a server instead of prioritizing the primary server address.
OpenVPN(R) Secondary Port	Specifies the port of the secondary OpenVPN(R) server.
Randomly Select Server	Enables or disables random server selection for OpenVPN(R) connections. When enabled, the phone randomly selects a server from the configured server list. When disabled, servers are used according to their configuration order. Disabled by default.
OpenVPN(R) Transport	Specifies the OpenVPN(R) transport protocol. The available options are UDP, TCP, UDP IPV4 Only, TCP IPV4 Only, UDP IPV6 Only, TCP IPV6 Only. The default setting is "UDP".
OpenVPN(R) CA	Uploads and allows viewing and deleting the Certificate Authority (CA) certificate for OpenVPN(R). To replace an existing certificate, delete the current certificate before uploading a new one.
OpenVPN(R) Certificate	Uploads and allows viewing and deleting the OpenVPN(R) client certificate. To replace an existing certificate, delete the current certificate before uploading a new one.

OpenVPN(R) Client Key	Uploads and allows viewing and deleting the OpenVPN(R) client key. To replace an existing key, delete the current key before uploading a new one.
OpenVPN(R) Client Key Password	Configures the password required to access the OpenVPN(R) client key.
OpenVPN(R) TLS Key	Uploads and deletes the OpenVPN(R) TLS key.
OpenVPN(R) TLS Key Type	Specifies the OpenVPN(R) TLS key type. The available options are: None, TLS-Auth, TLS-Crypt and TLS-Crypt V2.The default setting is "None".
OpenVPN(R) Cipher Method	Specifies multiple OpenVPN encryption algorithms to be used by the OpenVPN(R) server. The supported algorithms are: Blowfish AES-128 AES-256 Triple-DES AES-128-GCM AES-256-GCM CHACHA20-POLY1305 All the supported algorithms are selected by default.
OpenVPN(R) Username	Configures the optional username used for OpenVPN(R) authentication if supported by the OpenVPN(R) server.
OpenVPN(R) Password	Configures the optional password used for OpenVPN(R) authentication if supported by the OpenVPN(R) server.
OpenVPN(R) Comp-lzo	Enables or disables LZO compression. When LZO compression is enabled on the OpenVPN(R) server, this option must also be enabled on the phone. Enabled by default.
Additional Options	Configures additional OpenVPN(R) configuration options to be appended to the OpenVPN(R) configuration file. Multiple options should be separated by semicolons. For example: comp-lzo no;auth SHA256.Note: Use this option with caution. Ensure that the configured options are supported by OpenVPN(R) and do not override other settings unnecessarily.
Network Settings -> Advanced Settings	
Advanced Settings	
Advanced Network Settings	
DNS Refresh Timer (m)	Configures the refresh interval, in minutes, for DNS queries. If set to 0, the phone uses the DNS query TTL returned by the DNS server.The default is "0". The valid range is 0-1440.
DNS Failure Cache Duration (m)	Configures the duration, in minutes, for which the phone uses the previous DNS cache when a DNS query fails. If set to 0, this feature is disabled. This setting applies only to SIP registration.The default is "0". The valid range is 0-1440.
Enable LLDP	Enables or disables the Link Layer Discovery Protocol service.Enabled by default.
LLDP TX Interval	Configures the LLDP TX interval (in seconds). The default setting is "60". The valid range is 1 to 3600.
LLDP Timeout Before DHCP Request (s)	Configures the time, in seconds, the device waits for LLDP frames before sending a DHCP request. If set to "0", the device does not wait.The default setting is "0". The valid range is 0-30 seconds.
Enable CDP	Enables or disables the Cisco Discovery Protocol feature.Enabled by default.
Layer 3 QoS for SIP	Configures the Layer 3 QoS parameter for SIP. This parameter is used for IP Precedence, DiffServ, or MPLS.The default setting is "26".
Layer 3 QoS for RTP	Configures the Layer 3 QoS parameter for RTP. This parameter is used for IP Precedence, DiffServ, or MPLS.The default setting is "46".
Enable DHCP VLAN	Enables or disables auto-configuration of VLAN settings via DHCP.Disabled by default.
Enable Manual VLAN Configuration	Enables or disables whether the phone keeps the VLAN configuration without applying it.Enabled by default.
Layer 2 QoS 802.1Q/VLAN Tag	Configures the VLAN tag for Layer 2 QoS packets.The default setting is "0". The valid range is 0-4094.

Layer 2 QoS 802.1p Priority Value	Configures the VLAN Layer 2 QoS packet priority value.The default setting is "0". The valid range is 0 to 7.
Maximum Transmission Unit (MTU)	Defines the Maximum Transmission Unit (MTU) in bytes. The default setting is "1500" bytes. The valid range is 576 to 1500.
PC Port Mode	
PC Port Mode	Configures the PC port mode. When set to "Enabled and Mirrored", the traffic on the LAN port also passes through the PC port, allowing packets to be captured by connecting a PC to the phone.The default setting is "Enabled but Not Mirrored".
PC Port VLAN Tag	Configures the VLAN tag for the PC port.The default setting is 0. The valid range is 0-4094.
PC Port Priority Value	Configures the packet priority value for the PC port.The default setting is 0. The valid range is 0-7.
Proxy	
HTTP Proxy	Specifies the HTTP proxy URL for the phone to send packets through. The proxy server acts as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the phone to send packets through. The proxy server acts as an intermediary to route the packets to the destination.
Bypass Proxy for	Configures the destination IP address where no proxy server is needed. The phone will not use a proxy server when sending packets to the specified destination IP address.
Remote Control	
Action URI Support	Enables or disables the Action URI feature on the phone.Enabled by default.
Remote Control Pop up Window Support	Enables or disables displaying the "Allow Remote Control" pop up window.Enabled by default.
Action URI Allowed IP List	Specifies the list of IP addresses permitted to send Action URI commands to the phone. Multiple IP addresses must be separated by commas. Set this field to any to allow requests from any IP address. By default, the list is empty, which prevents remote control requests from all IP addresses.
CSTA Control	Enables or disables the CSTA control feature. Disabled by default.
CTI Settings	
Affinity Support	Enables or disables communication with the GS Affinity CTI application for computer-based call control. A reboot is required after enabling this feature.Disabled by default.
Preferred Account	Selects the affinity target SIP account.The default setting is "Account 1".
Static DNS Cache	

NAPTR	Configures Naming Authority Pointer (NAPTR) records used to define rules for rewriting one type of domain name to another, typically for handling Uniform Resource Identifiers (URIs). Configuring NAPTR records in the Static DNS Cache allows the phone to apply custom rules for resolving specific domain names or URIs. The following options are available: NAPTR DNS Cache Name: Specifies the domain name associated with the NAPTR record. NAPTR DNS Cache Time Interval (s): The time interval that the resource record may be cached before the source of the information should again be consulted. The default value is 300 seconds. NAPTR DNS Cache Order: A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules. NAPTR DNS Cache Preference: A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed, low numbers being processed before high numbers. NAPTR DNS Cache Replacement: Specifies the replacement domain name that is queried for the corresponding SRV records. NAPTR DNS Cache Service: Specifies the service(s) associated with the NAPTR record.
SRV	Configures Service (SRV) records used to identify the servers that provide specific services, such as SIP or email. Configuring SRV records in the Static DNS Cache allows the phone to resolve service-specific servers without relying solely on DNS queries. The following options are available: SRV DNS Cache Name: Specifies the domain name string with SRV prefix. SRV DNS Cache Time Interval (s): Specifies the time interval that the resource record may be cached before the source of the information should again be consulted. The default value is 300 seconds. SRV DNS Cache Priority: Set the priority of this target host. SRV DNS Cache Weight: Set server selection mechanism. SRV DNS Cache Target: The domain name of the target host. SRV DNS Cache Port: Set the port on the target host of this service.
A	A records are used to map a domain name to an IPv4 address. They are the most common type of DNS record and are used to resolve domain names to IP addresses, Configuring A records in the static DNS cache allows you to manually specify the IP addresses associated with specific domain names, ensuring that your IP phone always connects to the intended destination, the options to configure are: A DNS Cache Name: Sets the hostname. A DNS Cache Time Interval: Specifies the duration, in seconds, that the A record remains in the cache before being refreshed. The default setting is 300 seconds. A DNS Cache IP Address: Specifies the IPv4 address.

Network Settings Definitions

Programmable keys Page Definitions

Programmable keys -> Multi-Purpose Keys (GRP2604 only)
Keys Settings

Mode	Speed Dial: Select the Account to dial from. And enter the Speed Dial number in the Value field to be dialed or enter the IP address to set the Direct IP call as Speed Dial. Busy Lamp Field (BLF): Select the Account to monitor the BLF status. Enter the extension number in the Value field to be monitored. Presence Watcher: This option has to be supported by a presence server and it is tied to the "Do Not Disturb" status of the phone's extension. Eventlist BLF: This option is similar to the BLF option but in this case the PBX collects the information from the phones and sends it out in one single notify message. PBX server has to support this feature. 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 configured Speed Dial number using account 2 Dial DTMF: Enter a series of DTMF digits, a character from "A-D" or "R" (for Hook Flash) in the Value field to be dialed during the call. "Enable MPK Sending DTMF" has to be set to "Yes" first. Voicemail: Select Account and enter Voicemail access number in the Value field. CallReturn: The last answered calls can be dialed out by using Call Return. The Value field should be left blank. Also, this option is not binding to the account and the call will be returned based on the account with the last answered call. Transfer: Select Account and enter the number in the Value field to be transferred (blind transfer) during the call. CallPark: Select Account and enter the call park extension in the Value field to park/pick up the call. LDAP Search: This option is to narrow the LDAP search scope. Enter the LDAP search base in the Description field. It could be the same or different from the Base in LDAP configuration under Advanced Settings. The Base in LDAP configuration will be used if the Description field is left blank. Enter the LDAP Name/Number filter in the Value field. For example: If users set MPK 1 as "LDAP Search" for "Account 1", and set filters: Description ou=video,ou=SZ,dc=grandstream,dc=com Value sn=Li Since the Base for LDAP server configuration is: "dc=grandstream,dc=com", "ou=video,ou=SZ" is added to narrow the LDAP search scope. "sn=Li" is the example to filter the last name. Conference: Allow user to set their Multi-Purpose Key to "Conference" mode to trigger a conference. By setting the extension number in the value box, the users will be able to activate a 3-way conference by simply press the assigned MPK button. Multicast Paging: Allows the user to configure the address to send a multicast page to. Call History: Select Account and enter account number in the Value field to allow configuration of call log for other extension. Monitored Call Park: Select account from Account field and enter the call park extension in the Value field to park/pick up the call, and also monitor the parked call via Line Key's light. Menu: Select this feature in order to display the Menu from the MPK buttons, no field dis required for configuration. INFO: Select this feature in order to display the Information popup to show the firmware version, MAC address, IP address and IP Settings from the MPK buttons, no field dis required for configuration. Message: Select this feature in order to display the Message menu from the MPK buttons, no field dis required for configuration. Forward: Set the MPK Button to perform call forwarding to the destination number configured on the "Value Field". During ringing press the button to perform the call forward. DND: Press the configured key to enabled/Disable DND. Redial: On this mode, the configured key can be used to redial numbers. Presence Eventlist: This option is similar to the Presence Watcher option but in this case the PBX collects the information from the phones and sends it out in one single notify message. Note: The PBX server has to support this feature. Provision: Select this feature in order to make the phone trigger an instant provisioning. Opendoor: Select this feature in order to make the phone trigger an open-door action in conjunction with a GDS37xx Multicast Listen Address: This feature sets up a multicast listening address for the IP Phone. Multicast Paging Address: This Feature sets up a Multicast paging address for paging purposes. Note: An MPK configuration tutorial video link can be found on the MPK configuration page. HTTP Command: This Feature sets up a call through an HTTP command Call Flip: Call Flip with MPK is a feature that allows you to transfer an active call from one VoIP phone to another or to a different number using a programmable Multi-Purpose Key, ensuring a seamless transition. Visual Park: Used with PortSIP servers, this feature allows the GRP260x phone to act as a visual call parking location. Silent Call: This feature allow users to initiate calls from a GRP260x phone to an extension without any audible or visual indication on the LCD screen, providing discreet calling where the call's status remains hidden which is intended for emergency or panic scenarios. Note: In silent call mode, the device behaves as follows: The device's microphone is activated and transmits audio to the called party. The speaker remains muted, meaning the caller hears no audio
------	---

Account	Selects the account to associate with the configured MPK.
Value	Configures the value associated with the MPK, such as an extension number, multicast address, or SIP URI. Note: When a call is initiated using a valid SIP URI, the hostname part of the SIP URI is displayed on the LCD.
Label	Configures the label associated with the MPK.
Basic Settings	
Transfer Mode via MPK	Selects the transfer mode to perform when the user presses the Transfer MPK. The available options are blind transfer, attended transfer, and new call to the number specified in the Value field.
Enable Transfer via Non-Transfer MPK	Enables or disables using MPKs configured with types such as BLF or Speed Dial to perform transfers during an active call.
Programmable Keys -> Virtual Multi-Purpose Keys	
Mode	Selects the VPK's mode. The available options are: None Line Shared Speed Dial BLF Presence Watcher Eventlist BLF Speed Dial via Active Account Dial DTMF Voicemail CallReturn Transfer CallPark Intercom LDAP Search Conference Multicast Paging Call History Monitored Call Park Menu XML Application INFO Messages Forward DND Redial Multicast Listen Address OpenDoor Presence Eventlist Provision Multicast Paging Address HTTP Command Call Flip Visual Park Silent Call Note: When a monitored extension (BLF or Monitored Call Park) receives a call and the VPK is configured on a page other than the first page, the phone LCD backlight brightness activates, and the corresponding page number and navigation arrow flicker to indicate the incoming call.
Account	Selects the account to associate with the configured MPK.
Value	Configures the value associated with the MPK, such as an extension number, multicast address, or SIP URI. Note: When a call is initiated using a valid SIP URI, the hostname part of the SIP URI is displayed on the LCD.
Label	Configures the label associated with the MPK.
Preview	Displays a preview of the configured MPK label. After saving, the card label can be printed from the preview.
Programmable Keys -> Number Keys	
Number Key	Selects the function key's mode. The available options are: None Speed Dial Speed Dial via Active Account Dial DTMF Voicemail CallReturn LDAP Search Call History INFO Messages DND Redial OpenDoor Provision HTTP Command Depending on the selected function key mode, some or all of the following fields become available for configuration: Account: Selects the account to associate with the function key. Value (User ID): Configures the value associated with the function key, such as an extension number. Label: Configures the label associated with the function key.
Programmable Keys -> Navigate Keys	
Navigate Keys	Navigate Keys Up Navigate Key Down Navigate Key Left Navigate Key Right Navigate Key OK Key Short Press Function None Menu Settings VPK Page Left VPK Page Right Previous Account Next Account INFO Virtual Expansion Board QRCode Voicemail Instant Messages Missed Call History Dialed Call History Received Call History Local Phonebook Remote Phonebook BroadSoft Directory LDAP Long Press Function None Menu Settings VPK Page Left VPK Page Right Previous Account Next Account INFO Virtual Expansion Board QRCode Voicemail Instant Messages Missed Call History Dialed Call History Received Call History Local Phonebook Remote Phonebook BroadSoft Directory LDAP
Programmable keys -> Virtual Extension Note: For more information on configuring Virtual extensions, please refer to the following guide: GRP260x Virtual Extension User Guide?	

Access IP type	Specifies how to access the Virtual Extension module interface. Users can enter the phone's LAN IP address or mDNS domain in a browser, or scan the QR code on the webpage using a phone connected to the same network as the IP phone. After scanning, a new window prompts users to log in with their IP phone credentials.
Download App	Downloads the app by hovering over the icon for the desired operating system (iOS or Android) and scanning the displayed QR code.

Mode

Speed Dial: Select the Account to dial from. And enter the Speed Dial number in the Value field to be dialed or enter the IP address to set the Direct IP call as Speed Dial. Busy Lamp Field (BLF): Select the Account to monitor the BLF status. Enter the extension number in the Value field to be monitored. Presence Watcher: This option has to be supported by a presence server and it is tied to the "Do Not Disturb" status of the phone's extension. Eventlist BLF: This option is similar to the BLF option but in this case the PBX collects the information from the phones and sends it out in one single notify message. PBX server has to support this feature. 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 configured Speed Dial number using account 2. Dial DTMF: Enter a series of DTMF digits in the Value field to be dialed during the call. "Enable MPK Sending DTMF" has to be set to "Yes" first. Voicemail: Select Account and enter Voicemail access number in the Value field. Call Return: The last answered calls can be dialed out by using Call Return. The Value field should be left blank. Also, this option is not binding to the account and the call will be returned based on the account with the last answered call. Transfer: Select Account and enter the number in the Value field to be transferred (blind transfer) during the call. Call Park: Select Account and enter the call park extension in the Value field to park/pick up the call. LDAP Search: This option is to narrow the LDAP search scope. Enter the LDAP search base in the Description field. It could be the same or different from the Base in LDAP configuration under Advanced Settings. The Base in LDAP configuration will be used if the Description field is left blank. Enter the LDAP Name/Number filter in the Value field. For example: If users set MPK 1 as "LDAP Search" for "Account 1", and set filters: Description -> ou=video, ou=SZ, dc=grandstream, dc=com Value -> sn=Li Since the Base for LDAP server configuration is: "dc=grandstream, dc=com", "ou=video, ou=SZ" is added to narrow the LDAP search scope. "sn=Li" is the example to filter the last name. Conference: Allow user to set their Multi-Purpose Key to "Conference" mode to trigger a conference. By setting the extension number in the value box, the users will be able to activate a 3-way conference by simply press the assigned MPK button. Multicast Paging: Allows the user to configure the address to send a multicast page to. Call Log: Select Account and enter account number in the Value field to allow configuration of call log for other extension. Monitored Call Park: Select account from Account field and enter the call park extension in the Value field to park/pick up the call, and also monitor the parked call via Line Key's light. Menu: Select this feature in order to display the Menu from the MPK buttons, no field is required for configuration. Information: Select this feature in order to display the Information popup to show the firmware version, MAC address, IP address and IP Settings from the MPK buttons, no field is required for configuration. Message: Select this feature in order to display the Message menu from the MPK buttons, no field is required for configuration. Forward: Set the MPK Button to perform call forwarding to the destination number configured on the "Value Field". During ringing press the button to perform the call forward. DND: Press the configured key to enable/disable DND. Redial: On this mode, the configured key can be used to redial numbers. Presence Eventlist: This option is similar to the Presence Watcher option but in this case the PBX collects the information from the phones and sends it out in one single notify message. Note: The PBX server has to support this feature. Provision: Select this feature in order to make the phone trigger an instant provisioning. Opendoor: Select this feature in order to make the phone trigger an open-door action in conjunction with a GDS37xx. Multicast Listen Address: This feature sets up a multicast listening address for the IP Phone. Multicast Paging Address: This Feature sets up a Multicast paging address for paging purposes. Note: An MPK configuration tutorial video link can be found on the MPK configuration page. HTTP Command: This Feature sets up a call through an HTTP command. Call Flip: Call Flip with MPK is a feature that allows you to transfer an active call from one VoIP phone to another or to a different number using a programmable Multi-Purpose Key, ensuring a seamless transition. Visual Park: Used with PortSIP servers, this feature allows the GRP260x phone to act as a visual call parking location. Silent Call: Silent Call feature allows users to initiate a call to another extension without triggering any audible or visible notification. The GRP260x does not display caller ID or dialing screen. In this mode: The device's microphone is activated and transmits audio to the called party. The speaker remains muted, meaning the caller hears no audio from the callee. Functional keys on the phone are locked during the call, except number keys, softkeys, and line keys. Only emergency numbers can be dialed during an active Silent Call

Account	Selects the account to associate with the configured Virtual MPK.
Value	Configures the value associated with the Virtual MPK, such as an extension number or multicast address.
Label	Configures the label associated with the Virtual MPK.
Preview	Displays a preview of the configured Virtual MPK label.
Programmable Keys -> Idle Screen Softkeys	
Custom Idle Screen Softkey Layout	Enables or disables the custom idle screen softkey layout. Disabled by default.
Custom Softkey	
Add Custom Softkey	Adds a custom softkey to configure its icon, function, label, and associated user ID. Key Mode: Selects the icon and function of the custom softkey. The available options are Speed Dial, Speed Dial Active, DialDTMF, Voice Mail, and Silent Call. Label: Configures the label displayed for the custom softkey. Value (User ID): Configures the user ID for which the custom softkey is displayed.
Custom Softkey Layout	
Custom Softkey Layout	Configures the softkeys displayed on the phone's idle screen. Select softkeys from the "Available" list to add them to the "Enabled" list. Up to 6 softkeys can be enabled.
Programmable Keys -> Call Screen Softkeys	
Custom Call Screen Softkey Layout	Enables or disables the custom call screen softkey layout.Disabled by default.
Enforce Softkey Layout Position	Enables or disables enforcing the configured softkey positions. When enabled, the GUI preserves the space for a configured softkey even when it cannot be displayed.Disabled by default.
Custom Softkey	
Add Custom Softkey	Adds a custom softkey to configure its icon, function, label, and associated user ID. Key Mode: Selects the icon and function of the custom softkey. The available options are Speed Dial, Speed Dial Active, DialDTMF, Voice Mail, and Silent Call. Label: Configures the label displayed for the custom softkey. Value (User ID): Configures the user ID for which the custom softkey is displayed.
Custom Softkey Layout	
Call Status	Selects the phone status and configures the softkeys to enable for that status. The available statuses are: Dialing Ringing Calling Call Connected On Hold Call Failed Transfer Conference Conference Connected Onhook Dialing
Programmable Keys -> Advanced Settings	
Auto Provision List Starting Point	Selects the type of keys to use first for the Auto Provision Eventlist BLF feature. The available options are: VPK (Virtual Programmable Key): Uses virtual programmable keys on the device. Exty APP: Uses expansion modules or application-specific keys. The default setting is "VPK".
Transfer Mode via Programmable Keys	Selects the transfer mode to use when pressing the Transfer MPK. The available options are Blind Transfer, Attended Transfer, and New Call.The default setting is "Blind Transfer".
Enable Transfer via Non-Transfer Programmable Keys	Enables or disables using programmable keys configured as BLF, Speed Dial, or other types to perform transfers during an active call.Disabled by default.
Allow Programmable Key Configuration via LCD	Enables or disables configuring programmable keys through the LCD by pressing and holding an MPK/VPK.Enabled by default.
VPK Paging Auto Return Timeout(s)	Configures the timeout, in seconds, before returning to the main interface after navigating through VPK pages. Setting this value to 0 disables the automatic return. The default setting is "0".

System Settings Page Definitions

System Settings -> Time and Language	
Date and Time	
NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. The default setting is "pool.ntp.org".
Secondary NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. Allow user to configure 2 NTP server domain names. GRP will loop through all the IP addresses resolved from them.
Enable Authenticated NTP	Enables or disables NTP authentication. If enabled, a cryptographic signature appended to each network packet. If the key is incorrectly configured, the phone will refuse to use the time provided by the NTP server.Disabled by default.
Authenticated NTP Key ID	Configures the key ID for authenticated NTP.The default setting is "1".
Authenticated NTP Key	Uploads the key file for authenticated NTP. Note: Only support MD5 key type.
NTP Update Interval	Configures the interval, in minutes, for updating time from the NTP server.The default setting is "1440". The valid range is 5 to 1440.
Allow DHCP Option 42 to Override NTP Server	Enables or disables allowing DHCP Option 42 to override NTP server. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN.Enabled by default.
Time Zone	Selects the Time Zone for the phone.The default setting is "Auto".
Allow DHCP Option 2 to Override Time Zone Setting	Enables or disables allowing DHCP Option 2 to override the configured Time Zone.Enabled by default.
Self-Defined Time Zone	Defines a custom time zone when Time Zone is set to "Self-Defined Time Zone". The syntax is: std offset dst [offset], start [/time], end [/time]The default setting is "MTZ+6MDT+5,M4.1.0,M11.1.0". MTZ+6MDT+5: This indicates a time zone with a 6-hour offset from the Prime Meridian and a 1-hour adjustment during daylight saving time, corresponding to U.S. Central Time. If the offset is positive (+), the local time zone is west of the Prime Meridian (also known as the International Meridian or Greenwich Meridian). If the offset is negative (-), the local time zone is east of the Prime Meridian. M4.1.0,M11.1.0: Defines the month (1-12, January through December), the nth iteration of the weekday in the month (1-5), and the weekday (0-6, Sunday through Saturday), respectively. Therefore, the default setting specifies daylight saving time (DST) starting on the first Sunday of April and ending on the first Sunday of November.
Date Display Format	Configures the date display format on the LCD. The available options are: yyyy-mm-dd: 2019-03-02 mm-dd-yyyy: 03-02-2019 dd-mm-yyyy: 02-03-2019 dddd, MMMM dd: Saturday, March 02 The default setting is "yyyy-mm-dd".
Time Display Format	Selects whether the time display format on the LCD is 12-hour or 24-hour based.The default setting is "12 Hour".
Language	
Display Language	Selects display language on the phone from the supported languages.The default setting is "Auto".
System Settings -> Input Method	
Input Method for Contacts	Sets the input method for contacts. The available options are: 123 abc ABC Ab2 Q9 The default setting is "123".
Input Method for LDAP	Sets the LDAP input method.The default setting is "123".
System Settings -> Security Settings	
Web/SSH Access	

SSH Access	
Enable SSH	Enables or disables the SSH Access feature.Enabled by default.
SSH Port	Configures the port for SSH access.The default setting is "22".
SSH Public Key	Uploads the SSH public key for authentication as an alternative to password authentication. The SSH public key must be 2048 bits long.
LCD Access	
Configuration via Keypad Menu	Selects the keypad menu configuration access level. The available options are: Unrestricted: All options on the LCD menu can be accessed. Basic settings only: Only basic settings can be accessed on the LCD menu. Constraint Mode: Accessing options other than basic settings requires permission. Warning: If the admin password is lost while Constraint Mode is enabled, the device may become permanently unusable. Be careful when enabling Constraint Mode to avoid irreversible damage. Locked Mode: The MENU key is disabled. The default setting is "Unrestricted".
Factory Reset Security Level	Configures whether a password is required to perform a factory reset. The available options are: Default: A password is required when the keypad menu configuration access level is set to any mode other than "Unrestricted". Always Require Password: A password is required regardless of the keypad menu configuration access level. No Password Required: A password is not required regardless of the keypad menu configuration access level. The default setting is "Default".
Wi-Fi Settings Security Level	Configures whether a password is required to access Wi-Fi settings. The available options are: Default: A password is required when the keypad menu configuration access level is set to any mode other than "Unrestricted". Always Require Password: A password is required regardless of the keypad menu configuration access level. No Password Required: A password is not required regardless of the keypad menu configuration access level. The default setting is "Default".For GRP2602W only
Web Access	
HTTP Web Port	Specifies the HTTP port for the Web Access Mode.The default value is "80". The valid range is 80 - 65535.
HTTPS Web Port	Specifies the HTTPS port for the Web Access Mode.The default setting is "443". The valid range is 443 - 65535.
Web Access Mode	Configures the protocol(s) for web access. The available options are: HTTPS HTTP Disabled Both HTTP and HTTPS The default setting is "HTTPS".
Web Access Control	Restricts web access based on incoming IP addresses. The available options are: None: Web access is unrestricted. Allow List: Only IP addresses specified in the Web Access Control List can access the web interface. Block List: IP addresses specified in the Web Access Control List are blocked from accessing the web interface. The default setting is "None".
Web Access Control List	Specifies the IP addresses to allow or block from accessing the web interface, depending on the Web Access Control setting.
Web Session Timeout	Configures the idle time, in minutes, before the web session expires. The default setting is "10". The valid range is 2-60.
Enable User Web Access	Enables or disables web access for users. Disabled by default.
Validate Server Certificates	Enables or disables server certificate validation when downloading firmware or configuration files. If enabled, the phone downloads the firmware or configuration file only after validating the server certificate. Disabled by default.
Web/Restrict mode Lockout Duration	Configures the lockout duration, in minutes, after the number of failed login attempts specified in Web Access Attempt Limit is reached on the web interface or in LCD Restrict Mode administrator login.The default setting is "5". The valid range is 0-60.
Web Access Attempt Limit	Configures the number of failed web login attempts allowed before the account is locked out. The default setting is "5". The valid range is 1-10.

User Info Management	
Test Password Strength	Checks password strength to ensure better security. When enabled, the configured password must meet the following criteria: numerics (0-9) capital letters (A-Z) lower case (a-z) special characters ('./`@*-=, &?!%()~_#') Disabled by Default.
User Password	
Reset Password	Resets the user password.
New Password	Configures the user password for Web UI access. This field is case-sensitive and must meet the password requirements when Test Password Strength is enabled.
Confirm Password	Confirms the new user password.
Admin Password	
Reset Password	Resets the admin password.
Current Password	The current admin password is required to set a new admin password.
New Password	Configures the admin password for Web UI access. This field is case-sensitive and must meet the password requirements when Test Password Strength is enabled.
Confirm Password	Confirms the new administrator password.
Client Certificate	
TLS Version	
Minimum TLS Version	Configures the minimum TLS version supported by the phone. The minimum TLS version must be less than or equal to the maximum TLS version. The available options are: TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3 The default setting is "TLS 1.2".
Maximum TLS Version	Configures the maximum TLS version supported by the phone. The maximum TLS version must be greater than or equal to the minimum TLS version. The available options are: Unlimited TLS 1.0 TLS 1.1 TLS 1.2 TLS 1.3 The default setting is "Unlimited".
Global	
Enable LEGACY_SERVER_CONNECT	Enables or disables SSL_OP_LEGACY_SERVER_CONNECT. When enabled, this option permits legacy server connections and applies to TLS 1.2 and earlier versions.Disabled by default.
Enable/Disable Weak Cipher Suites	Defines the function for weak cipher suites. The available options are: Enable Weak TLS Ciphers Suites Disable Symmetric Encryption RC4/DES/3DES Disable Symmetric Encryption SEED Disable All Weak Symmetric Encryption Disable All Weak TLS Ciphers Suites The default setting is "Disable All Weak TLS Ciphers Suites".
SIP TLS Certificate	
SIP TLS Certificate	Specifies the SSL certificate used for SIP transport over TLS/TCP.
SIP TLS Private Key	Specifies the SSL private key used for SIP transport over TLS/TCP.
SIP TLS Private Key Password	Specifies the SSL private key password used for SIP transport over TLS/TCP.
DTLS Version	
Minimum DTLS version	Configures the minimum DTLS version supported by the phone. The minimum DTLS version must be less than or equal to the maximum DTLS version. The available options are: DTLS 1.0 DTLS 1.2 The default setting is "DTLS 1.0".
Maximum DTLS Version	Configures the maximum DTLS version supported by the phone. The maximum DTLS version must be greater than or equal to the minimum DTLS version. The available options are: Unlimited DTLS 1.0 DTLS 1.2 The default setting is "Unlimited".
Custom Certificate	

Custom Certificate	Uploads and allows viewing and deleting custom certificate for SSL/TLS communication.
Individual Certificate	
CA Signature Algorithm	Specifies the root CA signature algorithm used by the server. The available options are md5WithRSAEncryption and ecdsa-with-SHA384. The default setting is "ecdsa-with-SHA384".
Trusted CA Certificate	
Trusted CA Certificates (1 - 6)	Allows uploading and deleting up to 6 CA Certificate files to phone. Note: Users can upload the file directly through the Web UI or provision it through the cfg.xml file.
Load CA Certificates	Specifies the CA certificates used by the phone to verify server certificates. The phone can verify certificates using the default, custom, or both. The default setting is "Default Certificates".
SCEP	
Basic Settings	
Enable SCEP	Enables or disables the SCEP (Simple Certificate Enrollment Protocol) service on the device. Disabled by default.
SCEP Server URL	Fill in the SCEP server URL (CA URL or RA URL), the protocol header must be included in the URL. Only 'HTTP' URL is supported. This server issues certificates to the device after successful authentication. Example: http://ca.example.com/scep
Proxy Server URL	Defines the CA proxy server address if required for network communication.
CA FingerPrint Infomation	Defines the fingerprint of the CA certificate. This ensures the device only trusts the specified Certificate Authority and prevents man-in-the-middle attacks during enrollment.
Challenge Password	Defines the Challenge Password to be sent along with the CSR while applying for a certificate. This value is provided by the CA administrator and is used for initial authentication.
Local Configuration	
Local Public and Private Key Length	Specifies the cryptographic key length used when generating the local key pair. The available options are: 1024 bit 2048 bit 3072 bit 4096 bit. The default setting is "2048 bit".
The Name of Certificate Applicant	Specifies the name of the certificate applicant, which is a required field. The default setting is "name".
The Country of Certificate Applicant Located	Selects the country of the certificate applicant.
The State of Certificate Applicant Located	Specifies the state or province (ST) of the certificate subject.
The Locality of Certificate Applicant Located	Specifies the city or locality (L) of the certificate subject.
The Organization of Certificate Applicant Located	Specifies the organization name (O) associated with the certificate subject.
The organization unit of Certificate Applicant	Specifies the organizational unit (OU) associated with the certificate subject.
HTTP Authentication	
User ID	Defines the HTTP authentication username used to access the SCEP server.
Password	Defines the HTTP authentication password used to access the SCEP server.
Certificates and Updates	
CA Certificate	Allows viewing the CA certificate issued by CA institution via SCEP.

CA Certificate Alternative Name	Configure an alternative name for the CA-signed certificate. The following options are supported: DNS Name (dNSName): A hostname or domain name, e.g., www.example.com. IP Address (iPAddress): An IPv4 or IPv6 address, e.g., 192.168.0.1 or 2001:db8::1. Email Address (rfc822Name): An email address, e.g., user@example.com. X.500 Distinguished Name (directoryName): An X.500 directory name, e.g., /C=US/ST=CA/L=Los Angeles/O=Example Inc./CN=www.example.com. Uniform Resource Identifier (URI) (uniformResourceIdentifier): A URI, e.g., https://www.example.com. Kerberos Service Name (krb5PrincipalName): A Kerberos service name, e.g., HTTP/www.example.com. Note: The default value \$MAC refers to the MAC address printed on the label of the phone case.
Update Interval before Certificate Expiration	Configure the effective time interval (1-30 day) for updating certificates before expiration (CA public key expiration or CA certificate expiration), and update certificates after reaching this interval.Default setting is "20" days.
Scope of Use	Defines which services use the SCEP-issued certificate. Only the selected services will use the enrolled certificate. The available scopes are: SSL/TLS communication Ethernet 802.1X OpenVPN(R)
Keypad Lock	
Enable Keypad Locking	Enables or disables keypad locking. When enabled, the keypad can be locked by pressing and holding the STAR (*) key for 4 seconds. Disabled by default.
Keypad Lock Type	Configures the keypad lock type. When set to "All Keys", all keys are locked and emergency calls cannot be made. When set to "Customized", only "Functional Keys" will be locked but you are still allowed to make emergency calls.The default setting is "All Keys".
Password to Lock/Unlock	Configures the password required to lock or unlock the keypad.
Keypad Lock Timer	Configures the idle timeout, in seconds, before the keypad is locked.The default setting is "0". The valid range is 0 to 3600.
Emergency	Defines emergency call numbers. If multiple emergency call numbers are entered, separate them with ",".The default setting is "112,911,110".
System Settings -> Preferences	
Display Control	
LCD	
Backlight Brightness: Active	Configures the LCD brightness when the phone is active.The default setting is "8". The valid range is 0 to 8, where 8 is the brightest.
Backlight Brightness: Idle	Configures the LCD brightness when the phone is idle.The default setting is "1". The valid range is 0 to 8, where 0 is off and 8 is the brightest.
Active Backlight Timeout	Configures the LCD backlight timeout interval.The default setting is "1". The valid range is 0 to 90.
Enable Missed Call Backlight	Enables or disables turning on the LCD backlight when there is a missed call on the phone. The default setting is "Yes"
Configure the softkey bar style	Configures the softkey bar style, four options are available for selection.The default setting is "Style 1".
LED	
New Message LED Indicator	Enables or disables the LED indicator when new voicemails or text messages are received.The default setting is "Blinking".
Enable Incoming Call Indicator	Enables or disables incoming call indicator. When enabled, the upper right corner LED indicator will light up for the GRP2603(P)/GRP2604(P), while the message waiting indicator LED will light for GRP2602(P/G/W)/GRP2601(P/W), signaling that there is an incoming call.Disabled by Default.
Line LED Color Scheme	Selects the line key LED color scheme. The available options are: Default: off(idle)/green(in use) Light up: green(idle)/red(in use) The default setting is "Default".

Audio Control	
Call Tone Volume	Sets the call tone volume.The default setting is "0". The valid range is -15 to 15.
Speaker Ring Volume	Sets the speaker ring volume.The default setting is "4". The valid range is 0 to 8.
Lock Speaker Volume	Enables or disables locking the volume adjustment. The available options are: No: Speaker volume isn't locked. Ring: Only ringing volume will be locked Talk: Only volume during the call is locked during a call. Both: The speaker volume is locked during both ring time and call. The default setting is "No".
Enable Warning Tone	Enables or disables the warning tone of the phone. If disabled, all pop-up and notifications will play no tone.Enabled by default.
Headset	
Headset Key Mode	Select the Headset Key Mode. The available options are: Default Mode: When the phone is in idle, press HEADSET button to off hook the phone and make calls by using headset. Headset icon will display on the screen in dialing/talking status. When there is an incoming call, press HEADSET button to pick up the call-using headset. When there is an active call using headset, press HEADSET button to hang up the call. When Speaker/Handset is being used in dialing/talking status, press HEADSET button to switch to headset. Press it again to hang up the call. Or, press speaker/Handset to switch back to the previous mode. Toggle Headset/Speaker: When the phone is in idle, press HEADSET button to switch to Headset mode. The headset icon will display on the left side of the screen In this mode, if pressing Speaker button or Line key to off hook the phone, headset will be used. When there is an active call, press HEADSET button to toggle between Headset and Speaker. Disable Headset Key: In this mode, the headset key will be disabled, no action will be performed when pressing the headset key. The default setting is "Default Mode"
Headset Type	Selects whether the connected headset is Normal, Plantronics EHS, Jabra EHS, Sennheiser EHS headset, or VBeT EHS.The default setting is "Normal"
Always Ring Speaker	Enables or disables speaker ringing when the headset is used on "Toggle Headset/Speaker" mode. The available options are: No Yes, Both Yes, Speaker Only The default setting is "Yes, Both"
Group Listen with handset	Enables or disables audio playback through the handset when it is picked up during a call using a headset.Disabled by Default.
Group Listen with Speaker	Enables or disables the softkey that plays audio through the speaker while using the handset or headset.Disabled by Deafult.
Headset TX Gain (dB)	Configures the transmission gain of the headset. The default setting is "0 dB"
Headset RX Gain (dB)	Configures the receiving gain of the headset.The default setting is "0 dB"
Enable Headset Noise Shield	Enables or disables Headset Noise Shield. When enabled, the feature reduces environmental noise heard by the remote party during a call using a headset. The available options are: Disabled Loud Headset Thin Headset Moderate Headset Plantronics SP11-A The default setting is "Moderate Headset".
Headset Equalizer Mode	Selects the headset equalizer mode. The available options are: Disabled Mode 1 Mode 2 Mode 3 The default setting is "Disabled".
Handset	
Handset TX Gain (dB)	Configures the transmission gain of the handset.The default setting is "0 dB"
Enable Handset Noise Shield 2.0	Enables or disables Handset Noise Shield. When enabled, the feature reduces environmental noise heard by the remote party during a call. The available options are High Shielding, which filters out most environmental noise, and Soft Shielding, which retains some ambient noise for the remote party.The default setting is "High Shielding"

Handset Sidetone Volume	Sets the Handset sidetone volume. The default setting is "15". The valid range is 0 to 30.
Enable HAC	Enables or disables HAC. when enabled, the phone will compatible with nearby hearing AIDS.Disabled by Default.
Other Noise Cancellation	
Noise Suppression mode	Selects the priority method for built-in noise cancellation. The available options are: AI Noise Cancellation: this will prioritize AI Noise Cancellation during calls. Traditional Noise Cancellation: this will prioritize Noise Shield 2.0 during calls. The default setting is "AI Noise Cancellation".
System Settings -> Energy Saving	
Instantaneous energy saving ratio	Shows a live energy-saving ratio preview based on the energy-saving mode selected.
Usage	Displays the Deep energy saving duration relative to the phone's enabling duration
Energy saving	Displays a diagram of energy spent in MWh throughout the phone's activity period. By default, it shows a comparison between the energy spent in the current day and the day before.
Energy Saving Master Control	Selects the energy saving mode. The available options are: Standard Mode: The device will behave as it has been prior to addition of the Energy Saving Control feature. All energy related features will function according to the individual configurations. Customized Energy Saving Mode: The device will enable relevant energy-saving measures and support users to operate some basic configuration items. Maximum Energy Saving Mode: The device will ignore all individual configurations and use the setting that will maximize energy saving. No customization is possible under this mode. Note: In the Customized Energy Saving mode, if the configured idle LCD brightness is greater than active LCD brightness , an error message will be displayed.The default setting is "Standard Mode".
Backlight Brightness: Active	Configures the LCD brightness when the phone is active.The default setting is "8". The valid range is 0 to 8, where 8 is the brightest.
Backlight Brightness: Idle	Configures the LCD brightness when the phone is idle. It cannot exceed Backlight Brightness: Active.The default setting is "1". The valid range is 0 to 8, where 0 is off and 8 is the brightest.
Active Backlight Timeout	Configures the LCD backlight timeout interval.The default setting is "1". The valid range is 0 to 90.
Enable Missed Call Backlight	Enables or disables turning on the LCD backlight when there is a missed call on the phone.The default setting is "Yes" except in "Maximum Energy Saving Mode".
System Settings -> Management Settings	
Management Interface	
Enable Secondary Network Interface	Enables or disables the Secondary Network Interface, which creates a virtual network interface layered on top of the physical interface to separate management traffic from VoIP traffic. Disabled by default.
Web/SSH Via	Specifies the network interface used for Web UI and SSH access. The available options are Secondary Network Interface and All Network Interfaces.The default setting is "All Network Interfaces".
SNMP Via	Specifies the network interface used for SNMP traffic.The default setting is "Primary Network Interface".
TR069 Via	Specifies the network interface used for TR-069 communication.The default setting is"Primary Network Interface".
Syslog Via	Specifies the network interface used for Syslog traffic.The default setting is "Primary Network Interface".
Secondary Network Interface IPv4 Address	
802.1Q/VLAN Tag	Specifies the VLAN tag assigned to the Secondary Network Interface. The default setting is "0". The valid range is 0 to 4094.

802.1p Priority Value	Specifies the Layer 2 QoS priority value for the Secondary Network Interface.The default setting is "0". The valid range is 0 to 7.
IPv4 Address Type	Specifies how the Secondary Network Interface obtains its IPv4 address. The available options are DHCP and Static IP.The default setting is "Dynamically assigned via DHCP".
IPv4 Address	Specifies the static IPv4 address when Static IP is selected.
Subnet Mask	Specifies the subnet mask when a static IP is selected.
Gateway	Specifies the default gateway when a static IP is selected.
TR-069	
Enable TR-069	Enables or disables the TR-069 feature.Enabled by default.
ACS URL	Specifies the URL of the Auto Configuration Server (ACS). The default setting is "https://acs.gdms.cloud".
TR-069 Username	Specifies the username used to authenticate with the ACS.
TR-069 Password	Specifies the password used to authenticate with the ACS.
Periodic Inform Enable	Enables or disables periodic Inform messages. When enabled, the phone periodically sends Inform messages to the ACS.Enabled by default.
Periodic Inform Interval	Specifies the interval between Inform messages sent to the ACS.The default setting is "60".
Connection Request Username	Specifies the username used by the ACS to establish a connection with the phone.
Connection Request Password	Specifies the password used by the ACS to establish a connection with the phone.
Connection Request Port	Specifies the port used by the ACS to establish a connection with the phone.The default setting is "7547".
CPE SSL Certificate	Uploads and allows viewing and deleting the SSL certificate used by the phone to establish secure connections with the ACS.
CPE SSL Private Key	Uploads and allows viewing and deleting the SSL private key used by the phone to establish secure connections with the ACS.
Start TR-069 at Random Time	Enables or disables randomized startup for the first TR-069 Inform message. When enabled, the phone sends the first Inform message to the ACS at a random time between 1 and 3600 seconds after boot.Disabled by default.
SNMP Settings	
Enable SNMP	Enables or disables the SNMP feature.Disabled by default.
Version	Specifies the SNMP version used by the phone. The available options are: Version 1, Version 2, and Version 3.The default setting is "Version 3".
Port	Specifies the SNMP port.The default setting is "161". The valid range is 161 or 1025 to 65535.
Community	Specifies the SNMP community string.
Security Level	Specifies the SNMPv3 security level. The available options are: noAuthUser, authUser, and privUser.The default setting is "noAuthUser".
SNMP Username	Specifies the SNMPv3 username.
Authentication Protocol	Specifies the authentication protocol used for SNMPv3. The available options are: None, MD5, and SHA.The default setting is "None".
Privacy Protocol	Specifies the privacy protocol used for SNMPv3. The available options are: None, DES, and AES.The default setting is "None".
Authentication Key	Specifies the authentication key used for SNMPv3.
Privacy Key	Specifies the privacy key used for SNMPv3.

SNMP Trap Version	Specifies the SNMP version used for trap messages. The available options are: Trap Version 1, Trap Version 2, and Trap Version 3.The default setting is "Trap Version 2".
SNMP Trap IP	Specifies the IP address of the SNMP trap receiver.
SNMP Trap Port	Specifies the port used by the SNMP trap receiver.The default setting is "162".
SNMP Trap Interval	Specifies the interval, in seconds, between SNMP trap messages sent to the receiver.The default setting is "5" seconds.
SNMP Trap Community	Specifies the community string associated with the SNMP trap receiver. This value must match the community string configured on the trap receiver.
SNMP Trap Username	Specifies the SNMPv3 username used for trap receiver.
Trap Security Level	Specifies the SNMPv3 security level used for the trap receiver. The available options are: noAuthUser, authUser, and privUser.The default setting is "noAuthUser".
Trap Authentication Protocol	Specifies the authentication protocol used the trap receiver. The available options are: None, MD5, and SHA.The default setting is "None".
Trap Privacy Protocol	Specifies the privacy protocol used for SNMPv3 the trap receiver. The available options are: None, DES, and AES.The default setting is "None".
Trap Authentication Key	Specifies the authentication key used for SNMPv3 the trap receiver.
Trap Privacy Key	Specifies the privacy key used for SNMPv3 the trap receiver.

System Settings Definitions

Maintenance Page Definitions

Maintenance -> Upgrade and Provisioning	
Firmware	
Upgrade via Manually Upload	
Upload Firmware File to Update	Uploads and starts the firmware upgrade process.
Upgrade via Network	
Firmware Upgrade via	Allows to select the firmware upgrade method. The available options are TFTP, HTTP, HTTPS, FTP, and FTPS.The default setting is "HTTP".
Firmware Server Path	Defines the path for the firmware server.
Firmware Server Username	Configures the username for the firmware server.
Firmware Server Password	Configures the password for the firmware server.
Firmware File Prefix	Specifies the encrypted prefix used to identify the firmware file. If configured, only firmware files with the matching prefix are downloaded and flashed to the phone.
Firmware file Postfix	Specifies the encrypted postfix used to identify the firmware file. If configured, only firmware files with the matching postfix are downloaded and flashed to the phone.
Upgrade Detection	
Upgrade	Starts the upgrade process immediately.
Config File	
Configure Manually	

Download Device Configuration	Downloads the phone's configuration file in .txt format.Note: The configuration file does not include passwords or CA/custom certificates.
Download Device Configuration (XML)	Downloads the phone's configuration file in .xml format.Note: The configuration file does not include passwords or CA/custom certificates. Click "XML Help document" to download a template.
Download User configuration	Downloads a configuration file that excludes private data, such as usernames and passwords. The file includes changes manually made through the Web UI or uploaded through "Upload Device Configuration", but does not include changes received through server provisioning via TFTP/FTP/FTPS/HTTP/HTTPS.
Upload Device Configuration	Uploads a configuration file to the phone.
Upload Third-party Vendor Configuration	Uploads configuration files of other manufacturers. Currently, only Yealink and Fanvil are supported.
Export Backup Package	Exports a backup package containing the device configuration and personal data.
Restore from Backup package	Uploads a backup package and restores the phone configuration.
Configure via Network	
Config Upgrade Via	Selects the configuration upgrade method. the available options are TFTP, FTP, FTPS, HTTP, and HTTPS.The default setting is "HTTPS".
Config Server Path	Defines the path for provisioning server.Note: Protocol header can be added in the Config Server path (Eg:https://) without the need to configure it on the "Config Upgrade via" parameter, once configured, it will override the selection on the "Config Upgrade via"
Config Server Username	Configures the username for the HTTP/HTTPS server.
Config Server Password	Configures the password for the HTTP/HTTPS server.
Always Authenticate Before Challenge	Enables or disables authentication before challenge for HTTP/HTTPS. When enabled, the phone sends authentication credentials before receiving an authentication challenge from the server.Disabled by default.
Config File Prefix	Specifies the encrypted prefix used to identify the config file. If configured, only config files with the matching prefix are downloaded and applied to the phone.
Config File Postfix	Specifies the encrypted postfix used to identify the config file. If configured, only config files with the matching postfix are downloaded and applied to the phone.
Authenticate Conf File	Authenticates the configuration file before accepting it.Disabled by default.
XML Config File Password	Configures the password used to encrypt XML configuration files with OpenSSL. This password is required for the phone to decrypt encrypted XML configuration files.
Provision	
Auto Upgrade	
Automatic Upgrade	Enables or disables automatic firmware upgrade and provisioning.The default setting is "No".
Automatic Upgrade Check Interval (m)	Specifies the interval, in minutes, to check for firmware upgrades.The default setting is "10080".
Hour of the Day (0-23)	Specifies the hour of the day to check the HTTP/HTTPS/TFTP/FTP/FTPS server for firmware upgrades or configuration file changes.The default setting is "1:00".
Day of the Week (0-6)	Specifies the day of the week to check the HTTP/HTTPS/TFTP/FTP/FTPS server for firmware upgrades or configuration file changes.The default setting is "Monday".
Start Upgrade at Random Time	Enables or disables randomizing automatic upgrades within the configured hour range or postponing the upgrade by a random interval between 1 and the configured number of minutes.Disabled by default.

Firmware Upgrade and Provisioning	Specifies how firmware upgrade and provisioning requests are handled. The available options are: Always Check for New Firmware Check New Firmware only when F/W Prefix/Suffix Changes Always Skip the Firmware Check. The default setting is "Always Check for New Firmware".
Firmware Upgrade Confirmation	Enables or disables firmware upgrade confirmation. When enabled, the phone prompts the user to confirm the upgrade. If no response is received after a period of time, the phone proceeds with the upgrade. When disabled, the phone will upgrade automatically.Enabled by default.
DHCP Option	
Allow DHCP Option 43 and Option 66 Override Server	Enables or disables DHCP Option 43 and Option 66 from overriding the configured provisioning settings. When enabled, the phone uses DHCP Option 43 for CPE, firmware upgrade, network VLAN tag, and priority configuration. When set to "Prefer, fallback when failed", the phone falls back to the configured firmware and configuration server paths if the server provided by DHCP Option 43 or Option 66 fails.Enabled by default.
Allow DHCP Option 120 to override SIP Server	Enables or disables allowing DHCP Option 120 to override the SIP Server setting on the phone.The default setting is "No".
Additional Override DHCP Option	Configures additional DHCP Option to be used for firmware server instead of the configured firmware server or the server from DHCP Option 33 and 66. This option will be effective only when "Allow DHCP Option 43 and Option 66 to Override Server" is enabled. The available options are: None Option 150 Option 160 The default setting is "Option 150".
Config Provision	
Download and Process All Available Config Files	Enables or disables the phone downloading and processing all available configuration files. By default, GrandStream devices provision the first available configuration file in the following order: cfgMAC -> cfgMAC.xml -> cfgMODEL.xml -> cfg.xml (corresponding to device-specific, model-specific, and global configurations). When enabled, the device downloads and processes all configuration files in the mentioned order, overwriting previous configurations.Disabled by default.
User Protection	Enables or disables user protection. When enabled, P-values configured by the user are not changed by provisioning or provider updates. Disabled by default.
Auto Provision	Enables or disables automatic provisioning. When enabled, the phone sends multicast SUBSCRIBE messages for provisioning to the multicast address in LAN during bootup for automatic provisioning. This feature requires IPPBX support such as 3CX, UCM, etc..Enabled by default.
Advanced Settings	
Validate Hostname in Certificate	Enables or disables validating the hostname in the SSL certificate.Disabled by default.
Enable SIP Notify Authentication	Enables or disables SIP NOTIFY authentication. When enabled, the device challenges NOTIFY requests with a 401 response.Enabled by default.
Factory reset	Starts the Factory Reset process.Warning: Factory reset restores the phone to its default settings and permanently deletes all user-configured settings and data.
Maintenance -> System Diagnosis	
Syslog	
Syslog Protocol	Configures the protocol used to send syslog messages to the syslog server. When set to "SSL/TLS", syslog messages are sent through a secure TLS connection.The default setting is "UDP".Notes: A CA certificate is required to connect to a TLS server.

Syslog Server	Configures the URL or IP address of the syslog server used to receive syslog messages from the phone.Note: A port number can be added to the Syslog Server field (for example, 172.18.1.1:1000) to send syslog messages to the specified port.
Syslog Level	Configures the syslog logging level. The available options are DEBUG, INFO, WARNING, and ERROR.The default setting is "None".Syslog messages are generated based on the following events: Product model/version on boot up (INFO level). NAT related info (INFO level). sent or received SIP message (DEBUG level). SIP message summary (INFO level). inbound and outbound calls (INFO level). registration status change (INFO level). negotiated codec (INFO level). Ethernet link up (INFO level). SLIC chip exception (WARNING and ERROR levels). Memory exception (ERROR level).
Syslog Header Format	Configures the preferred syslog header format. The available options are: Legacy RFC3164 Compliant The default setting is "Legacy ".Note: The RFC3164 compliant header begins with "PRI", which represents the Facility (0-23) and severity level (0-7) of the event. The message includes the timestamp, hostname, process ID, and log message.
Syslog Keyword Filter	Filters syslog messages based on specified keywords. Multiple keywords must be separated by "," without spaces.
Send SIP Log	Enables or disables including SIP logs in syslog messages. Disabled by default.Note: When enabled, the phone sends SIP logs through syslog even when Syslog Level is set to "None".
Maintain System Log Information after Factory Reset	Enables or disables maintaining the system log information across a factory reset.Disabled by default.
Packet Capture	
With RTP Packets	Enables or disables including RTP packets in the packet capture file.Disabled by default.
With Secret Key Information	Enables or disables including secret key information in the packet capture file.Enabled by default.
Packet Capture Data Coverage	Enables or disables overwriting packet capture data when the data reaches 5 MB. When enabled, the latest packet capture data overwrites the oldest data. When disabled, packet capturing stops when the data reaches 5 MB.Disabled by default.
Ping	
Start	Tests connectivity to the specified IP address or URL using a ping request.
Traceroute	
Start	Tests the network path to the specified IP address or URL using a traceroute request.
Remote Diagnostics	
Start	Starts remote diagnostics, enabling remote access and log collection. The session ends automatically when it expires.
Access Address	Displays the IP address and port number used to access the device remotely.
Expiration Time	Displays the expiration time of the remote diagnostics session, which is set to 48 hours after the session starts.
Stop	Manually stops the remote diagnostics session.
Maintenance -> Outbound Notification	
Action URL	
Phone Status	
Setup Completed	Configures the Action URL to send when phone finishes setup process.
Registered	Configures the Action URL to send when phone successfully registers a SIP account.

Unregistered	Configures the Action URL to send when phone unregisters a SIP account.
Register failed	Configures the Action URL to send when phone fails to register a SIP account.
Idle to Busy	Configures the Action URL to send when phone's state changes from idle to busy.
Busy to Idle	Configures the Action URL to send when phone's state changes from busy to idle.
Auto Provision Completed	Configures the Action URL to send when phone's auto provisioning process is completed.
IP Change	Configures the Action URL to send when the IP address changes.
Call Operation	
Off-hook	Configures the Action URL to send when phone is in off-hook state.
On-hook	Configures the Action URL to send when phone is in on-hook state.
Incoming Calls	Configures the Action URL to send when phone receives an incoming call.
Outgoing Calls	Configures the Action URL to send when phone places a call.
Missed Call	Configures the Action URL to send when phone has a missed call.
Established Call	Configures the Action URL to send when phone establishes a call.
Forwarded Call	Configures the Action URL to send when phone forwards an incoming call.
Terminated Call	Configures the Action URL to send when phone terminates a call.
Answered Call	Configures the Action URL to send when phone answers an incoming call.
Rejected Call	Configures the Action URL to send when phone rejects an incoming call.
Blind Transfer	Configures the Action URL to send when phone performs blind transfer.
Attended Transfer	Configures the Action URL to send when phone performs attended transfer.
Transfer Completed	Configures the Action URL to send when phone successfully transfers a call.
Transfer Failed	Configures the Action URL to send when phone fails to transfer a call.
Hold Call	Configures the Action URL to send when phone places a call on hold.
Unhold Call	Configures the Action URL to send when phone resumes the call on hold.
Mute Call	Configures the Action URL to send when phone mutes a call.
Unmute Call	Configures the Action URL to send when phone unmutes a call.
Call Settings	
Enable DND	Configures the Action URL to send when phone enables DND.
Disable DND	Configures the Action URL to send when phone disables DND.
Enable Call Forward	Configures the Action URL to send when phone enables Call Forward.
Disable Call Forward	Configures the Action URL to send when phone disables call forward.
Open Forward Always	Configures the Action URL to send when phone enables call forward always function.
Close Forward Always	Configures the Action URL to send when phone disables call forward always function.

Open Call Forward Busy	Configures the Action URL to send when phone disables call forward always function.
Close Call Forward Busy	Configures the Action URL to send when phone disables call forward busy function
Open Call Forward No Answer	Configures the Action URL to send when phone enables call forward no answer function.
Close Call Forward No Answer	Configures the Action URL to send when phone disables call forward no answer function.
Destination	
Add Destination	Allows adding an outbound notification destination by configuring the following settings: Destination Name: Configures the destination name. Protocol: Configures the protocol used for the destination. The available options are XMPP and SMTP. Enable SSL: Enables or disables SSL for the destination connection. Disabled by default. Server Address: Configures the server address. Port: Configures the server port. Domain: Configures the domain name. Username: Configures the username used for authentication. Password: Configures the password used for authentication. From: Configures the sender address. To: Configures the recipient address. Extra Attribute Name: Configures the name of the extra attribute. Extra Attribute Value: Configures the value of the extra attribute.
Delete All Destinations	Deletes all saved destinations.
Notification	
Add Notification	Allows adding an outbound notification by configuring the following settings: Event: Configures the event that triggers the outbound notification. Destination: Selects the destination where the outbound notification is sent. Subject: Configures the subject of the email notification. This option is available only when the destination protocol is SMTP. Message: Configures the message body of the outbound notification. Extra Attribute Name: Configures the name of the extra attribute. Extra Attribute Value: Configures the value of the extra attribute.
Delete All Notifications	Deletes all saved notifications.
Maintenance -> Voice Monitoring	
Session Report	
VQ RTCP-XR Session Report	Enables or disables sending a session quality report to the central report collector at the end of each call.Disabled by default.Note: the GRP260x uses the same server/port that is used for SIP registration to process XR session reports
Interval Report	
VQ RTCP-XR Interval Report	Enables or disables sending interval quality reports to the central report collector periodically during a call.Disabled by default.
VQ RTCP-XR Interval Report Period	Configures the interval, in seconds, for sending interval quality reports to the central report collector during a call.The default setting is "20".
Alert Report	
Warning Threshold for Moslq	Configures the warning threshold for the listening MOS score (MOS-LQ x 10). When the threshold is reached, the phone sends a warning quality report to the central report collector.The default setting is "0".
Critical Threshold for Moslq	Configures the critical threshold for the listening MOS score (MOS-LQ x 10). When the threshold is reached, the phone sends a critical quality report to the central report collector.The default setting is "0".
Warning Threshold for Delay	Configures the warning threshold for one-way delay, in milliseconds. When the threshold is reached, the phone sends a warning quality report to the central report collector.The default setting is "0".
Critical Threshold for Delay	Configures the critical threshold for one-way delay, in milliseconds. When the threshold is reached, the phone sends a critical quality report to the central report collector.The default setting is "0".

Display Report	
Display Report on Web UI	Enables or disables displaying the quality report on the Web UI.Enabled by default.
Display Report on LCD	Enables or disables displaying the quality report on the LCD.Disabled by Default.
Custom Display Layout on LCD	Selects the items displayed in the LCD quality report.
Maintenance -> Scheduled Tasks	
Working Time	Configures office hours for scheduled tasks, such as locking the phone or enabling call forwarding outside working hours.The default setting is "09:00 - 17:00".
Scheduled Tasks	
Add	Creates a new scheduled task by configuring the following settings: Scheduled Tasks Type: Selects the type of scheduled task. The available options are Scheduled Reboot, Scheduled Lock, Scheduled Unlock, and Scheduled Forward. The default setting is "Scheduled Reboot". Repetition period: Selects how often the scheduled task repeats. The available options are Every Day, Every Week, Every Month, and No Repeat. The default setting is "No Repeat". Effective Time: Configures the time or time period when the scheduled task takes effect. The available options are Custom, Office Hours Start Time, and Non-Office Hours Start Time. The default setting is "Custom" with a time of "00:00".
Delete	Deletes the selected scheduled task.

Maintenance Settings Definitions

Application Page Definitions

Application -> Web Service	
Use Auto Location Service	Enables or disables auto-location services on the phone. A reboot is required.Enabled by default.
Application -> XML Application	
Idle Screen	
Idle Screen XML Download	Configures to enable idle screen XML download via HTTP, HTTPS or TFTP.
Download Screen XML at Boot-up	Enables or disables downloading the the idle screen XML file when the phone boots up.Disabled by default.
Use Custom Filename	Enables or disables using a custom file name for the idle screen XML file.Disabled by default.
Idle Screen XML Server Path	Configures the server path to download the idle screen XML file. This field could be IP address or URL, with up to 256 characters.
XML File Example	Downloads an example XML file that can be customized as needed.Note: To allow users to customize the idle screen softkeys and ignore those configured in the XML file, add the following attribute: <SoftKeys ignore="true">.
Top Screen	
Softkey Label	Specifies the softkey name displayed on the idle screen for the users to enter XML application.
Server Path	Configures the server path to download the idle screen XML file. This field can be an IP address or URL, with up to 256 characters.
Application -> Contacts	
Contacts	

Add Contact	Adds a new contact. The following attributes can be configured: First Name Last Name Company Department Job Title Work Home Mobile Conference Accounts Groups Ringtone Note: "Work" field's maximum length is 128 characters. The maximum numbers of groups that a single contact can be added to is 128 groups The Conference field must be configured with a conference number that can be used to join meetings directly from the contact information.
Edit	Edits the contact information.
Delete	Deletes a specific contact.
Delete All Contacts	Deletes all saved contacts.
Group Management	
Add Group	Adds a new group. Configure the Group Name and Ringtone. Up to 30 groups are supported.
Edit Group	Edits a specific group.
Delete Group	Deletes a specific group.
Phonebook Management	
Enable Phonebook XML Download	Enables or disables phonebook XML download via HTTP, HTTPS or FTP.The default setting is "Disabled".
HTTP/HTTPS Username	Configures the username for the HTTP/HTTPS server.
HTTP/HTTPS Password	Configures the password for the HTTP/HTTPS server.
Phonebook XML Server Path	Configures the server path used to download the phonebook XML file. This field supports IP addresses or URLs with a maximum length of 256 characters.
Phonebook Download Interval	Configures the phonebook XML download interval, in minutes.The default setting is "0", which disables the automatic download. The valid range is 5 to 720 minutes.
Remove Manually-edited Entries on Download	Enables or disables removing manually added entries when the XML phonebook is downloaded.Enabled by default.
Import Group Method	Configures how imported groups are handled. The available options are: Replace: Replaces all existing groups with the imported groups. Append: Adds imported groups to the existing groups. The default setting is "Replace".
Sort Phonebook by	Configures the phonebook sorting method based on first name or last name.The default setting is "Last Name".
Download XML Phonebook	Downloads the XML phonebook file.
Upload XML Phonebook	Uploads an XML phonebook file to the phone.
Default Search Mode	Configures the default phonebook search mode. Available options are Quick Match and Exact Match.The default setting is "Exact Match".
Application -> LDAP	
Obtain from UCM Server	
Obtain LDAP configuration file	Obtains the LDAP configuration file from the UCM to which the phone is registered. The existing LDAP configuration file will be overwritten.
Enable UCM LDAP Auto-config Feature on LCD	Enables or disables automatic UCM LDAP configuration. When disabled, the soft key for UCM LDAP automatic configuration is no longer displayed on the LCD.Enabled by default.
Manual Import	
Import LDAP configuration file	Uploads an XML LDAP configuration file. The existing LDAP configuration file will be overwritten.Press "Click to download an example XML file" to download an example XML configuration file.
Local Configuration	
LDAP Protocol	Configures the LDAP protocol to LDAP or LDAPS. LDAPS is a feature to support LDAP over TLS.The default setting is "LDAP".

LDAP Version	Selects the LDAP protocol version for the phone to send the bind requests. The available options are: Version 2 Version 3 The default setting is "Version 2".
Server Address	Configures the IP address or DNS name of the LDAP server.
Port	Configures the LDAP server port.The default port number is "389".
Base DN	Configures the LDAP search base. This is the location in the directory where the search is requested to begin.Example:dc=grandstream, dc=comou=Boston, dc=grandstream, dc=com
Username	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds, in which case the setting can be left blank.
Password	Configures the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
LDAP Number Filter	Configures the filter used for number lookups.Examples:((telephoneNumber=%)(Mobile=*)) returns all records that have 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 the "cn" field set.
LDAP Name Filter	Configures the filter used for name lookups.Examples:((cn=*)(sn=*)) returns all records that have the "cn" or "sn" field starting with the entered prefix;(!(sn=*)) returns all the records that 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 the "telephoneNumber" field set.
LDAP Mail Filter	Configures the filter used for email lookups.Examples:((mail=*)(mailBox=*)) returns all records which has the "mail" or "mailbox" field containing the entered filter value;(!(mail=*)) returns all the records which do not have the "mail" field containing the entered filter value;(&(mail=*) (cn=*)) returns all the records with the "mail" field containing the entered filter value and "cn" field set
LDAP Position Filter	Configures the filter used for position lookups.Examples:(position=*) returns all the records which have the "position" field containing the entered filter value;
LDAP Department Filter	Configures the filter used for department lookups.Examples:(department=*) returns all the records which have the "department" field containing the entered filter value;
LDAP Number Attributes	Specifies the "number" attributes of each record that are returned in the LDAP search result. This field allows you to configure multiple space-separated number attributes.Example:telephoneNumbertelephoneNumber Mobile
LDAP Name Attributes	Specifies the "name" attributes of each record that are returned in the LDAP search result. This field allows users to configure multiple space-separated name attributes.Example:gncn sn description
LDAP Mail Attributes	Specifies the "mail" attributes of each record which are returned in the LDAP search result. This field allows users to configure multiple space separated email attributes. Example: mailmail mailBox
LDAP Position Attributes	Configure the attributes of the LDAP position.
LDAP Department Attributes	Configure the attributes of the LDAP department.
LDAP Display Name	Configures the entry information to be shown on the phone's LCD. Up to 3 fields can be displayed.Example:%cn %sn %telephoneNumber
Max. Hits	Specifies the maximum number of results returned by the LDAP server. When set to "0", the server returns all search results.The default setting is "50".
Search Timeout	Specifies the timeout interval, in seconds, for the server to process the request and return results to the client.The default setting is "30".
Sort Results	Enables or disables sorting the search results.Disabled by default.

Exact Match Search	Enables or disables searching for exact-match results.Disabled by default.
LDAP Dialing Default Account	Configures the default account used when dialing an LDAP contact.The default setting is "Auto".
LDAP Lookup	Enables or disables LDAP number search separately for incoming and outgoing calls.Both options are disabled by default.
Lookup Display Name	Configures the display name when LDAP looks up the name for an incoming call or an outgoing call. This field must be a subset of the LDAP Name Attributes.Example:gncn sn description
Application -> Remote Phonebook	
The user can configure up to 5 XML Remote Phonebooks.Note: It is now possible to configure multiple departments on each remote phonebook.	
Display Name	Configures the phonebook name displayed on the phone.
URL	Configures the XML phonebook URL.
Username	Configures the username used to authenticate with the remote phonebook server.
Password	Configures the username used to authenticate with the remote phonebook server.
Remote Phonebook Update Interval	Configures the remote phonebook download interval, in minutes.The default setting is "0", which disables automatic download. The valid range is 5 to 720.
Application -> Call History	
Delete	Deletes the selected call history entries.
Delete All	Deletes all call history entries stored on the phone.Note: The drop-down list allows users to filter call history by type: All, Answered, Dialed, Missed, or Transferred.
Application -> Online Contacts	
Contacts Search URL	Configures the URL to search contacts. This field could be protocol,server address,path,or query parameters, with up to 256 characters. Path and query parameters can use built-in variables in the format of {var}. Optional variables include: {localNumber}: Local number {remoteNumber}: Remote number {sipServer}: Account registration server {model}: Phone model {version}: Version number {mac}: Phone MAC address {Exactsearch}:whether to query accurately (0-fuzzy, 1-exact) {Condition}:query criteria (entered number/name, etc.) {Pagecount}:The maximum number of query results displayed on a page {Pagenum}:Number of pages at the beginning of the queryExample: URL="http://ip:port/getUserInfoByNumber/{remoteNumber}"
Contacts search HTTP POST	Configures the HTTP POST to search contacts. This field could be protocol, server address, path, or query parameters, with up to 1024 characters. Path and query parameters can use built-in variables in the format of {var}. Optional variables include: {localNumber}: Local number {remoteNumber}: Remote number {sipServer}: Account registration server {model}:Phone model {version}:Version number {mac}:Phone MAC address {Exactsearch}:whether to query accurately (0-fuzzy, 1-exact) {Condition}: query criteria (entered number/name, etc.) {Pagecount}: The maximum number of query results displayed on a page {Pagenum}: Number of pages at the beginning of the queryWhen the configuration item is empty (including all blank data), the phone sends a get request, otherwise, the phone sends a post request. It Supports XML and JSON data formats.
Contacts Search Auth Username	Configures the username for the HTTP/HTTPS searching server.
Contacts Search Auth Password	Configures the password for the HTTP/HTTPS searching server.

Contact Search Response Syntax	Configure contact search response syntax. Response syntax is mandatory. Enter a URL or response content to parse. If you enter a URL and click respond, the system automatically obtains the response content and result. The format of response syntax is key:val[,key:val]. Each line displays one rule. The comma ", "is a newline character.The key includes:? success? reason? counts? total? name? company? department? title? email? firstName? lastName? extensionCompany? extensionHome? extensionMobile
Application -> Account Sharing	
General Settings	
Enable Account Sharing	Enables or disables the Account Sharing feature. Disabled by default.
Role in Account Sharing	Selects the role of the current device in the network. The host device registers an account on the IPPBX, while guest devices can make and receive calls inside and outside the network through the account configured on the host device. The available options are: Host Device Guest Device The default setting is "Host Device".
Group Name	Configures the group name. In Account Sharing mode, devices with the same group name can discover each other.
Group Password	Configures the group password. In Account Sharing mode, a guest device must have the same group password as the host device to register an account on the host device. Note: This field is required when using Account Sharing.
SIP Server Port	Configures the SIP service port for Account Sharing. Displayed when Role in Account Sharing is set to "Host Device". When set to "0" a random port is used. The valid range is 0-65535.
Account Settings	
Account	Selects the account used for Account Sharing. For the host device, this setting determines which host device account guest devices use to make and receive calls outside the Account Sharing group. For the guest device, this setting determines which account the guest device registers on the host device.
Account Name	Specifies the account name corresponding to the account used by the guest device. Displayed when Role in Account Sharing is set to "Guest Device".
Ringing Tone Settings	
Sync Ringing In Group	Enables or disables synchronization of ringtones across all successfully registered guest devices in the group. Displayed when Role in Account Sharing is set to "Host Device".Disabled by default.
Discovered Host/Guest Device List	Lists discovered host or guest devices based on the device's role and configuration. The list displays information such as IP address, MAC address, account name, and registration status.

Application Settings Definitions

External Service Page Definitions

External Service -> GDS

GDS	Configures the phone to connect with up to 10 GDS37xx access systems and send OpenDoor requests. Service Type: Selects the service type. The available options are Others and GDS. Account: Configures the account used to send OpenDoor requests to the GDS37xx. Access Number: Configures the SIP extension or IP address of the GDS37XX based on the deployment scenario (Peering or Registration). Ringtone: Select the system ringtone from the dropdown list to be played when there is an incoming call from the configured access number of the GDS37xx. Access Identification: Configures the label used to identify the GDS37xx. Access Password: Configures the password used to unlock the door on the GDS37XX. Notes: When using the Peering scenario, configure the Access Number field with the IP address of the peered GDS37xx. When using the Registration scenario where the phone and GDS37XX are registered to the same SIP server, configure the Access Number field with the SIP extension of the GDS37XX. The Access Password configured on the phone must match the Remote PIN to Open the Door configured on the GDS37xx.
External Service -> Call Center	
Call Center Codes	Configures the Disposition Codes and the Unavailable Code for quick selection on the phone side.
Wrap-up Countdown(m)	Configures the duration of the "Wrap-Up" status and displays the countdown on the LCD. When the countdown expires, the agent status switches back to "Available". If set to "0", the countdown is disabled.
External Service -> Broadsoft XSI	
Authentication Login	
Server	Configures the Broadsoft Xsi server address, including the protocol.
Port	Configures the Broadsoft Xsi server port.
Xsi Actions Path	Configures the deployment path for Broadsoft Xsi Actions. If left empty, the default path "com.broadsoft.xsi-actions" is used.
Xsi Authentication Type	Configures the authentication method for Broadsoft Xsi. The available options are Login Credentials and SIP Credentials. When SIP Credentials is selected, select the SIP account from the drop-down list.
BroadSoft User ID	Configures the user ID for the Broadsoft Xsi server.
Login Password	Configures the password for Broadsoft Xsi server authentication.
SIP Authentication ID	Configures the SIP username for Broadsoft Xsi server authentication.
SIP Authentication Password	Configures the SIP authentication password for Broadsoft Xsi server authentication.
Auto Login	Enables or disables automatic login. When enabled, the device will automatically login in the background after booting up, so that the BS Xsi always remains logged in. LCD can get the latest Directories, can directly enter the BS Xsi user service, and trigger the update of data in the background.Disabled by default.
Service Settings	
Sort Phonebook by	Configures the Broadsoft phonebook to sort based on the selection of first name or last name. If you select "Last name", the contact's last name will be displayed first, and the phone book will be sorted by last name; if you select "First name", the contact's first name will be displayed first, and the phone book will be sorted by first name. The default setting is "Last Name".
BroadSoft Directory Update Interval (m)	Configures the BroadSoft phonebook download interval, in minutes. When set to "0", automatic download is disabled.The default setting is "4320". The valid range is 5 to 4320.
Broadsoft Contacts Download Limit	Configures the maximum number of contacts that can be downloaded from each BroadSoft XSI server directory. When the number of contacts returned by the server exceeds this limit, the contacts are not downloaded and the device only supports remote search. When set to "0", the server default contact limit is used.The default setting is "1000". The valid range is 0 to 2000.

BroadSoft Contacts Search Limit	Configures the maximum number of remote search results that can be downloaded from the BroadSoft XSI server directory. When the search results exceed this limit, the results are not downloaded and the search scope must be narrowed. When set to "0", no limit is applied. The default setting is "100". The valid range is 0 to 2000.
Network Directories	
Type	Enable or Disable Broadsoft Network directories. The directory types are: Group Directory: Enable/Disable and rename the Broadsoft Xsi Group Directory features on the phone. If keep the Name box blank, the phone will use the default name "Group" for it. Enterprise Directory: Enable/Disable and rename the Broadsoft Xsi Enterprise Directory features on the phone. If keep the Name box blank, the phone will use the default name "Enterprise" for it. Group Common: Enable/Disable and rename the Broadsoft Xsi Group Common Directory features on the phone. If keep the Name box blank, the phone will use the default name "Group Common" for it. Enterprise Common: Enable/Disable and rename the Broadsoft Xsi Enterprise Common Directory features on the phone. If keep the Name box blank, the phone will use default name "Enterprise Common" for it. Personal Directory: Enable/Disable and rename the Broadsoft Xsi Personal Directory features on the phone. If keep the Name box blank, the phone will use the default name "Personal" for it. Missed Call Log: Enable/Disable and rename the Broadsoft Xsi Missed Call Log features on the phone. If keep the Name box blank, the phone will use the default name "Missed" for it. Placed Call Log: Enable/Disable and rename the Broadsoft Xsi Placed Call Log features on the phone. If keep the Name box blank, the phone will use the default name "Outgoing" for it. Received Call Log: Enable/Disable and rename the Broadsoft Xsi Placed Call Log features on the phone. If keep the Name box blank, the phone will use the default name "Incoming" for it.
Name	Defines the directory name.
External Service -> E911 Service	
Enable E911	Enable or disables Enhanced 911 calls. Disabled by default.
HELD Protocol	Configures the HELD transfer protocol. The available options are HTTP and HTTPS. The default setting is "HTTP".
HELD Synchronization Interval.	Configures the synchronization interval in minutes. The default setting is "0", which disables the synchronization. The valid range is 30 to 1440 minutes.
Location Server	Configures the primary Location Information Server (LIS) address.
Location Server Username	Configures the username for the primary Location Information Server (LIS).
Location Server Password	Configures the password for the primary Location Information Server (LIS).
Secondary Location Server	Configures the secondary Location Information Server (LIS) address.
Secondary Location Server Username	Configures the username for the secondary Location Information Server (LIS).
Secondary Location Server Password	Configures the password for the secondary Location Information Server (LIS).
HELD Location Types	Configures the "locationType" element included in the location request. The available options are geodetic, civic, and location URI.
HELD Use LLDP Information	Enables or disables using LLDP information from the LLDP-supported switch to generate the ChassisID and PortID. When disabled, the MAC addresses of the gateway and phone are used by default. Disabled by default.
HELD NAI	Enables or disables including the Network Access Identifier (NAI) as the device identity in the location request sent to the Location Information Server (LIS). Disabled by default.
HELD Identity	Configures up to 10 HELD identities.
HELD Identity Value	Configures the corresponding values for each configured HELD identities.

E911 Emergency Numbers	Configures multiple emergency numbers separated by the delimiter symbol ",".
Geolocation-Routing Header	Enables or disables including the "Geolocation-Routing" header with the value "Yes" in E.911 INVITE messages.Disabled by default.
Geolocation Header Format	Specifies how the phone encodes and inserts location information (like building, floor, room) into SIP INVITE Geolocation header during emergency (911) calls. The available options are: RFC6442: Sends the Geolocation value in RFC6442-compliant format. (E.g., Geolocation: <cid: 8476BD6B-5FDD-339D-900B-AEAB0AA0429A>) Legacy: Sends the Geolocation value as plain text (e.g., Geolocation: 8476BD6B-5FDD-339D-900B-AEAB0AA0429A). The default setting is "Legacy".
Priority Header	Enables or disables including the "Priority" header with the value "emergency" in E.911 INVITE messages.Disabled by default.

External Service Settings Definitions

NAT SETTINGS

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

- STUN Server

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

- Use Random Ports

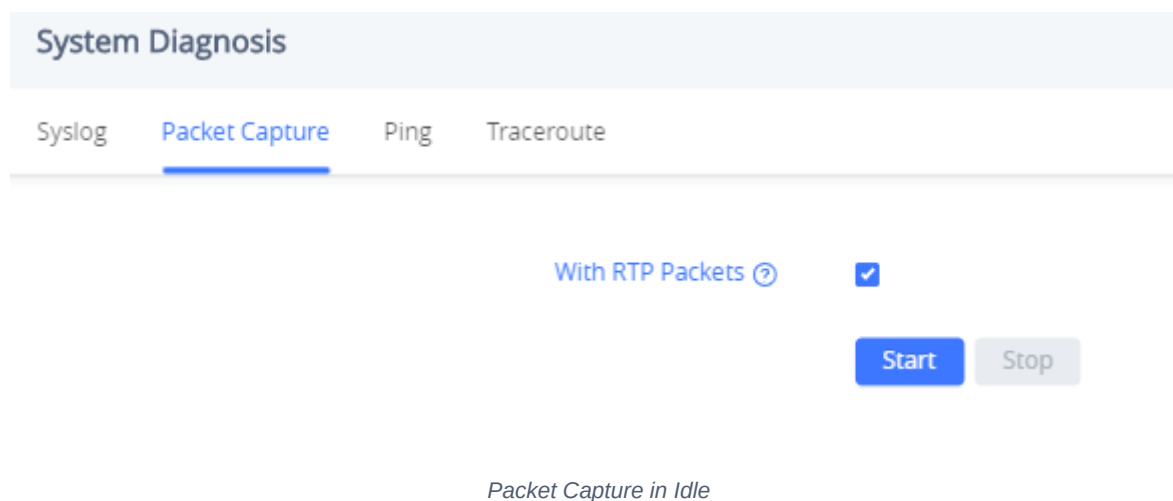
It is under **Settings->General Settings**. This setting depends on your network settings. When set to "Yes", it will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple GRPs are behind the same NAT.If using a Public IP address, set this parameter to "No".

- NAT Traversal

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

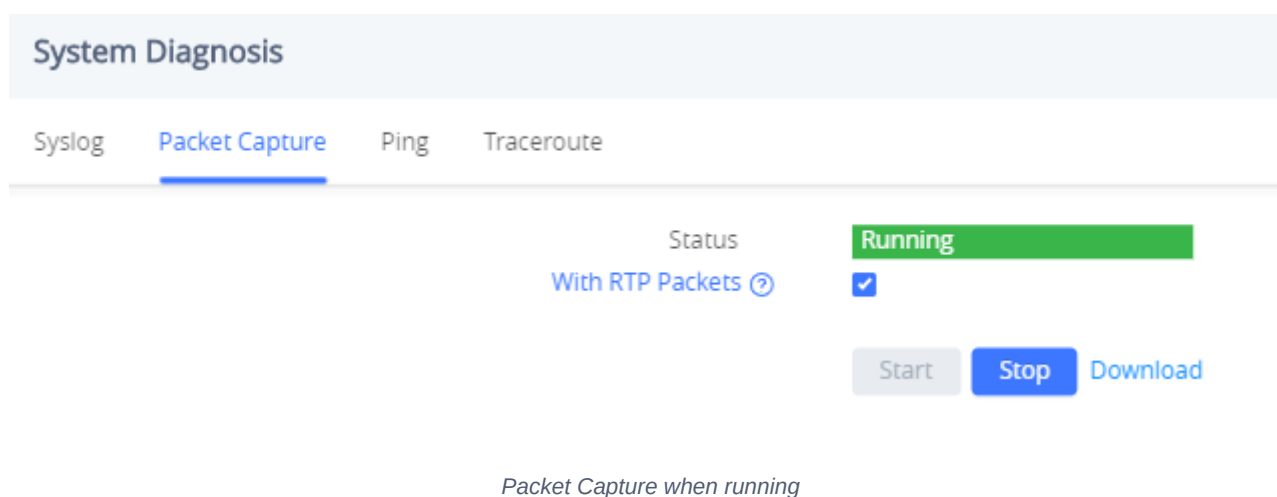
PACKET CAPTURE

GRP260X is embedded with a packet capture function. The related options are under **Maintenance->System Diagnosis->Packet Capture**.



Users can also define whether RTP packets will be captured or not from the **With RTP Packets** option. When the capture configuration is set, press the Start button to start packet capture. The Status will become RUNNING while capturing, as shown in Figure 7: Packet Capture when running. Press the **Stop** button to end the capture.

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

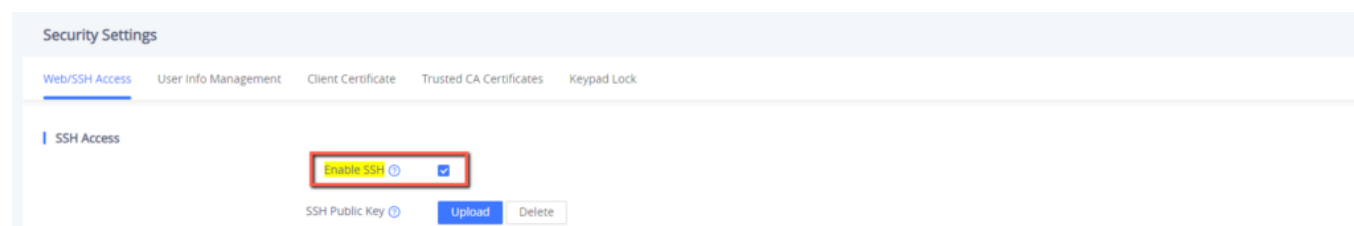


Remote SSH capture

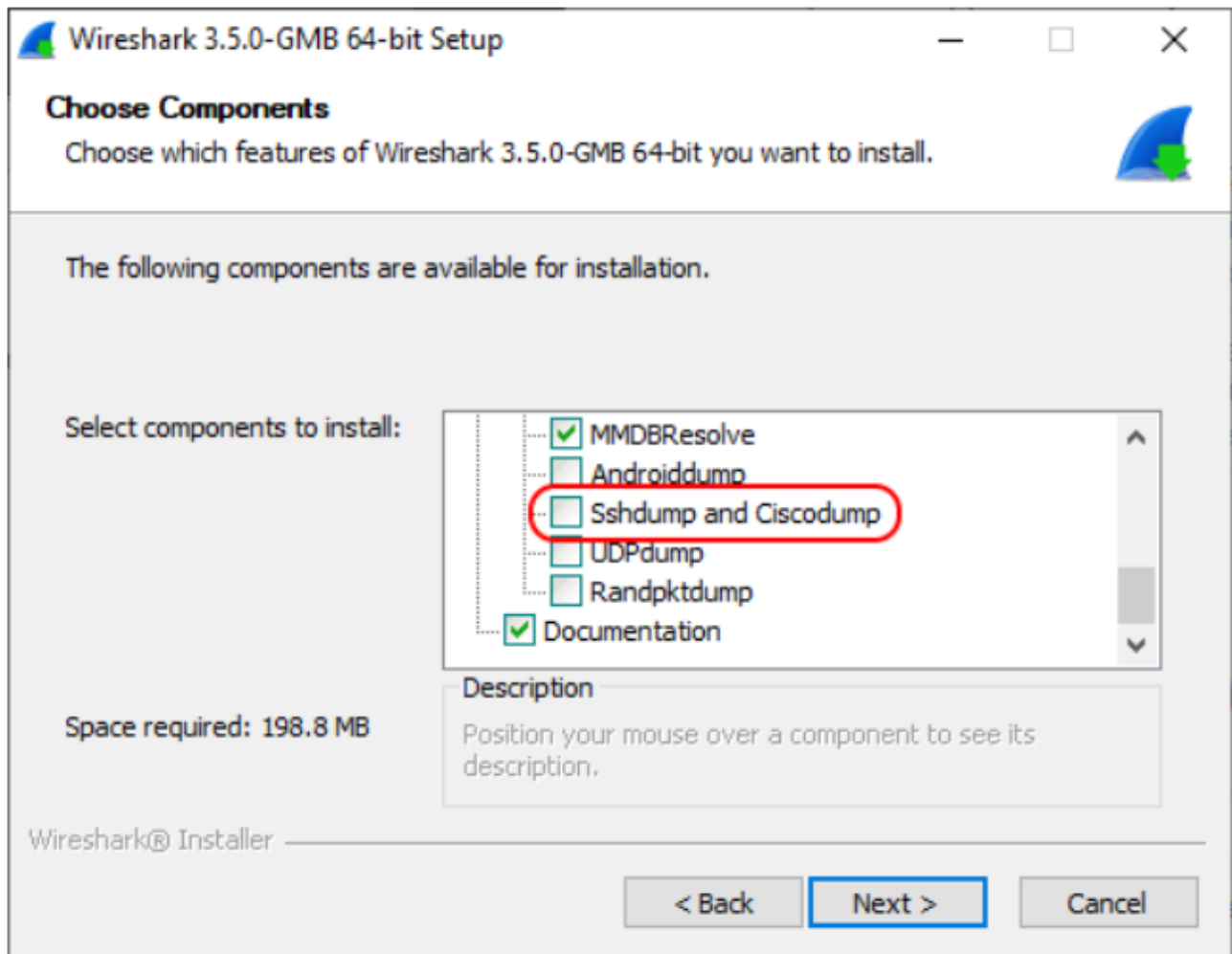
Remote SSH capture is the process of remotely accessing and capturing network traffic on a target machine via a secure shell (SSH) connection.

When configured, The Remote SSH option will allow us to capture the network traffic that is flowing through the GRP260x IP phone. This allows us to inspect the traffic, analyze it, and potentially identify any security issues or anomalies, to do this on the Wireshark network analyzer, we will need to follow the below steps :

1. Enable SSH under System settings -> Security settings -> SSH Access



2. Enable the sshdump and ciscodump components when installing Wireshark.



3. Once Wireshark is installed with the needed components, Launch the SSH remote capture configuration page, By clicking the icon shown below



4. Define the SSH server address and port, which are the captured device IP address and port.

Wireshark · Interface Options: SSH remote capture

Server Authentication Capture Debug

Remote SSH server address 192.168.5.55

Remote SSH server port 22

☒ Save parameter(s) on capture start

Restore Defaults Save Close Help

5. Authenticate using the credentials of the device's web UI.

Wireshark · Interface Options: SSH remote capture

Server Authentication Capture Debug

Remote SSH server username admin

Remote SSH server password

Path to SSH private key ... Clear

SSH key passphrase

ProxyCommand

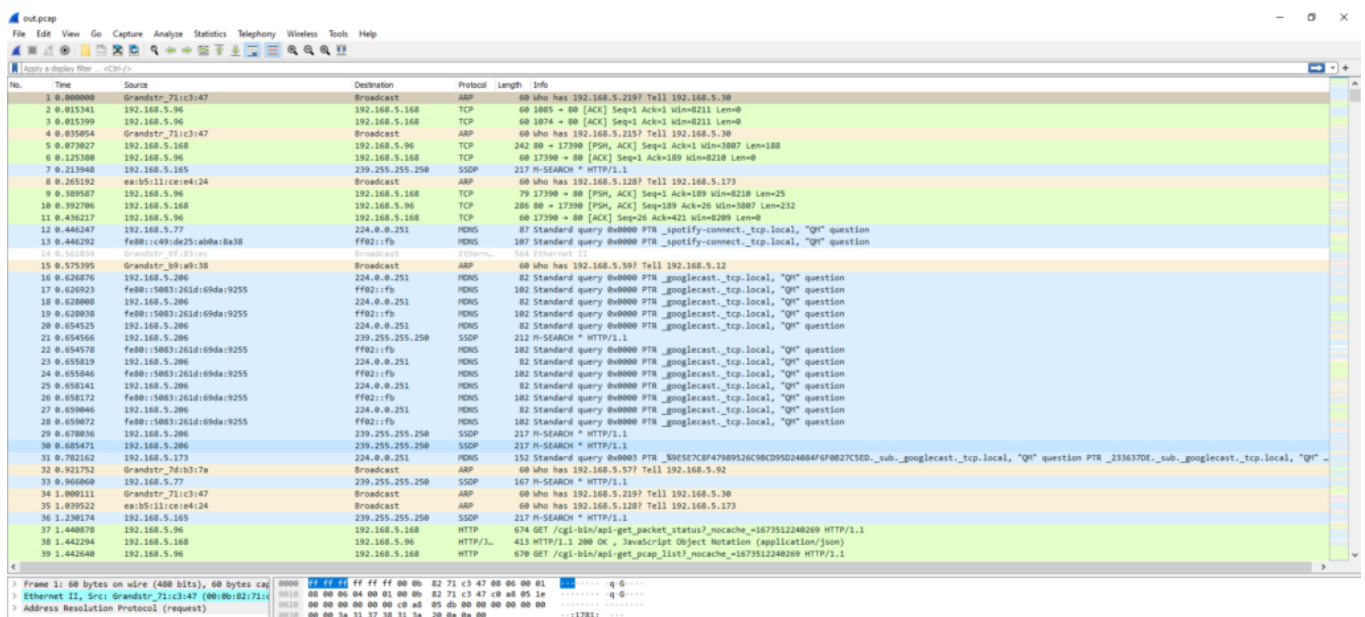
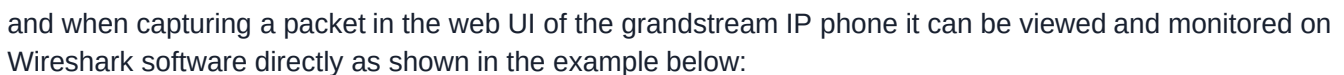
☒ Save parameter(s) on capture start

Restore Defaults Save Close Help

6. Set the remote capture command to other:pcap.



Once the steps are followed, an "SSH remote capture" option will be displayed on the main page of Wireshark, to start capturing, click on "SSH remote capture" as shown below



Please contact technical support for steps to decrypt encrypted captured packets.

UPGRADING AND PROVISIONING

The following hardware versions do not support firmware downgrade after upgrading to version 1.0.5.37:

- GRP2601(P) hardware version 1.9A
- GRP2602(P) hardware version 1.9A
- GRP2604(P) hardware version 1.7A
- GRP2603P / GRP2604P hardware version 1.5A
- GRP2603P hardware version 1.5B
- GRP2603 / GRP2604 hardware version 1.6B

Unified Firmware

The GRP2601 / GRP2601P / GRP2602 / GRP2602P / GRP2602W / GRP2603 / GRP2603P / GRP2604 / GRP2604P support unified firmware for all GRP260X models.



Firmware Upgrade

The GRP260X series can be upgraded via TFTP / FTP / FTPS / HTTP / HTTPS by configuring the URL/IP Address for the TFTP / HTTP / HTTPS / FTP / FTPS server and selecting a download method. Configure a valid URL for TFTP, FTP/FTPS, or HTTP/HTTPS, the server name can be FQDN or IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

fw.mycompany.com

Upgrade via Web GUI

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

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

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

No Local TFTP/FTP/HTTP Servers

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

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

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

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

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

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the phone 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 phone.

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

Custom Ringtones Provisioning

The custom ringtones can be provisioned from the link configured under the firmware server path, up to 6 ringtones can be customized. The phone will be looking for ringx.ogg as shown below, where x can be from 1 to 6:

```
155 GRP2603P [c0:74:ad:27:76:65]: PROVN INFO [1.0.1.36] Ring upgrade from URL http://fm.grandstream.com/gs/ring1.ogg\n145 GRP2603P [c0:74:ad:27:76:65]: PROVN INFO [1.0.1.36] Downloading http://fm.grandstream.com/gs/ring1.ogg\n
```

Custom ringtone provisioning

- Codec: must be Opus
- Frequency: 16K
- Audio Channel: Mono

Phone Provisioning

Configuration File Download

Grandstream SIP Devices can be configured via the Web Interface as well as via a Configuration File (binary or XML) through TFTP, FTP/FTPS, or HTTP/HTTPS. The "Config Server Path" is the TFTP, FTP/FTPS, or HTTP/HTTPS server path for the configuration file.

It needs to be set to a valid URL, either an FQDN or IP address format. The "Config Server Path" can be the same or different from the "Firmware Server Path".

A configuration parameter is associated with each field on the web configuration page. A parameter consists of a Capital letter P and 2 to 5-digit numeric numbers. i.e., P2 is associated with the "New Password" in the **Web GUI→System Settings→Security Settings → User Info Management → Admin Password**. For a detailed parameter list, please refer to the corresponding configuration template.

When the GRP260x series boots up or reboots, it will issue a request to download an XML file named "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If the download of the "cfgxxxxxxxxxxxx.xml" file is not successfully followed by a configuration file named "cfgxxxxxxxxxxxx", the phone will issue a request to download a specific model configuration file "cfg<model>.xml", where <model> is the phone model, i.e., "cfggrp2601.xml" for the GRP2601, "cfggrp2602" for the GRP2602, "cfggrp2603" for the GRP2603 and "cfggrp2604" for the GRP2604. If this file is not available, the phone will issue a request to download the generic "cfg.xml" file. The configuration file name should be in lowercase letters, If not found, the phone will request a file named "dev[MacAddress].cfg" where "MacAddress" is the MAC address of the device, With this provisioning file, users can provision the device with both P-values and aliases.

```
download http://fm.grandstream.com/gs/cfgc074ad224d4a.xml (No error)\n
download http://fm.grandstream.com/gs/cfgc074ad224d4a (No error)\n
download http://fm.grandstream.com/gs/cfggrp2601.xml (No error)\n
download http://fm.grandstream.com/gs/cfg.xml (No error)\n
download http://fm.grandstream.com/gs/devc074ad224d4a.cfg (No error)\n
download https://fm.grandstream.com/gs/cfgc074ad224d4a.xml (No error)\n
download https://fm.grandstream.com/gs/cfgc074ad224d4a (No error)\n
download https://fm.grandstream.com/gs/cfggrp2601.xml (No error)\n
download https://fm.grandstream.com/gs/cfg.xml (No error)\n
download https://fm.grandstream.com/gs/devc074ad224d4a.cfg (No error)\n
```

Config File Download

When doing provision on the phone, if your first config file contains p-values listed below, the phone will try to download the potential second cfg.xml file and apply the second file without rebooting. Maximum 3 extra attempts.

Those P-values are:

```
*212 -- Config upgrade via*234 -- Config prefix*235 -- Config postfix *237 -- Config upgrade
Server*240 - Authenticate Config File*1359 - XML Config File Password *8463 - Validate Server
Certificate *8467 - Download and process ALL Available Config Files *20713 - Always authenticate
before challenge*22011 - Bypass Proxy For *22030 - Enable SSL host verification for provision
```

Note: (P-values that trigger Auto-Provision)

If the p-values listed below are changed while managing configuration on web UI or LCD, the provisioning process will be triggered:

```
* 192 -- Firmware upgrade server* 232 -- Firmware prefix * 233 -- Firmware postfix * 6767 --
Firmware Upgrade Via * 6768 -- Firmware HTTP/HTTPS Username * 6769 -- Firmware HTTP/HTTPS Password
* 237 -- Config upgrade Server* 212 -- Config upgrade via * 234 -- Config prefix * 235 -- Config
postfix * 1360 -- Config HTTP/HTTPS username * 1361 -- Config HTTP/HTTPS password.
```

P-Value that forces reboot when changes are applied by downloading the config file

When P-value 22421 (or alias "provision.config.forceReboot") is set to 1 in the config file, the phone will need to reboot if any change is applied by downloading the config file. Specifically following the process below:

- First-time download:

1. Phone downloaded a config file (in any supported format) with P22421 set to 1 included.
2. Phone found there is change(s) compared with the current setting on the phone (Any valid P-value change, no matter if it does need a reboot to apply or not).
3. The phone will update to the new setting (will not save P22421 itself) and will go into the normal reboot process (e.g.: if there is an active call, the phone will wait until it is finished)

- Second-time download:

1. After reboot, the phone may download the same config file again (if the config file path did not change).
2. Phone checked the config file and found no P-value needed to be updated.
3. The phone will not reboot again.

Users can configure the phone to get all the needed certificates during boot up. Instead of putting the certificate/key content in the text directly from the Web interface or uploading them manually, they can choose to provision them from the configuration file by putting the URL in the P-value field of each certificate and/or

key. (e.g., http://ProvisionServer_address/SIP-TLS-Certificate.pem) The phone will then process the URL, search for the appropriate certificate/Key file, download it, and then apply it to the phone.

```
HTTP GET /SIP-TLS-Private-Key.key HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /SIP-TLS-Certificate.pem HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-1.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-2.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-3.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-4.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-5.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /Trusted-certificate-6.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /OpenVPN-CA.crt HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /OpenVPN-Certificate.pem HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
HTTP GET /OpenVPN-Key.key HTTP/1.1
HTTP HTTP/1.1 200 OK (application/octet-stream)
```

Certificates Files Download

For more details on XML provisioning, please refer to:

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

No Touch Provisioning

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

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

Starting from firmware version 1.0.3.83, the option to display an upgrade prompt on the LCD screensaver page was added

RESTORE FACTORY DEFAULT SETTINGS

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

Restore Factory Settings using the LCD menu

Please follow the instructions below to reset the phone:

1. Press the MENU button to bring up the keypad configuration menu.
2. Navigate to **Settings > Advanced Settings**.
3. Select "Factory Reset".
4. A warning window will pop out to make sure a reset is requested and confirmed.

Press the "Yes" Softkey to confirm and the phone will reboot, or "No" Softkey to cancel the Reset.

Restore to Factory Default via Web GUI

1. Login GRP2601/GRP2602/GRP2603/GRP2604 Web GUI.
 2. Navigate to **Maintenance -> Upgrade and provision -> Advanced Settings -> Factory Reset**.
 3. Press on **the Start** Button situated against the Factory reset option
- Click "OK" to confirm and the phone will reboot, or "Cancel" to cancel the Reset.

CHANGELOG

This section documents significant changes from previous versions of user manuals for GRP260X. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.7.71

- Added Support for including the Accept-Language header in SIP messages. [[Use Accept-Language Header](#)]
- Added Support for account selection mode when placing a call from the dialing interface. [[Account Selection Mode for Dialing](#)]
- Added support for Marathi and Hindi as LCD languages. [[Feature Highlights](#)]

Firmware Version 1.0.7.66

- No major changes.

Firmware Version 1.0.7.64

- No major changes.

Firmware Version 1.0.7.63 (Beta Version)

- Added support for Call Monitor Function for Zoom. [[Advanced Features](#)]
- Added support for Local Call Features Mode. [[Feature Codes](#)]

- Added support for BLF and Monitored Call Park call indication on non-primary page. [[Virtual Multi-Purpose Keys](#)]

Firmware Version 1.0.7.49

- Added support to control the registration retry interval when the server returns 403 Forbidden [[Registration Retry Wait Time\(s\) Upon 403 Forbidden](#)]
- Added support to set Geolocation Header Format [[Geolocation Header Format](#)]
- Added support to add Auth Header on Re-Register [[Add Auth Header on RE-REGISTER](#)]
- Added support to add control reboot when receiving SIP NOTIFY with "Event: Check-Sync" header for each SIP account [[Reboot on check-sync event without "reboot="](#)]
- Added support to upload Third-party Vendor Configuration (Yealink and Fanvil are supported). [[Upload Third-party Vendor Configuration](#)]

Firmware Version 1.0.7.39

- Added support for to change Call-ID to use host IP address [[Call-ID Domain Mode](#)]
- Added support for alert-info Bellcore mapping [[Enable Alert-Info Bellcore Mapping](#)]
- Added support for generation WLAN session keys file to debug Wi-Fi related issues [[Generate WLAN Session Keys File](#)]
- Added support of "Dial DTMF" key mode for Custom Call Screen Softkeys [[Add Custom Softkey](#)]
- Increased the Maximum allowed length for "SIP TLS Private" to more than 2048 characters [[SIP TLS Private Key](#)]

Firmware Version 1.0.7.32

- Added support of Security Version display on the web UI [[Security Version](#)]
- Web access protocol is now set to HTTPS by default [[Web Access Mode](#)]
- Direct IP Call is now disabled after factory reset. [[Enable Direct IP Call](#)]
- Limited SSH public key length to 2048 bits [[SSH Public Key](#)]
- Disabled All Weak TLS Cipher Suites by default [[Enable/Disable Weak Cipher Suites](#)]
- Set minimum TLS Version default value to TLS version 1.2 [[Minimum TLS Version](#)]
- Added support to configure media NAT traversal strategies [[Media NAT Traversal](#)]
- Added support of ICE function [[Candidate Type](#)]

Firmware Version 1.0.7.24

- No major changes.

Firmware Version 1.0.7.23

- Added Support to change the style of softkey bar. [[Configure the softkey bar style](#)]

Firmware Version 1.0.7.19

- Added support of Silent Call Mode to VPK/MPK. [[Silent Call](#)]

Firmware Version 1.0.7.15

- Added Support of Syslog Header Format. [[Syslog Header Format](#)]

Firmware Version 1.0.7.11

- Added support of Monitored Voicemail Access Number. [[Monitored Voicemail Access Number](#)]

Firmware Version 1.0.7.10

- Added support of sharing desktop and files using the Click2Dial add-on. [[Click-To-Dial Feature](#)]
- Added support to use existing SIP session used for registration/calls for the RTCP-XR VQ collector. [[VQ RTCP-XR Collector Address Selection](#)]
- Improved XML customization idle screen. [[XML File Example](#)]

- Added support to enable local dialing DTMF tone in speaker mode. [[Enable Local In-call DTMF Tone in Speaker Mode](#)]
- Added support to make calls when LCD has "missed calls" notification. [[Enable Missed Call Notification](#)]
- Added "LDAP search" custom softkey to dial window. [[Custom Softkey Layout](#)]
- Added support of 802.1x under Ethernet for non Wi-Fi models. [[802.1X Mode](#)]
- Added support of SCEP. [[SCEP](#)]
- Added support of "AI Noise Suppression". [[Priority Noise Cancellation Method](#)]

Firmware Version 1.0.5.71

- Added Support of LLDP Timeout before DHCP Request. [[LLDP Timeout before DHCP Request](#)]

Firmware Version 1.0.5.68

- Added support to disable voicemail key. [[Voicemail Key Mode](#)]
- Added support to configure a failover OpenVPN(R) server. [[OpenVPN\(R\) Server Secondary Address](#)]

Firmware Version 1.0.5.65

- Changed wording from blacklist to block list and from whitelist to allow list. [[Web Access Control](#)]

Firmware Version 1.0.5.60

- Added Support of [x\~X*]+ in dial plan. [[Dial Plan](#)]
- Added Support of Enhanced Call Park. [[Enable Call Park Softkey](#)]
- Added Support of Tertiary SIP Server. [[Tertiary SIP Server](#)]
- Added Support to send "R" as a DTMF event. [[Dial DTMF](#)]
- Added Support to setup speed dial using the numeric keys on the keypad. [[Configuration via Keypad](#)]

Firmware Version 1.0.5.54

- Added Support to stop the warning beep sound when receiving a multicast paging call. [[Multicast Tone](#)]
- Disabled the user account by default (Factory reset needs to be performed in order for this change to take effect). [[Enable User Web Access](#)]

Firmware Version 1.0.5.50

- No major changes.

Firmware Version 1.0.5.46

- Improved Maximum group number in Contacts to 128 [[Add contact](#)]
- Improved Maximum XML remote phone book number to 5 [[Remote Phonebook](#)]
- Added the ability to disable the call recording indicator [[Enable the Indicator in Recording](#)]
- Added Support to disable local DTMF tone on the dialing page. [[Enable Local Dialing DTMF Tone in Speaker Mode](#)]
- Added Support to do direct SIP URI calls with VPK/MPK [[SIP URI](#)]
- Added Support of valid hostname for sip uri dialing [[Hostname](#)]

Firmware Version 1.0.5.38

- Added support to configure static DNS SRV records. [[Static DNS Cache](#)]
- Added support for codec G.726-16/24/40. [[Preferred Vocoder](#)]
- Added support to disable the Headset key for the option "Headset Key Mode". [[Headset Key Mode](#)]
- Added ability to enable/disable incoming call indicator. [[Enable Incoming Call Indicator](#)]
- Added ability to transfer to VM Feature code. [[Transfer to VM feature code](#)]
- Added support for the feature "VPK PAGING AUTO RETURN TIMEOUT(S)". [[VPK Paging Auto Return Timeout\(s\)](#)]
- Added Support to send syslog debug messages after factory reset. [[MAINTAIN SYSTEM LOG INFO](#)]

[AFTER FACTORY RESET](#)

Firmware Version 1.0.5.26

- Increased work field maximum length in Contact to 128. [\[Work Field\]](#)
- Improved Device to use the same server/port that is used for SIP registration to process XR reports. [\[VQ RTCP-XR Session Report\]](#)

Firmware Version 1.0.5.25

- Added Serial under display on Web UI System Info page. [\[Serial Number\]](#)
- Added Support of multicast timer. [\[Multicast Call Timeout\]](#)

Firmware Version 1.0.5.19

- Added Support to hide LCD pop-up options. [\[HIDE POP-UP OPTIONS\]](#)
- Added Support of MPK/VPK mode HTTP command. [\[HTTP Command\]](#)
- Added Support of MPK/VPK mode Call Flip. [\[Call Flip\]](#)
- Updated VPK Value name max length to 256. [\[Label\]](#)
- Added Support of Trusted Domain Name List. [\[TRUSTED DOMAIN NAME LIST\]](#)
- Added Support for Phonebook Matching. [\[PHONEBOOK MATCHING\]](#)
- Added Support of Virtual Extension Board. [\[Virtual Extension\]](#)
- Added Support of Exty App for the option Auto Provision List Starting Point. [\[Auto Provision List Starting Point\]](#)
- Added Support to configure SSH port. [\[SSH PORT\]](#)
- Added Support for Online Contacts. [\[ONLINE CONTACTS\]](#)
- Added Support of TLS 1.3 for Client Certificate. [\[Minimum TLS Version\]](#)
- Added Support for In-call Contact Info Display. [\[IN-CALL CONTACT INFO DISPLAY\]](#)
- Added Support to play the ringtone contained in Alert-Info sent from the server. [\[Match Incoming Caller ID\]](#)

Firmware Version 1.0.3.98

- Added Support to stop Packet Capture automatically after reaching the design's upper limit. [\[Packet Capture Data Coverage\]](#)
- Added Support to allow adding protocol header in Config Server Path field (Eg:https://) and ignore "Upgrade Via" [\[Config Server Path\]](#)
- Added Support to display recording indicator when a call is recorded [\[ENABLE THE INDICATOR IN RECORDING\]](#)
- Added Support to adjust Inbound DTMF Volume [\[INBOUND DTMF VOLUME\]](#)
- Added Support of VBeT EHS headset type. [\[Headset Type\]](#)
- Added Support for multiple departments for the remote phonebook. [\[Remote phonebook\]](#)
- Added "XML Help Document" link for "Download Device Configuration (XML)" config file. [\[Download Device Configuration \(XML\)\]](#)
- Added Support to modify the speed dial custom softkey icon. [\[Speed dial custom softkey\]](#)
- Updated the timezone for Mexico. [\[Time Zone\]](#)
- Added Support to stream a ringtone based on a remote URL. [\[Match Incoming Caller ID\]](#)

Firmware Version 1.0.3.87

- Added Support of Public Mode Timeout. [\[Public Mode Timeout\]](#)

Firmware Version 1.0.3.86

- Improved Web UI displays for Deep energy-saving duration.
- Added warning message for invalid custom certificate uploading. [\[Custom Certificate\]](#)
- Added MPK configuration and installation tutorial video link on web UI [\[MPK Configuration and Installation\]](#)

- Removed ChaCha20-Poly1305 algorithm from OpenVPN(R) Cipher Method dropdown list [[OpenVPN\(R\) Cipher Method](#)]
- Added Support to enable UCM LDAP Auto-config Feature on LCD [[UCM LDAP AUTO-CONFIG FEATURE ON LCD](#)]
- Added support for Remote SSH capture. [[Remote SSH Capture](#)]

Firmware Version 1.0.3.83

- Improved Arabic and Hebrew web UI display languages.
- Added Support to display the QR code of its SSID to share with cellphones (GRP2602W) [[Connecting the GRP260X](#)]
- Added Support to dial BLF number with dial plan prefix when pressing the BLF key. [[Account Page Definitions](#)]
- Added Support For Energy Saving. [[ENERGY SAVING](#)]
- Added Support for the Total Number of Custom Ringtone Update. [[Total number of Custom Ringtone Update](#)]
- Removed Call Waiting Tone Gain from Ringtone Settings. [[Phone Settings Page Definitions](#)]
- Added Support to synchronize time via sip header when the NTP server is not configured. [[Time and Language](#)]
- Added Support to clear user data if a different user logs in. [[Clean User Data While Different Users Log In](#)]
- Updated "Enable Busy Tone on Remote Disconnect" default value to Yes. [[Call Settings](#)].
- Added Scheduled Tasks Maintenance Option. [[Maintenance Page Definitions](#)]
- Added Display Report in Voice Monitoring. [[Maintenance Page Definitions](#)]
- Updated Customized softkey icons. [[Programmable Keys Settings](#)]
- Added Error prompt if configured idle LCD brightness is greater than active LCD brightness. [[Energy Saving Master Control](#)]
- Added Support to display upgrade prompt on LCD screensaver page.

Firmware Version 1.0.3.72

- Added Support to adjust call tone volume [[System Settings Page Definitions](#)]
- Added Support to disable speaker phone [[Phone Settings Page Definitions](#)]
- Added Support of OpenVPN(R) Client Key Password [[Network Settings Page Definitions](#)]
- Added Support to customize Early media response [[Account Page Definitions](#)]

Firmware Version 1.0.3.70

- Added Support for Weak Cipher Suites. [[System Settings Page Definitions](#)]

Firmware Version 1.0.3.63

- Added Support of E911 Service [[External Service Page Definitions](#)]
- Added Support of Zoom E911 X-switch-info SIP Header
- Added Support of SIP Intercom config on the Web UI

Firmware Version 1.0.3.59

- Improved device web UI display strings.
- Added support to configure the CA Signature Algorithm. [[System Settings Page Definitions](#)]
- Added display of "Device Individual Certificate" in web UI under System Info.

Firmware Version 1.0.3.57

- Added support of Input Method for Contacts and LDAP. [[System Settings Page Definitions](#)]
- Added support to set distinctive ringtones based on alert-info syntax.

Firmware Version 1.0.3.51

- Added Support for the LDAP filter used for email lookups [[Application Page Definitions](#)]

Firmware Version 1.0.3.44

- Added support to adjust the speaker ring volume. [[System Settings Page Definitions](#)]
- Added support of an alert tone when a multicast paging is received.

Firmware Version 1.0.3.42

- Added support to access the Wi-Fi network settings on the GRP2602W LCD when the device is in the Constraint Mode. [[System Settings Page Definitions](#)]
- Added support to configure UCM user SIP password. [[Account Page Definitions](#)]
- Added support to disable the mute key in the call feature. [[Phone Settings Page Definitions](#)]
- Added support of TCP Keep-alive for the TCP connection between the terminal and the SIP server. [[Account Page Definitions](#)]
- Added support of RTCP Keep-alive method. [[Account Page Definitions](#)]
- Added support of RTP Keep-alive method. [[Account Page Definitions](#)]

Firmware Version 1.0.3.31

- Added ability to configure programmable keys via LCD. [[Programmable Keys Page Definition](#)]
- Added support of Rport (RFC3581). [[Account Page Definitions](#)]
- Added ability to enable DND from web UI. [[Phone Settings Page Definitions](#)]
- Added ability to remove password requirement during factory reset. [[System Settings Page Definitions](#)]

Firmware Version 1.0.3.18

- Added Support of XML Application [[XML Application](#)]
- Added Support of Call Forward Always feature [[Call Forward Always](#)]
- Added Support of Show SIP Error Response feature [[Show SIP Error Response](#)]
- Added Support of Enable Hook Switch feature [[Enable Hook Switch](#)]
- Added Support of Contact Source Priority feature [[Contact Source Priority](#)]
- Added Support of Direct IP Call [[Enable Direct IP Call](#)]
- Added Support of Use Quick IP Call Mode [[Use Quick IP Call Mode](#)]
- Added Support of Predictive Dialing Feature [[Predictive Dialing Feature](#)]
- Added Support of Predictive Dialing Source [[Predictive Dialing Source](#)]
- Added Support of On-hook Dial Barging feature [[Onhook Dial Barging](#)]
- Added Support of Auto Redial feature [[Auto Redial](#)]
- Added Support of Call Completion Service [[Enable Call Completion Service](#)]
- Added Support of Incoming Call Popup feature [[Incoming Call Popup](#)]
- Added Support of Missed Call Notification feature [[Missed Call Notification](#)]
- Added Support of Call Waiting Tone [[CALL WAITING TONE](#)]
- Added Support of In-call DTMF Display [[In-Call DTMF Display](#)]
- Added Support of Show on Hold Duration feature [[Show On Hold Duration](#)]
- Added Support of Auto Unmute feature [[Enable Auto Unmute](#)]
- Added Support of Busy Tone on Remote Disconnect feature [[Enable busy tone remote disconnect](#)]
- Added Support for enabling or disabling transfer function [[Enable Transfer](#)]
- Added Support of Attended Transfer Mode [[Attended transfer mode](#)]
- Added Support for enabling or disabling conference function [[Enable Conference](#)]
- Added Support of Hold Call Before Adding Conferee feature [[Hold Call Before Adding Conferee](#)]
- Added Support of Hidden Number Plan [[Hidden Number Plan](#)]

- Added Support of Warning tone [[Enable warning Tone](#)]
- Added Support of Group listening with handset/speaker [[Group Listen with handset](#)][[Group Listen with Speaker](#)]
- Added Support of multiple retries for the device to send requests to the server [[Max Number Of Sip Request Retries](#)]
- Added Support of Failback Expiration time [[Failback Expiration](#)]

Firmware Version 1.0.1.57

- Added System time zone display in web UI. [[System Time-Zone](#)]
- Added Support of [[Recommend Time Zone](#)]

Firmware Version 1.0.1.50

- Added ability to Use Route Set in NOTIFY. [[USE ROUTE SET IN NOTIFY](#)]
- Added support for Auto Answer Numbers. [[AUTO ANSWER NUMBERS](#)]
- Added support for configuring the number to be dialed as DTMF using the TRANSFER button. [[IN-CALL DIAL NUMBER ON PRESSING TRANSFER KEY](#)]
- Added Multicast Paging mode for MPKs on GRP2604/P. [[MULTICAST PAGING MPK](#)]
- Added ability to configure VPKs. [[VPK](#)]
- Added ability to use up to 3 XML Phonebook URLs. [[Remote Phonebook](#)]

Firmware Version 1.0.1.41

- Added VLAN tag settings on the device LCD menu. [Figure 5: GRP260x LCD settings]
- Added support for Line LED color scheme. [Line LED Color Scheme]
- Added support to force a reboot after provisioning by P-values. [P-value 22421]
- Added support to configure remaining accounts with a SIP account when the public mode is enabled. [Allow Multiple Accounts]
- Added support of the dial now option in the dial plan types. [[Type](#)]
- Added support to set up a Forward Always softkey on the idle screen. [[Custom Softkey Layout](#)]
- Added support of "Ring for call waiting". [[Ring for Call Waiting](#)]

Firmware Version 1.0.1.36

- Added Greek language support. [[Multi-language](#)]

Firmware Version 1.0.1.18

- This is the initial version.

COPYRIGHT

(C)2025 Grandstream Networks, Inc. <https://www.grandstream.com>

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

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

CAUTION

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

WARNING

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

CERTIFICATION

U.S. FCC Part 68 Regulatory Information

This equipment complies with Part 68 of the FCC rules. Located on the equipment is a label that contains, among other information, the ACTA registration number and ringer equivalence number (REN). If requested, this information must be provided to the telephone company.

The REN is used to determine the quantity of devices which may be connected to the telephone line. Excessive REN's on the telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed five (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's contact the telephone company to determine the maximum REN for the calling area.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If any trouble experienced with this equipment, please contact (Agent in the US):

Company Name: Grandstream Networks, Inc.

Address: 126 Brookline Ave, 3rd Floor Boston, MA 02215, USA

Tel: 1-617-5669300

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

This equipment uses the following USOC jacks: RJ45C.

It is recommended that the customer install an AC surge arrester in the AC outlet to which this device is connected. This is to avoid damaging the equipment caused by local lightning strikes and other electrical surges.

Since this device has the HAC function, the earpiece is easy to absorb small, please take care to avoid scratching.

U.S. FCC Part 15 Regulatory Information

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

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

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio

Frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in 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.

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

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	LI
ES	FR	HR	IT	CY	LV	LT	LU	CH
HU	MT	NL	AT	PL	PT	RO	SI	TR
SK	FI	SE	NO	IS	UK	UK(NI)		

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

Hereby, Grandstream Networks, Inc. declares that the radio equipment GRP2602W are 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

GRP260x 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 the Grandstream website from:

<https://www.grandstream.com/legal/open-source-software>