Grandstream Networks, Inc.

GRP2601(P) | GRP2602(P/W)

GRP2603(P) | GRP2604(P)

Essential IP Phones

Administration Guide

GRP2601 / GRP2601P

GRP2602 / GRP2602P / GRP2602W

GRP2603 / GRP2603P

GRP2604 / GRP2604P

COPYRIGHT

CAUTION

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

WARNING

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

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 the 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 trouble is 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

Fax: 1-617-2491987

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.

GRP260x Administration Guide
Version 1.0.1.18
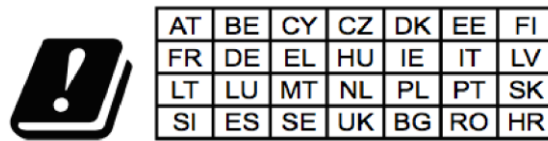
Caution: Exposure to Radio Frequency Radiation

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

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

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

Hereby, Grandstream Networks, Inc. declares that the radio equipment GRP2601/GRP2601P, GRP2602/GRP2602P/GRP2602W, GRP2603/GRP2603P and GRP2604/GRP2604P are in compliance with Directive 2014/53/EU.

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

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

GRP260x Administration Guide
Version 1.0.1.18

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 Grandstream web site from:

http://www.grandstream.com/sites/default/files/Resources/grp_gpl_color.tar.gz

Table of Contents

GRP260x Administration Guide
Version 1.0.1.18

GRP260x Administration Guide
Version 1.0.1.18

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes how to configure GRP260X features via phone's LCD menu and Web GUI menu. The intended audiences of this document are phone administrators.

To learn the basic functions of GRP2601(P)/GRP2602(P/W), GRP2603(P) and GRP2604(P), please visit http://www.grandstream.com/support to download the latest "GRP260X User Guide".

This guide covers the following topics:

- Product Overview

- Getting Started

- Configuration Guide

- NAT Settings

- Packet Capture

- Upgrading and Provisioning

- Restore Factory Default Settings

- Experiencing GRP260X

GRP260x Administration Guide
Version 1.0.1.18

CHANGE LOG

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 1.0.1.18

- This is the initial version.

GUI INTERFACE EXAMPLES

http://www.grandstream.com/sites/default/files/Resources/GRP260X_web_gui.zip

1. Screenshot of Login Page

2. Screenshots of Status Pages

3. Screenshots of Accounts Pages

4. Screenshots of Settings Pages

5. Screenshots of Network Pages

6. Screenshots of Maintenance Pages

7. Screenshots of Phonebook Pages

WELCOME

Thank you for purchasing Grandstream GRP260X Essential IP Phones.

Part of the GRP series of Carrier-Grade IP Phones, the GRP2601/GRP2602 is an essential 2-line model designed with zero-touch provisioning for mass deployment and easy management. It features a sleek design and a suite of next-generation features including 5-way voice conferencing to maximize productivity and dual band Wi-Fi support (GRP2602 only), EHS support for Plantronics & Jabra & Sennheiser headsets and multi-language support. The GRP series includes carrier-grade security features to provide enterprise-level security, including secure boot, dual firmware images and encrypted data storage. For cloud provisioning and centralized management, the GRP260X is supported by Grandstream's Device Management System (GDMS), which provides a centralized interface to configure, provision, manage and monitor deployments of Grandstream endpoints. Built for the needs of desktop workers and designed for easy deployment by enterprises, service providers and other high-volume markets, the GRP2601/GRP2602 offers an easy-to-use and easy-to-deploy voice endpoint.

Part of the GRP series of Carrier-Grade IP Phones, the GRP2603/GRP2604 is an essential 3-line model designed with zero touch provisioning for mass deployment and easy management. It features a sleek design and a suite of next generation features including: 5-way voice conferencing to maximize productivity, integrated PoE (GRP2603P), full HD audio on both the speaker and handset to allow users to communicate with the utmost clarity, EHS support for Plantronics & Jabra & Sennheiser headsets and multi-language support. The GRP series includes carrier-grade security features to provide enterprise-level security, including secure boot, dual firmware images and encrypted data storage. For cloud provisioning and centralized management, the GRP2603/GRP2604 is supported by Grandstream's Device Management System (GDMS), which provides a centralized interface to configure, provision, manage and monitor deployments of Grandstream endpoints. Built for the needs of desktop workers and designed for easy deployment by enterprises, service providers and other high-volume markets, the GRP2603/GRP2604 offers an easy-to-use and easy-to-deploy voice endpoint.

The GRP260X series deliver superior HD audio quality, rich and leading-edge telephony features, protection for privacy, and broad interoperability with most 3rd party SIP devices and leading SIP/NGN/IMS platforms. GRP260X series is the perfect choice for enterprise users looking for a high quality, feature rich multi-line executive IP phone with advanced functionalities and performance.

PRODUCT OVERVIEW

Feature Highlights

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

Table 1: GRP260X Features in a Glance

	GRP2601 **GRP2601P**	• 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.
	GRP2602 **GRP2602P** **GRP2602W**	• 2 SIP account keys with dual-color LED • 4 programmable context-sensitive soft keys. • 10/100M network ports. • Integrated PoE(for GRP2602P only). • 5-way conference. • Electronic Hook Switch (EHS) support for Plantronics & Jabra & Sennheiser. • Wi-Fi support (GRP2602W only).
	GRP2603 **GRP2603P**	• 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.

	GRP2604 **GRP2604P**	• 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.

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.

Table 2: GRP2601/GRP2601P 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 (GRP2601P only)
Graphic Display	132 x 48 (2.21") LCD display
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 G7.29A/B, G.711µ/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, 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, both on handset and full-duplex hands-free speakerphone
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	English, Chinese, Korean, Japanese, German, Italian, French, Spanish, Portuguese, Russian, Croatian, and more
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°C Storage: -10°C to 60°C Humidity: 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;

GRP260x Administration Guide
Version 1.0.1.18

Table 3: GRP2602/GRP2602P/GRP2602W 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 (GRP2602P only)
Graphic Display	132 x 48 (2.21") backlit graphical LCD display
Wi-Fi	Yes, dual-band (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 G7.29A/B, G.711µ/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

GRP260x Administration Guide
Version 1.0.1.18

Multi-language	English, German, Italian, French, Spanish, Portuguese, Russian, Croatian, Chinese, Korean, Japanese, and more
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 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;

Table 4: 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.711µ/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 (*wall mount sold separately)
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	English, German, Italian, French, Spanish, Portuguese, Russian, Croatian, Chinese, Korean, Japanese, and more
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;

Table 5: 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 G7.29A/B, G.711μ/a-law, G.726, G.722(wide-band), G723, iLBC, OPUS, in- band and out-of-band DTMF (in audio, RFC2833, SIP INFO)Support for G7.29A/B, G.711μ/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

GRP260x Administration Guide
Version 1.0.1.18

Base Stand	Yes, 2 angle positions available, Wall Mountable (*wall mount sold separately)
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	English, German, Italian, French, Spanish, Portuguese, Russian, Croatian, Chinese, Korean, Japanese, and more
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;

GRP260x Administration Guide
Version 1.0.1.18

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

Table 6: 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.
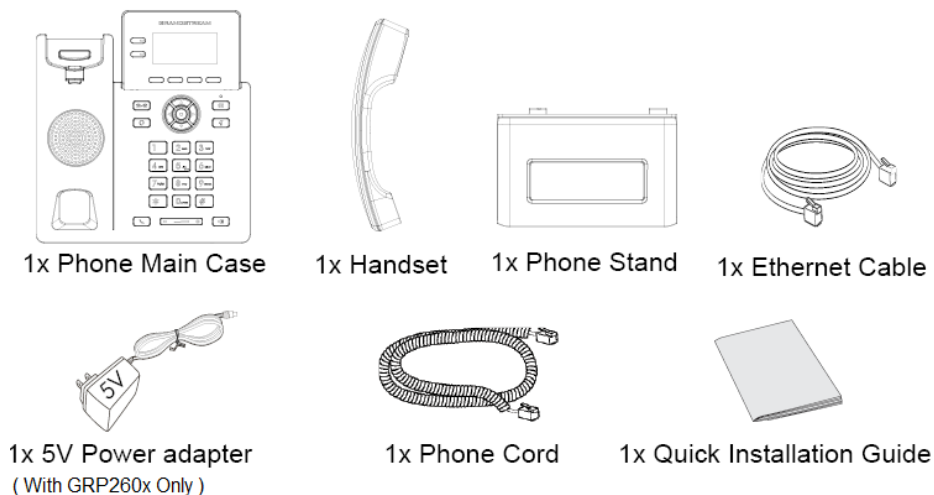
Figure 1: GRP260X Package Content

Note: 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 on the wall using the slots for wall mounting.
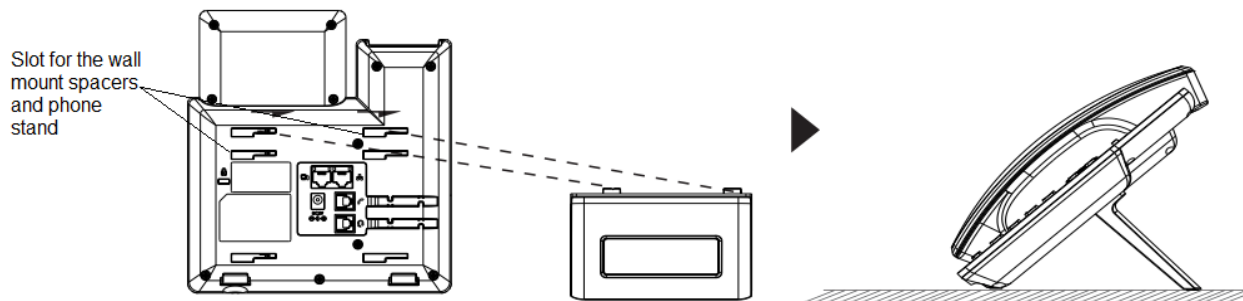
Figure 2: Phone Stand and Mounting Slots on the GRP260X

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).
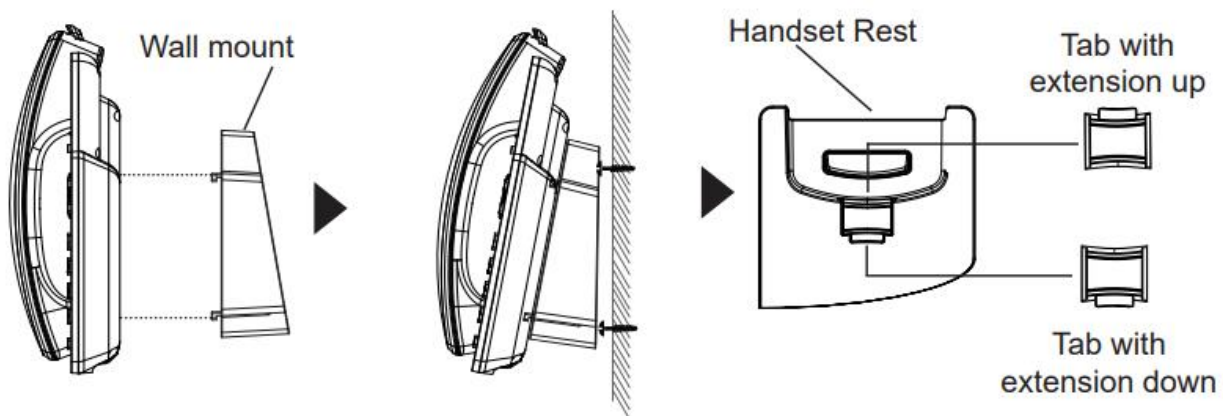
Figure 3: Tab on the Handset Cradle

GRP260x Administration Guide
Version 1.0.1.18

Connecting the GRP260X

To setup 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 PoE switch is used in step 3, this step could be skipped (For GRP260xP).

4. The LCD will display 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 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 press on Add softkey ✚. Then enter the Network's information.

Notes:

- 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 "Wi-Fi Network" page by pressing on the Wi-Fi softkey.

- For easy deployment, The GRP2602W is out of the box is preconfigured to connect to a default SSID named **wp_master** with a password (WPA/WPA2 PSK) 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.
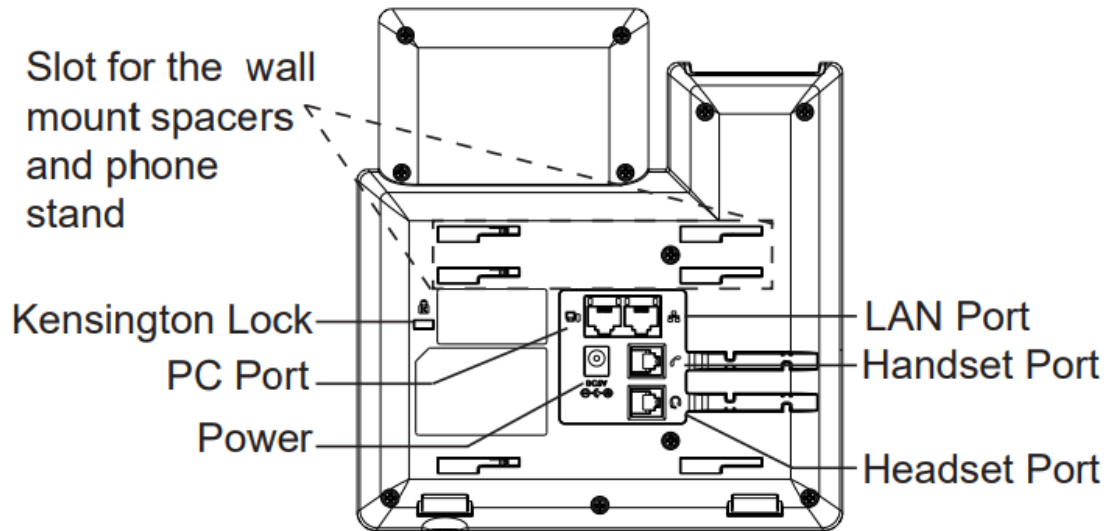
Figure 4: GRP260X Back Side View

Configuration via Keypad

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

- **Enter MENU options**. When the phone is in idle, press the round MENU button or Menu Softkey ≡ to enter the configuration menu.

- **Navigate in 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 ↩ to exit to the previous menu.

- **Return to Home page**.

The MENU options are listed in the following table.

Table 7: Configuration Menu

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** o **Sounds** Configures account ringtone and adjusts volume settings by pressing left/right arrow key. o **Date Time** Adjusts Time and Date displaying format. o **Time Zone** Choose your Time Zone from the list by scrolling with UP/DOWN keys. o **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. o **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. o **Headset Type** Choose the headset type of the headset connect to the phone. Users could choose Normal, Plantronics EHS, Jabra EHS, Sennheiser EHS. • **Advanced settings** o **Upgrade** Check for upgrade by contacting the firmware upgrade server.

- o **Syslog**

Configures Syslog level, Transport protocol and Syslog Server's address.

- o **Security**

Enables disables Web and SSH access.

- o **Alternative Firmware**

Press ⇄ softkey to switch between the dual firmware versions loaded to the phone. The phone will reboot with the chosen version.

- o **Factory Reset:**

Perform Factory reset to the phone. All device configuration and user data will be lost after factory reset.

- **Ethernet Settings**
  - o **Internet Protocol**

Selects Prefer IPv4 / Prefer IPv6 / IPv4 only or IPv6 only. The default setting is "IPv4 only".

- o **IPv4 Setting**

Selects IP mode (DHCP/Static IP/PPPoE); Configures PPPoE account ID and password; Configures static IP address, Netmask, Gateway, Preferred DNS server.

- o **IPv6 Setting**

Selects IP mode (DHCP/Static IP); Configures static IP address, IPv6 Prefix (64 bits), IPv6 Preferred DNS server.

- **Wi-Fi Settings (GRP2602W only)**
  - o **Wi-Fi**

Enables/disables Wi-Fi;

- o **Wi-Fi Band**

Choose Wi-Fi band (2G , 5G or 2G&5G).

- o **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 Menu button 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.
Reboot	Reboots the phone.

The following picture shows the keypad MENU configuration flow:
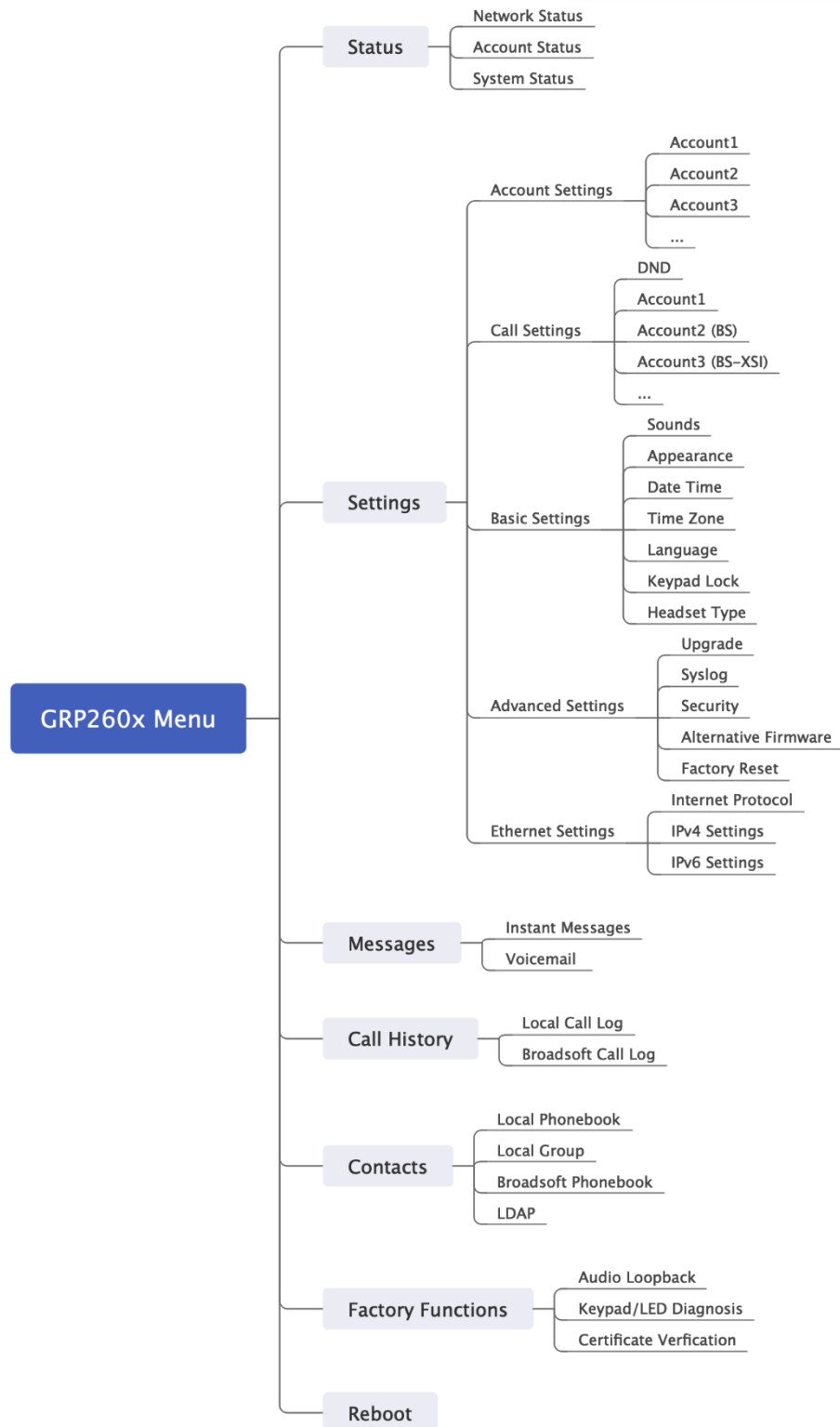
Figure 5: GRP260x LCD settings

GRP260x Administration Guide
Version 1.0.1.18

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 phone is at 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.

Notes:

- 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 connected to. In absence of a hub/switch (or free ports on the hub/switch), please connect the computer directly to the PC port on the back of the 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 IP address 192.168.40.154, please enter "http://192.168.40.154" in the address bar of the browser.

- There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed
End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	Random password available on the sticker at the back of the unit.	Browse all pages

- When changing any settings, always SUBMIT them by pressing the "Save" or "Save and Apply" button on the bottom of the page. If the change is saved only but not applied, after making all the changes,

click on the "APPLY" button on top of the page to submit. After submitting the changes in all the Web GUI pages, reboot the phone to have the changes take effect if necessary (All the options under "Accounts" page and "Phonebook" page do not require reboot. Most of the options under "Settings" page do not require reboot).

Saving Configuration Changes

After users makes changes to the configuration, press the "Save" button will save but not apply the changes until the "Apply" button on the top of web GUI page is clicked. Or users could directly press "Save and Apply" button. We recommend rebooting or powering cycle the phone after applying all the changes.

Rebooting from Remote Locations

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

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, 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 web access, upgrading and provisioning, syslog, language settings, TR-069, security , Outbound Notifications , Voice monitoring etc.

- **Application:** Configures Web Service settings, Contacts, LDAP , Call History.

- **External Service:** Configures GDS Settings, Call Center, BroadSoft XSI.

Status Page Definitions

Table 8: Status Page Definitions

Status → Account Status	
Account	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, it will display Yes/No with Green/Red background.
Status → Network Status	
MAC Address	Global unique ID of device, in HEX format. The MAC address will be used for provisioning and can be found on the label coming with original box and on the label located on the back of the device.

IP Setting	The configured address type: DHCP, Static IP or PPPoE.
IPv4 Address	The IPv4 address obtained on the phone.
IPv6 Address	The IPv6 address obtained on the phone.
OpenVPN® IP	The OpenVPN® IP obtained on the phone.
Subnet Mask	The subnet mask obtained on the phone.
Gateway	The gateway address obtained on the phone.
DNS Server 1	The DNS server address 1 obtained on the phone.
DNS Server 2	The DNS server address 2 obtained on the phone.
PPPoE Link Up	PPPoE connection status.
NAT Type	The type of NAT connection used by the phone.
NAT Traversal	Display the status of NAT connection for each account on the phone.
Status → System Info	
Product Model	Product model of the phone.
Part Number	Product part number.
Software Version	• **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	• **Language:** displaying language. • **Time Zone:** displaying time zone;
System Up Time	System up time since the last reboot.
System Time	Current system time on the phone system.
Service Status	GUI, Phone and CPE service status.
System Information	Download system information
User Space	Shows the percentage of the user space used and the status of the Database

Core Dump	Shows the status of the core dump and the core dump files generated if any. It also gives the ability to generate GUI/Phone core dump files manually.
Special Feature	**OpenVPN® Support:** displaying if the phone supports OpenVPN®.

Account Page Definitions

Table 9: Account Page Definitions

Account x → General Settings	
Account Register	
Account Active	This field indicates whether the account is active. The default setting is "No".
Account Name	The name associated with each account to be displayed on the LCD.
SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (ITSP).
Secondary SIP Server	The URL or IP address, and port of the SIP server. When configured, phone will register to both Primary and Secondary SIP Server. If Primary SIP Server is not reachable then the phone will use Secondary SIP Server for phone services (including making/receiving calls).
SIP User ID	User account information provided by your VoIP service provider (ITSP). It is usually in the form of digits like phone number or actually a phone number.
SIP Authentication ID	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	The account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After it is saved, this will appear as hidden for security purpose.
Name	The SIP server subscriber's name (optional) that will be used for Caller ID display.
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request.

Voice Mail Access Number	Allows users to access voice messages by pressing the MESSAGE button on the phone. This value is usually the VM portal access number.
BLF Server	Optional server used for SUBSCRIBE requests to indicate other extensions status on the SIP server.
Account Display	This option allows you to configure how your SIP account label will be displayed on the phone's screen. If set to "Username", LCD account label will display the Account Name configured for this SIP account. If set to "User ID", it will then display the SIP User ID configured for this SIP account.
Network Settings	
Outbound Proxy	IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller. It is used by the phone for Firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and ONLY an Outbound Proxy can provide a solution.
Secondary Outbound Proxy	IP address or Domain name of the Secondary Outbound Proxy which will be used when the primary proxy cannot be connected.
DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. If "Use Configured IP" is selected, please fill in Primary IP, Backup IP 1, and Backup IP 2. • A Record • SRV • NAPTR/SRV • Use Configured IP
DNS SRV Failover Mode	Configure the preferred IP mode for DNS SRV. If selected "default", first IP from query result will be applied; If selected "Saved one until DNS TTL", previous IP will be applied before reaches DNS timeout; If selected "Saved one until no response", and previous IP will be applied even after DNS time out until it cannot response. • **Default** If the option is set with "default", it will again try to send register messages to one IP at a time, and the process repeats. • **Saved one until DNS TTL** If the option is set with "Saved one until DNS TTL", it will send register messages to the previously registered IP first. If no response, it will try to

	send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up. • **Saved one until no responses** If the option is set with "Saved one until no responses", it will send register messages to the previously registered IP first, but this behavior will persist until the registered server does not respond.
Primary IP	Configures the primary IP address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 1	Configures the backup IP 1 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 2	Configures the backup IP 2 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
NAT Traversal	This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, STUN, Keep-alive, UPnP, Auto or VPN. The default setting is "Auto". If set to "STUN" and STUN server is configured, the phone will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the phone will try to use public IP addresses and port number in all the SIP&SDP messages. The phone will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be "Keep-alive". Configure this to be "No" if an outbound proxy is used. "STUN" cannot be used if the detected NAT is symmetric NAT. Set this to "VPN" if OpenVPN is used.
Proxy-Require	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall. Do not configure this parameter unless this feature is supported on the SIP server.
Use SBC	Indicate whether an SBC server is used. If users want to work under SBC associated with 3CX, they should enable this feature to have better communication with the server.
Account x → SIP Settings	
Basic Settings	
SIP Registration	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is "Enabled".

UNREGISTER on Reboot	Allows the SIP user's registration information to be cleared when the phone reboots. The SIP REGISTER message will contain "Expires: 0" to unbind the connection. Three options are available: The default setting is "No". • If set to "**All**", the SIP user's registration information will be cleared when the phone reboots. The SIP Contact header will contain "*" to notify the server to unbind the connection. • If set to "**Instance**", the SIP user will be unregistered on current phone only. • If set to "**No**", the phone will not unregister the SIP account when rebooting.
REGISTER Expiration	Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar. The default value is 60 minutes. 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 maximum value is 64800 (about 45 days). The default value is 60 minutes.
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.
Registration Retry Wait Time	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
Add Auth Header on Initial REGISTER	Add authorization Header on initial REGISTER from the first REGISTER
Enable OPTIONS Keep Alive	Enable OPTIONS Keep Alive to check SIP Server. Default is "Disabled".
OPTIONS Keep Alive Interval	Time interval for OPTIONS Keep Alive feature in seconds. Default is "30" seconds.
OPTIONS Keep Alive Max Lost	Number of max lost packets for OPTIONS Keep Alive feature before the phone re-registration. Default is "3".
SUBSCRIBE for MWI	When set to "Yes", a SUBSCRIBE for Message Waiting Indication will be sent periodically. The phone supports synchronized and non-synchronized MWI. The default setting is "No".
SUBSCRIBE for Registration	When set to "Yes", a SUBSCRIBE for Registration will be sent out periodically. The default setting is "No".

Use Privacy Header	Controls whether the Privacy header will present in the SIP INVITE message or not, whether the header contains the caller info. • **Default:** The Privacy Header will show in INVITE only when "Huawei IMS" special feature is on. • **Yes:** The Privacy Header will always show in INVITE. • **No:** The Privacy Header will not show in INVITE. The default setting is "default".
Use P-Preferred-Identity Header	Controls whether the P-Preferred-Identity Header will present in the SIP INVITE message. • **Default:** The P-Preferred-Identity Header will show in INVITE unless "Huawei IMS" special feature is on. • **Yes:** The P-Preferred-Identity Header will always show in INVITE. • **No:** The P-Preferred-Identity Header will not show in INVITE. The default setting is "default".
Use X-Grandstream-PBX Header	Enables / disables the use of X-Grandstream-PBX header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "Yes".
Use P-Access-Network-Info Header	Enables / disables the use of P-Access-Network-Info header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "Yes".
Use P-Emergency-Info Header	Enables / disables the use of P-Emergency-Info header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "Yes".
Use MAC Header	• If **Yes for REGISTER only**, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header. • If **Yes to all SIP**, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP message including REGISTER will attach the MAC address to the User-Agent header. • If **No**, neither will the MAC header be included in the register or unregister message nor the MAC address be attached to the User-Agent header for any outgoing SIP message. The default setting is "No".

Add MAC in User-Agent	If Yes except REGISTER, the SIP messages for register or unregister will not contain MAC address in the User-Agent header, and all the other outgoing SIP messages will attach MAC address to the User-Agent header; If Yes to ALL, all the outgoing SIP messages will attach MAC address to the User-Agent header; If No, MAC address will not be attached to the User-Agent header for any outgoing SIP message.
SIP Transport	Determines the network protocol used for the SIP transport. Users can choose from TCP, UDP and TLS. The default setting is "UDP".
SIP Listening Mode	Determines whether to listen to multiple SIP protocols. • **Transport Only:** will listen to configured transport protocol only. • **Dual:** will listen to TCP when UDP is selected. • **Dual (Secured):** will listen to TLS/TCP when UDP is selected. If TCP or TLS/TCP is selected, UDP will be listened to • **Dual (BLF Enforced):** 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	Defines the local SIP port used to listen and transmit.
SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	This option is used to control the port information in the Via header and Contact header. If set to No, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. The default setting is "No".
Support SIP Instance ID	Defines whether SIP Instance ID is supported or not. Default setting is "Yes".
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
Outbound Proxy Mode	The Outbound proxy mode is placed in the route header when sending SIP messages, or they can be always sent to outbound proxy.

	• **In route** • **Not in route** • **Always send to** Default is "in route".
Enable 100rel	The use of the PRACK (Provisional Acknowledgment) method enables reliability to SIP provisional responses (1xx series). This is very important to support PSTN internetworking. To invoke a reliable provisional response, the 100rel tag is appended to the value of the required header of the initial signaling messages. The default setting is "No".
Session Timer	
Enable Session Timer	This option is used to enable or disable session timer on the phone side when server side can provide both session timer UPDATE and session audit UPDATE. The default setting is "No".
Session Expiration	The SIP Session Timer extension (in seconds) that enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180. The valid range is from 90 to 64800.
Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
Caller Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it makes outbound calls. The default setting is "No".
Callee Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it receives inbound calls. Default setting is "No".
Force Timer	If Force Timer is set to "Yes", the phone will use the session timer even if the remote party does not support this feature. If Force Timer is set to "No", the phone will enable the session timer only when the remote party supports this feature. To turn off the session timer, select "No". The default setting is "No".
UAC Specify Refresher	As a Caller, select UAC to use the phone as the refresher; or select UAS to use the Callee or proxy server as the refresher. The default setting is "UAC".
UAS Specify Refresher	As a Callee, select UAC to use caller or proxy server as the refresher; or select UAS to use the phone as the refresher. The default setting is "UAC".

GRP260x Administration Guide
Version 1.0.1.18

Force INVITE	The Session Timer can be refreshed using the INVITE method or the UPDATE method. Select "Yes" to use the INVITE method to refresh the session timer. The default setting is "No".

Account x → 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.
Codec Negotiation Priority	Configures the phone to use which codec sequence to negotiate as the callee. When set to "Caller", the phone negotiates by SDP codec sequence from received SIP Invite. When set to "Callee", the phone negotiates by audio codec sequence on the phone. The default setting is "Callee".
Use First Matching Vocoder in 200OK SDP	When it is set to "Yes", the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is "No".
iLBC Frame Size	This option determines the iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is "30ms".
iLBC Payload Type	This option is used to specify iLBC payload type. Valid range is 96 to 127. The default setting is "97".
G.726-32 Packing Mode	Selects "ITU" or "IETF" for G726-32 packing mode. The default setting is "ITU".
G.726-32 Dynamic Payload Type	Specifies G.726-32 payload type. Valid range is 96 to 127. Default is 127.
Opus Payload Type	Specifies OPUS payload type. Valid range is 96 to 127. Cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
Send DTMF	This parameter specifies the mechanism to transmit DTMF digits. There are 3 supported modes: • **In audio**: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs). • **RFC2833** sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. • **SIP INFO** uses SIP INFO to carry DTMF. Default setting is "RFC2833".

DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call. The default setting is "Yes".
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 126. The default value is 121.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 126. The default value is 124.
Silence Suppression	Controls the silence suppression/VAD feature of the audio codecs except forG.723 (pending) and G.729. If set to "Yes", a small quantity of RTP packets containing comfort noise will be sent during the periods of silence. If set to "No", this feature is disabled. Default setting is "No"
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. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is 2.
G.723 Rate	Selects encoding rate for G723 codec.
RTP Settings	
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu. • **No** • **Enabled but Not forced** • **Enabled and Forced** • **Optional** The default setting is "No".
SRTP Key Length	Allows users to specify the length of the SRTP calls. Available options are: • **AES 128&256 bit** • **AES 128 bit** • **AES 256 bit** Default setting is AES 128&256 bit

Crypto Lifetime	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. The default setting is "Yes".
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	Configure 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.
Symmetric RTP	Defines whether symmetric RTP is supported or not. Default setting is "No".
RTP Timeout (s)	Configures the RTP timeout of the phone. If the phone does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. The default range is 0 and 6-600. If set to 0, the phone will not hang up the call automatically.
Account x → Call Settings	
Call Features	
Auto Answer	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep. Default setting is "No".
Custom Alert-Info for Auto Answer	Allows to customize Alert-Info header for auto answer. The phone will auto answer only if matching content of the custom Alert-info header.
Allow Auto Answer by Call-Info/Alert-Info	Allows the phone to automatically turn on the speaker phone to answer incoming calls after a short reminding beep when enabled, based on the SIP Call-Info/Alert-Info header sent from the server/proxy. Default is "Yes".
Allow Barging by Call-Info/Alert-Info	When enabled, the phone will automatically put 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. Default setting is "No".
Send Anonymous	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous, blocking the Caller ID to be displayed. Default is "No".
Anonymous Call Rejection	If set to "Yes", anonymous calls will be rejected. The default setting is "No".
Call Log	Configures Call Log setting on the phone. • **Log All Calls**

	• **Log incoming/Outgoing Only (missed calls NOT recorded)** • **Disable Call Log** The default setting is "Log All Calls".
Transfer on Conference Hangup	If set to "Yes", when the phone hangs up as the conference initiator, the conference call will be transferred to the other parties so that other parties will remain in the conference call. The default setting is "No".
Key as Send	Allows users to configure either the "*" or "#" keys as the "Send" key. Please make sure the dial plan is properly configured to allow dialing * and # out. The default setting is "Pound (#)".
Record Key Default Function	Configure whether to turn the recording function on or off when the "Record" key is pressed for the first time in a call under this account, and switch between the two. For example, the SIP server can be configured with the automatic start call recording function. In this case, Record key default function needs to be configured as "Record off".
Call Recording On	Configures the DTMF sequence sent when pressing the Record key during a call on this account. Toggles between this value and the off code if possible; otherwise always sends this code.
Call Recording Off	Configures the DTMF sequence sent when pressing the Recording key during a call on this account when turning recording off.
Enable Recovery on Blind Transfer	Disables recovery to the call to the transferee on failing blind transfer to the target. The default setting is "Yes". **Notes:** 1) This feature only applies to blind transfer. 2) 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. 3) 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. Valid range is 30 to 300. Default setting is "30".
No Key Entry Timeout	Defines the timeout (in seconds) for no key entry. If no key is pressed after the timeout, the digits will be sent out. The default value is 4 seconds. The valid range is from 1 to 15.

Ring Timeout	Defines the timeout (in seconds) for the rings on no answer. The default setting is 60. The valid range is from 10 to 300.
Refer-To Use Target Contact	If set to "Yes", the "Refer-To" header uses the transferred target's Contact header information for attended transfer.
RFC2543 Hold	Allows users to toggle between RFC2543 hold and RFC3261 hold. RFC2543 hold (0.0.0.0) allows user to disable the hold music sent to the other side. RFC3261 (a line) will play the hold music to the other side. The default setting is "No".
Enable Call Waiting	Enables / disables the call waiting feature for the current account. When set to "Default", global call feature setting will be used. Default value is "Default".
Dial plan	
Dial Plan Prefix	Configures the prefix added to dialed number.
Bypass Dial Plan	Bypass the dial plan when dialing from one of the available items: Contacts ; Call History Incoming Call ; Call History Outgoing Call ; Dialing Page ; MPK ; API
Dial Plan	A dial plan 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: 1. Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d; 2. Grammar: **x** – any digit from 0-9; 3. Grammar: **X** – any character from 0-9, a-z, A-Z. a) **xx+** - at least 2 digit numbers b) **xx** – only 2 digit numbers c) **XX** – two characters (AA, Ab, 1C, f5, 68,…) d) **\t\e\s\t** : only string "test" will pass the dial plan check e) **^** - exclude f) **[3-5]** – any digit of 3, 4, or 5 g) **[147]** – any digit of 1, 4, or 7 h) **<2=011>** - replace digit 2 with 011 when dialing i) **|** - the OR operand • Example 1: {[369]11 | 1617xxxxxxx} Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617; • Example 2: {^1900x+ | <=1617>xxxxxxx}

	Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers;
	• Example 3: {1xxx[2-9]xxxxxx	<2=011>x+}
	Allows any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR Allows any length of numbers with leading digit 2, replacing the 2 with 011 when dialed.
	Example of a simple dial plan used in a Home/Office in the US:
	{ ^1900x.	<=1617>[2-9]xxxxxx	1[2-9]xx[2-9]xxxxxx	011[2-9]x.	[3469]11 }
	Explanation of example rule (reading from left to right):
	• ^1900x. – prevents dialing any number started with 1900;
	• <=1617>[2-9]xxxxxx – allows dialing to local area code (617) numbers by dialing7 numbers and 1617 area code will be added automatically;
	• 1[2-9]xx[2-9]xxxxxx |- allows dialing to any US/Canada Number with 11 digits length;
	• 011[2-9]x – allows international calls starting with 011;
	• [3469]11 – allows dialing special and emergency numbers 311, 411, 611 and 911.
	Note: In some cases, where the user wishes to dial strings such as *123 to activate voice mail or other applications provided by their service provider, the * should be predefined inside the dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.
	Max length of dial plan is up to 1024 characters.
Call Display	
Caller ID Display	When set to "Auto", the phone will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. When set to "Disabled", all incoming calls are displayed with "Unavailable".
Callee ID Display	When set to "Auto", the phone will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in the 180 Ringing. When set to "Disabled", callee id will be displayed as "Unavailable". When set to "To Header", caller id will not be updated and displayed as To Header.
Ringtone	

Account Ring Tone	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu. **Note**: User can also choose silent ring tone.
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* Selects the distinctive ring tone for the matching rule. When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone.

Account x → Advanced Settings	
Security Settings	
Check Domain Certificates	Choose whether the domain certificates will be checked or not when TLS/TCP is used for SIP Transport. The default setting is "No".
Validate Certificate Chain	Validate certification chain when TCP/TLS is configured. Default setting is "No".
Validate Incoming SIP Messages	Choose whether the incoming messages will be validated or not. The default setting is "No".
Omit charset=UTF-8 in MESSAGE	Omit charset=UTF-8 in MESSAGE content-type
Allow Unsolicited REFER	Allow unsolicited REFER to accomplish an outgoing call

Accept Incoming SIP from Proxy Only	When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is "No".
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is "No".
Allow SIP Reset	Allow SIP Notification message to perform factory reset
Authenticate Incoming INVITE	If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. Default setting is "No".
MOH	
On Hold Reminder Tone	Plays a reminder tone when you have a call on hold
Music On Hold URI	Music On Hold URI to call when a call is on hold if server supports it.
Advanced Features	
Special Feature	Different soft switch vendors have special requirements. Therefore, users may need select special features to meet these requirements. Users can choose from Standard, Nortel MCS, Broadsoft, CBCOM, RNK, Sylantro, Huawei IMS, PhonePower and UCM Call center depending on the server type. The default setting is "Standard".
Feature Key Synchronization	This feature is used for Broadsoft call feature synchronization. When it is enabled, DND, Call Forward features and Call Center Agent status can be synchronized between Broadsoft server and phone. Default is "Disabled".
Conference URI	Configures the conference URI when using Broadsoft N-way calling feature.
Broadsoft Call Center	When set to "Yes", a Softkey "BSCCenter" is displayed on LCD. User can access different Broadsoft Call Center agent features via this Softkey. Please note that "Feature Key Synchronization" will be enabled regardless of this setting. Default setting is "No". **Note:** To activate this feature, users need to change the special feature to Broadsoft and setup the Broadsoft Call Center to take effect.
Hoteling Event	Broadsoft Hoteling event feature. Default setting is "No". With "Hoteling Event" enabled, user can access the Hoteling feature option by pressing the "BSCCenter" softkey.
Call Center Status	When set to "Yes", the phone will send SUBSCRIBE to the server to obtain call center status. The default setting is "No".

Broadsoft Executive Assistant	When enabled, Feature Key Synchronization will be enabled regardless of web settings.
Broadsoft Call Park	When enabled, it will send SUBSCRIBE to Broadsoft server to obtain Call Park notifications. The default setting is "Disabled".
SCA	
Enable SCA (Shared Call Appearance)	If set to "Yes", the Shared Call Appearance (BroadSoft Standard) will be used for the registered account.
Line-Seize Timeout	Configures the interval (in seconds) when the line-seize is considered timed out when Shared Call Appearance feature is used. Valid range is 15 to 60.
BLF (Busy Lamp Field) - GRP2604 only	
Presence Eventlist URI	Configures Presence Eventlist URI to monitor the extensions on Multi-Purpose Keys.
Eventlist BLF URI	Configures Eventlist BLF URI to monitor the extensions on Multi-Purpose Keys
Auto provision Eventlist	Select the type of Eventlist to get automatically provisioned onto available MPKs. Whether its BLF Eventlist or Presence Eventilist.
BLF Call-pickup	Configures BLF Call-pickup method: • **If select Auto:** The phone will do either Prefix or barge in code for BLF pickup depend on which on is set. • **If select Force BLF Call-pickup by prefix:** The phone will only use Prefix as BLF pickup method. • **If select Disabled:** The phone will ignore both BLF pickup method, now the monitored VPK will only dial the extension if pressed
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	Set feature access code of Call Pickup with Barge-In feature.
PUBLISH for Presence	Enables presence feature on the phone. The default setting is "No".
Account x → Dial Plan	
Name	Enter the name for the configured rules.

GRP260x Administration Guide
Version 1.0.1.18

Rule	Enter the rule settings (number pattern, prefix to add …etc.).
Type	Choose the type of the rule (pattern, block, dial now, prefix & second tone).

Account x → Feature codes

Enable Local Call Features	When enabled, Do Not Disturb, Call Forwarding and other call features can be used via the local feature codes on the phone. Otherwise, the provisioned feature codes from the server will be used. User configured feature codes will be used only if server provisioned feature codes are not provided. **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	The extension the call will be forwarded to.

Call Forward No Answer

On	Configures Call Forward No Answer feature code to activate no answer call forwarding.
Off	Configures Call Forward No Answer feature code to deactivate no answer call forwarding.
Target	The extension the call will be forwarded to.
Call Forward No Answer Timeout (s)	Defines the timeout (in seconds) before the call is forwarded on no answer. 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**: Make sure to press "Start" to complete the process.

Phone Settings Page Definitions

Phone Settings → General settings	
Basic Settings	
Local RTP Port	This parameter defines the local RTP port used to listen and transmit. It is the base RTP port for channel 0. When configured, channel 0 will use this port _value for RTP; channel 1 will use port_value+2 for RTP. Local RTP port ranges from 1024 to 65400 and must be even. Default value is 5004.
Local RTP Port Range	Gives users the ability to define the parameter of the local RTP port used to listen and transmit. This parameter defines the local RTP port from 48 to 10000. This range will be adjusted if local RTP port + local RTP port range is greater than 65486. Default setting is 200.
Use Random Port	When set to "Yes", this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is "No" **Note:** This parameter must be set to "No" for Direct IP Calling to work.
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 to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN Server	The IP address or Domain name of the STUN server. STUN resolution results are displayed in the STATUS page of the Web GUI. Only non-symmetric NAT routers work with STUN.
Use NAT IP	The NAT IP address used in SIP/SDP messages. This field is blank at the default settings. It should ONLY be used if it is required by your ITSP.
Delay Registration	Configures specific time that the account will be registered after booting up.
Test Password Strength	Only Allow password with some constraints to ensure better security.
Enable Outbound Notification	Configures whether to enable outbound notifications such as Action URL.
Public Mode	
Enable Public Mode	Configures to turn on/off public mode for hot desking feature.
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.

Key Mode	**Account Mode** In Calling State, each key displays the call status of the corresponding account. Click to switch to the first line under this account or select the account to initiate a new call. **Line Mode** In Calling State, each key controls a line, and the call line can be switched by pressing the key.
Click-To-Dial Feature	Enables Click-To-Dial feature. If this feature is enabled, user could click the green dial button on left top corner of phone's Web GUI, then choose the account and dial to the target number. The default setting is "Disabled".
Enable Call Waiting	Disables the call waiting feature. The default setting is "Yes".
Hold Call before Completing Transfer	When set to "No", phone will neither hold the current call in transfer window nor hold the call with the transfer target before referring the call in the attended transfer.
Hold Call before Adding Conferee	Configures whether to put current call on hold when adding new member to conference. If set to "Yes", the current call will be put on hold when the host presses conference or add key to invite new member. When the invited member answers the call and agrees to attend conference, the host needs to manually resume the conference with the new member added. If set to "No", the current call will not be put on hold and the invited member will join meeting automatically after answering the call.
Enable DND Feature	If set to "No", a user cannot turn on Do Not Disturb feature via MUTE key, MPK, or menu on LCD
Mute Key Functions While Idle	If this feature is enabled, MUTE key will take effect in idle state and future incoming call will be answered with mute.
Enable Sending DTMF via specific MPKs	Allows certain MPKs to send DTMF in-call. This option does not affect Dial DTMF. This option is available for the GRP2604 only.
Preferred Default Account	Select the preferred default account when off-hook/on-hook dialing. When selected account is unavailable, system will fall back to use the first available account instead.
Off-hook Auto Dial	Configures the digits to be dialed via the first account when the phone is off hook.

Off-hook Auto Dial Delay	Defines the timeout (in seconds) for off-hook auto dial. Valid range is 0-30. If set to 0, it will be dialed out immediately; If set to other values, it will be dialed out after the delay.
Off-hook / On-hook Timeout	If configured, when the phone is in the off-hook or on-hook dialing state, it will go idle after the timeout (in seconds). Valid range is 10 to 60.
Enable Live Keypad	If enable phone will automatically dials out and turns on handsfree mode as soon as a dial pad key or softkey is pressed.
Live Keypad Expire Time	Set the Live DialPad expire time, interval is between 2s and 15s, default value is 5s.
Bypass Dial Plan Through Call History and Directories	Enable/Disable the dial plan check while dialing through the call history and any phonebook directories.
Do Not Escape # as %23 in SIP URI	Specifies whether to replace # by %23 or not for some special situations. The default setting is "No".
Return Code When Refusing Incoming Call	When refusing the incoming call. The phone will send the selected type of SIP message of the call. Available options are: • **Busy (486).** • **Temporarily Unavailable (480).** • **Not found (404).** • **Decline (603).** Default setting is "Busy 486".
Return Code When Enable DND	When DND is enabled, the phone will send the selected type of SIP message. Available options are: • **Busy (486).** • **Temporarily Unavailable (480).** • **Not found (404).** • **Decline (603).** Default setting is "Temporarily Unavailable (480)".
Allow Incoming Call Before Ringing	This allows incoming calls after dialed but before ringing. This can be used under custom user configuration based on need.
User-Agent Prefix	Configure the prefix in the User-Agent header
Ringtone	
Call Progresses Tones: • System Ring Tone	Configures ring or tone frequencies based on parameters from local telecom. The default value is North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds.

• Dial Tone • Second Dial Tone • Message Waiting • Ring Back Tone • Call-Waiting Tone • Busy Tone • Reorder Tone	**Syntax**: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. To set a continuous ring, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported.
Call Waiting Tone Gain	Configures the call waiting tone gain to adjust call waiting tone volume (Low, Medium, or High). The default setting is "Low".
Lock Speaker Volume	Lock volume adjustment when the option is enabled so it cannot be changed from phone LCD. The option can be set to: "No", "Ring", "Talk" or "Both". Default setting is "No".
Multicast Paging	
Multicast Paging Function	Enable or disable multicast paging
Allowed In DND Mode	Allow Multicast Paging when DND mode is enabled. Default Setting is "No".
Paging Barge	During active call, if incoming multicast page is higher priority (1 being the highest) than this value, the call will be held, and multicast page will be played. The default setting is "Disabled".
Paging Priority Active	If enabled, during a multicast page if another multicast is received with higher priority (1 being the highest) that one will be played instead. The default setting is "Enabled".
Multicast Channel Number	Multicast Channel Number (0-50). 0 for normal RTP packets, 1-50 for Polycom multicast format packets.
Multicast Paging Codec	The codec for sending multicast pages, there are 5 codecs could be used: G.731.1 PCMU, PCMA, G.726-32, G.729A/B, G.722 (wide band). Default setting is "PCMU".
Multicast Sender ID	Outgoing caller ID that displays to your page group recipients (for multicast channel 1 – 50).
Multicast Listening	Defines multicast listening addresses and labels. For example: • "Listening Address" should match the sender's Value such as "237.11.10.11:6767"

	• "Label" could be the description you want to use. For details, please check the "Multicast Paging User Guide" on our Website.

Network Settings Page Definitions

<div align="center">Table 11: Network Page Definitions</div>

Network Settings → Ethernet Settings	
Internet Protocol	Selects "IPv4 Only", "IPv6 Only", "Both, prefer IPv4" or "Both, prefer IPv6". The default setting is "IPv4 only".
IPv4 Address	
IPv4 Address	Allows users to configure the appropriate network settings on the phone to obtain IPv4 address. Users could select "DHCP", "Static IP" or "PPPoE". By default, it is set to "DHCP".
IPv4 Address	Enter the IP address when static IP is used.
Subnet Mask	Enter the Subnet Mask when static IP is used for IPv4.
Gateway	Enter the Default Gateway when static IP is used for IPv4.
DNS Server 1	Enter the DNS Server 1 when static IP is used for IPv4.
DNS Server 2	Enter the DNS Server 2 when static IP is used for IPv4.
Preferred DNS Server	Enters the Preferred DNS Server for Ipv4.
IPv6 Address	
IPv6 Address Type	Allows users to configure the appropriate network settings on the phone to obtain IPv6 address. Users could select "Auto-configured" or "Statically configured" for the IPv6 address type.
Static IPv6 Address	Enter the static IPv6 address when Full Static is used in "Statically configured" IPv6 address type.
IPv6 Prefix Length	Enter the IPv6 prefix length when Full Static is used in "Statically configured" IPv6 address type.
DNS Server 1	Enter the DNS Server 1 for IPv6.
DNS Server 2	Enter the DNS Server 2 for IPv6.
Preferred DNS server	Enter the Preferred DNS Server for IPv6.
802.1X	
802.1X mode	Allows the user to enable/disable 802.1X mode on the phone. The default value is disabled. To enable 802.1X mode, this field should be set to EAP-

	MD5, users may also choose EAP-TLS, or EAP-PEAPv0/MSCHAPv2.
802.1X Identity	Enter the Identity information for the 802.1x mode. **Note:** Letters, digits and special characters including @ and – are accepted.
MD5 Password	Enter the MD5 Password for the 802.1X mode. **Note:** Letters, digits and special characters including @ and – are accepted.
802.1X CA Certificate	Uploads / deletes the 802.1X CA certificate to the phone; or delete existed 802.1X CA certificate from the phone.
802.1X Client Certificate	Uploads / deletes 802.1X Client certificate to the phone; or delete existed 802.1X Client certificate from the phone.
Network Settings → Wi-Fi Settings (GRP2602W Only)	
Wi-Fi Function	Enables / Disables the Wi-Fi on the phone. Three options are available: • **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.
Wi-Fi Band	Set the type of Wi-Fi Band whether its 2G or 5G or 5G&2G.
Country Code	Configures Wi-Fi country code.
ESSID	This parameter sets the ESSID for the Wireless network. Press "Scan" to scan for the available wireless network. Click on "Connect" and enter the authentication credentials of the Wi-Fi network to connect to. Users can connect to hidden networks by pressing on "Add Network" and configure: • **ESSID**: Configure the hidden ESSID name. • **Security Mode**: Defines the security mode used for the wireless network when the SSID is hidden. Default is "None". • **Password**: Determines the password for the selected Wi-Fi network. • **Advanced**: Configures IPv4 and IPv6 modes.
Network Settings → OpenVPN® Settings	
OpenVPN® Enable	Enables/Disables OpenVPN® feature. Default is "No".
OpenVPN® Server Address	Specify the IP address or FQDN for the OpenVPN® Server.
OpenVPN® Port	Specify the listening port of the OpenVPN® server. The valid range is 1 – 65535. The default value is "1194".

OpenVPN® Transport	Specify the Transport Type of OpenVPN® whether UDP or TCP. The default value is "UDP".
OpenVPN® CA	Click on "Upload" to upload the Certification Authority of OpenVPN®. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN® Certificate	Click on "Upload" to upload OpenVPN® certificate. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN® Client Key	Click on "Upload" to upload OpenVPN® Key. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN® Cipher Method	Specifies the Cipher method used by the OpenVPN® server. The available options are: **Blowfish** **AES-128** **AES-256** **Triple-DES** The default setting is "Blowfish".
OpenVPN® Username	Configures the optional username for authentication if the OpenVPN server supports it.
OpenVPN® Password	Configures the optional password for authentication if the OpenVPN server supports it.
Additional Options	Additional options to be appended to the OpenVPN® config file, separated by semicolons. For example, comp-lzo no;auth SHA256 **Note**: Please use this option with caution. Make sure that the options are recognizable by OpenVPN® and do not unnecessarily override the other configurations above.
Network Settings → Advanced Settings	
Advanced Network Settings	
Enable LLDP	Controls the LLDP (Link Layer Discovery Protocol) service. The default setting is "Enabled".
LLDP TX Interval	Defines LLDP TX Interval (in seconds). Valid range is 1 to 3600. The default setting is "60".

Enable CDP	Enables/Disables CDP "Cisco Discovery Protocol". The default setting is "Enabled".
Layer 3 QoS for SIP	Defines the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 26.
Layer 3 QoS for RTP	Defines the Layer 3 QoS parameter for RTP. This value is used for IP Precedence, Diff-Serv or MPLS. The default value is 46.
Enable DHCP VLAN	Enables auto configure for VLAN settings through DHCP. Disabled by default.
Enable Manual VLAN Configuration	Enables/disables manual VLAN configuration. When this option is set to Disabled, the phone will bypass VLAN configuration and only use the DHCP VLAN to configure VLAN tag and priority. Default is "Enabled".
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets. The valid range is 0 – 4094.The default value is 0.
Layer 2 QoS 802.1p Priority Value	Assigns the priority value of the Layer2 QoS packets. The valid range is 0 – 7. The default value is 0.
Maximum Transmission Unit (MTU)	Defines the MTU in bytes. The valid range is 576 – 1500. The default value is 1500 bytes.
PC Port Mode	
PC Port Mode	Configure the PC port mode. When set to "Mirrored", the traffic in the LAN port will go through PC port as well and packets can be captured by connecting a PC to the PC port. The default setting is "Enabled".
PC Port VLAN Tag	Assigns the VLAN Tag of the PC port. The valid range is 0 – 4094. The default value is 0.
PC Port Priority Value	Assigns the priority value of the PC port. The valid range is 0 – 7. The default value is 0.
Proxy	
HTTP Proxy	Specifies the HTTP proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Remote Control	

Action URI Support	Indicate whether the phone is enabled to receive and handle Action URI request.
Remote Control Pop up Window Support	Indicate whether the phone is enabled to pop up Allow Remote Control window.
Action URI Allowed IP List	List of allowed IP addresses from which the phone receives the Action URI
CSTA Control	Indicates whether CSTA Control feature is enabled. Change of this configuration will need the system reboot to make it take effect.
CTI Settings	
Affinity Support	Indicate whether Affinity feature is supported.
Preferred Account	Affinity target SIP account.
Network Settings → SNMP Settings	
Enable SNMP	Enable/Disable SNMP service. Default is No.
Version	Choose between (Version 1, Version 2, or Version 3).
Port	Listening Port of SNMP daemon (Default 161).
Community	Name of SNMP community.
Security Level	**noAuthUser**: Users with security level noAuthnoPriv and context name as noAuth. **AuthUser**: Users with security level authNoPriv and context name as auth. **privUser** : Users with security level authPriv and context name as priv.
SNMP Username	Username for SNMPv3.
Authentication Protocol	Select the Authentication Protocol: "None" or "MD5" or "SHA."
Privacy Protocol	Select the Privacy Protocol: "None" or "AES" or "DES".
Authentication Key	Enter the Authentication Key for SNMPv3.
Privacy Key	Enter the Privacy Key for SNMPv3.
SNMP Trap Version	Choose the Trap version of the SNMP trap receiver.
SNMP Trap IP	IP address of trap destination.
SNMP Trap port	Port of Trap destination (Default 162)
SNMP Trap Interval	Time interval between traps (Default is 5).
SNMP Trap Community	Community string associated to the trap. It must match the community string of the trap receiver.

SNMP Trap Username	Username for SNMPv3 Trap.
Trap Security Level	**noAuthUser:** Users with security level noAuthnoPriv and context name as noAuth. **authUser:** Users with security level authNoPriv and context name as auth. **privUser:** Users with security level authPriv and context name as priv.
Trap Authentication Protocol	Select the Authentication Protocol: "None" or "MD5" or "SHA".
Trap Privacy Protocol	Select the Privacy Protocol: "None" or "AES/AES128" or "DES".
Trap Authentication Key	Enter the Trap Authentication Key.
Trap Privacy Key	Enter the Trap Privacy Key.

Programmable keys Page Definitions

Table 12: 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 in the Value field to be dialed during the call. "Enable MPK Sending DTMF" has to be set to "Yes" first.

- **Voice Mail**

  Select Account and enter Voice Mail 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.

- **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.

- **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 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.
Account	Select the account to be associated with the configured MPK.
Value	Enter the value to be associated with the configured MPK
Label	Enter the name to be associated with the MPK.
Preview	Shows a preview of the configured MPKs label. After saving, you can print the card style in the preview. For more info about how to install the BLF paper label check the **Quick Installation guide**.
Basic Settings	
Transfer Mode via MPK	Perform blind transfer, attended transfer, or a new call with the specific in the Value field when a user presses "Transfer" multiple-purpose key
Enable Transfer via Non-Transfer MPK	MPK with type BLF, Speed dial, etc, will perform as transfer MPK under active call
Programmable Keys → Idle screen softkey	
Custom Idle Screen Softkey Layout	Enables/disables custom softkey layout. Default is disabled.
Custom Softkey	Press on **Add Custom Softkey** radio button to add/configure up to 3 custom softkeys. Supported key modes are speed dial , speed dial via active account and voicemail.
Custom Softkey Layout	The softkeys listed under "Enabled" tab will be displayed on the phone's idle screen. Select the softkey from "Available" list to enable it.
Programmable Keys → Call screen softkeys	
Custom Call Screen Softkey Layout	Enables/disables custom softkey layout. Default is disabled.
Enforce Softkey Layout Position	Whether to enforce the custom softkey layout position. When set to 'YES', GUI will still preserve the space if the configured softkey is unable to show. Default is disabled.
Custom Softkey	Press on **Add Custom Softkey** radio button to add/configure up to 3 custom softkeys. Supported key modes are speed dial , speed dial via active account

	and voicemail.
	• **Dialing State** Custom softkey layout when device is under DIALING state. **Available softkeys:** EndCall, Backspace, Contacts, Call History. • **Ringing State** Custom softkey layout when device is under RINGING state. **Available softkeys:** Answer, Reject, Forward, Ring silence. • **Calling State** Custom softkey layout when device is under CALLING state. **Available softkeys: End Call, Conference.** • **Call Connected State** Custom softkey layout when device is under CALL CONNECTED state. **Available softkeys:** End Call, Conference , New Call, Swap , Transfer , call park, Call record, Noise shield, BS Call Center. • **On Hold State** Custom softkey layout when device is under ON HOLD state. **Available softkeys: End Call , Resume , New Call, Conference , Swap , Transfer, BS call center.** • **Call Failed State** Custom softkey layout when device is under CALL FAILED state. **Available softkeys:** EndCalls, Redial. • **Transfer State** Custom softkey layout when device is under TRANSFER state. **Available softkeys:** Cancel, Backspace, Transfer , Contacts, Call History. • **Conference State** Custom softkey layout when device is under CONFERENCE state. **Available softkeys:** Cancel, Dial , Backspace, Contacts , Call History. • **Conference Connected State** Custom softkey layout when device is under CONFERENCE CONNECTED state. **Available softkeys:** EndCall, Conference Info , Hold , Add , Noise Shield.
Custom Softkey Layout	

	• **Onhook Dialing State** Custom softkey layout when device is under ONHOOK DIALING state **Available softkeys:** End Call , Back Space , Dial , Contacts , Call History. The softkeys listed under "Enabled" tab will be displayed on the phone's idle screen. Select the softkey from "Available" list to enable it.

System Settings Page Definitions

Table 13: 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.
NTP Update Interval	Time interval for updating time from the NTP server. Valid time value is in between 5 to 1440 minutes. The default setting is "1440" minutes.
Allow DHCP Option 42 Override NTP Server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is "No".
Time Zone	Configures the date/time used on the phone according to the specified time zone. The default setting is "Auto".
Allow DHCP Option 2 to Override Time Zone Setting	Allows device to get provisioned for Time Zone from DHCP Option 2 in the local server. The default setting is enabled.
Self-Defined Time Zone	This parameter allows the users to define their own time zone, when "Time Zone" parameter is set to "Self-Defined Time Zone". The syntax is: **std offset dst [offset], start [/time], end [/time]** Default is set to: **MTZ+6MDT+5,M4.1.0,M11.1.0** **MTZ+6MDT+5** This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is

west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east.

M4.1.0,M11.1.0

The 1st number indicates Month: 1,2,3.., 12 (for Jan, Feb, .., Dec)

The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…)

The 3rd number indicates weekday: 0,1,2,..,6(for Sun, Mon, Tues, … ,Sat)

Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.

Date Display Format	Configures the date display format on the LCD. The following formats are supported. • **yyyy-mm-dd**: 2019-03-02 • **mm-dd-yyyy**: 03-02-2019 • **dd-mm-yyyy**: 02-03-2019 • **dddd, MMMM dd**: Saturday, March 02 • **MMMM dd, dddd**: March 02, Saturday The default setting is yyyy-mm-dd.
Time Display Format	Configures the time display in 12-hour or 24-hour format on the LCD. The default setting is in 12-hour format.
Language	
Display Language	Selects display language on the phone.
System Settings → Security Settings	
SSH Access	
Enable SSH	Disables SSH access. The default setting is "Yes"
SSH Public Key	Enable the device to use public key authentication as an alternative option to password authentication.
Keypad Mode	
Configuration via Keypad Menu	Configures access control for keypad Menu settings. • **Unrestricted:** all options on LCD menu can be accessed; • **Basic settings only**: only options for basic setting can be displayed on LCD menu; • **Constraint Mode:** accessing options other than basic settings will require permission; • **Locked Mode:** MENU is disabled

Web Access	
HTTP Web Port	Configures the HTTP port under the HTTP web access mode. The valid range is 80 – 65535. The default value is "80".
HTTPS Web Port	Configures the HTTPS port under the HTTPS web access mode. The valid range is 443 – 65535. The default setting is "443".
Web Access Mode	Sets the protocol for web interface. • **HTTPS** • **HTTP** • **Disabled** • **Both HTTP and HTTPS** The default setting is "HTTP".
Web Access Control	Web access control by using Whitelist or Blacklist on incoming IP addresses
Web Access Control List	Only allow the IP address list as a whitelist or restrict the IP address list as a blacklist to access the Web.
Web Session Timeout	Configures timer to logout web session during idle. The valid range is 2-60 min. The default value is 10 min
Enable User Web Access	Administrator can disable or enable user web access. The default setting is "Enabled".
Validate Server Certificates	After enabling this feature, phone will validate the server's certificate. If the server that our phone tries to register on is not on our list, it will not allow server to access the phone.
Web/Restrict mode Lockout Duration	Specifies the time in minutes that the web or LCD login interface will be locked out to user after five login failures. This lockout time is used for web login, and LCD restrict mode admin login. Range is 0-60 minutes. The default setting is "5".
Web/Restrict Mode lockout Attempt Limit	Configure attempt limit before lockout. Default is 5. Range is 1-10.
User Info Management	
User Password	
New Password	Set new password for web GUI access as User. This field is case sensitive.
Confirm Password	Enter the new User password again to confirm.
Admin Password	
Current Password	The current admin password is required for setting a new admin password.

New Password	Set new password for web GUI access as Admin. This field is case sensitive.
Confirm Password	Enter the new Admin password again to confirm.
Client certificate	
SIP TLS Certificate	SSL Certificate used for SIP Transport in TLS/TCP.
SIP TLS Private Key	SSL Private key used for SIP Transport in TLS/TCP.
SIP TLS Private Key Password	SSL Private key password used for SIP Transport in TLS/TCP.
Custom Certificate	The uploaded custom certificate will be used for SSL/TLS communication instead of the phone default certificate.
Trusted CA Certificate	
Trusted CA Certificates (1 – 6)	Allows to upload and delete the CA Certificate file to phone. **Note:** Users can either upload the file directly from web or they can choose to provision it from their cfg.xml file.
Load CA Certificates	Phone will verify the server certificate based on the built-in, custom or both trusted certificates list. The default setting is "Default Certificates".
Keypad Lock	
Enable Keypad Locking	If set to "Yes", the keypad can be locked by pressing and holding the STAR * key for about 4 seconds. And will also allow automatic locking.
Keypad Lock Type	If set to "Functional Keys", only "Functional Keys" will be locked but you are still allowed to make emergency calls. If set to "All Keys", all keys will be locked, and no emergency calls can be made.
Password to Lock/Unlock	Configures the password to lock/unlock the keypad.
Keypad Lock Timer	Configures the timeout (in seconds) of idle screen for locking keypad. Valid range is 0 to 3600.
Emergency	Defines emergency call numbers. If multiple emergency call numbers are entered, they should be separated by ','.
System Settings → Preferences	
Display Control	
New Message LED Indicator	Configure the LED indicator mode when there is new voicemail or text message on the phone. If set to "Off", LED indicator will not light up.
Audio Control	

Headset	

Headset Key Mode	When headset is connected to the phone, users could use the HEADSET button in "Default Mode" or "Toggle Headset/Speaker".
	
	• **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.

Headset Type	Selects whether the connected headset is normal RJ11 headset, Plantronics EHS, Jabra EHS, Sennheiser EHS headset.
Always Ring Speaker	Configures to enable or disable the speaker to ring when headset is used on "Toggle Headset/Speaker" mode. If set to "Yes", when the phone is in Headset "Toggle Headset/Speaker" mode, both headset and speaker will ring on incoming call. The default setting is "No".
Headset TX Gain (dB)	Configures the transmission gain of the headset. The default value is -6dB.
Headset RX Gain (dB)	Configures the receiving gain of the headset. The default value is -6dB.

Enable Headset Noise Shield	When enabled, the remote party will not hear the environmental noise during a call using the headset. Choose according to the TX loudness of the earphone. When the TX loudness of the headset is loud, please select the "Loud Headset", and when the TX loudness of the headset is soft, please select the "Thin Headset". "Moderate Headset" is selected by default.
Handset	
Handset TX Gain (dB)	Configures the transmission gain of the handset.
Enable EDRC Feature	Enable EDRC feature, the remote party will not hear the environmental noise during a call
Upload Audio Parameter Mode	Developer function to upload audio parameters for different audio modes.
Upload Audio Parameter Volume	Developer function to upload audio parameters for each audio volumes
System Settings → TR-069	
Enable TR-069	Enables TR-069
ACS URL	URL for TR-069 Auto Configuration Servers (ACS). Default setting is: https://acs.gdms.cloud
TR-069 Username	ACS username for TR-069.
TR-069 Password	ACS password for TR-069.
Periodic Inform Enable	Enables periodic inform. If set to "Yes", device will send inform packets to the ACS. The default setting is "No".
Periodic Inform Interval	Sets up the periodic inform interval to send the inform packets to the ACS. Default is 86400.
Connection Request Username	The username for the ACS to connect to the phone.
Connection Request Password	The password for the ACS to connect to the phone.
Connection Request Port	The port for the ACS to connect to the phone.
CPE SSL Certificate	The Cert File for the phone to connect to the ACS via SSL.
CPE SSL Private Key	The Cert Key for the phone to connect to the ACS via SSL.
Start TR-069 at Random Time	When enabled, TR-069 will send out first INFORM message to server on randomized timing between 1 to 3600 seconds after phone boots up.

Maintenance Page Definitions

Maintenance → Upgrade and Provisioning	
Firmware	
Upgrade via Manually Upload	
Upload Firmware File to Update	Upload and start upgrade firmware.
Upgrade via Network	
Firmware Upgrade via	Allows users to choose the firmware upgrade method via TFTP, HTTP or HTTPS.
Firmware Server Path	Defines the server path for the firmware server.
Firmware Server Username	The username for the firmware server.
Firmware Server Password	The password for the firmware server.
Firmware File Prefix	If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone.
Firmware file Postfix	If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.
Upgrade Detection	
Upgrade	Press to start upgrade process.
Config File	
Configure Manually	
Download Device Configuration	Click to download phone's configuration file in .txt format. **Note:** Configuration file does not include passwords or CA/Custom certificate
Download Device Configuration (XML)	Click to download phone's configuration file in .xml format. **Note:** Configuration file does not include passwords or CA/Custom certificate
Download User configuration	This allows users to download part of the configuration that does not include any personal settings like Username and Passwords. Also, it will include all the changes manually made by user from web UI, or config file uploaded from "Upload Device Configuration", but not include the changes from the server provision via TFTP/FTP/FTPS/HTTP/HTTPS.

Upload Device Configuration	Uploads configuration file to phone.
Export backup Package	Export backup package which contains device configuration along with personal data.
Restore from Backup package	Click to upload backup package and restore.
Configure via Network	
Config Upgrade Via	Allows users to choose the config upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is "HTTPS".
Config Server Path	Defines the server path for provisioning.
Config Server Username	The username for the HTTP/HTTPS server.
Config Server Password	The password for the HTTP/HTTPS server.
Always Authenticate Before Challenge	Only applies to HTTP/HTTPS. If enabled, the phone will send credentials before being challenged by the server.
Config File Prefix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
Config File Postfix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Authenticate Conf File	Authenticates configuration file before acceptance.
XML Config File Password	The password for encrypting XML configuration file using OpenSSL. This is required for the phone to decrypt the encrypted XML configuration file.
Provision	
Auto Upgrade	
Automatic Upgrade	Enables automatic upgrade and provisioning. The default setting is "No".
Automatic Upgrade Check Interval (m)	Specifies the time period to check for firmware upgrade (in minutes). The default value is 10080.
Hour of the Day(0-23)	Defines the hour of the day to check the HTTP/TFTP/FTP server for firmware

	Upgrade or configuration files changes. The default value is 1.
Day of the Week(0-6)	Defines the day of the week to check HTTP/TFTP/FTP server for firmware Upgrade or configuration files changes. The default value is 1.
Randomized Automatic Upgrade	Randomized Automatic Upgrade within the range of hours of the day or Post pone the upgrade every X minute(s) by random 1 to X minute(s). The default setting is "No"
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent: Always Check for New Firmware, Check New Firmware only when F/W pre/suffix Changes, Always Skip the Firmware Check. The default setting is "Always Check for New Firmware".
Firmware Upgrade Confirmation	If set to "Yes", the phone will ask the user to upgrade. If there is no response, The phone will proceed with the upgrade. If set to "No", the phone will automatically upgrade without user input. Default is Yes.
DHCP Option	
Allow DHCP Option 43 and Option 66 Override Server	DHCP option 66 originally was only designed for TFTP server. Later, it was extended to support an HTTP URL. GRP phones support both TFTP and HTTP server via option 66. Users can also use DHCP option 43 vendor specific option to do this. DHCP option 43 approach has priorities. The phone is allowed to fall back to the original server path configured in case the server from option 66 fails. The default setting is "Yes".
Allow DHCP Option 120 to override SIP Server	Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is "No"
Additional Override DHCP Option	When enabled, users could select Option 150 or Option 160 to override the Firmware server instead of using the configured firmware server path or the server from option 43 and option 66 in the local network. Please note this option will be effective only when option "Allow DHCP Option 43 and Option 66 to Override Server" is enabled. The default setting is "None".
Config Provision	
Download and Process ALL Available Config Files	By default, device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, cfg.xml and devMAC.cfg (corresponding to device specific, model specific, and global configs). If set

	to Yes, device will download and apply (overwrite) all available configs in the same order.
User Protection	When user protection is on, pvalues that user sets will not be changed by provision or provider.
3CX Auto Provision	Phone will multicast SUBSCRIBE for provision if this feature is enabled.
Advanced Settings	
Validate Hostname in Certificate	To validate the hostname in the SSL certificate
Enable SIP Notify Authentication	Device will challenge NOTIFY with 401 when set to Yes
Factory reset	Press Start to begin Factory Reset of the phone.
Maintenance → System Diagnosis	
Syslog	
Syslog Protocol	If set to SSL/TLS, the syslog messages will be sent through secured TLS protocol to syslog server. Default setting is "UDP". **Note**: The CA certificate is required to connect with the TLS server.
Syslog Server	The URL or IP address of the syslog server for the phone to send syslog to. **Note**: By adding port number to the Syslog server field (i.e., 172.18.1.1:1000), the phone will send syslog to the corresponding port of that IP.
Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels: DEBUG, INFO, WARNING and ERROR. Syslog messages are sent based on the following events: • 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 Keyword Filter	Syslog will be filtered based on keywords provided. If you enter multiple keywords, it should be separated by ','. Please note that no spaces are allowed.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages. The default setting is "No". **Note:** By setting Send SIP Log to Yes, the phone will still send SIP log from syslog even when Syslog Level set to NONE.
Packet Capture	
With RTP Packets	Defines whether the packet capture file contains RTP or not. The default setting is "No".
Ping	
Ping	Enter Ping target's IP address or URL and click on start.
Traceroute	
Traceroute	Input target's IP address or URL and click on start
Maintenance → Outbound Notification	
Action URL	
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.
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.
Terminated Call	Configures the Action URL to send when phone terminates a call.
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.
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.
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.
Destination	
Destination Name	Identify the destination name. It must be unique.
Protocol	Configure the protocol associated with the destination server. Currently XMPP and SMTP are supported.
Enable SSL	Configure whether to use SSL to encrypt for SMTP protocol. This option is not editable for XMPP.
Destination Address	Configure destination server address, e.g., talk.google.com.
Port	Configure destination server port, e.g., 5222.
Domain	Configure the destination server domain for XMPP protocol. This option is not editable for SMTP.
Username	Configure the authorization username of the destination server.
Password	Configure the authorization user password for the destination server.
From	Configure the sender name for SMTP protocol. This option is not editable for XMPP.
To	Configure the receiver's address.
Extra Attribute Name	Configure extra attribute's name reserved for protocol specific attributes such as "jid" for XMPP protocol. If "jid" is specified, username and domain will be overridden.
Extra Attribute Value	Configure extra attribute's value reserved for protocol specific attributes such as "abc@gmail.com" for "jid" of XMPP protocol. If it is specified, username and domain will be overridden.
Destination	
Event	Configures the event, which will trigger an outbound notification.
Destination	Configures the name of the destination where the outbound notification will be sent to.
Subject	Configures the subject of Email notification. This option is only applicable to SMTP protocol and it is not editable for other protocols.
Message	Configures the message body or the outbound notification.
Extra Attribute Name	Configure extra attribute's name reserved for specific attributes for a given notification in the future.

Extra Attribute Value	Configures extra attribute's value reserved for specific attributes for a given notification in the future.
Maintenance → Voice Monitoring	
Session Report	
VQ RTCP-XR Session Report	When enabled, phone will send a session quality report to the central report collector at the end of each call.
Interval Report	
VQ RTCP-XR Interval Report	When enabled, phone will send an interval quality report to the central report collector periodically throughout a call.
VQ RTCP-XR Interval Report Period	Configure the interval (in seconds) of phone sending an interval quality report to the central report collector periodically throughout a call.
Alert Report	
Warning Threshold for Moslq	Configure the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector.
Critical Threshold for Moslq	Configure the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector.
Warning Threshold for Delay	Configure the threshold value of one way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector.
Critical Threshold for Delay	Configure the threshold value of one way delay (in milliseconds) that causes the phone to send a critical alert quality report to the central report collector.

Application Page Definitions

Table 15: Application Page Definitions

Application → Web Service	
Use Auto Location Service	To enable or disable auto location services on the phone. (Reboot Required)
Application → Contacts	
Contacts	
Add Contact	Press Add to create a new contact.
Edit	Edits the contact parameters.
Delete All Contacts	Press to delete all contacts.

Group Management	
Add Group	Specifies Group's name to add new group. More than 30 Groups supported.
Edit Group	Edits selected group.
Delete Group	Delete Selected group
Phonebook Management	
Enable Phonebook XML Download	Configures to enable phonebook XML download. Users could select HTTP/HTTPS/TFTP to download the phonebook file. The default setting is "Disabled".
HTTP/HTTPS Username	The username for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.
Phonebook XML Server Path	Configures the server path to download the phonebook XML. This field could be IP address or URL, with up to 256 characters.
Phonebook Download Interval	Configures the phonebook download interval (in minutes). If set to 0, automatic download will be disabled. The default value is 0. Valid range is 5 to 720 minutes.
Remove Manually-edited Entries on Download	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed. The default setting is "Yes".
Import Group Method	• When set to "**Replace**", existing groups will be completely replaced by imported one. • When set to "**Append**", the imported groups will be attended with the current one. The default setting is "Replace".
Sort Phonebook by	Sort phonebook based on the selection of first name or last name. The default setting is "Last Name".
Download XML Phonebook	Click on "Download" to download the XML phonebook file to local PC
Upload XML Phonebook	Click on "Upload" to upload local XML phonebook file to the phone.
Default Search Mode	Configure the default phone book search mode.
Application → LDAP	

LDAP Protocol	Configures the LDAP protocol to LDAP or LDAPS. The default setting is "LDAP". LDAPS is a feature to support LDAP over TLS.
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=com ou=Boston, dc=grandstream, dc=com
Username	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	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 which has the "telephoneNumber" or "Mobile" field starting with the entered prefix; (&(telephoneNumber=%) (cn=*)) returns all the records with the "telephoneNumber" field starting with the entered prefix and "cn" field set.
LDAP Name Filter	Configures the filter used for name lookups. Examples: (|(cn=%)(sn=%)) returns all records which has the "cn" or "sn" field starting with the entered prefix; (!(sn=%)) returns all the records which do not have the "sn" field starting with the entered prefix; (&(cn=%) (telephoneNumber=*)) returns all the records with the "cn" field starting with the entered prefix and "telephoneNumber" field set.
LDAP Version	Selects the protocol version for the phone to send the bind requests. The default setting is "Version 3".
LDAP Name Attributes	Specifies the "name" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes. Example: gn cn sn description

LDAP Number Attributes	Specifies the "number" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated number attributes. <u>Example:</u> telephoneNumber telephoneNumber Mobile
LDAP Display Name	Configures the entry information to be shown on phone's LCD. Up to 3 fields can be displayed. <u>Example:</u> %cn %sn %telephoneNumber
Max. Hits	Specifies the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. The default setting is 50.
Search Timeout	Specifies the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 30 seconds.
Sort Results	Specifies whether the searching result is sorted or not. Default setting is "No".
LDAP Lookup	Configures to enable LDAP number searching when dialing / receiving calls.
Lookup Display Name	Configures the display name when LDAP looks up the name for incoming call or outgoing call. This field must be a subset of the LDAP Name Attributes. <u>Example:</u> gn cn sn description
LDAP Dialing Default Account	Configures the default account used when dialing LDAP contact
Exact Match Search	Search for exact match result. Default setting is "No".
Application → Call History	
Delete	Users can select an entry, then click "Delete" to remove it from the list.
Delete All	Click on Delete All to remove all Call History stored in the phone. Note: Users could use the drop-down list to show only selected call history type (All, Answered, Dialed, Missed, and Transferred) and use navigation keys to browse pages when many entries exist.

External Service Page Definitions

Table 16: External Service Page Definitions

External Service → GDS	

GDS	Connect to a GDS37XX and send OpenDoor request.
	• **Service Type**
	  Select GDS as service type.
	• **Account**
	  The account to be used on the phone to interact with the GDS37XX.
	• **System Identification**
	  A name or a number to identify the GDS37XX.
	• **System Number**
	  The SIP extension or the IP address of the GDS37XX depending on the deployed scenario, Peering or Registration.
	• **Access Password**
	  The password set on the GDS37XX to unlock the door.
	• **System Ringtone**
	  Select the system ringtone from the dropdown list to be played when there is an incoming call from the configured system number of the GDS37xx.
	Notes:
	- When using Peering scenario, on "System Number" field of the GRP260x specify the IP address of the peered GDS37XX.
	- When using Registration scenario and both GRP260x and GDS37XX are registered on the same SIP server, specify the SIP extension of the GDS37XX on "System Number" field on GXP16XX. The "Access Password" on GRP260x should be matching "Remote PIN to Open the door" on GDS37XX.

External Service → Call Center	
Call Center Codes	Set the disposition code and the unavailable code for quick selection on the phone side
Wrap-up Countdown	Configure the countdown times when the agent status is Wrap-up and execute the countdown on the LCD. If set to 0, the countdown is disabled
External Service → Broadsoft XSI	
Authentication Login	

Server	Broadsoft XSI server address with protocol.
Port	Port of the Broadsoft XSI server.
XSI Action Path	Configure the deployment path for Broadsoft XSI Actions. If it is empty, the path "com.broadsoft.xsi-actions" will be used.
XSI Authentication Type	Defines the authentication type to use login credentials or SIP credentials. If set to "Login Credentials", please fill in User ID and Password in the following options; If set to "SIP Credentials", please fill in user ID, Authentication ID, and Authentication Password.
BroadWorks User ID	SIP User ID for Broadsoft XSI server.
SIP Authentication ID	SIP Username for Broadsoft XSI server.
SIP Authentication Password	SIP Password for Broadsoft XSI server.
Auto Login	If set to "Yes", 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.
Service Settings	
Sort Phonebook by	Sort phonebook based on the selection of first name or last name.
BroadSoft Directory Update Interval (m)	Configures the BroadSoft phonebook download interval (in minutes). If set to 0, automatic download will be disabled. Valid range is 5 to 4320.
Broadsoft Contacts Download Limitation	The maximum contacts that can be downloaded for each BroadSoft XSI server directory. The valid range is from 0 to 2000. If set to 0, the server's default contact limit will be used. If the total contact records returned by the server is larger than this limit then it will not be downloaded, and the device will be limited to remote search.
BroadSoft Contacts Search limitation	The maximum remote search records that can be downloaded for the BroadSoft XSI server directory. The valid range is from 0 to 2000. If set to 0, there is no limit. If the search result total records exceed this value, it will not be downloaded, and you will need to narrow the search scope.
Network Directories	
Type	Enable/Disable Broadsoft Network directories. The directory types are: • **Group Directory** Enable/Disable and rename the BroadWorks 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 BroadWorks 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 BroadWorks 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 BroadWorks 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 BroadWorks 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 BroadWorks 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 BroadWorks 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 BroadWorks 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.

NAT SETTINGS

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

- **STUN Server**

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

- **Use Random Ports**

  It is under **Settings→General Settings**. This setting depends on your network settings. When set to "Yes", it will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple 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**. Default setting is "No". Enable the device to use NAT traversal when it is behind firewall on a private network. Select Keep-Alive, Auto, STUN (with STUN server path configured too) or other option according to the network setting.

PACKET CAPTURE

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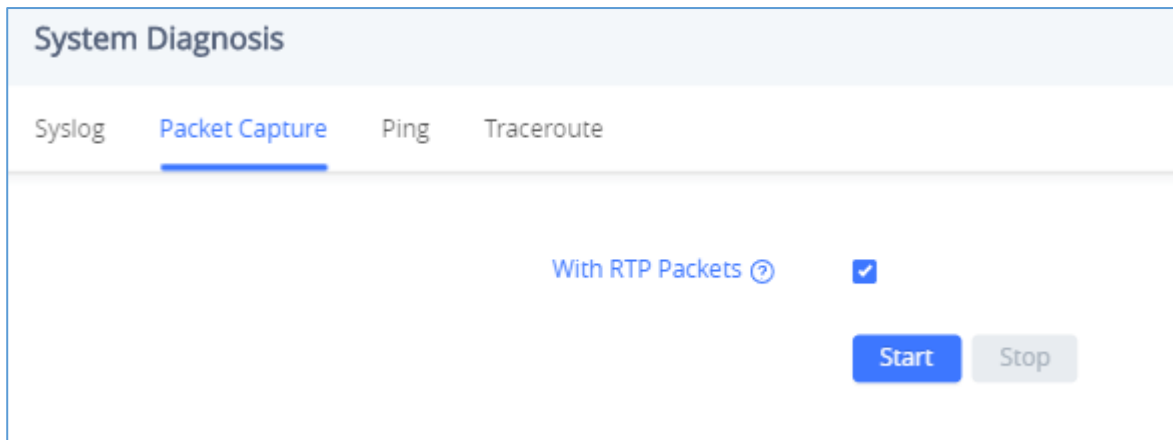

Figure 6: Packet Capture in Idle

User can also define whether RTP packets will be captured or not from **With RTP Packets** option.

When the capture configuration is set, press **Start** button to start packet capture. The Status will become RUNNING while capturing, as showed in *Figure 7: Packet Capture when running*. Press **Stop** button to end capture.

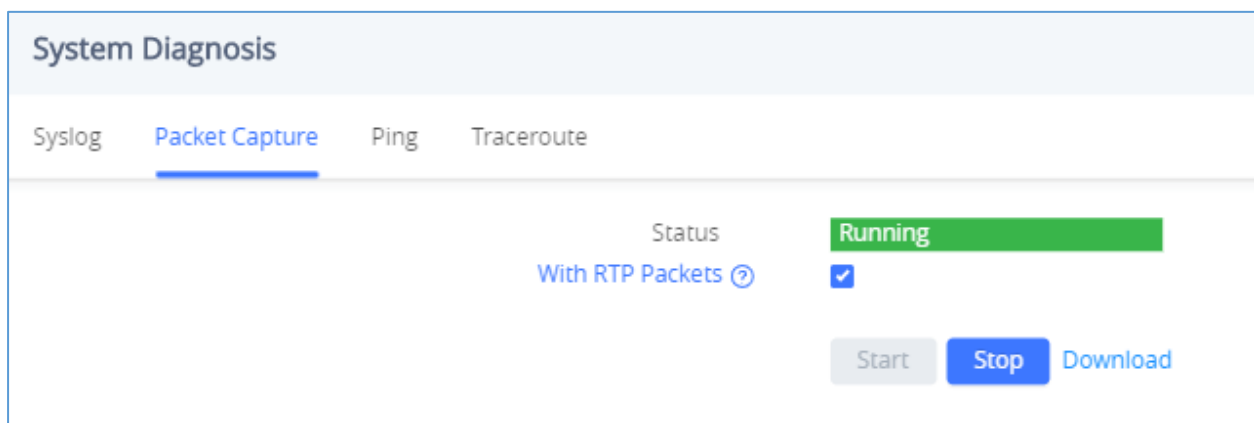Press Download button to download capture file to local PC. The capture file is in .pcap format.

Figure 7: Packet Capture when running

GRP260x Administration Guide
Version 1.0.1.18

UPGRADING AND PROVISIONING

Unified Firmware

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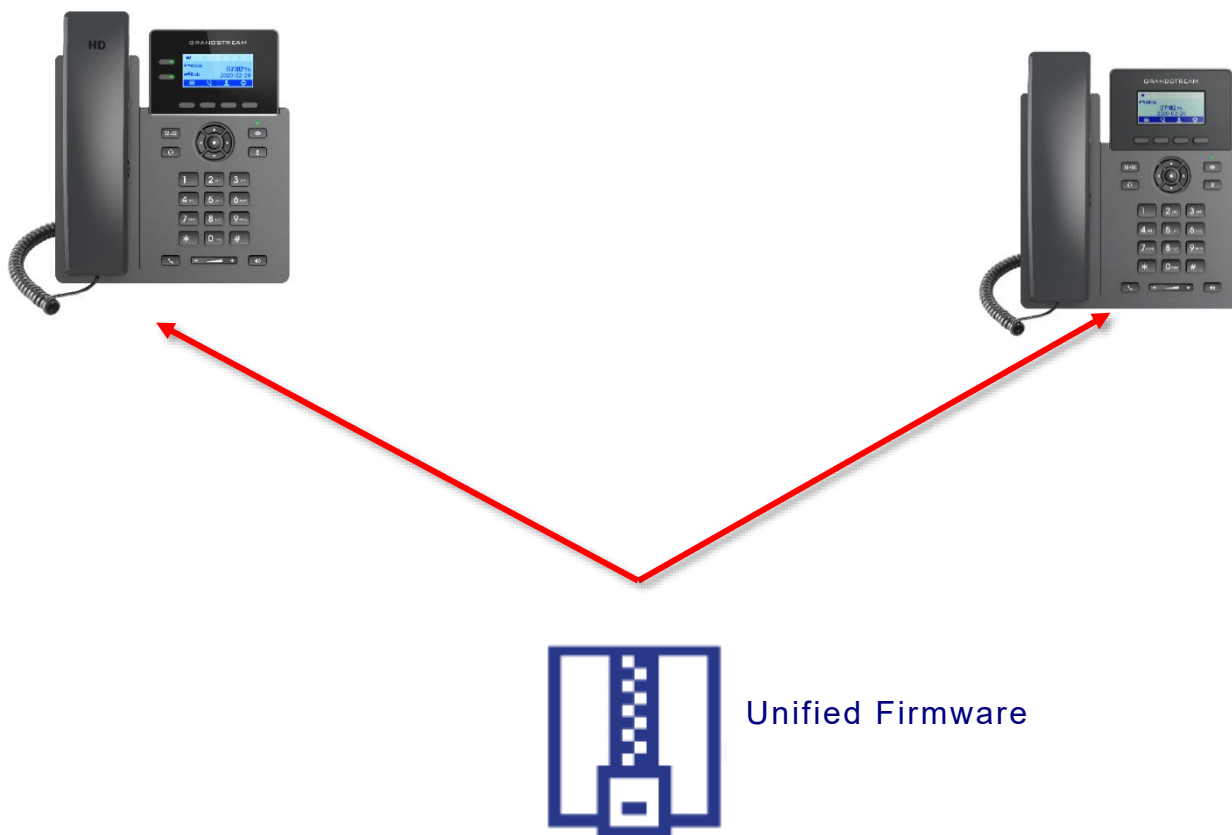

Figure 8: GRP260X Unified Firmware

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.

GRP260x Administration Guide
Version 1.0.1.18

Examples of valid URLs:

firmware.grandstream.com/BETA

fw.mycompany.com

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

Upgrade via Keypad Menu

Follow the steps below to configure the upgrade server path via phone's keypad menu:

1. Press MENU button and navigate using Up/Down arrow to select **Settings**.

2. In the Settings options, select **Advanced Settings and then Upgrade**.

3. Enter the firmware server path and select upgrade method. The server path could be in IP address format or FQDN format.

4. Select **Start Provision** option and press the "Select" Softkey.

5. A warning window will be prompt for provision confirmation. Press "YES" Softkey to start upgrading/provisioning immediately.

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

Upgrade via Web GUI

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

When upgrading starts, the screen will show 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 that would like to use remote upgrading without a local TFTP/FTP/HTTP server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for their phone 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

Microsoft IIS web server.

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 in FQDN or IP address format. The "Config Server Path" can be the same or different from the "Firmware Server Path".

A configuration parameter is associated with each field in the web configuration page. A parameter consists of a Capital letter P and 2 to 5-digit numeric numbers. i.e., P2 is associated with the "New Password" in the Web GUI→**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 "cfgxxxxxxxxxxxx.xml" file is not successful 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, "cfgrp2602" for the GRP2602, "cfgrp2603" for the GRP2603 and "cfgrp2604" 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 lower case 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 provision file, users are able to provision the device with both Pvalues 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
```

Figure 9: Config File Download

Note: (Attempt to download Config File again)

When doing provision on the phone, if your first config file contains p-values listed below, 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 provision 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

GRP260x Administration Guide
Version 1.0.1.18

* 234 -- Config prefix

* 235 -- Config postfix

* 1360 -- Config HTTP/HTTPS username

* 1361 -- Config HTTP/HTTPS password.

Note: Certificates and Keys provisioning

Users can configure the phone to get all the needed certificates during boot up. Instead of putting the certificate/key content in 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 Pvalue 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 into 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)
```

Figure 10: Certificates Files Download

For more details on XML provisioning, please refer to:

http://www.grandstream.com/sites/default/files/Resources/gs_provisioning_guide.pdf

No Touch Provisioning

After the phone sends, 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 user to enter username and password. Once correct username and password are entered, the

GRP260x Administration Guide
Version 1.0.1.18

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

GRP260x Administration Guide
Version 1.0.1.18

RESTORE FACTORY DEFAULT SETTING

⚠️ **Warning:**

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

Restore Factory Settings using LCD menu

Please follow the instructions below to reset the phone:

1. Press 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 provisioning → Advanced Settings → Factory reset.

3. Press on **Start** Button situated against Factory reset option

Click "OK" to confirm and the phone will reboot, or on "Cancel" to cancel the Reset.

EXPERIENCING GRP260X

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

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

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

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