Grandstream Networks, Inc.

WP820

Enterprise Portable Wi-Fi Phone

Administration Guide

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.

FCC warning

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

Changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This equipment has been tested and found to comply with 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 instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

RF Radiation Exposure Statement (SAR)

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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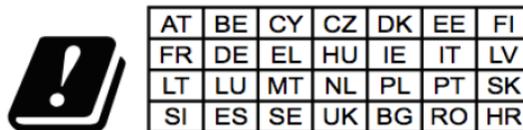
In all EU member states, operation of 5150 - 5350 MHz is restricted to indoor use only.

Hereby, Grandstream Networks, Inc. declares that the radio equipment WP820 is in compliance with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: http://www.grandstream.com/support/resources/

SPECIFICATION

Operating Frequency Band(RF):

BT: 2402-2480MHz(TX&RX)

BLE: 2402-2480MHz(TX&RX)

2.4GHz WIFI: 2412-2472MHz(TX&RX)

5GHz WIFI: 5150-5250MHz,5250-5350MHz,5470-5725MHz(TX&RX)

Max. Of Transmit Power:

BT: 9.55dBm

BLE: 2.45dBm

2.4GHz WIFI:

802.11b:19.78dBm;802.11g:18.12dBm;

802.11n20:18.91dBm;802.11n40:18.39dBm;

5GHz WIFI:

5150-5250MHz:

802.11a:16.93dBm;802.11n20:17.49dBm;802.11n40:16.40dBm

5250-5350MHz:

802.11a:15.69dBm;802.11n20:15.53dBm;802.11n40:15.46dBm

5470-5725MHz:

802.11a:16.42dBm;802.11n20:16.63dBm;802.11n40:15.82dBm

GNU GPL INFORMATION

WP820 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/support/faq/gnu-general-public-license/gnu-gpl-information-download

Table of Contents

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes how to configure WP820 Enterprise Portable Wi-Fi phone features via the LCD menu and Web GUI menu. The intended audiences of this document are VoIP administrators. To learn the basic functions of WP820, please visit http://www.grandstream.com/support to download the latest "WP820 User Guide".

This guide covers following topics:

- Product Overview
- Getting Started
- Web GUI Access Configuration
- Web GUI Settings
- Upgrading and provisioning
- Restore factory default settings.

CHANGE LOG

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

Firmware Version 1.0.1.15

- No major changes.

Firmware Version 1.0.1.12

- This is the initial version for WP820.

GUI INTERFACE EXAMPLES

http://www.grandstream.com/sites/default/files/Resources/WP820_web_gui.zip

1. Screenshot of Login page
2. Screenshots of Status pages
3. Screenshots of Account pages
4. Screenshots of Phone Settings pages
5. Screenshots of System Settings pages
6. Screenshots of Maintenance pages
7. Screenshots of Application pages
8. Screenshots of Value-added Service pages

WELCOME

Thank you for purchasing Grandstream WP820. This powerful Enterprise Portable Wi-Fi Phone features dual-band 802.11a/b/g/n Wi-Fi, supports Wi-Fi roaming, and integrated Bluetooth. The combination of advanced telephony features and durability make it ideal for mobilizing your VoIP network in residences, warehouses, retail stores, hotels and many more environments. Due to a durable design, this sleek phone is drop safe from 1.2 meters, with 150 hours standby time and 7.5 hours talk time making it an ideal addition for homes and businesses alike.

PRODUCT OVERVIEW

Feature Highlights

The following table contain the major features of the WP820:

Table 1: WP820 Features at a Glance

WP820	
	• 2 SIP accounts and 2 lines. • 3-way audio conference calls. • Dual-band 802.11a/b/g/n Wi-Fi. • Wi-Fi roaming and integrated Bluetooth. • 150 hours standby time. • 7.5 hours talk time. • 300m range outdoor / 50m range indoor.

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 Base station WP820.

Table 2: WP820 Technical Specifications

Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, SSH, TFTP, NTP, STUN, SIMPLE, TR-069, 802.1x, TLS, SRTP, IPv6
Voice Codecs and Capabilities	Support for G.711µ/a, G.729A/B, G.722 (wide-band), iLBC, Opus, in-band and out-of-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Graphic Display	2.4-inch (240x320) TFT color LCD
Peripherals	3 soft keys, 3 function keys: Volume up, volume down, Push to Talk key, navigation keys, dial, hang-up, speakerphone, phonebook, backlit keypad, proximity sensor, accelerator, vibration motor
Push-to-Talk	Customizable button for push-to-talk, panic call and other related functions
Bluetooth	Yes, Bluetooth v4.2
Auxiliary Ports	3.5 mm headset jack, Micro-USB port for charging, dual-MIC, dual-color LED.

Telephony Features	Hold, transfer, forward, 3-way audio conference, downloadable phonebook (XML, up to 500 items), call waiting, call log (up to 100 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, push to talk
Security	User and administrator level passwords, MD5 and MD5-sess based authentication, 256-bit AES based secure configuration file, SRTP, TLS, 802.1x media access control
HD Audio	Yes, both on handset and speakerphone with support for wideband audio, HAC supported
QoS	Layer 2 (802.1p), 802.11e and Layer 3 (ToS, DiffServ, MPLS) QoS
Multi-language	English, Arabic, Chinese, Czech, Dutch, German, French, Hebrew, Italian, Japanese, Polish, Portuguese, Russian, Spanish, Turkish and more
Upgrade/ Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS, manual upload, mass provisioning using TR-069 or encrypted XML configuration file, manual upload, USB upgrade
Power & Green Energy Efficiency	Universal power adapter included Input: 100-240VAC; Output: +5VDC, 1A (5W) 1500mA Li-ion battery, 150h standby time and 7.5h talk time
Physical	Handset Dimensions: 168.5 x 52.5 x 21.8mm Charger cradle dimensions : 76 x 73 x 81mm Handset weight: 161g Handset package weight (not including QIG): 456g
Temperature and Humidity	Operating Temperature: 0~45°C; Operating Humidity: 10~90%(non-condensing) Storage Temperature: -20~60°C; Storage Temperature:10~90%(non-condensing
Package Contents	Handset unit, universal power supply, charger cradle, belt clip, 1 Li-ion battery, Quick Installation Guide.
Durability	Drop-safe from 1.2 meters height
Compliance	FCC, CE, RCM

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining best performance with the WP820.

Equipment Packaging

Table 3: Equipment Packaging

WP820
1x Handset unit   1x Universal power supply 5V   1x Charger cradle   1x Belt clip   1x Rechargeable battery   1x Quick Installation Guide   1x GPL Statement
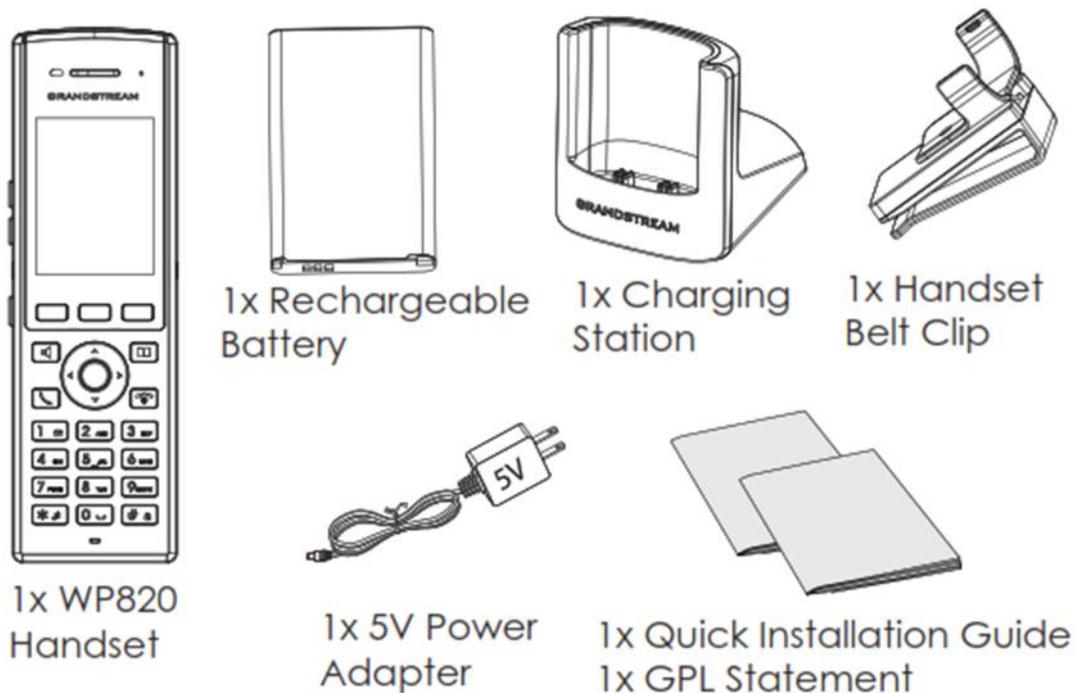
Figure 1: WP820 Package Content

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

Setting up the WP820

Charging Station

Plug the power adapter into a power source socket to start using the charging station.
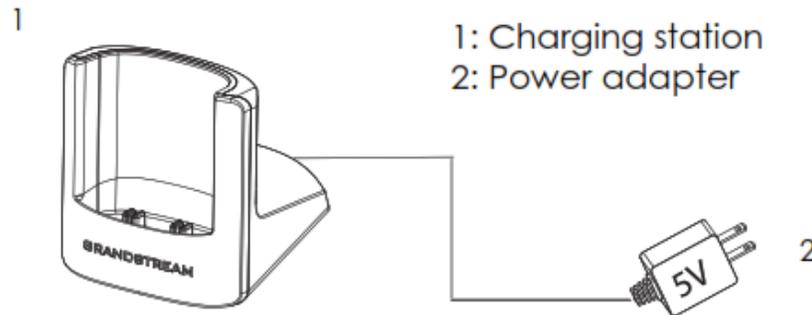
Figure 2: Charging Station

Handset

Please refer to the following steps in order to setup your WP820:
1. Open the battery cover.
2. Insert the battery with the electrodes in the bottom left corner.
3. Close the battery cover.

Note: Please charge the battery fully before using the handset for the first time. (For more information about the battery, please refer to **Battery Information**.
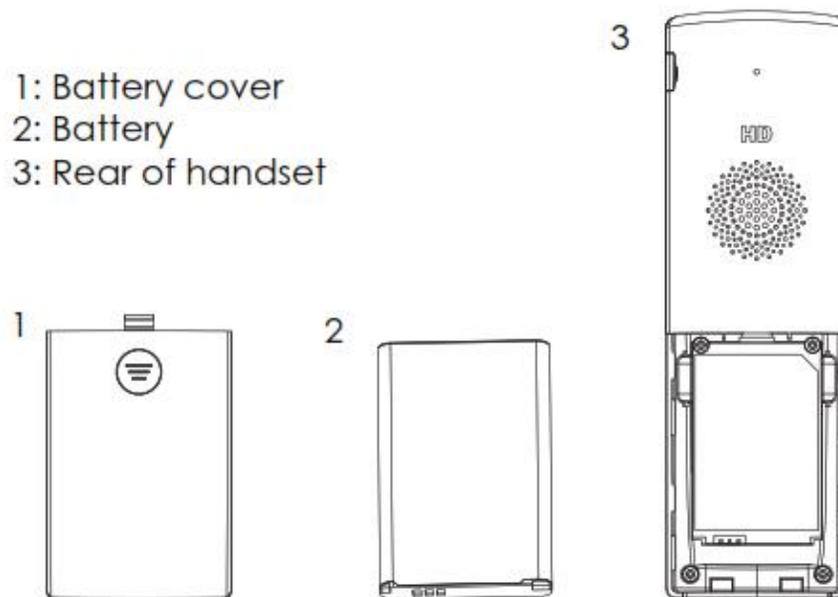
Figure 3: WP820 Handset Setup

Battery Information

- **Technology:** Rechargeable Li-ion Battery

- **Voltage:** 3.8V (Nominal Voltage 3.8V / Limited charge Voltage: 4.35V)

- **Capacity:** 1500mAh

- **Standby time:** up to 150 hours

- **Talk time:** up to 7.5 hours' active talk time

In order to get the best performance of your WP820, we recommend using original battery provided in the package. The specifications may differ depending on the age and capacity of the battery used.

Important Note: Be careful when inserting the battery into your handset to avoid any risk of short-circuit, which lead to damage your battery and/or the handset itself. Do not use damaged batteries which can increase the risk of serious harm.

WP820 Handset Keys Description

The WP820 enhances communication and combines usability and scalability in industries such as warehousing, catering and retail as well as in factory settings. The following screenshot describe the WP820 LCD screen and the main hardware components.
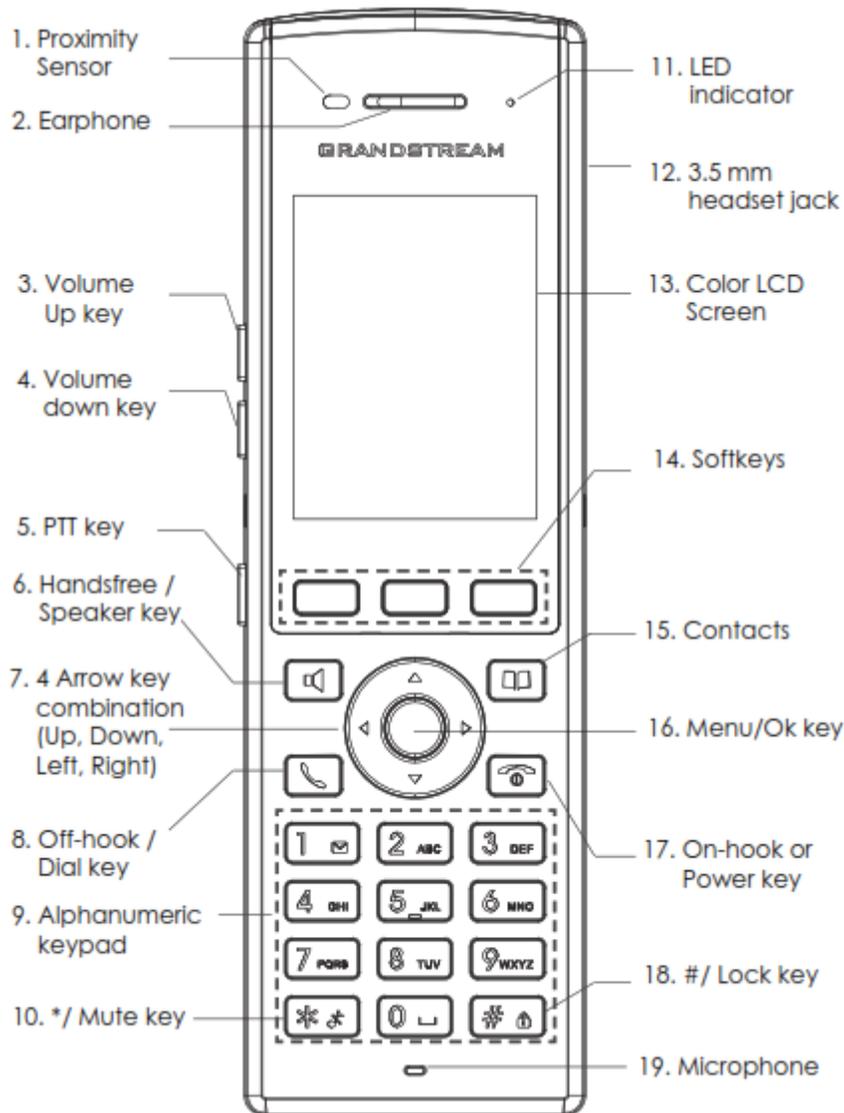
Figure 4: WP820 Description

The following table describe the WP820 keypad keys.

Table 4: WP820 Description

	Key	Description
1.	**Proximity sensor**	The proximity senor can detect and measure gravitational acceleration, tilt, vibration, altitude changes, and static position.
2.	**Earphone**	Delivers audio output.
3,4	**Volume up / Down Keys**	Configure the handset and ringtone volume.
5.	**PTT Key**	PTT (Push-to-Talk) button, to initiate PTT call.
6.	**Hands-free / Speaker key**	Switches between Handset and Hands-free / Speaker modes.

7.	Arrow key combination (Up, Down, Left, Right)	Allows navigation of the cursor through the displayed menu options.
8.	Off-hook / Dial key	Enters dialing mode, or dials number entered.
9.	Alphanumeric Keypad	Provides the digits, letters, and special characters in context-sensitive applications. For + sign, press and hold key 0.
10.	* / Mute key	Activates or deactivates the mute feature when keep pressing on * in idle screen.
11.	LED indicator	1dual-color LED indicator indicating: power, call, battery, message waiting…
12.	3.5 mm headset jack	Phone connector for the headphones/headsets.
13.	Color LCD Screen	2.4-inch (240x320) TFT color LCD
14.	Softkeys	Correspond to functions displayed on the LCD. These functions change depending on the current context.
15.	Contacts	Access to contacts list.
16.	Menu/OK key	Selects the option chosen by the cursor or enters the main menu from the home screen.
17.	On-hook or Power key	Terminates calls or turns the handset on / off.
18.	# / Lock key	Locks keypad against unintentional entries when keep pressing #. • Press and hold # key for approximately 2 seconds to lock the keys. • Press **Unlock** softkey and then **#** to unlock the keys.
19.	Microphone	Picks up audio earpiece and hands-free calls.

WP820 Icons Description

Following table contains description of each icon that might be displayed on the screen of the WP820.

Table 5: WP820 Icons Description

	Battery status Charging
	Wi-Fi not enabled/configured
	Wi-Fi signal status
	Speaker enabled icon
	Ringtone status
	Outgoing Call notification

	Missed Call notification
	Incoming Call notification
	Voicemail notification (Urgent)
	Voicemail notification (Ordinary)
	Mute enabled icon
	DND enabled icon
	Bluetooth enabled icon
	Bluetooth connected icon
	Contacts
	SMS
	Call History
	Voice Mail
	Diagnosis
	Settings
	Tools
	Status

WP820 Handset Menu

The handset has an easy-to-use menu structure. Every menu opens a list of options. To open the main menu, unlock first the handset and press "Menu" (softkey in the middle). Press Arrow keys to navigate to the menu option you require. Then press "Select" (left softkey) or **OK/Selection key** to access further options or confirm the setting displayed. To go to the previous menu item, press "Back" (right softkey). You can press **Power** key at any time to cancel and return to standby mode.

Contacts
- Options
- Search

Call History
- All
- Missed
- Outgoing
- Incoming

SMS
- Options
- New

Voice Mail
- Urgent
- Normal

Diagnosis
- LCD diagnosis
- LCD off
- LED diagnosis
- Keypad diagnosis
- Audio loopback
- Acceleration sensor
- Proximity sensor
- Vibrator
- Certificate Verification

Settings
- Account
- Personalized account
- Speed dial
- Network settings ●
- Basic settings ●
- Advanced Settings ●

Network settings
- Preferred Internet Protocol
- Wi-Fi
- Wi-Fi Settings
- Wi-Fi Roaming Mode
- Bluetooth
- Bluetooth Settings
- Additional Network Settings

Basic settings
- Sound
- Display
- Language
- Do Not Disturb
- Date and time
- Accessibility

Advanced Settings
- System Upgrade
- Paging/PTT Setting
- Disable Web UI Access
- Syslog
- Factory Reset
- Reboot

Tools
- Alarm

Status
- Account Status
- System Status
- Network Status
- Network statistics

Figure 5: WP820 Menu Structure

Contacts	Display the list of the registered contacts and also the groups contacts with the ability of searching, adding or editing the entries and also deleting the selected contacts.
Call History	Display the call history: **Missed Calls**, **Accepted Calls**, **Outgoing Calls** or **All Calls**. You can add contacts to **Shared Contacts** directly from call logs.
SMS	**SMS** stands for Short Message Service and referred to as a "text message". With a SMS, you can send a message by pressing **"New"** of up to 160 characters to another device or check the received ones.
Voice Mail	• **Play Message:** Play voice mail messages received. • **Set Voice Mail:** Configure voice mail parameters.
Diagnosis	• **LCD diagnosis** • **LCD off** • **LED diagnosis** • **Keypad diagnosis** • **Audio loopback** • **Acceleration sensor** • **Proximity sensor** • **Vibrator** • **Certificate Verification**
Settings	• **Account** Configure/View SIP accounts settings. • **Personalized Account** Configure the account ringtones, auto answer and call forwarding. • **Speed Dial** Assign contact numbers as speed dial. • **Network Settings** Configure the networks settings including Wi-Fi settings, Bluetooth settings, and additional networks settings. • **Basic Settings** Configure the basic settings including voice settings, display and language settings, date/time settings and accessibility. • **Advanced Settings** Configure the advanced settings including system upgrade, paging/PTT settings, syslog settings and factory reset/reboot.
Tools	• **Alarm Clock** Configures the alarm clock settings
Status	Displays account status, system status, Network status and network statistics • **Account status.**

| | • **System status:**
Press to enter the sub menu for Total amount of memory, Available space, System version, Recovery version, U-boot version, Kernel version, Hardware version, PN number, Country code and Running time.
• **Network status:**
Press to enter the sub menu for MAC address, IP setting information (DHCP/Static IP), Ipv4 address, Ipv6 address, Subnet Mask, Gateway; DNS server and VPN.
• **Network Statistics:**
Press to enter the sub menu for Network SSID, BSSID, IP address, Signal strength, Connection speed, Channel, Frequency, Tx packets, Tx error packets, Tx error rate, Tx drop packets, Tx drop rate, Rx packets, Rx error packets, Rx error rate, Rx drop packets, Rx drop rate. |
|---|---|

Connecting WP820 to Wi-Fi Network

The WP820 supports dual-band 802.11a/b/g/n Wi-Fi, please refer to the following steps in order to connect your WP820 to the Wi-Fi networks:

1. On LCD menu, press Menu key and navigate to **Settings → Network Settings → Wi-Fi**.

2. Set Wi-Fi to "On" and navigate to "Wi-Fi Settings". A list of Wi-Fi networks will be displayed.

3. Select the desired network to connect to. (Enter the correct password to connect if requested)

WP820 will display Wi-Fi icon on the main LCD menu if the connection to the Wi-Fi network is successful.
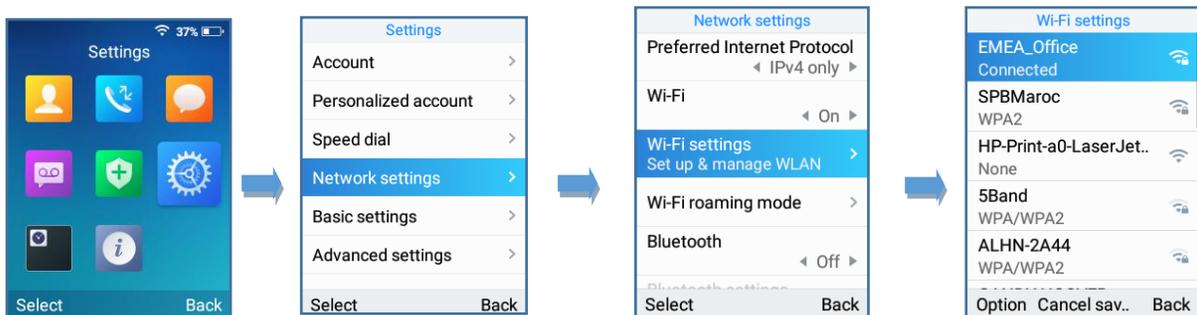
Figure 6 : Wi-Fi Settings

Note: If 5GHz and 2.4Ghz are both available, the WP820 will use 5GHz, but it may switch to 2.4GHz if the signal of 5GHz is poor.

Obtain WP820 IP Address

In order to know which IP address is assigned to your WP820, please follow below steps:

1. Unlock first your WP820 and press "**Menu**" (Middle softkey) or **Ok** button to view operation menu.

2. Press Arrow (Up, Down, Left, Right) keys to move the cursor to **Status** icon , then press "**Select**" (left softkey) or **Ok** button.

3. Access **Network Status** menu to obtain the IP address of the WP820.
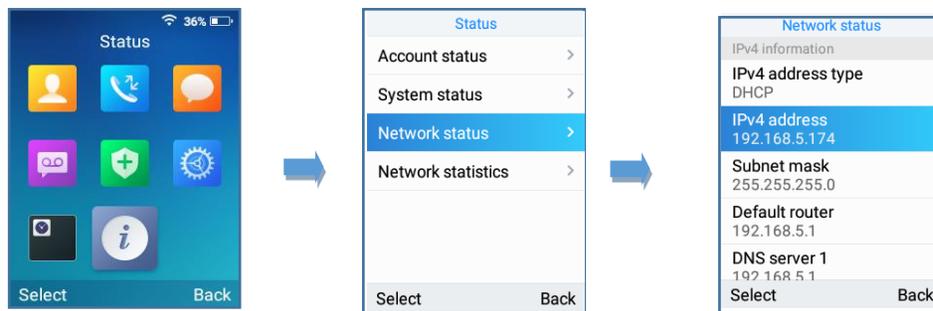
Figure 7: Obtaining IP Address

WP820 WEB GUI ACCESS CONFIGURATION

The WP820 can be configured using:

- Web GUI embedded on the WP820 using PC's web browser.

- LCD Configuration Menu using the WP820 keypad.

Note: From the Web GUI, you can configure all the functions supported by the WP820; while via keypad menu, you can access limited configuration.

Configuration via Web Browser

The WP820 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the WP820 through a Web browser such as Google Chrome, Mozilla Firefox.

Note: Please note that Microsoft's IE 9 and below are not supported, also the records from the web can't be played with IE10, Edge and Safari. We highly recommend using Google Chrome or Mozilla Firefox.

Accessing the Web UI

1. Connect the computer to the same network as WP820.

2. Make sure the WP820 is booted up and powered correctly.

3. You may check WP820 IP address via a subscribed WP820 on its LCD menu **Status → Network Status.** Please see **Obtain WP820 IP Address**

4. Open Web browser on your computer and enter the WP820 IP address in the address bar of the browser.

5. Enter the administrator's username and password to access the Web Configuration Menu.

Notes:

- The computer must be connected to the same sub-network as the WP820. This can be easily done by connecting the computer to the same hub or switch as the WP820.

- The default administrator username and password are "admin"; the default end-user username is "user" and the password is "123".

Web GUI Languages

Currently the WP820 web GUI supports English, Chinese languages.
Users can select the displayed language in web GUI login page, or at the upper right of the web GUI after logging in
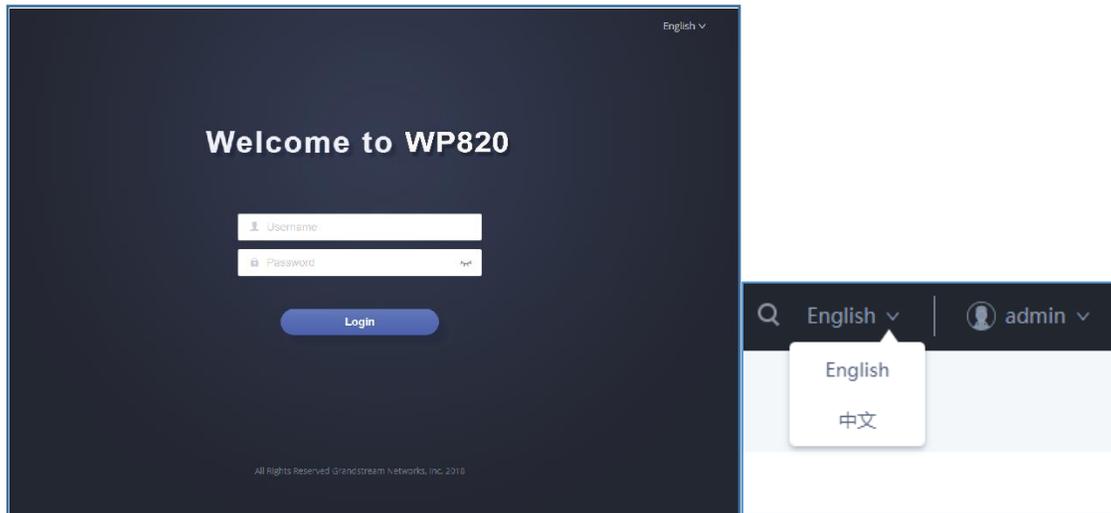
Figure 8: WP820 Web GUI Language

Saving the Configuration Changes

When changing any settings, always submit them by pressing **Save** and **Apply** buttons. If using the **Save** button, after making all the changes, click on the **Apply** button on top of the page to submit.

Web UI Access Level Management

There are two default passwords for the login page:

User Level	Username	Password	Web Pages Allowed
End User Level	user	123	Only Status, Phone Settings, System Settings, Maintenance and System Application with limited options.
Administrator Level	admin	admin	All pages

Changing User Level Password

1. Access the Web GUI of your WP820 using the admin's username and password. (Default username and password is: admin/admin).

2. Press **Login** to access your settings.

3. Go to **System Settings → Security Settings.**

4. In **User Info Management**, locate **user password** section:

    a. Type in the admin password in the **Current Admin Password** field.

    b. Type in your new user password in **New User Password** field.

    c. Type in again same entered password in **Confirm New User Password** field.

5. Press **Save** button to save your new settings.
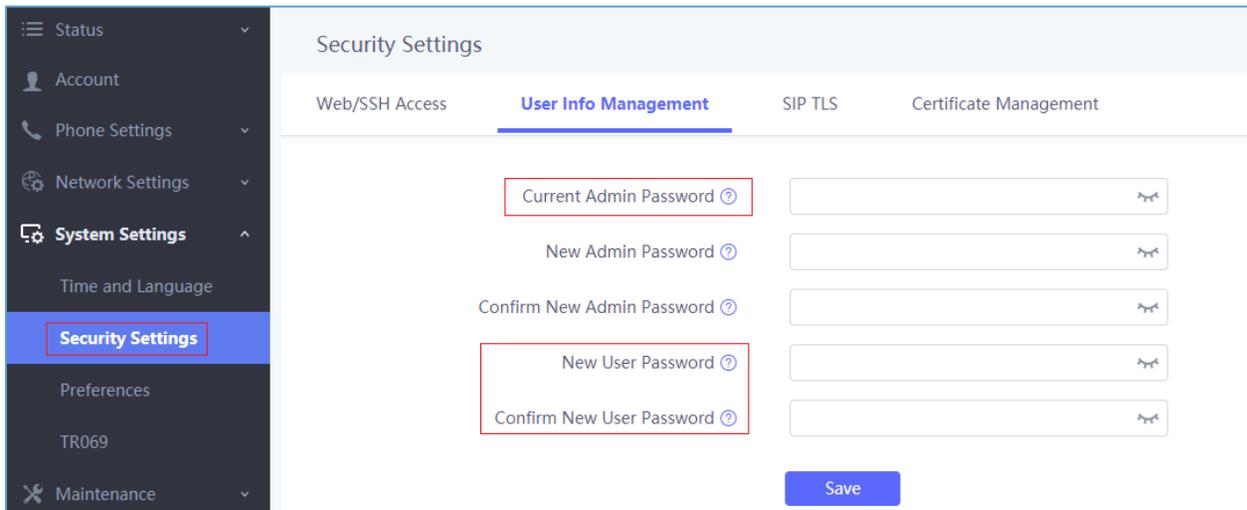
Figure 9: User Level Password

Notes:

- DO NOT USE same password for both user and admin accounts.

- The password is case sensitive with maximum length of 25 characters.

Changing Admin Level Password

1. Access the Web GUI of your WP820 using the admin's username and password. (Default username and password is: admin/admin).

2. Press **Login** to access your settings.

3. Go to **System Settings → Security Settings.**

4. In **User Info Management**, locate **admin password** section:

    a. Type in the admin password in the **Current Admin Password** field

    b. Type in your new user password in **New Admin Password** field.

    c. Type in again same entered password in **Confirm New Admin Password** field.

5. Press **Save** button to save your new settings.
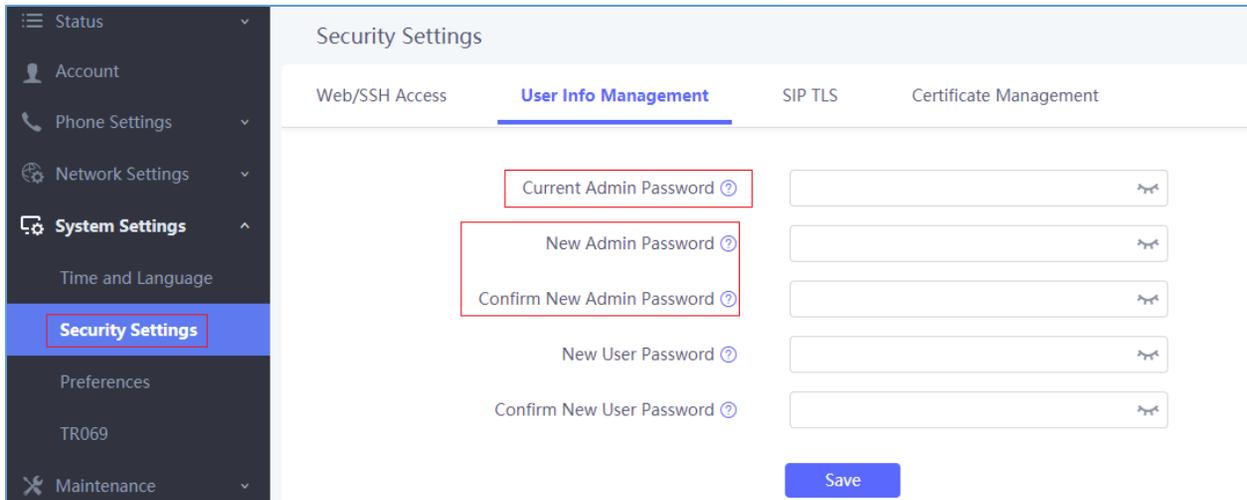
Figure 10: Admin Level Password

Notes:

- DO NOT USE same password for both user and admin accounts.

- The password is case sensitive with maximum length of 25 characters.

Changing HTTP / HTTPS Web Access Port

1. Access the Web GUI of your WP820 using the admin's username and password. (Default username and password is: admin/admin).

2. Press **Login** to access your settings.

3. Go to **System Settings → Security Settings.**

4. In **Web/SSH Access** page, select the access method depending on desired protocol (HTTP or HTTPS)

5. Locate **HTTP / HTTPS Web Port** field and change it to your desired/new HTTP / HTTPS port.
   Note: By default, the HTTP port is 80 and HTTPS is 443.

6. Press **Save** button to save your new settings.

Note: A reboot is required for this change to take effect.
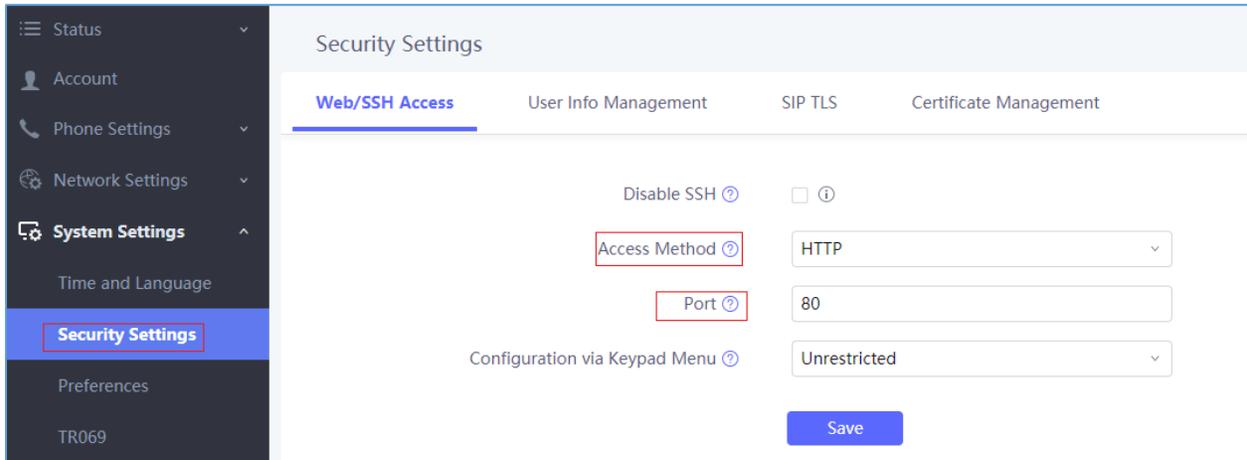
Figure 11: Web Access Port

WP820 WEB GUI SETTINGS

This section describes the options in the WP820 Web UI. As mentioned, you can log in as an administrator or an end user.

- **Status:** Display account status, network status and system info.

- **Account:** Configure accounts with general settings, SIP settings, codec settings, call settings and advanced settings.

- **Phone Settings:** Configure general settings, call settings, ring tones and PTT/multicast paging.

- **Network Settings:** Wi-Fi settings, OpenVPN settings and advanced network settings.

- **System Settings:** Time/language settings, security settings, preferences settings and TR069 settings.

- **Maintenance:** Configure upgrade and provisioning settings, system diagnosis and event notification settings.

- **Application:** Configure phonebook settings and call recording settings.

- **Value-added Service:** Configure GDS settings.

Status Page Definitions

Status/Account Status

Account	Displays list of configured accounts'.
Number	Displays the numbers of the configured accounts'.
SIP Server	Displays list of SIP Server user by the configured accounts'.
Status	Shows the status of SIP registration. If the SIP account is successfully registered, it will display "Registered" with green background. If the SIP account is not registered, it will display "Unregistered" with grey background.

Status/Network Status

MAC Address	Shows Device ID in hexadecimal format. This is needed by network administrators for troubleshooting. The MAC address will be used for provisioning and can be found on the label on original box and on the label located on the bottom panel of

	the device.
NAT Type	Indicates type of NAT for each Profile. (Based on STUN protocol.)
IPv4	
Address Type	Indicates the configured address type: DHCP or Static IP
IPv4 Address	Displays assigned IP address. Example: 192.168.5.110
Subnet Mask	Displays assigned subnet mask. Example: 255.255.255.0
Default Gateway	Displays assigned default gateway. Example: 192.168.5.1
DNS Server 1	Shows assigned DNS server address 1. Example: 8.8.8.8
DNS Server 2	Shows assigned DNS server address 2. Example: 8.8.4.4
IPv6	
IPv6Address Type	Indicates the configured address type: DHCP or Static IP
IPv6 Address	Displays assigned IP address.
IPv6 DNS Server 1	Shows assigned DNS server address 1.
IPv6 DNS Server 2	Shows assigned DNS server address 2.

Status/System Info

Product Model	Displays product model info. Default is **WP820**.
Hardware Revision	Displays the Hardware version number. Example: V1.2A
Part Number	Shows product part number. Example: 9620008212A (last 2 digits show HW version, in this example 12A for HW version 1.2A)
System Version	Displays Firmware version. This is the main software release version.
Recovery Version	Displays the Recovery image version
Boot Version	Displays the Booting code version.
Kernel Version	Displays the Kernel version.
System Up Time	Indicates system uptime since last reboot.

Account Page Definitions

Account/General Settings

Account Registration	
Account Active	This field indicates whether the account is active. The default setting is "Yes".
Account Name	Configure the name associated with each account to be displayed on the LCD.
SIP Server	Configures the URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (ITSP).
Secondary SIP Server	Configures the URL or IP address, and port of the SIP server. This will be used when the primary SIP server fails.
SIP User ID	Configures the user account information, provided by your VoIP service provider (ITSP). It's usually in the form of digits similar to phone number or actually a phone number.
SIP Authentication ID	Configures the SIP service subscriber's ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	Configures the account password required for the phone to authenticate with the ITSP (SIP) server before the account can be registered. After it is saved, this will appear as hidden for security purpose.
Display Name	Configures the SIP server subscriber's name (optional) that will be used for Caller ID display.
Tel URI	Indicates E.164 number in "From" header by adding "User=Phone" parameter or using "Tel:" in SIP packets, if the base has an assigned PSTN Number. • **Disabled:** Will use "SIP User ID" information in the Request-Line and "From" header. • **User=Phone:** "User=Phone" parameter will be attached to the Request-Line and "From" header in the SIP request to indicate the E.164 number. If set to "Enable". • **Enabled:** "Tel:" will be used instead of "sip:" in the SIP request. Please consult your carrier before changing this parameter. Default is **Disabled**.
Voice Mail Access Number	Defines the voice mail portal access number to allow users accessing their voice messages.

Network Settings	
Outbound Proxy	Configures the IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller. It's 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	Configures the IP address or Domain name of the Secondary Outbound Proxy, Media Gateway, or Session Border Controller. Secondary outbound proxy will be used when the primary outbound proxy fails.
DNS Mode	Selects DNS mode to use for the client to look up server. One mode can be chosen. • **A Record:** resolves IP Address of target according to domain name. • **SRV:** DNS SRV resource records indicate how to find services for various protocols. • **NAPTR/SRV:** Naming Authority Pointer according to RFC 2915. Default is **A Record**.
DNS SRV Fail-over Mode	The option will decide which IP is going to be used in sending subsequent SIP packets (ex: Register refresh requests) after the list of IPs for SIP server host is resolved with DNS SRV. • **Default (prefer server with lowest SRV priority):** The phone will always prefer to send SIP requests to the available server having the lowest priority, and in case it's down it contacts the next one, but once the server having lowest priority is UP again, the phone will switch over to this one. • **Saved one until DNS TTL (Stay on responding IP until DNS timeout):** On this mode, the phone will resolve DNS SRV records and tries to send the request to the server having lowest priority and if it doesn't respond, it will move on to the next IP until one of the servers responds, once this happen the phone will keep contacting this responding IP until DNS timeout (30 minutes) before starting over. • **Saved one until no response (Stay on responding IP until its failure):** On this mode, the phone will send SIP requests to the last responding IP, and it doesn't failover/switchover to the next one until this responding server is down.

NAT Traversal	Specifies which NAT traversal mechanism will be enabled on the phone. It can be selected from the dropdown list: • NAT NO • STUN • Keep-alive • Auto • OpenVPN If the outbound proxy is configured and used, it can be set to "NAT NO". If set to "STUN" and STUN server is configured, the phone will periodically send STUN message to the SUTN server to get the public IP address of its NAT environment and keep the NAT port open. STUN will not work if the NAT is symmetric type. If set to "Keep-alive", the phone will send the STUN packets to maintain the connection that is first established during registration of the phone. The "Keep-alive" packets will fool the NAT device into keeping the connection open and this allows the host server to send SIP requests directly to the registered phone. If it needs to use OpenVPN to connect host server, it needs to set it to "OpenVPN". The default setting is "NAT NO".
Proxy-Require	Adds the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server.

Account/SIP Settings

SIP Basic Settings	
SIP Registration	Allows the phone to send SIP REGISTER messages to the proxy/server. The default setting is "Yes".
Unregister before New Registration	Controls whether to clear SIP user's information by sending un-register request to the proxy server. When set to "All", the un-registration is performed by sending a REGISTER message with "Contact" header set to * and Expires=0 parameters to the SIP server when the phone starts pre-registration after rebooting. If set to "Instance", the phone only cleans the current SIP user's info by sending REGISTER message with "Contact" header set to concerned SIP user's info and Expires=0 parameters to the SIP server. The default setting is "Instance".
Register Expiration (m)	Configures the time period (in minutes) in which the phone refreshes its registration with the specified registrar. The default setting is **60**. The maximum value is 64800 (about 45 days).

Re-register before Expiration (s)	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default setting is **0**. The range is from 0 to 64800.
Registration Retry Wait Time (s)	Configures the time period (in seconds) in which the phone will retry the registration process in the event that is failed. The default setting is **20**. The maximum value is 3600 (1 hour).
Add Auth Header On RE-REGISTER	Configure if the SIP account needs to add Auth header in RE-REGISTER. • If the option is checked, device will always add authentication header in REGISTER. • If the option is unchecked, device will only send authentication for the first REGISTER.
Enable SIP OPTIONS Keep Alive	Enables SIP OPTIONS to track account registration status so the phone will send periodic OPTIONS message to server to track the connection status with the server. The default setting is "**No**".
SIP OPTIONS Keep Alive Interval (s)	Configures the time interval when the phone sends OPTIONS message to SIP server. The default setting is 30 seconds, which means the phone will send an OPTIONS message to the server every 30 seconds. The valid range is 1-64800.
SIP OPTIONS Keep Alive Maximum Tries	Configures the maximum times of sending OPTIONS message consistently from the phone to server. Phone will keep sending OPTIONS messages until it receives response from SIP server. The default setting is "3", which means when the phone sends OPTIONS message for 3 times, and SIP server does not respond this message, the phone will send RE-REGISTER message to register again. The valid range is 3-10.
Subscribe for MWI	Configures the phone to subscribe voice message service. If it is set to "Yes", the phone will periodically send SIP SUBSCRIBE message for Message Waiting Indication service. WP820 phone supports both synchronized and non-synchronized MWI. The default setting is "**No**".
Use Privacy Header	Determines if the Privacy header will be presented in the SIP INVITE message and if it includes the caller info in this header. If it is set to "Default", the Privacy Header will be omitted in INVITE when "Huawei IMS" special feature is active. If set to "Yes", it will always be presented. If set to "No", it will always be omitted. The default setting is "**Default**".

Use P-Preferred-Identity Header	Specifies if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to "default", the P-Preferred-Identity Header will be omitted in SIP INVITE message when "Huawei IMS" special feature is active. If set to "Yes", the P-Preferred-Identity Header will always be presented. If set to "No", it will be omitted. The default setting is "**Default**".
SIP Transport	Determines the network protocol used for the SIP transport. Users can choose from TCP/UDP/TLS. Default setting is "**UDP**".
Local SIP Port	Defines the local SIP port used to listen and transmit. The default value is 5060 for Account 1 and 5062 for Account 2.
SIP URI Scheme When Using TLS	Defines which SIP header, "sip" or "sips", will be used if TLS is selected for SIP Transport. The default setting is "**sip**".
Use Actual Ephemeral Port in Contact with TCP/TLS	Determines the port information in the Via header and Contact header of SIP message when the phone use TCP or TLS. If set to No, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the particular connection. The default setting is "**No**".
Support SIP Instance ID	Determines if the phone will send SIP Instance ID. The SIP instance ID is used to uniquely identify the device. If set to "Yes", the SIP Register message Contact header will include +sip.instance tag. The default setting is "**Yes**".
SIP T1 Timeout	Defines an estimate of the round-trip time of transactions between a client and server. If no response is received in T1, the figure will increase to 2*T1 and then 4*T1. The request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is **0.5** sec.
SIP T2 Interval	Specifies the maximum retransmit time of any SIP request messages (excluding the SIP INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. The default setting is **4** sec.
SIP Timer D Interval	Defines the amount of time that the server transaction can remain when unreliable response (3xx-6xx) received. The valid value is 0-64 seconds. Default value is **0**.
Remove OBP from Route	Configures to remove outbound proxy from route. If set to "Enable", the SIP account will notify the server to remove the proxy in NAT/Firewall environment; If set to "Always", the SIP account will notify the server to remove the proxy unconditionally. The default setting is "**Disable**".

Enable 100rel	Actives PRACK (Provisional Acknowledgment) method. PRACK improves the network reliability by adding an acknowledgement to the provisional Responses (1xx). It is set to "Yes", the phone will response to the 1xx response from the remote party. The default setting is "**No**".
Session Timer	
Enable Session Timer	This parameter is to enable/disable session timer function. • If set to "Yes", the phone will configure the related parameters when send session timer according to "Session Expiration". • If set to "No", disables session timer.
Session Expiration(s)	Configures the phone's SIP session timer. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is **180**. The valid range is from 90 to 64800.
Min-SE (s)	Determines the minimum session expiration timer (in seconds) if the phone act as a timer refresher. The default setting is **90**. The valid range is from 90 to 64800.
UAC Specify Refresher	Sets which party will refresh the active session if the phone makes outbound calls. If it is set to "UAC" and the remote party does not support Refresher feature, the phone will refresh the active session. If it is set to "UAS", the remote party will refresh it. If it is set to "Omit", the header will be omitted so that it can be selected by the negotiation mechanism. The default setting is "**Omit**".
UAS Specify Refresher	Specifies which party will refresh the active session if the phone receives inbound calls. If it is set to "UAC", the remote party will refresh the active session. If it is set to "UAS" and the remote party does not support refresh feature, the phone will refresh it. The default setting is "**UAC**".
Caller Request Timer	Sets the caller party to act as refresher by force. If set to "Yes" and both party support session timers, the phone will enable the session timer feature when it makes outbound calls. The SIP INVITE will include the content "refresher=uac". The default setting is "**No**".
Callee Request Timer	Sets the callee party to act as refresher by force. If set to "Yes" and the both parties support session timers, the phone will enable the session timer feature when it receives inbound calls. The SIP 200 OK will include the content "refresher=uas". The default setting is "**No**".

Force Timer	Configures the session timer feature on the phone by force. If it is set to "Yes", the phone will use the session timer even if the remote party does not support this feature. If it 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**".
Force INVITE	Sets the SIP message type for refresh the session. If it is set to "Yes", the Session Timer will be refreshed by using the SIP INVITE message. Otherwise, the phone will use the SIP UPDATE or SIP OPTIONS message. Default is "**No**".

Account/Codec Settings

Preferred Vocoder	
Preferred Vocoder	Lists the available and enabled Audio codecs for this account. Users can enable the specific audio codecs by moving them to the selected box and set them with a priority order from top to bottom. This configuration will be included with the same preference order in the SIP SDP message. The Supported vocoders are: PCMU, PCMA, G722, G729A/B, iLBC and Opus.
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.
Use First Matching Vocoder in 200OK SDP	Includes only the first matching vocoder in its 200OK response, otherwise it will include all matching vocoders in same order received in INVITE. Default is **No**.
iLBC Frame Size	Specifies iLBC packet frame size (20ms or 30ms). Default is **30ms**.
Opus Payload Type	Determines payload type for Opus codec. The valid range is between 96 and 126. Default is **123**.
DTMF	Specifies the mechanism to transmit DTMF (Dual Tone Multi-Frequency) signals. There are 3 supported modes: The default setting is "**RFC2833**". • **In audio**, which means DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs); • **RFC2833**, which means to specify DTMF with RTP packet. Users could know the packet is DTMF in the RTP header as well as the type of DTMF. • **SIP INFO**, which uses SIP INFO to carry DTMF. The defect of this mode is that it's easily to cause desynchronized of DTMF and media packet if the SIP and RTP messages are required to transmitted respectively.

DTMF Payload Type	Configures the RTP payload type using RFC2833 that indicates the transmitted packet contains DTMF digits. Valid range is from 96 to 127. Default value is **101**.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call. The default setting is "**No**".
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 127. The default value is **121**.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 127. The default value is **124**
Silence Suppression	Enables the silence suppression/VAD feature. If it is set to "Yes", when silence is detected, a small quantity of VAD packets (instead of audio packets) will be sent during the period of no talking. If set to "No", this feature is disabled. The default setting is "**No**".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet (It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120Kbit/s). When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used in the codec table or negotiate the payload type during the actual call. For example, if the setting is set to 2 and the first code is G. 729 or G. 711, the "ptime" value in the SDP datagram of the INVITE request is 20 milliseconds. If the "Voice Frame/TX" setting exceeds the maximum allowable value, the phone will use and save the maximum allowable value for the selection of the first encoding. It is recommended to use the default setting provided, and incorrect setting may affect the voice quality.
RTP Settings	
SRTP Mode	Sets if the phone will enable the SRTP (Secured RTP) mode. It can be selected from dropdown list: • **Disable** • **Enabled but not forced** • **Enabled and forced** The default setting is "**Disable**". SRTP uses encryption and authentication to minimize the risk of denial of service. (DoS). If the server allows to use both RTP and SRTP, it should be configured as "Enabled but not forced". It uses SDP security description to exchange key. Please refer to: **SDES**: https://tools.ietf.org/html/rfc4568 **SRTP**: https://tools.ietf.org/html/rfc3711

SRTP Key Length	Configures all the AES (Advanced Encryption Standard) key size within SRTP. It can be selected from dropdown list:
	  • **AES128&256 bit**
	  • **AES 128 bit**
	  • **AES 256 bit**
	If it is set to "AES 128&256 bit", the phone will provide both AES 128 and 256 cipher suite for SRTP. If set to "AES 128 bit", it only provides 128-bit cipher suite; if set to "AES 256 bit", it only provides 256-bit cipher suite.
	The default setting is "**AES128&256 bit**".

Enable SRTP Key Life Time	Defines the SRTP key life time. When this option is set to be enabled, during the SRTP call, the SRTP key will be valid within 2^{31} SIP packets, and phone will renew the SRTP key after this limitation. Default is "**Yes**".
RTCP Destination	Configures the server address. When there is a call, the RTCP package sent from the phone will also be sent to this address. **Note**: The address should contain port number.
Symmetric RTP	Configures if the phone enables the symmetric RTP mechanism. If it is set to "Yes", the phone will use the same socket/port for sending and receiving the RTP messages. The default setting is "**No**".
RTP IP Filter	Receives the RTP packets from the specified IP address and Port by communication protocol. If it is set to "IP Only", the phone only receives the RTP packets from the specified IP address based on the communication protocol; If it is set to "IP and Port", the phone will receive the RTP packets from the specified IP address with the specified port based on the communication protocol. The default setting is "Disable".

Account/Call Settings

Call Features	
Auto Answer	If set to "Yes", the phone will automatically turn on the speaker to answer incoming calls after a short reminder beep. If set to "Enable Intercom/Paging", it will answer the call based on the SIP Info header sent from the server/proxy. The default setting is "No".
Play Warning Tone for Auto Answer Intercom	When enabled, the phone will play warning tone when auto answer Intercom. By default, it's enabled.

Intercom Barging	Configures whether to answer the incoming intercom call when there is already an active call on the phone. When "Intercom Barging" is enabled, if the current active call is an intercom call, the incoming intercom call will be automatically rejected; if the current active call is not an intercom call, the current active call will be put on hold and the incoming intercom call will be automatically answered. When "Intercom Barging" is disabled, a prompt will show up indicating the incoming intercom call without interrupting the current active call.
Send Anonymous	Sets the phone to make anonymous outgoing calls; when set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous, essentially blocking the Caller ID to be displayed. The default setting is "No".
Anonymous Call Rejection	Rejects the calls whose SIP INVITE message includes Anonymous information in from header when enabled. The default setting is "No".
Call Log	Categorizes the call logs saved for this account. • If it is set to "**Log All**", all the call logs of this account will be saved. • If set to "**Log Incoming/Outgoing Calls (Missed Calls Not Record)**", the whole call history will be saved other than missed call. • If it is set to "**Disable Call All**", none of the call history will be saved. • If it is set to "**Don't Prompt Missed Call**", the phone will log the missed call histories, but there is no prompt to indicate the missed calls on phone LCD. The default setting is "**Log All**".
Enable Call Features	Configures the local call features. If set to "Yes", call features (including call forwarding, DND and etc) will be supported locally instead of using the feature code supported on SIP server/proxy.
Transfer on 3-way Conference Hangup	Transfers conference from hosted party when hang up, thus other parties can continue the conference without interruption. The default setting is unchecked.
DND Call Feature On	Configures the feature code to enable the DND (Do Not Disturb) feature for this account. If it is configured, the phone will dial the feature code automatically when the DND feature is enabled.
DND Call Feature Off	Configures the feature code to disable the DND (Do Not Disturb) feature for this account. If it is configured, the phone will dial the feature code automatically when the DND feature is disabled.

No Key Entry Timeout (s)	Determines the expiration timer (in seconds) for no key entry. The dialed digits will be sent out if no other digits entered within the set period. The default value is 4 seconds. The valid range is from 1 to 15.
Ring Timeout (s)	Defines the expiration timer (in seconds) for the rings with no answer. The default setting is 60. The valid range is from 10 to 300.
Refer-To Use Target Contact	Sets the phone to use the target's Contact header tag to the Refer-To header in the SIP REFER message during an attended transfer. The default setting is "No".
RFC2543 Hold	Allows users to toggle between RFC2543 hold and RFC3261 hold. RFC2543 hold allows user to disable the hold music sent to the other side (c=0.0.0.0 will be used in INVITE SDP for hold). RFC3261 will play the hold music to the other side.
Call Forward	

Call Forward Type	Sets the Call Forwarding feature for this account.
	
	 • **None:** Disable call forwarding feature.
	
	 • **Unconditional:** Set to forward all calls to a specified account.
	
	 • **Time based:** Set the call forwarding rule based on time. The system can forward incoming calls to the accounts of In Time Forward to and Out Time Forward to.
	
	 • **Others**: Set the call forwarding rule based on following account status.
	
	   ✓ **Enable Busy Forward:** The call will be forward to number set under "Busy To" when the account is busy.
	
	   ✓ **Enable No Answer Forward**: The call will be forwarded to the number set under "No Answer To" after the configured timeout. (range 1- 120s)
	
	   ✓ **Enable DND Forward:** When the phone is on DND mode the call will be forwarded to number configured under "DND To".

Dial Plan	
Dial Plan Prefix	Adds specified prefix to dialed number.
Disable Dial Plan	Enables/disables the Dial plan mechanism for different cases. If the specific case is checked, the Dial plan mechanism will be disabled. • **Dial Page:** It controls the pattern of dialing numbers from the keypad, phone app and account widget.

	• **Contact:** It controls the pattern of dialing numbers from local and Broadsoft contacts. • **Incoming call history:** It controls the pattern of dialing numbers from inbound call logs. • **Outgoing Call History:** It controls the pattern of dialing numbers from outbound call logs. The default setting is unchecking all the cases.

Dial Plan	**Dial Plan Rules**:
	
	1. Accept Digits: +,1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d
	
	2. Grammar: **x** – any digit from 0-9;
	
	    a. **xx+** - at least 2-digit number;
	    b. **xx** – exactly 2-digit number;
	    c. **xx?** - 1 or 2-digit numbers from 0-9
	    d. **^** - exclude;
	    e. **.** – wildcard, matches one or more characters
	    f. **[3-5]** – any digit of 3, 4, or 5.
	    g. **[147]** – any digit 1, 4, or 7.
	    h. **<2=011>** - replace digit 2 with 011 when dialing.
	    i. **<=1>** - add a 1 to dialed number.
	    j. **<1=>** - remove 1 from the number dialed.
	    k. **|** - or
	    l. **\+** - + sign
	
	• **Example 1:** {[369]11 | 1617xxxxxxx} –
	Allow 311, 611, 911, and any 10-digit numbers of leading digits 1617
	
	• **Example 2:** {^1900x+ | <=1617>xxxxxxx} –
	Block any number with leading digits 1900 and add prefix 1617 for any dialed 7-digit numbers
	
	• **Example 3:** {1xxx[2-9]xxxxxx | <2=011>x+} –
	Allow any length of number with leading digit 2 and 10 digit-numbers of leading digit 1 and leading exchange number between 2 and 9; If leading digit is 2, replace leading digit 2 with 011 before dialing.
	
	• **Example 4:** Replace / Add / Remove digits:
	    • <u>Replace:</u>

{123<611=456>} - dial 123611 will be become 123611

{<611=456>789} – dial 611789 will be become 456789

{123<456=0>789} – dial 123456789 will become 1230789

- • Add:

    {<=1>x+} - dial 3000 will be become 13000

    {<=611>555} – dial 555 will become 611555

    {123<=907>456} – dial 123456 will become 123907456

- • Remove:

    {<611=>555} – dial 611555 will become 555

    {123<907=>456} – dial 123907456 will become 123456

    {123<555=>} - dial 123555 will become 123

3. Default: Outgoing –

    { x+ | \+x+ | *x+ | *xx*x+ | x+*x+*x+*x+ | x+*x+*x+*x+#x+ }

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 | \+x+}

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 dialing 7 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
- • **\+x+ -** allows dialing any digit with leading + sign; example: +16175669300

Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider.

In this case * should be predefined inside dial plan feature. An example dial plan will be: **{ *x+ }** which allows the user to dial * followed by any length of numbers.

Caller IDs	
Caller ID Display	Specifies which header tag will be used from the SIP INVITE message for the Caller ID display. • If it is set to "**Auto**", the phone will use the one of the available headers in the priority hierarchy of P-Asserted Identify Header, Remote-Party-ID Header and FROM Header.

	• If it is set to "**From Header**", it will use the FROM header information for the Caller ID. • If it is set to "**Disabled**", all the incoming calls Caller ID will be displayed with "Unavailable". The default setting is "**Auto**".
Ring Tones	
Account Ring Tone	Allows users to configure the ringtone for the account. Users can choose different ringtones from the dropdown list. **Note:** User can also choose silent ring tone.
Ignore Alert-Info Header	If checked, configured default ringtone will be played by ignoring Alert-Info header.
Match Incoming Caller ID	Specifies matching rules with number, pattern or Alert Info text (up to 3 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/Advanced Settings

Security Settings	
Check Domain Certificates	Defines whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is "**No**".

Validate Certification Chain	Configures whether to validate certification chain, when TLS/TCP is configured for SIP Transport. If this is set to "Yes", phone will validate server against the new certificate list. The default setting is "**No**".
Validate Incoming SIP Messages	Specifies if the phone will check the incoming SIP messages caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "**No**".
Allow Unsolicited REFER	Configures whether to dial the number carried by Refer-to after received Out-of-dialog SIP REFER request actively. • If set to "**Disabled**", the phone will send error warning and stop dialing. • If set to "**Enabled/Force Auth**", the phone will dial the number after send authentication, if the authentication failed, then stop dialing. • If set to "**Enabled**", the phone will dial up all numbers carried by SIP REFER. The default is "**Disabled**".
Only Accept SIP Requests from Known Servers	Answers the SIP request from saved servers when set to "Yes", only the SIP requests from saved servers will be accepted; and the SIP requests from the unregistered server will be rejected. The default setting is "**No**".
Check SIP User ID for Incoming INVITE	Configures the phone to check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it doesn't match the phone's SIP User ID, the call will be rejected. The default setting is "**No**".
Allow SIP Reset	Configures if allow SIP Notification message to perform factory reset. The default setting is "**No**".
Authenticate Incoming INVITE	Configures the phone to authenticate the SIP INVITE message from the remote party. If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. The default setting is "**No**".
SIP Realm Used for Challenge INVITE & NOTIFY	Configure this item to validate incoming INVITE, but you must enable authenticate incoming INVITE first to make it take effect. You can verify the NOTIFY information for the provision, including check- sync, resync and reboot, but only when SIP NOTIFY authentication enabled first to make it take effect.
MOH	
Upload Local MOH Audio File	Loads the MOH (Music on Hold) file to the phone. Click on "Browse" button to upload the music file from local PC. The MOH audio file has to be in .wav or .mp3 format.

	Note: Please be patient while the audio file is being uploaded. It could take more than 3 minutes to finish the uploading especially the file size is large. The button will show as "Processing" during the uploading. Once done, it will show as "Browse" again. Click on "Save" on the bottom of the web page and "Apply" on the top of the web page to save the change.
Enable Local MOH	Plays local MOH file if the call is being hold by the phone. Users need to upload local MOH audio file. The default setting is "**No**".
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, Broadsoft, China Mobile, ZTE IMS, Mobotix, ZTE NGN, Huawei IMS, NEC or WorldStone depending on the server type. Default setting is "**Standard**".

Phone Settings Page Definitions

Phone Settings/General Settings

Basic Settings	
Local RTP Port	Defines local RTP port used to listen and transmit RTP packets. Valid range is 50040 – 65000. Default is **50040**.
Use Random Port	Forces the phone to use random ports for both SIP and RTP messages. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is "**No**". **Note:** This parameter must be set to "No" for Direct IP Calling to work.
Disable In-call DTMF Display	Disables the phone to omit displaying DTMF digits during call on the LCD screen. The default setting is "**No**".
Keep-alive Interval (s)	Specifies how often the phone will send a Binding Request packet to the SIP server in order to keep the "ping hole" on the NAT router to open. The valid range is from 10 to 160. The default setting is **20** seconds.
STUN Server	Specifies the IP address or the Domain name of the STUN (Simple Traversal of UDP for NAT) server. The phone will send STUN Binding Request packet to the STUN server to learn the public IP address of its network. STUN resolution results are displayed in the status page of the phone Web GUI. Only non-symmetric NAT routers work with STUN. Default is "**stun.ipvideotalk.com**".

Use NAT IP	Configures the IP address for the Contact header and Connection Information in the SIP/SDP message. It should ONLY be used if it's required by your ITSP. The default setting is keep the box blank.

Guest Features	
Guest Settings	
Guest Login	Enable/disable guest login. Users should configure SIP domain name when using this function. Users should input SIP username and password on LCD. **Note:** A reboot is required for this setting to take effect.
Guest Login PIN Code	When set "Guest Login" option to "Yes" and "Expire" on the guest login page through LCD to "Always", users should input the PIN code to login.
SIP Domain	
Server Alias	The server alias is used to customize the server name.
Server List	The server list consists all the domain names or IP addresses of the SIP servers under the selected sever alias. The registration priority of addresses in the list is from top to bottom and supports up to 2 SIP domains per alias.

Phone Settings/Call Settings

Call Features	
Disable Call-Waiting	Disables the call waiting feature. If it is checked, the phone will reject the second incoming call during an active session without user's knowledge. But this missed call record will be saved to remind users. The default setting is "**No**".
Disable Call-Waiting Tone	Sets the phone to play the call waiting tone if there is another incoming call. If it is set to "Yes", the phone will only display the indicator on the LCD screen for another incoming call. The default setting is "**No**".
Disable DND Reminder Ring	Configures the phone to play the DND reminder ringtone for the incoming call if the DND feature is enabled. If it set to "Yes", the phone will keep mute instead of playing a ring splash to indicate an incoming call when DND is enabled. The default setting is "**No**".
Disable Transfer	Disables the transfer feature. When set to "Yes", the phone will block the TRANSFER key on the LCD screen. The default setting is "**No**".
Hold Call Before Completing Transfer	When set to "Yes" the phone holds the second call before completing the attended transfer (it sends the INVITE method to hold the call before sending the REFER method). The default setting is "**Yes**".

Disable Conference	Disables the conference. When set to "Yes", the phone will block the conference function. The default setting is "**No**".
Auto Mute on Entry	Configures whether to mute the call on entry automatically. • If set to "**Disable**", then do not use auto mute function. • If set to "**Auto Mute on Outgoing Call**", then mute automatically when the other party answers the outgoing call. • If set to "**Auto Mute on Incoming Call**", then mute automatically when answers the incoming call. • If set to "**Mute on Incoming & Outgoing Call**", then mute automatically when the call gets through. **Note:** This function only take effect when the phone is switching from the idle status to call status. Users could click the Mute button on call interface to cancel the current mute status.
Use # as Dial Key	Allows users to configure the "#" key as the "Send" key. If set to "Yes", the "#" key will immediately dial out the input digits. In this case, this key is essentially equivalent to the "Send" key. If set to "No", the "#" key is treated as part of the dialed string. The default setting is "**Yes**".
Always Ring Speaker	Determines if the speaker will play the ringtone if the speaker channel is not set as default channel. If set to "Yes", the phone will force to play the ring speaker in speaker channel even if a headset is connected. The default setting is "**No**".
Offhook Auto Dial	Configures a User ID/Extension to dial up automatically after the offhook auto dial delay time ends when the phone is offhook or hands-free. The phone will use the first account to dial out by default.
Offhook Auto Dial Delay (s)	Defines the delay time of Offhook Timeout. Once configured Offhook Timeout, the phone will dial out automatically after the delay time ends. If not configured Offhook Timeout, there will be no delays and the phone will dial up the User ID/Extension automatically.
Offhook/Onhook Timeout (s)	If configured, the phone will exit the dial-up screen when timeout after off hook or on hook. The valid range is 10-60s.
Off-cradle Pickup	Enables offhook of handset when picked up from cradle.
On-cradle Hangup	Enables onhook of handset when repositioned on cradle.
Number Of Accounts The Virtual Account Group Register	Configures the number of concurrent registrations with the main server and standby server(s), each account supports 1 SIP main server and 4 standby server registration(s).

Filter Characters	Sets the characters for filter when dial out numbers. Multiple characters could be set. For example, if set to "[()-]", when dial (0571)-8800-8888, the character "()-" will be filtered and dial 057188008888 directly. The default setting is **[()-]**
Escape '#' as %23 in SIP URI	Determines which characters will be included in the SIP INVITE URI if end users input #. If it is set to "Yes", the phone will replace the # by %23. Otherwise, it will include # in the SIP INVITE message. The default setting is "**Yes**".

Phone Settings/Ring Tone

Auto Config CPT by Region	Configures whether to choose Call Progress Tone automatically by region. If set to "Yes", the phone will configure CPT (Call Progress Tone) according to different regions automatically. If set to "No", you can manual configure CPT parameters. The default setting is "**No**".
Call Progress Tones: •**Dial Tone** •**Second Dial Tone** •**Ring Back Tone** •**Busy Tone** •**Reorder Tone** •**Confirmation Tone** •**Call-Waiting Tone**	Configures 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. **Syntax**: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous ring, OFF should be zero. Otherwise it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported. Please refer to the document below to determine your local call progress tones: http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf
Call-Waiting Tone Gain	Adjusts the call waiting tone volume. Users can select "Low", "Medium" or "High". The default setting is "**Low**".
Default Ring Cadence	Defines the ring cadence for the phone. The default setting is: **c=2000/4000**.

Phone Settings/PTT/Multicast Settings

PTT	
Settings	
PTT multicast address	Defines PTT multicast address.

Port	Defines port number for PTT multicast address.
Emergency PTT/paging volume	Set default volume for PTT/paging when emergency channel/group is used.
Paging Config	
Group paging	Enable or disable group paging.
Default group	Defines default paging group. When pressing and holding the PTT button, paging will be initiated using the default group.
Priority group	Defines priority paging group. Paging received on priority group will take precedence over active paging on normal group.
Emergency group	Defines emergency group for paging. Emergency group has the highest priority. Paging using emergency group will take precedence over paging on priority or normal group. Please note paging to emergency group will not be rejected even when device has enabled DND.
Accept while busy	Defines whether to accept paging while device is in active call. If set to "No", device will ignore paging while in active call. If set to "Yes", while in active paging call, device will accept paging if it has the same priority; If device is in active SIP call, device will accept paging and put the SIP call on hold.
Caller ID	Set Caller ID displayed on the call interface during paging
Payload size (ms)	Set payload size for paging.
Audio codec	Selects the codec type for the paging call. The list includes: G.722, G.711, Opus.
Multicast settings	Defines paging group. Users can configure whether to use the group for transport, accept, join group and its label. Only available and joined group will be displayed in paging group list. If users need send or receive paging, "Transport" and "Accept" must be enabled for this group.
PTT Config	
PTT	Enable or disable PTT.
Default Channel	Defines default channel for PTT. When pressing and holding the PTT button, PTT will be initiated using the default channel.
Priority Channel	Defines priority channel for PTT. PTT received on priority channel will take precedence over active PTT on normal channel.

Emergency Channel	Defines emergency channel for PTT. Emergency channel has the highest priority. PTT using emergency channel will take precedence over PTT on priority or normal channel. Please note PTT to emergency channel will not be rejected even when device has enabled DND.
Accept while busy	Defines whether to accept PTT calls while device is in active call. If set to "No", device will ignore PTT calls while in active call. If set to "Yes", while in active PTT call, device will accept PTT if it has the same priority; If device is in active SIP call, device will accept PTT and put the SIP call on hold.
Caller ID	Set Caller ID displayed on the call interface during a PTT call.
Payload size (ms)	Set payload size for PTT.
Audio codec	Selects the codec type for the PTT call. The list includes: G.722, G.711, Opus.
Channel	Defines PTT channel. Users can configure whether to use the channel for "Available", "Transmit", "Subscribe" and "Join Channel" and its label. Only available and joined channel will be displayed in PTT channel list. If users need send or receive PTT, "Transmit" and "Available" must be enabled for this channel.

Multicast paging

Setting

Paging Barge	Sets the threshold of paging calls. If the paging call's priority is higher than the threshold, the existing call will be hold and the paging call will be answered. Otherwise, the existing call does not be affected. If it is set to Disable, any paging call will not be answered. The default setting is "**Disable**".
Paging Priority Active	Determines if a new paging call whose priority is higher than the existing paging call will be answered. If it is checked, this feature will be enabled. The default setting is disabled.
Multicast Paging Codec	Selects the codec type for the multicast paging call. The list includes: PCMU, PCMA, G.722, G.726-32, G.729A/B, iLBC, Opus. The default setting is "**PCMU**".

Paging Config

Multicast Paging	Enable or disable multicast paging.
Multicast Paging Address	Set multicast paging address for sending and receiving. This option requires reboot to take effect. Valid range is from 224.0.0.0 to239.255.255.255.

Network Settings Page Definitions

Network Settings/Wi-Fi Settings

Wi-Fi Basics	
Wi-Fi Function	Enables/disables the Wi-Fi feature. The default setting is "Disable".
ESSID	Allows to scan and select the available Wi-Fi networks within the range if the Wi-Fi feature is enabled. Click on "Connect" to select the Wi-Fi network and connect to. The ESSID will be auto filled in the ESSID filed, users can also click on "Details" to have more details about the connected ESSID with its status, strength, speed, frequency and security mode.
Wi-Fi Security	
ESSID	Determines the ESSID of the default Wi-Fi network. The default password is "**wp!987@dmin**" and it uses WPA2PSK security access.
Password	Determines the password for the default wp_matser ap Wi-Fi network.
Security Mode for Hidden SSID	Defines the security mode used for the wireless network when the SSID is hidden. Supported modes are: WEP, WPA/WPA2 PSK or 802.1x EAP. The default setting is "**None**".
Advanced Settings	
Layer 2 QoS 802.1p Priority Value (Wi-Fi)	Assigns the priority value of the Layer 2 QoS packets for Wi-Fi. The default value is **0**.
Country Code	Configures Wi-Fi country code. The default value is "**United States of America**". **Note:** Reboot is requested to take effect.
Host Name (Option 12)	Specifies the name of the client. This field is optional but may be required by some Internet Service Providers.
Vendor Class ID (Option 60)	Used by clients and servers to exchange vendor class ID.

Network Settings/OpenVPN® Settings

Enable OpenVPN®	Enables/disables OpenVPN® functionality and requires the user to have access to an OpenVPN® server. **Note**: To use OpenVPN® functionalities, users must enable OpenVPN® and configure all of the settings related to OpenVPN®, including server address, port, OpenVPN® CA, certificate and key. Additionally, the user must also set the SIP

	account to use "VPN" for the "Nat Traversal" (under Account → Network Settings). The default setting is **No**.
OpenVPN® Server Address	Defines the URL/IP address for the OpenVPN® server.
OpenVPN® Port	Defines the network port for the OpenVPN® server. The default setting is **1194**.
OpenVPN® Transport	Determines network protocol used for OpenVPN® (UDP or TCP). The default setting is **TCP**.
OpenVPN® CA	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Client Certificate	OpenVPN® CA file (ca.crt) required by the OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Client Key	OpenVPN® Client key (*.key) required by OpenVPN® server for authentication purposes. Press "Upload" to upload the corresponding file to the device.
OpenVPN® Cipher Method	The cipher method of OpenVPN®, must be the same cipher method used by the OpenVPN® server. Supported methods are: Blowfish, AES-128, AES-256 and Triple-DES.
OpenVPN® Username	Configures the OpenVPN® authentication username (optional).
OpenVPN® Password	Configures the OpenVPN® authentication password (optional).

Network Settings/Advanced Network Settings

Alternate DNS Server	Defines the secondary DNS IP address if the static IP is used
Second Alternate DNS Server	Configures the secondary alternate DNS IP address to failover during both: the default DNS server and alternate DNS server's outage.
Layer 3 QoS for SIP	Defines the Layer 3 packet's QoS parameter for SIP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is **26** which is equivalent to the DSCP name constant CS6.
Layer 3 QoS for Audio	Defines the Layer 3 packet's QoS parameter for RTP messages in decimal pattern. This value is used for IP Precedence, Diff-Serv or MPLS. The default setting is **46** which is equivalent to the DSCP name constant CS6.

HTTP/HTTPS User-Agent	Sets the user-agent for HTTP/HTTPs Request.
SIP User-Agent	Sets the user-agent for SIP. The default setting is **Grandstream WP820 $version** (where $version is replaced by firmware version loaded to the phone).
Proxy	
HTTP/HTTPS Proxy Hostname	Specifies the HTTP/HTTPS proxy hostname for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTP/HTTPS Proxy Port	Specifies the HTTP/HTTPS proxy port for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Bypass Proxy For	Defines the destination IP address where no proxy server is needed. The phone will not use a proxy server when sending packets to the specified destination IP address.

System Settings Page Definitions

System Settings/Time and Language

Time Settings	
Assign NTP Server Address	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. The default setting is **pool.ntp.org**
DHCP Option 42 Override NTP Server	Obtains NTP server address from a DHCP server using DHCP Option 42; it will override configured NTP Server. If set to "No", the phone will use configured NTP server to synchronize time and date even if an NTP server is provided by DHCP server. The default setting is enabled. **Note:** Reboot is required to take effect.
DHCP Option 2 to Override Time Zone Setting	Obtains time zone setting (offset) from a DHCP server using DHCP Option 2; it will override selected time zone. If set to "No", the phone will use selected time zone even if provided by DHCP server. The default setting is enabled. **Note:** Reboot is required to take effect.
Time Zone	Specifies the local time zone for the phone. It covers the global time zones and user can selected the specific one from the drop-down list.
Time Display Format	Specifies which format will be used to display the time. It can be selected from 12-hour and 24-hour format.

Date Display Format	Determines which format will be used to display the date. It can be selected from the drop-down list. • **Normal (M/DD/YYYY)**: 1/31/2018 • **YYYY/MM/DD**: 2018/01/31 • **MM/DD/YYYY**: 01/31/2018 • **DD/MM/YYYY**: 31/01/2018 The default setting is **DD/MM/YYYY**.
Language	
Language	Selects the language displayed on the phone from drop-down list. User can select "Custom Language" and upload language file.

System Settings/Security Settings

Web/SSH Access	
Disable SSH	Disables SSH access to the phone. The default setting is **No**.
Access Method	Determines which protocol will be used to access the phone 's Web GUI. It can be selected from HTTP and HTTPS. The default setting is **HTTP**.
Port	Specifies which port to use to access the phone Web UI. By default, if HTTP, the port number will be **80**; if HTTPS is selected, the port number will be **443**.
Configuration via Keypad Menu	Configures the access control for the users to configure from keypad Menu. There are four different options: • **Unrestricted:** All the options can be accessed in keypad Menu. • **Basic settings only:** The Advanced Settings option will not be available in LCD Menu. • **Basic settings & Network settings:** Only basic settings and network settings can be available in LCD Menu. • **Constraint Mode:** The phone will require administration password to change Wireless & network and Advanced Settings. The default setting is "**Unrestricted**".
User Info Management	
Current Admin Password	Enters current logged-in user's password. This field is case sensitive.

New Admin Password	Allows the user to change the admin password. The password field is purposely blank after clicking the "Save" button for security purpose. This field is case sensitive with a maximum length of 32 characters.
Confirm New Admin Password	Enters the new Admin password again to confirm.
New User Password	Allows the administrator to set the password for user-level web GUI access. This field is case sensitive with a maximum length of 32 characters.
Confirm New User Password	Enters the new user password again to confirm.
SIP TLS	
SIP TLS Certificate	Specifies SSL certificate used for SIP over TLS in X.509 format. The phone has built-in private key and SSL certificate.
SIP TLS Private Key	Specifies SSL certificate key used for SIP over TLS in X.509 format. The phone has built-in private key and SSL certificate.
SIP TLS Private Key Password	Specifies SSL certificate key password used for SIP over TLS in X.509 format.
Certificate Management	
CA Certificate	
Import Trusted CA Certificates	Allows to upload the CA Certificate file to phone.
Trusted CA Certificates	Lists trusted CA certificates previously uploaded. Administrator can delete a certificate from here.
User Certificate	
Add Certificate	Allows to upload & Install User Certificate file to phone.
Certificate Application	Specifies on which application, the user certificate will be applied. Administrator can select either "VPN and other applications" or "Wi-Fi".
Select Certificate	Browse your computer and upload the user certificate.
Certificate Name	Enter a name to identify the user certificate.

Custom Certificate	
Import Custom Certificates	Allows to upload the Custom Certificate file to phone.
Custom Certificate	Lists Custom certificates previously uploaded. Administrator can delete a certificate from here.

System Settings/Preferences

LED Management	
Disable Missed Call Indicator	Turns off the LCD backlight when there are new missed call logs on the phone. If it set to "Yes", the LCD backlight will be turned off if the phone has new missed call log. Otherwise, the LCD backlight will keep on. The default setting is "**No**".
Disable MWI Indicator	Turns on the LED indicator at device's upper right corner when there are unread Voice Mails. If it set to "Yes", the LED indicator will keep off if the phone receives SIP NOTIFY message about unread voice mail. Otherwise, the LED indicator will be turned on. The default setting is "**No**".
Disable New Message Indicator	Turns on the LED indicator at device's upper right corner when there are unread Messages. If it set to "Yes", the LED indicator will keep off if the phone has new messages. Otherwise, the LED indicator will be turned on. Default setting is "**No**".
Enable Keypad Backlight	If set to "Yes", the backlight will light up when the button is pressed. Default setting is "**No**".

System Settings/TR-069

Enable TR-069	Sets the phone to enable the "CPE WAN Management Protocol" (TR-069). The default setting is "No".
ACS URL	Specifies URL of TR-069 ACS (e.g., http://acs.mycompany.com), or IP address.
ACS Username	Enters username to authenticate to ACS.
ACS Password	Enters password to authenticate to ACS.
Periodic Inform Enable	Sends periodic inform packets to ACS. The default setting is "**No**".
Periodic Inform Interval (s)	Configures to sends periodic "Inform" packets to ACS based on specified interval. The default setting is **86400**.

Connection Request Username	Enters user name for the ACS to connect to the phone.
Connection Request Password	Enters password for the ACS to connect to the phone.
Connection Request Port	Enters the port for the ACS to connect to the phone.
CPE Cert File	Uploads Cert File for the phone to connect to the ACS via SSL.
CPE Cert Key	Uploads Cert Key for the phone to connect to the ACS via SSL.

Maintenance Page Definitions

Maintenance/Upgrade

Firmware	
Complete Upgrade	If enabled, all files will be replaced except user data. Default is disabled.
Upload Firmware File to Update	Allows users to load the local firmware to the phone to update the firmware.
Firmware Upgrade Mode	Allows users to choose the firmware upgrade method: TFTP, HTTP, HTTPS or Manual Upload. The default setting is "**HTTPS**".
Firmware Server Path	Sets IP address or domain name of firmware server. The URL of the server that hosts the firmware release. Default is "**fm.grandstream.com/gs**".
HTTP/HTTPS User Name	Enters the user name for the firmware HTTP/HTTPS server.
HTTP/HTTPS Password	Enters the password for the firmware HTTP/HTTPS server.
Firmware File Prefix	Checks if firmware file is with matching prefix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
Firmware File Postfix	Checks if firmware file is with matching postfix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.

Firmware Upgrade	Click the **"Upgrade"** button to check whether the firmware in the firmware server has an updated version, if so, update immediately.

Config File	

Config File	
Use Grandstream GAPS	Configures the download path and update mode for the configuration file server. • If set to "**Yes**", the device will set the download path of the configuration file to "fm.grandstream.com/gs" by default and use HTTPS protocol to connect to the server. • If set to "**No**", then users can manually configure the path and update mode for the configuration file server. The default setting is "**Yes**".
HTTP/HTTPS User Name	Configures the user name for the config HTTP/HTTPS server.
HTTP/HTTPS Password	Configures the password for the config HTTP/HTTPS server.
Always send HTTP Basic Authentication Information	Includes configured user name and password in HTTP request before receiving authentication challenge from the server. The default setting is "**No**".
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	Sets the phone to authenticate configuration file before applying it. When set to "Yes", the configuration file must include value P1 with phone's administration password. If it is missed or does not match the password, the phone will not apply it. The default setting is "**No**".
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file is using OpenSSL.
Download Device Configuration	Downloads the phone's configuration file in text format. The config file includes all the P value parameters for phone's current settings except password for security purpose. Users can use the Grandstream configuration file generator to generate binary config file from this text file.

Upload Device Configuration	Uploads configuration file "cfgMAC.xml" or "cfgwp820.xml" to the phone. **Note:** Reboot is required to take effect.

Provision

Automatic Upgrade

Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options: **No**: The phone will only do upgrade once at boot up. **Check every day**: User needs to specify "Hour of the day (0-23)". **Check every week**: User needs to specify "Hour of the day (0-23)" and "Day of the week (0-6)". **Check at a period Time:** User needs to specify "Hour of the day (0-23)" **Note**: Day of week is starting from Sunday. The default setting is "**No**".
Firmware Upgrade and Provisioning	Defines the phone's rules for automatic upgrade. It can be selected from: - Always Check at bootup. - Always Check at bootup, when Firmware/Config pre/suffix changes. - Skip the Firmware Check. The default setting is "**Always Check at bootup**".
Upgrade without Prompt	If set to "Yes", the phone will automatically start upgrading after downloading the firmware file. Otherwise, users would need to confirm in the prompted message on the LCD screen to start upgrading process. The default setting is "**Yes**".

DHCP Option

Allow DHCP Option 43 and Option 66 to Override Server	Obtains configuration and upgrade server's information from DHCP server using options 66 and 43. **Note:** If DHCP Option 66 is enabled, the phone will attempt downloading the firmware file from the server URL provided by DHCP, even though **Config Server Path** is left blank. Default setting is "**Yes**".
DHCP Option 120 Override SIP Server	Configures the phone to allow the DHCP offer message to override the Config Server Path via the Option 120 header. The default setting is "**Yes**".
Allow DHCP Option 242 (Avaya IP Phones)	Enables DHCP Option 242. Once enabled, the phone will use the configuration info issued by the local DHCP in Option 242 to configure proxy, transport protocol and server path. The default setting is "**Yes**".

Advanced Settings

Disable SIP NOTIFY Authentication	Disables the SIP NOTIFY Authentication on the phone. If set to "Yes", the phone will not challenge NOTIFY with 401. The default setting is "**No**".

Validate Certification Chain	Configures whether to validate the server certificate when download the firmware/config file. If it is set to "Yes", the phone will download the firmware/config file only from the legitimate server. The default setting is "**No**".
mDNS Override Server	Sets the phone to broadcast the Multicast DNS (mDNS) message during booting up to allow itself to be discovered and be configured by the SIP platform. If it is set to "User Type A', the phone will broadcast the mDNS message "A_grandstream-cfg.local"; if it is set to "Use Type SRV", the mDNS message will be "SRV_grandstream-cfg.local". The default setting is "**Use Type A**".
Factory Reset	Resets the phone to the default factory setting mode.

Maintenance/System Diagnosis

Syslog	
Syslog Protocol	Select the transport protocol over which log messages will be carried. • **UDP:** Syslog messages will be sent over UDP. • **SSL/TLS:** Syslog messages will be sent securely over TLS connection. The default setting is "**UDP**".
Syslog Server	Configures the URI which the phone will send the syslog messages to. The default setting is "**log.ipvideotalk.com**".
Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet: • **DEBUG** (Sent or received SIP messages). • **INFO** (Product model/version on boot up, NAT related info, SIP message summary, Inbound and outbound calls, Registration status change, negotiated codec, Ethernet link up). • **WARNING** (SLIC chip exception). • **ERROR** (SLIC chip exception, Memory exception). **Note**: Changing syslog level does not require a reboot to take effect.
Send SIP Log	Configures whether to send the SIP log to the system log server. If check, users could filter display the obtained log file by setting up the filter condition: syslog.msg contains "sip log:" on Wireshark.

Syslog Keyword Filter	Only send the syslog with keyword, multiple keywords are separated by comma. Example: set the filter keyword to "SIP" to filter SIP log.
Logcat	
Clear Log	Clears the log files saved in the phone by pressing the clear button.
Log Tag	Configures the filter to display the specified process log file.
Log Priority	Selects the log priority to display. It can be selected from list below: • Verbose (Default Setting) • Debug • Info • Warn • Error • Fatal • Silent (suppress all output)
Get Log	Get the log files saved in the phone.
Debug	
One-click Debugging	
One-click Debugging	Captures the checked info in the debugging list, click "Start" to debug if including "Capture trace" item and click "Stop" to end, Click "Capture" in another situation. All retrieved files will be generated to a package, and the last package will be overwritten, while the trace file will stay remain.
Debug Info Menu	Displays a list of info items that can be debugged, currently supports system logs, info log, capture package, tombstones and ANR log. The captured data can be viewed in "Debug information list". The default is all selected.
Debug Info List	Selects the existing debugging info package or grab package. Click the "Delete" button on the right to delete the file.
View Debug Info	Click "list" to view the existing debugging info package or trace file. The captured files are sorted in chronological order, click to download the file to the computer for analysis.
Core Dump	
Enable Core Dump Generation	Configures whether to generate and save the core dump file when the program crashes. The default setting is "**No**".

Core Dump List	Selects the existing core dump file in the drop-down box. Users could delete the file by pressing on "Delete" button.
View Core Dump	Press "List" button to view all existing core dump files. The files are listed in chronological order, users could click the file name to download the file to the local computer.
Record	
Record	Click to start capturing audio data, click the "Stop" button to end. To capture the audio data of the device can help to locate audio issues. The default is not enabled. You can record up to 1-minute audio data.
Recording List	Choose the existing audio file. Click the "Delete" button on the right to delete this file.
View Recording	Click on the "List" button to view. The captured audio data will be sorted by time. Click to download the data to the computer for analysis. Users can also delete files under this folder.
Screenshot	
Screenshot	Click the screenshot to capture and save the current phone screen image.
Screenshot List	Selects the existing screenshot file and click the "Delete" button on the right to delete the file.
View Screenshot	Click the "List" button to view the existing screenshot file. Click the file name to open or save the screenshot to the computer.
Traceroute	
Target Host	Configures the IP address or URL for the Target Host of the Traceroute. Press Start to send traceroute request to configured target host. Press Stop to end traceroute running process.

Maintenance/Event Notification

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

1. The IP address of the destination server needs to be added at the beginning. The server address and dynamic variables needs to be separated with a "/".

---

2. The dynamic variables need to have a "$" at the beginning. For example: *local=$local*

3. If users need to add multiple dynamic variables in the same event, users could use "&" to connect with different dynamic variables.

   For example : *192.168.40.207/mac=$mac&local=$local*

   When the corresponding event occurs on the phone, the phone will send the MAC address and phone number to server address 192.168.40.207.

Here below the supported events by the phone:

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

Here below list of supported dynamic variables:

$phone_ip	The IP address of the phone.
$mac	The MAC address of the phone.
$product	The product name of the phone.
$program_version	The software version of the phone.
$hardware_version	The hardware version of the phone.
$language	The display language of the phone.
$local	The called number on the phone.
$display_local	The display name of the called number on the phone.
$remote	The call number on the remote phone.
$display_remote	The display name of the call number on the remote phone.
$active_user	The account number during a call on the phone.

Application Page Definitions

Application/Contacts

General Settings	
Sort Phonebook by	Sets which part of name, first name or last name, will be sorted in alphabetical order to display. The default setting is "**Last Name**".
Import/Export Contacts	
Import	
Clear the Old List	Determines if the phone will delete the previous contacts before downloading the new contact file. The default setting is "**No**".
Clear Old History Mode	• If set to "**Clear all**", the phone will delete all previous records before importing the new records. • If set to "**Keep Local Contacts**", the new-added local new contacts will not be deleted when importing new records. The default setting is "**Clear all**".

Replace Duplicate Items	Configures the phone to keep the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the phone will replace the original entries to the new one. Otherwise, the phone will save both contact entries. The default setting is "**No**".
Replace Duplicate Entries Mode	• If set to "**Replace by name**", replace the records of the same name automatically when importing new records. • If set to "**Replace by number**", replace the records of the same number automatically when importing new records. The default setting is "**Replace by name**".
File Encoding	Specifies the encoding format for phonebook file importing. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR The default setting is "**UTF-8**".
File Type	Sets the type format for phonebook file importing. It can be selected from the dropdown list. • **XML** • **vCard** The default setting is "**XML**".
Import Local File	Uploads the contact file from PC to the phone.
Export	
File Encoding	Specifies the encoding format for phonebook file exporting. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16

	UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR The default setting is "**UTF-8**".

File Type	Sets the type format for phonebook file importing. It can be selected from the dropdown list.
	
	    • **XML**
	    • **vCard**
	The default setting is "**XML**".

Export	Downloads the phonebook file from the phone to PC.
Download Contacts	
Clear The Old List	Determines if the phone will delete the previous contacts before downloading the new contact file. The default setting is "**No**".
Clear Old History Mode	• If set to "**Clear all**", the phone will delete all previous records before downloading the new records. • If set to "**Keep Local Contacts**", the new-added local new contacts will not be deleted when downloading new records. The default setting is "**Clear all**".
Replace Duplicate Items	Configures the phone to keep the original contact entries when duplicated contact entries are included in the contact file. If set to "Yes", the phone will replace the original entries to the new one. Otherwise, the phone will save both contact entries. The default setting is "**No**".
Replace Duplicate Entries Mode	• If set to "**Replace by name**", replace the records of the same name automatically when downloading new records. • If set to "**Replace by number**", replace the records of the same number automatically when downloading new records. The default setting is "**Replace by name**".

Download Mode	Enables the phone to download phonebook file and select the server and protocol to download the phonebook file. It can be selected from TFTP, HTTP, and HTTPS. The default setting is "**OFF**".
File Encoding	Selects the encoding format for phonebook file download. It can be selected from the dropdown list: • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR The default setting is "**UTF-8**".
Download Server	Configures the server URL to download the phonebook file. The phone will send a request to the server to download the phonebook file with filename ***phonebook.xml***.
HTTP/HTTPS User Name	Configures user name for HTTP/HTTPS server to download the phonebook file.
HTTP/HTTPS Password	Specifies password for HTTP/HTTPS server to download phonebook file.
Automatic Download Interval	Determines how the phone to send the request to the server to download the phonebook file. It can be selected from the dropdown list: • None • 2 Hour • 4 Hour • 6 Hour • 8 Hour • 12 Hour
Download Now	Starts downloading the XML phonebook to the phone immediately.

Application/Recording

Call Record	
Call Record	Lists the call recordings files with their name, duration, date and operation.

Value-added Service Page Definitions

Value-added Service/GDS Settings

GDS Name	Specifies the name to identify the GDS3710. It displays info on LCD when incoming call matched with GDS number, used to identification door position, e.g: "east gate" or "3rd floor gate". **Note**: The WP820 supports up 10 GDS items.
GDS Number	Specifies the GDS number which is the SIP user ID configured on GDS3710 or the IP address of the GDS3710 itself, if the GDS3710 is using IP call. It enables to show open door button when caller number or IP address matches with this setting. e.g:"36311" or "192.168.124.81"
GDS Password	Determines the GDS password which should match the one configured on "Remote PIN to Open the Door" field on GDS3710 settings.

UPGRADING AND PROVISIONING

The WP820 can be upgraded via TFTP/HTTP/HTTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP or HTTPS; the server name can be FQDN or IP address.

Examples of valid URLs:

firmware.grandstream.com/BETA

fw.mycompany.com

Upgrade and Provisioning Configuration

There are two ways to setup upgrade and provisioning on WP820. They are Keypad Menu and Web GUI.

Configure via keypad Menu

1. In WP820 Settings, select **Advanced Settings → System Upgrade**.

2. Navigate to **Firmware** and configure the firmware upgrade and config settings.
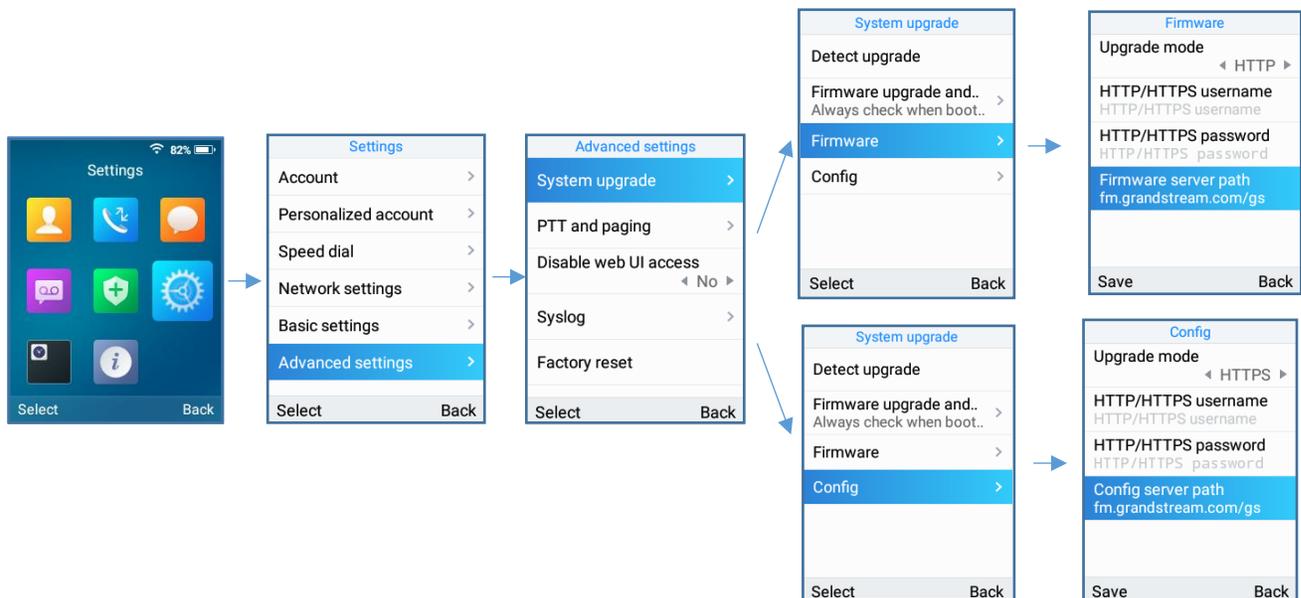
Figure 12: WP820 Upgrade Configuration via Keypad Menu

Configure via Web GUI

Open a web browser on PC and enter the IP address for the WP820. Then login with the administrator username and password. Go to **Maintenance → Upgrade → Firmware**. In the Upgrade web page, enter the IP address or the FQDN for the upgrade server and choose to upgrade via TFTP, HTTP or HTTPS (The default setting is HTTPS). Save and apply the changes, press **Upgrade** button or reboot the phone to initiate firmware upgrade process.
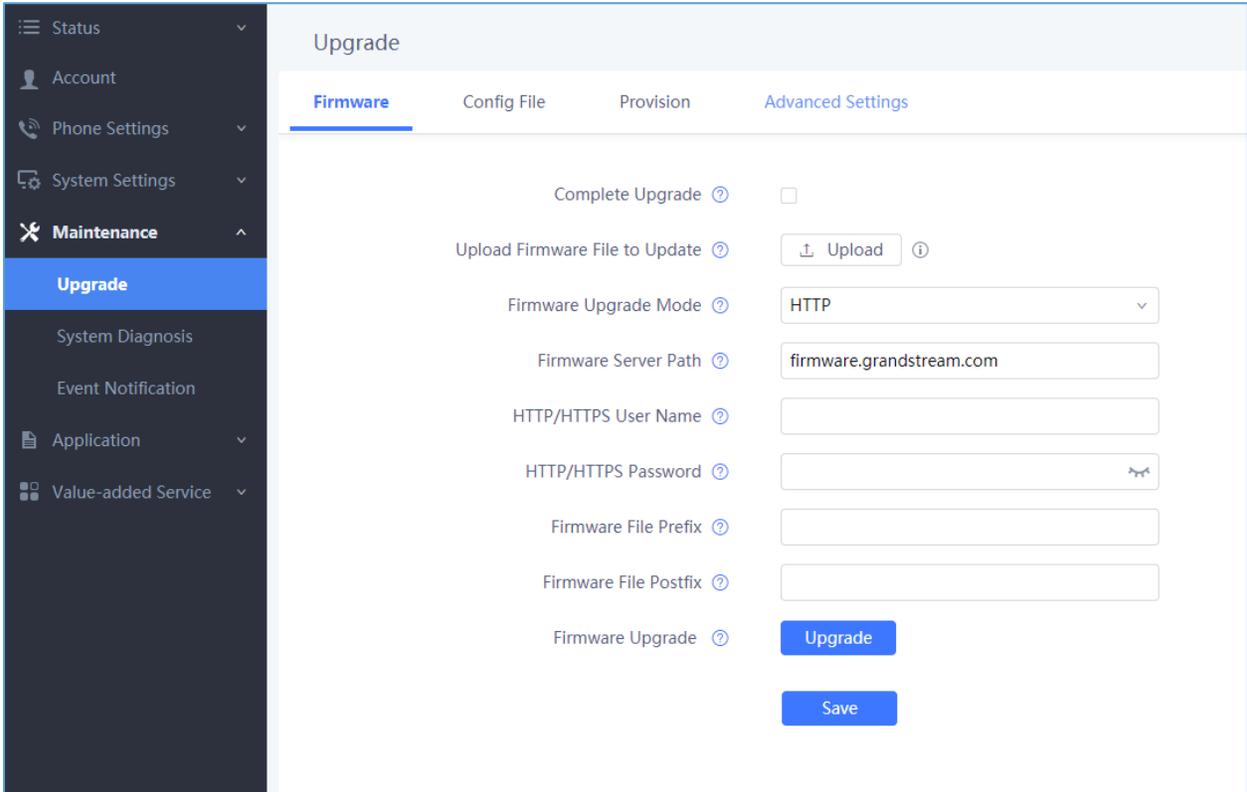

Figure 13: WP820 Upgrade Configuration via Web GUI

⚠ **Note:** Please do not power off or unplug the WP820 when the upgrading process is on.

Upload Firmware Locally

If there is no HTTP/TFTP server, users could also upload the firmware to the WP820 directly via Web GUI. Please follow the steps below to upload firmware to WP820 locally.

1. Download the latest WP820 firmware file from the following link and save it in your PC.

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

2. Log in the Web GUI as administrator in the PC.

3. Go to Web GUI→**Maintenance**→**Upgrade**→**Firmware**.

4. Click the "Upload" button, a window will be prompted to select firmware file to upload.

5. Select the firmware file from your PC. Then uploading progress will show at the button where it was "Upload" in the above step.

6. When uploading is done, users can see the upgrading process starts on the WP820 LCD.

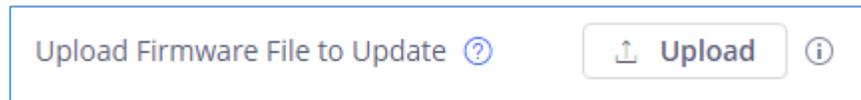7. The phone will reboot again with the new firmware version upgraded.

Figure 14: Upload Firmware File to Update

No Local Firmware Servers

Service providers should maintain their own firmware upgrade servers. For users who do not have a TFTP/HTTP/HTTPS server, some free Windows version TFTP servers are available for download from: http://www.solarwinds.com/free-tools/free-tftp-server and http://www.tftpd64.com/
Please check our web site at http://www.grandstream.com/support/firmware for latest firmware.

Instructions for local firmware upgrade via TFTP:

1. Unzip the firmware files and put all of them in the root directory of the TFTP server;

2. Connect the PC running the TFTP server and the WP820 device to the same LAN segment;

3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade;

4. Start the TFTP server and configure the TFTP server in the phone's web configuration interface;

5. Configure the Firmware Server Path on your WP820 to the IP address of the PC;

6. Update the changes and reboot the WP820.

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

Firmware Upgrade via USB

For users that could not use remote upgrade or could not access the phone's Web GUI to upload firmware, upgrading via external USB flash drive is an alternative. Follow the steps below to upgrade the WP820 via USB:

1. Download the firmware file to PC and save it in the USB flash drive
2. Insert the USB flash drive to the WP820.
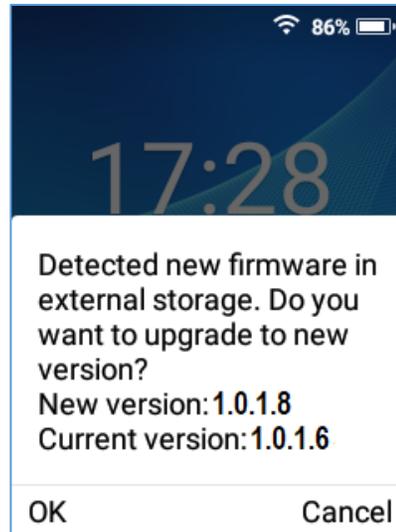3. Power cycle the WP820 and wait for the device to detect the firmware.

Figure 15: New Firmware Detected

4. Press Ok to start the upgrade.

Note: The USB flash drive should be on **FAT32** format and the firmware file should be necessarily named **wp820fw.bin**

Provisioning and Configuration File Download

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

A configuration parameter is associated with each field in the web configuration page. A parameter consists of a Capital letter P and 1 to 5 (could be extended to more in the future) digit numeric numbers. i.e., P2 is associated with the "Admin Password" in the Web GUI→**System Settings**→**Security Settings**→**User Info Management** page. For a detailed parameter list, please refer to the corresponding firmware release configuration template in the following link:
http://www.grandstream.com/support/tools

When the WP820 boots up, it will issue TFTP or HTTP(S) request to download a configuration XML file named "cfgxxxxxxxxxxxx" followed by "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If downloading "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file. The configuration file name should be in lower case letters.

For more details on XML provisioning, please refer to the following document:
http://www.grandstream.com/sites/default/files/Resources/gs_provisioning_guide.pdf

FACTORY RESET

Restore to Factory Default via LCD Menu

⚠️ **Warning**:

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

There are two methods to restore the WP820 to the factory default settings.

1. On WP820 idle screen, go to **Settings → Advanced Settings → Factory reset**.

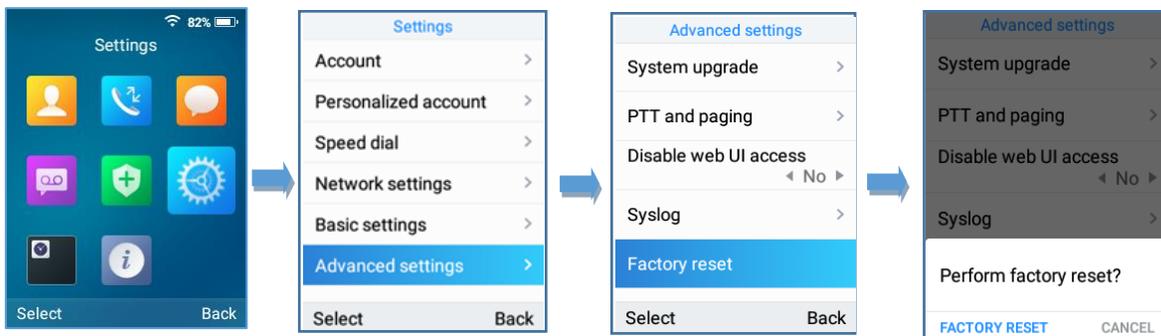2. In the new window, confirm the reset using the left softkey.

Figure 16: WP820 LCD - Confirm Factory Reset

3. Once confirming the reset the phone will reboot with the default factory settings.

Restore to Factory Default via the Web GUI

1. Login WP820 Web GUI and go to **Maintenance → Upgrade → Advanced Settings**;

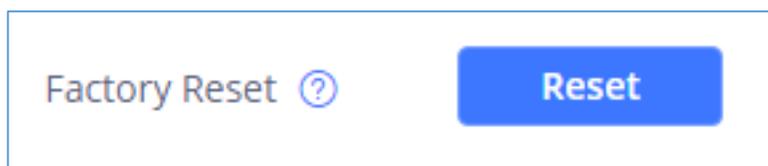2. At the bottom of the page, click on the **Reset** button for Factory reset.

Figure 17: WP820 Web GUI - Factory Reset

3. A dialog box will pop up to confirm factory reset.
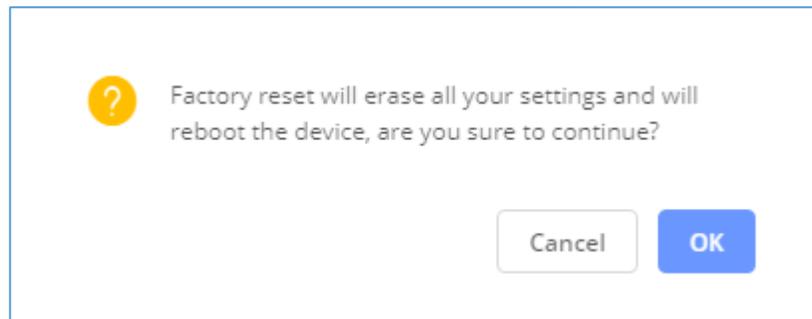
4. Click OK to restore the phone to factory settings.

> ? Factory reset will erase all your settings and will reboot the device, are you sure to continue?
>
> Cancel   OK

Figure 18: WP820 Web GUI - Confirm Factory Reset

Restore to Factory Default Using Hard Keys

To perform hard reset of the phone using keypad buttons please follow below steps:

1. Power cycle the WP820.

2. Press key **1** + key **9** immediately and hold it until the LCD shows the factory reset message

3. Release the buttons and the phone will boot up with the default settings.

EXPERIENCING WP820 ENTERPRISE PORTABLE WI-FI PHONE

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 Enterprise Portable Wi-Fi Phone, it will be sure to bring convenience and color to both your business and personal life.