

Grandstream Networks, Inc.

WP820

Enterprise Portable Wi-Fi Phone

Administration Guide



COPYRIGHT

©2021 Grandstream Networks, Inc. <https://www.grandstream.com/>

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

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

<https://www.grandstream.com/support>

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

CAUTION

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

WARNING

Please do not use a different power 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



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:
<https://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:

<https://blog.grandstream.com/faq/gnu-general-public-license/gnu-gpl-information-download>



Table of Contents

DOCUMENT PURPOSE	11
CHANGE LOG	12
Firmware version 1.0.7.30	12
Firmware version 1.0.7.26	12
Firmware Version 1.0.7.22	12
Firmware Version 1.0.7.15	12
Firmware Version 1.0.7.7	12
Firmware Version 1.0.5.5	13
Firmware Version 1.0.3.20	13
Firmware Version 1.0.3.6	14
Firmware Version 1.0.3.5	14
Firmware Version 1.0.1.15	15
Firmware Version 1.0.1.12	15
WELCOME	16
PRODUCT OVERVIEW	17
Feature Highlights	17
Technical Specifications	17
GETTING STARTED	19
Equipment Packaging	19
Setting up the WP820	20
<i>Charging Station</i>	20
<i>Handset</i>	20
<i>Battery Information</i>	21
WP820 Handset Keys Description	21
WP820 Icons Description	23
WP820 Handset Menu	24



Connecting WP820 to Wi-Fi Network	27
Obtain WP820 IP Address	28
WP820 WEB GUI ACCESS CONFIGURATION	29
Configuration via Web Browser	29
<i>Accessing the Web UI</i>	29
<i>Web GUI Languages</i>	30
<i>Saving the Configuration Changes</i>	30
Web UI Access Level Management	30
<i>Changing User Level Password</i>	30
<i>Changing Admin Level Password</i>	31
<i>Changing HTTP / HTTPS Web Access Port</i>	32
WP820 WEB GUI SETTINGS	34
Status Page Definitions	34
<i>Status/Account Status</i>	34
<i>Status/Network Status</i>	34
<i>Status/System Info</i>	35
Account/General Settings	36
<i>Account/SIP Settings</i>	38
<i>Status/System Info</i>	42
<i>Account/Codec Settings</i>	43
<i>Account/Call Settings</i>	47
<i>Account/Advanced Settings</i>	52
Phone Settings Page Definitions	54
<i>Phone Settings/General Settings</i>	54
<i>Phone Settings/Call Settings</i>	55
<i>Phone Settings/Ring Tone</i>	58
<i>Phone Settings/Video Settings</i>	58
<i>Phone Settings/PTT/Multicast Settings</i>	59
<i>Phone Settings/Wallpaper Setting</i>	62



Network Settings Page Definitions	62
<i>Network Settings/Bluetooth</i>	62
<i>Network Settings/Wi-Fi Settings</i>	63
<i>Network Settings/OpenVPN® Settings</i>	64
<i>Network Settings/Advanced Network Settings</i>	66
System Settings Page Definitions.....	67
<i>System Settings/Time and Language</i>	67
<i>System Settings/Security Settings</i>	68
<i>System Settings/Preferences</i>	70
<i>System Settings/TR-069</i>	73
Maintenance Page Definitions	74
<i>Maintenance/Upgrade</i>	74
<i>Maintenance/System Diagnosis</i>	77
<i>Maintenance/Event Notification</i>	80
Application Page Definitions	82
<i>Application/Contacts</i>	82
<i>Application/LDAP Book</i>	86
<i>Application/Recording</i>	87
<i>Application/Call History</i>	87
Value-added Service Page Definitions	88
<i>Door System</i>	88
<i>BroadSoft Directories</i>	88
<i>SAFE/Panic Call</i>	89
UPGRADING AND PROVISIONING	91
Upgrade and Provisioning Configuration	91
<i>Configure via keypad Menu</i>	91
<i>Configure via Web GUI</i>	92
Upload Firmware Locally	92
No Local Firmware Servers	93
Firmware Upgrade via USB	93



Config Provision via USB.....	94
Wi-Fi Provision via USB.....	94
Provisioning and Configuration File Download.....	95
FACTORY RESET	96
Restore to Factory Default via LCD Menu.....	96
Restore to Factory Default via the Web GUI	96
Restore to Factory Default using Hard Keys	97
EXPERIENCING WP820 ENTERPRISE PORTABLE WI-FI PHONE.....	98



Table of Tables

Table 1: WP820 Features at a Glance	17
Table 2: WP820 Technical Specifications	17
Table 3: Equipment Packaging	19
Table 4: WP820 Description.....	22
Table 5: WP820 Icons Description	23
Table 6: WP820 Menu Structure	26

Table of Figures

Figure 1: WP820 Package Content	19
Figure 2: Charging Station	20
Figure 3: WP820 Handset Setup	20
Figure 4: WP820 Description	22
Figure 5: WP820 Menu Structure	25
Figure 6 : Wi-Fi Settings.....	28
Figure 7: Obtaining IP Address	28
Figure 8: WP820 Web GUI Language	30
Figure 9: User Level Password	31
Figure 10: Admin Level Password	32
Figure 11: Web Access Port.....	33
Figure 12: WP820 Upgrade Configuration via Keypad Menu.....	91
Figure 13: WP820 Upgrade Configuration via Web GUI	92
Figure 14: Upload Firmware File to Update	93
Figure 15: New Firmware Detected	94
Figure 16: WP820 LCD - Confirm Factory Reset.....	96
Figure 17: WP820 Web GUI - Factory Reset.....	96
Figure 18: WP820 Web GUI - Confirm Factory Reset.....	97



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 <https://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 1.0.7.30

- Added ability to disable proximity sensor. [Enable Proximity Sensor]
- Added ability to disable multi-function button completely. [Multi-function Button]
- Added option to map a key to be used as LDAP search button. [Button Customization]
- Added IPv6 DUID info display in Web GUI. [IPv6 DUID]
- Added additional options to OpenVPN settings. [Network Settings/OpenVPN® Settings]
- Added ability to lock volume. [Lock Volume]
- Added ability to select which account to have DND enabled or disabled when pressing DND button. [DND Mode]
- Added call history on WP820 web UI. [Application/Call History]
- Added support for weak TLS cipher suites. [Enable Weak TLS Cipher Suites]

Firmware version 1.0.7.26

- Added Sensor calibration feature code *****2223***. [Sensor Calibration]

Firmware Version 1.0.7.22

- Added IPv6 Preferred DNS field to Web UI. [IPv6 Preferred DNS Server]
- Added Restrict Call Settings menu access and DND. [Constraint Mode]
- Added Ability to upload custom wallpaper by server path. [Wallpaper Source]

Firmware Version 1.0.7.15

- Added Feature Key Synchronization [Feature Key Synchronization]
- Added Berlin and Dublin into time zone list [Time Zone]
- Added 5G Wi-Fi channels [144-165] support for Netherlands [Channel Mode]
- Added Wi-Fi Security mode WPA enterprise (802.1x) to the Web GUI [Add Network]
- Added Language package download via provisioning [Config File]

Firmware Version 1.0.7.7

- Added configuration of Wi-Fi Signal Warning from web UI. [Network Settings/Wi-Fi Settings]
- Added timeout setting for web UI auto logout. [System Settings/Security Settings]
- Added support for Fallback to provisioning server path when DHCP Option 66 failed. [Provision]
- Added IPv4 and IPv6 configuration of Wi-Fi config. [Network Settings/Wi-Fi Settings]



- Added support initiating video call on WP820. [Phone Settings/Call Settings]
- Added option to enable In-call Recording.[Phone Settings/Call Settings]
- Added option “Default Video Zoom Area” from web UI. [Phone Settings/Call Settings]
- Added Broadsoft XSI support. [BroadSoft Directories]
- Added option "Minimum TLS version" and "Maximum TLS version". [TLS]
- Added option to randomly trigger the provision when “Automatic Upgrade” is enabled. [Provision]
- Added support to "Add MAC in User-Agent". [Account/SIP Settings]
- Added video preview ability with 3rd party door system. [Door System]
- Added Web UI editing of “Charging Tone”, “Low Battery Warning Tone”, “Silent Mode”, “Vibrate Mode”, “Voicemail notification tone”, “Ringtone Volume”, “Media Volume” and “Alarm Volume”. [System Settings/Preferences]
- Added option start Video automatically when making call. [Account/Call Settings]
- Added option to allow PTT Key Press When Lock Screen is enabled. [Phone Settings/PTT/Multicast Settings]
- Added web UI option for font size customization from Web UI. [LCD & LED Management]

Firmware Version 1.0.5.5

- Added export battery log. [Debug Info Menu]
- Added Bluetooth interface on web UI. [Bluetooth]
- Added Wi-Fi Channel Mode. [Channel Mode]
- Added custom wallpaper support on web UI. [Wallpaper Setting]
- Added OpenVPN mode. [OpenVPN® Mode]
- Added Wi-Fi provision via USB. [Wi-Fi Provision via USB]
- Added config file provision via USB. [Config Provision]
- Added action URL notify when SAFE Panic Alarm triggers. [Event Notification]
- Added web feature for lock screen. [Lock Screen Settings]

Firmware Version 1.0.3.20

- Added OpenVPN LZO Compression Switch. [Network Settings/OpenVPN® Settings]
- Add web upgrade error message. [Configure via Web GUI]
- Added ability to enable/disable SSH access without requiring reboot. [Web/SSH Access]
- Added "RTP Timeout (s)" feature. [RTP Settings]
- Added ability to disable web UI access. [Accessing the Web UI]
- Added Detect firmware upgrade option. [Maintenance/Upgrade]
- Added custom ringtone for door system. [Door System]
- Added LCD screen timeout and brightness. [System Settings/Preferences]
- Changed configuration item name 'Multicast Paging' to 'Multicast Paging Function'. [Phone Settings/PTT/Multicast Settings]
- Added SAFE/Panic 'Emergency Dial Force Speaker'. [SAFE/Panic Call].
- Added support for Rejected Call Notification feature. [Phone Settings/Call Settings]



- Added support to use \$product and \$mac for config provision files. [Config Provision]
- Added SIP NOTIFY support to synchronize phonebook. [Account/Advanced Settings]
- Added uaCSTA support. [Remote Control]
- Enabled ACS and ACS URL by default. [System Settings/TR-069]
- Added support for phonebook management in WEB UI. [Application/Contacts]
- Added support for GDMS to monitor and provision the WP820 via TR-069. [System Settings/TR-069]
- Updated factory reset using hard key interface when constraint mode enabled. [Restore to Factory Default using Hard Keys]
- Added more options for distinctive ring tone option. [Ring Tones]
- Added support for uploading a custom language file. [System Settings/Time and Language]
- Added subscribe expiration option. [Account/SIP Settings]
- Added support for factory reset to first unregister sip message without contact head. [FACTORY RESET]
- Updated SRTP icon to display only when signaling and media are both encrypted. [WP820 Icons Description]

Firmware Version 1.0.3.6

- Changed voicemail notification from “Ordinary” to “Normal”. [WP820 Icons Description]

Firmware Version 1.0.3.5

- Supported TLSv1.2. [Technical Specifications]
- Added ability to enable/disable P-Access-Network-Info Header. [Use P-Access-Network-Info Header]
- Added ability to enable/disable P-Emergency-Info Header. [Use P-Emergency-Info Header]
- Added Preferred Video Codec settings to receive/display video for SIP Calls. [Preferred Video Codec]
- Added option to disable Video Call to the WP820. [Enable Video Call]
- Added option to set the default Ringtone and notification tone. [Default Ringtone] [Notification Tone]
- Add option “Auto Config CPT by Region”. [Auto Config CPT by Region]
- Added support for Ringtone customization. [Upload Ringtone]
- Added Noise Shield feature to eliminate background noises during the call. [Enable noise Shield]
- Supported configuring IGMP Keep-alive Interval for PTT/paging function. [IGMP Keep-alive Interval]
- Supported 4 types of Internet Protocol: IPv4 only, IPv6 only, Both but prefer IPv4, Both but prefer IPv6. [Network Settings/Wi-Fi Settings]
- Added support for Wi-Fi bands: 2.4G, 5G, or Dial band. [Wi-Fi Band]
- Added configuration for Wi-Fi Roaming parameter. [Wi-Fi Roaming]
- Added customization for SSH Port. [SSH Port]
- Added support for custom certificate for provisioning. [Custom Certificate]
- Supported Gesture Control configuration. [Gesture Control]
- Supported customizing the top three softkeys. [Soft key]
- Added ability to customize the function of PTT button. [Multi-function Button]
- Added config provision options to control config file retrieval. [Config Provision]



- Supported PNP 3CX Auto-provision option. [PNP Feature]
- Supported pinging other devices/systems. [Ping]
- Supported “nsLookup” to obtain information about Domain Name or IP address. [NSLookup]
- Added more options for phonebook automatic download interval. [Download Contacts]
- Supported LDAP. [Application/LDAP Book]
- Added SAFE/Panic Call Settings. [SAFE/Panic Call]
- Improved WP820 Web UI for user-friendly purposes.

Firmware Version 1.0.1.15

- No major changes.

Firmware Version 1.0.1.12

- This is the initial version for WP820.



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

 <p>WP820</p>	<ul style="list-style-type: none"> • 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.
---	--

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, LDAP, TR-069, 802.1x, TLS, SRTP, IPv6
Voice Codecs and Capabilities	Support for G.711 μ /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
Wi-Fi	Yes, integrated dual-band Wi-Fi 802.11 a/b/g/n (2.4GHz & 5GHz)
Wi-Fi Encryption	WEP, WPA/WPA2, WPA Enterprise
Graphic Display	2.4-inch (240x320) TFT color LCD
Peripherals	3 soft keys, dial, hang up, speakerphone, phonebook, backlit keypad, proximity sensor, accelerator, vibration motor, volume button and navigation keys
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 1000 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	802.11e (WMM) 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 Humidity: 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
<ul style="list-style-type: none"> • 1x Handset unit • 1x Universal power supply 5V • 1x Charger cradle • 1x Belt clip • 1x Rechargeable battery • 1x Quick Installation Guide • 1x GPL Statement

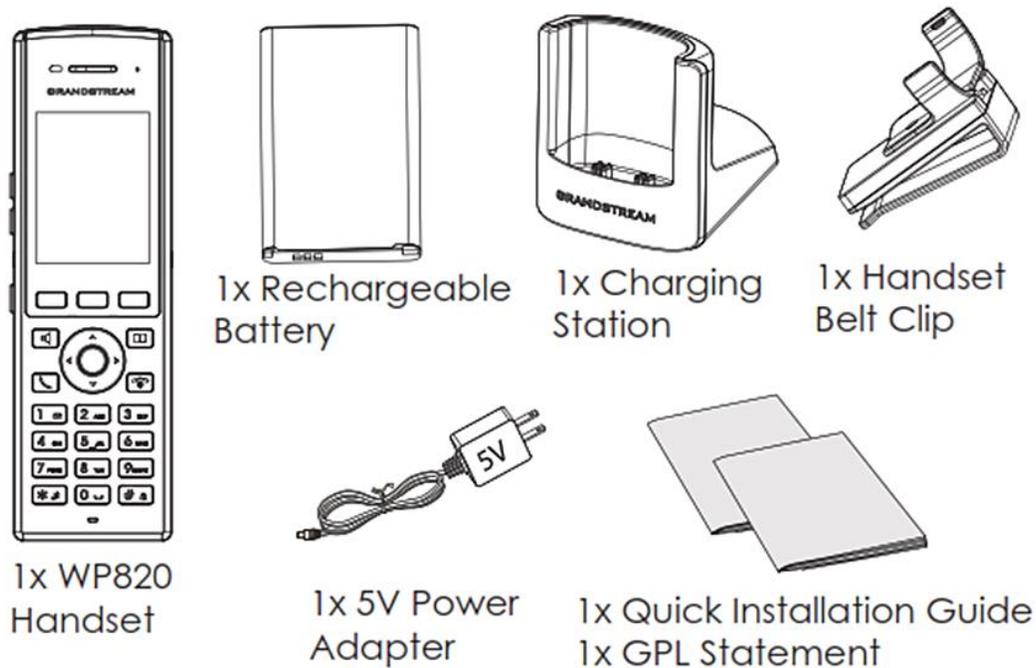


Figure 1: WP820 Package Content

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.

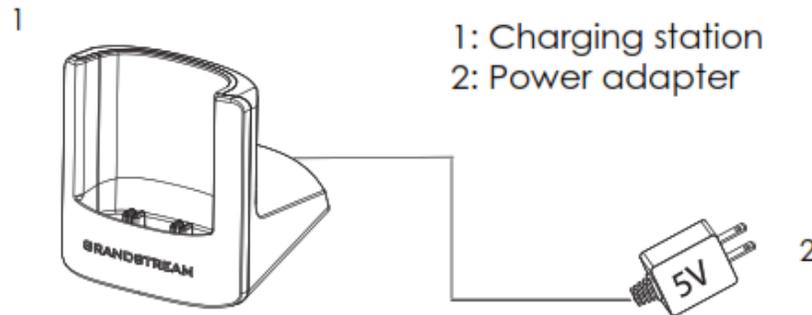


Figure 2: Charging Station

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](#).)

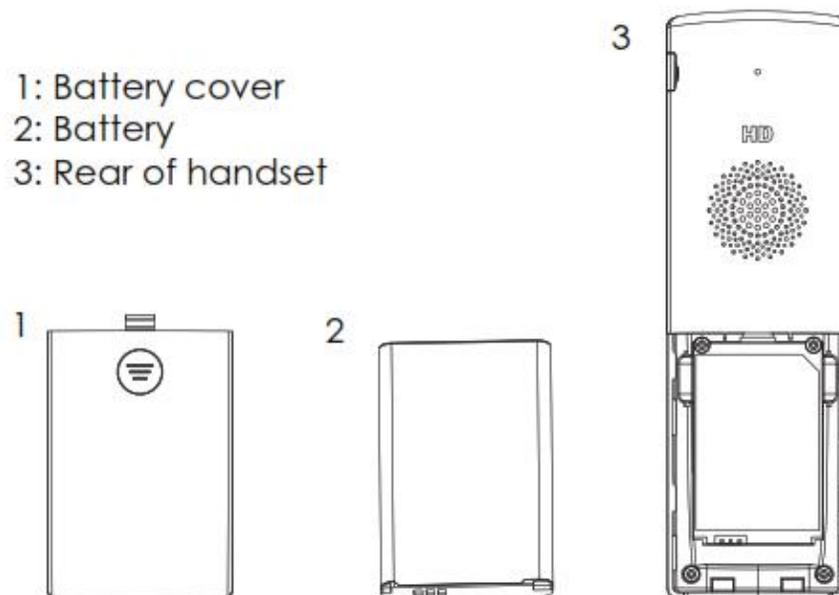


Figure 3: WP820 Handset Setup

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.



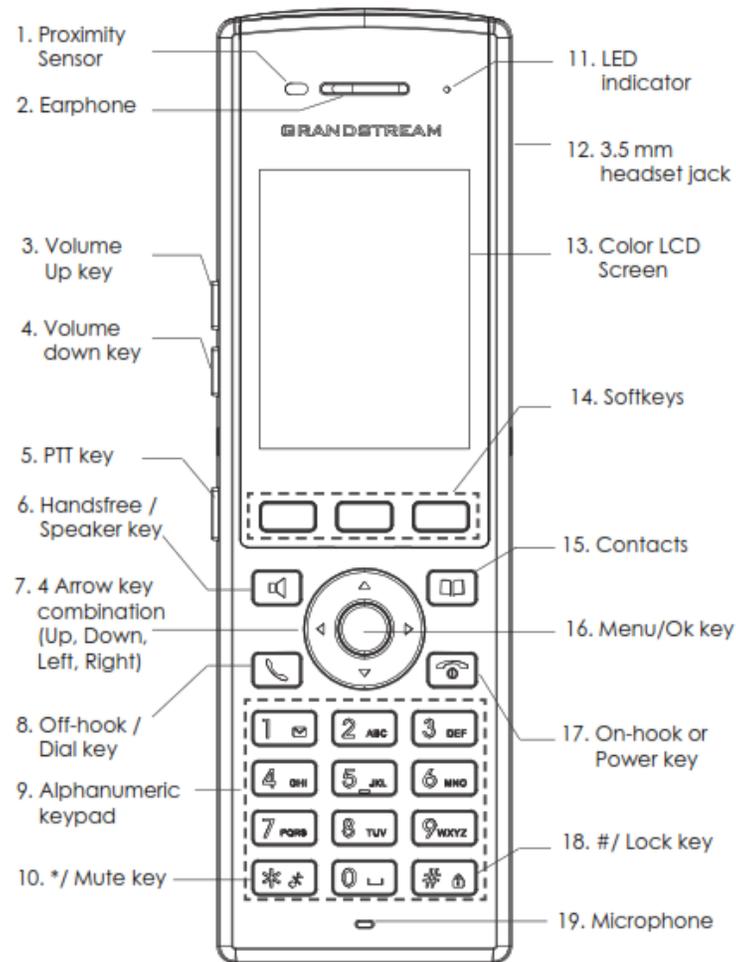


Figure 4: WP820 Description

The following table describe the WP820 keypad keys.

Table 4: WP820 Description

	Key	Description
1.	Proximity sensor	The proximity sensor 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. Note: PTT button can also be configured from Web GUI to have other functions such as: SAFE/Panic Call & Mute/Unmute during calls.
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	1 dual-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 #. <ul style="list-style-type: none"> • 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 (Normal)
	Mute enabled icon
	DND enabled icon
	Bluetooth enabled icon
	Bluetooth connected icon
	SRTP & TLS enabled icon
	Contacts
	SMS
	Call History
	Voice Mail
	Diagnostics
	Settings
	Applications
	Status
	Broadsoft XSI

Note: SRTP & TLS enabled icon will be displayed only in case signaling and media are both encrypted.

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.

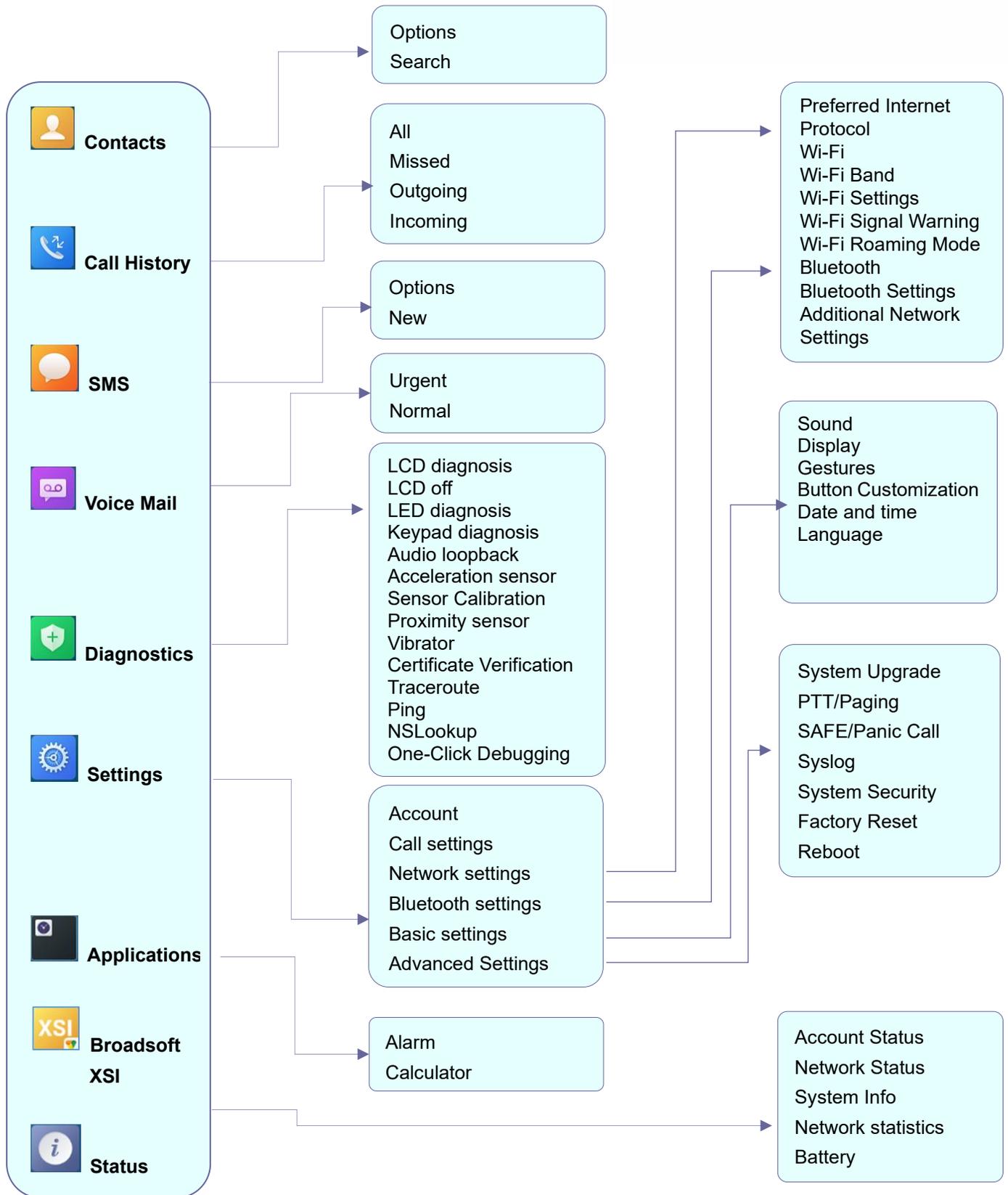


Figure 5: WP820 Menu Structure



Table 6: 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	<ul style="list-style-type: none"> • Play Message: Play voice mail messages received. • Set Voice Mail: Configure voice mail parameters.
Diagnostics	<ul style="list-style-type: none"> • LCD diagnosis • LCD off • LED diagnosis • Keypad diagnosis • Audio loopback • Acceleration sensor • Sensor Calibration • Proximity sensor • Vibrator • Certificate Verification • Traceroute • Ping • NSLookup • One-click Debugging
Settings	<ul style="list-style-type: none"> • Account Configure/View SIP accounts settings and account ringtone. • Call settings Configure the account auto answer, call forward, Proximity Sensor, DND and speed dial settings. • Network Settings Configure the networks settings including Wi-Fi settings, Bluetooth settings, and additional networks settings. • Bluetooth Settings Configure the Bluetooth settings including discovery, pairing and connection actions. • Basic Settings Configure the basic settings including voice settings, display settings, Gestures and button customization, language settings and date/time settings. • Advanced Settings



	Configure the advanced settings including system upgrade, PTT/Paging settings, system security settings, syslog settings and factory reset / reboot.
Applications	<ul style="list-style-type: none"> • Alarm Clock: Configures the alarm clock settings • Calculator: performs arithmetic operations on numbers.
Broadsoft XSI	<ul style="list-style-type: none"> • Broadsoft account.
Status	<p>Displays account status, system info, Network status and network statistics</p> <ul style="list-style-type: none"> • Account status. • System Info: Press to enter the sub menu for Running memory, Storage status, MAC address, 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. • Battery: Displays the battery status and the battery usage details.

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.



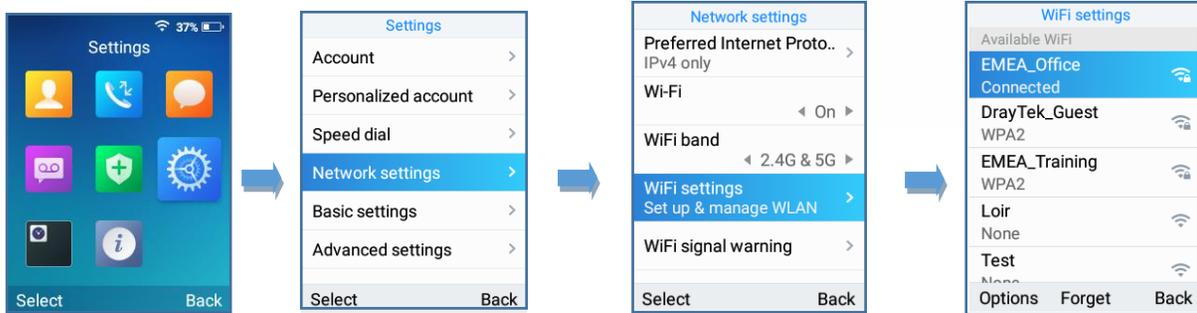


Figure 6 : Wi-Fi Settings

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. Users may also specify the Wi-Fi Band in order to fix it or to keep it Dual Band.

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.

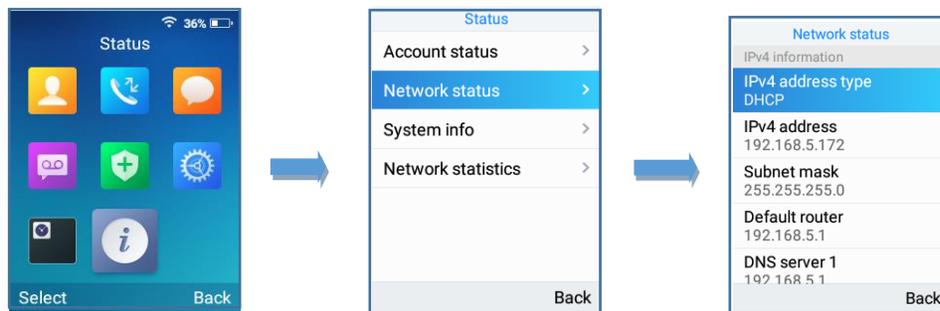


Figure 7: Obtaining IP Address



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 cannot 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".
- If '**Disable web UI access**' parameter is enabled under **Advanced settings → System security**; web UI access will be disabled.



Web GUI Languages

Currently the WP820 web GUI supports English, Chinese languages.

Users can select the language in web GUI login page, or at the upper right of the web GUI after logging in.

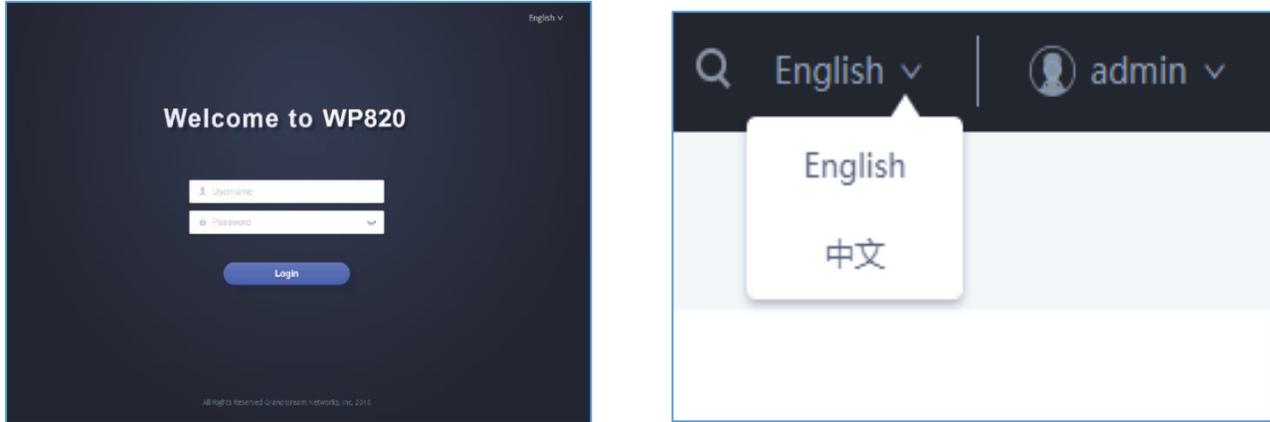


Figure 8: WP820 Web GUI Language

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.
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.

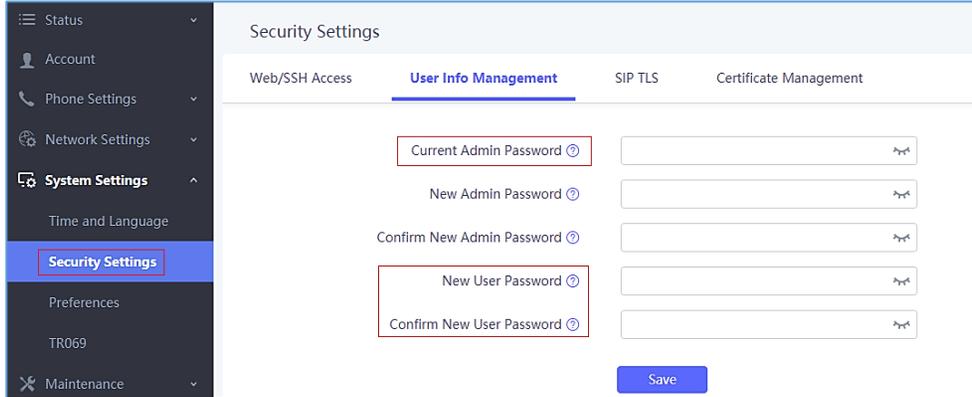


Figure 9: User Level Password

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.

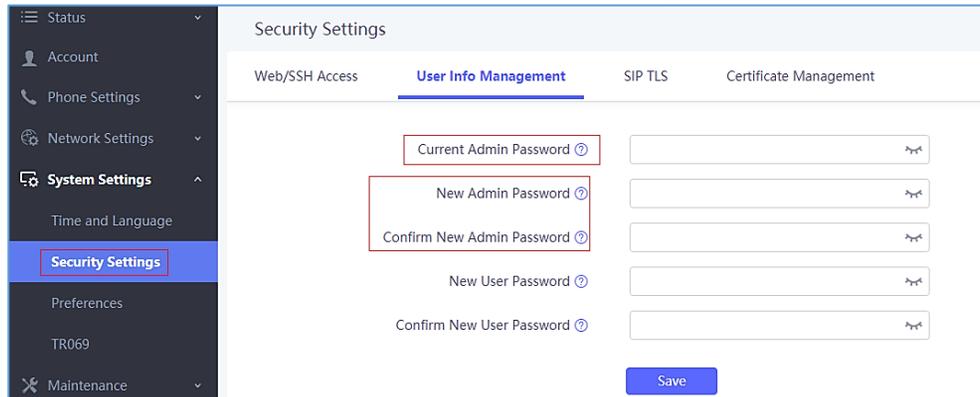


Figure 10: Admin Level Password

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 are 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: After modifying the connection method or port, the web GUI will be automatically logged out and redirected to the new address.

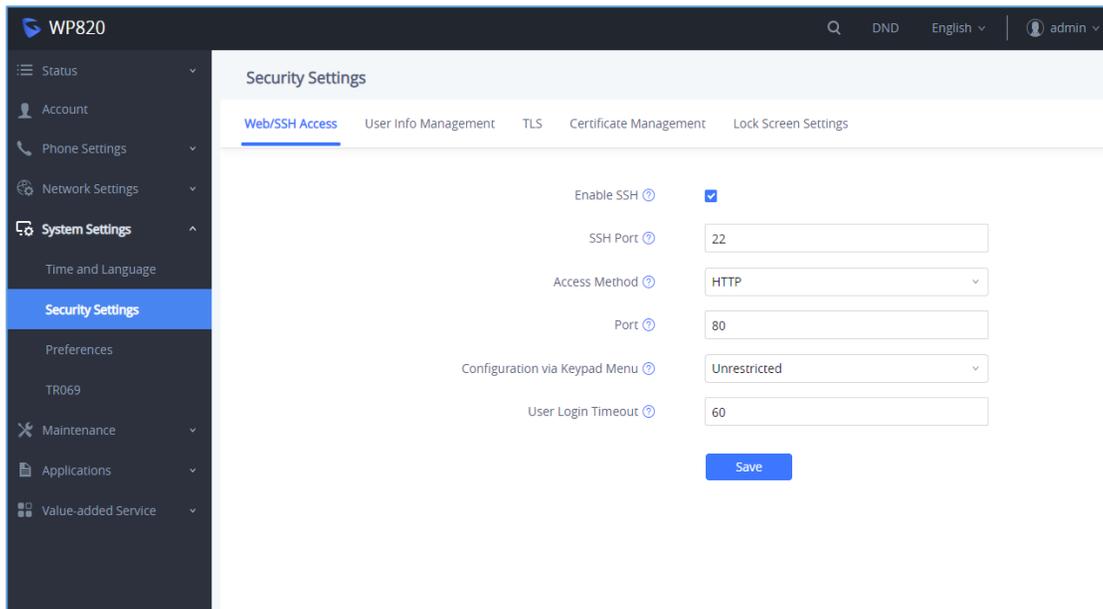


Figure 11: Web Access Port

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, ringtone, Video Settings, PTT/multicast paging and Wallpaper setting.
- **Network Settings:** Bluetooth, 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.
IPv6 DUID	Shows the IPv6 DUID

Status/System Info

Product Model	Product model of the phone.
Hardware Revision	Hardware version number.
Part Number	Product part number.
System Version	Firmware version.
Recovery Version	Recovery image version.
Boot Version	Boot code version.
Kernel Version	Kernel version.
CPE Version	CPE version.
System Up Time	System up time since last reboot.
LCD Serial Number	LCD Serial Number.



DDR Serial Number	DDR Serial Number.
Factory Serial Number	Factory Serial Number.

Account/General Settings

Account Settings	
Account Active	This field indicates whether the account is active. The default setting is "Yes". The default value for Account 2 is "No".
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 is usually in the form of digits similar to phone number or actually a phone number.
SIP Authentication ID	Configures the SIP service subscriber's 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	<p>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.</p> <ul style="list-style-type: none"> • 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. <p>Please consult your carrier before changing this parameter. Default is Disabled.</p>



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 is used by the phone for Firewall or NAT penetration in different network environments. If a symmetric NAT is detected, STUN will not work and ONLY an Outbound Proxy can provide a solution.
Secondary Outbound Proxy	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	<p>Selects DNS mode to use for the client to look up server. One mode can be chosen.</p> <ul style="list-style-type: none"> • 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. <p>Default is A Record.</p>
DNS SRV Fail-over Mode	<p>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.</p> <ul style="list-style-type: none"> • 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 is 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 does not respond, it will move on to the next IP until one of the servers responds, once this happen the phone will keep contacting this responding IP until DNS timeout (30 minutes) before starting over. • Saved one until no response (Stay on responding IP until its failure): On this mode, the phone will send SIP requests to the last responding IP, and it does not failover/switchover to the next one until this responding server is down.



NAT Traversal	<p>Specifies which NAT traversal mechanism will be enabled on the phone. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> • NAT NO • STUN • Keep-alive • Auto • OpenVPN <p>If the outbound proxy is configured and used, it can be set to "NAT NO".</p> <p>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.</p> <p>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.</p> <p>If it needs to use OpenVPN to connect host server, it needs to set it to "OpenVPN". The default setting is "NAT NO".</p>
Proxy-Require	<p>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.</p>

Account/SIP Settings

SIP Basic Settings	
SIP Registration	<p>Allows the phone to send SIP REGISTER messages to the proxy/server. The default setting is "Yes".</p>
Unregister before New Registration	<p>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".</p>
Register Expiration (m)	<p>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).</p>



Subscribe Expiration (m)	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified register. 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. <ul style="list-style-type: none"> • 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 ".
Use P-Access-Network-Info Header	Use P-Access-Network-Info header in SIP request.
Use P-Emergency-Info Header	Use P-Emergency-Info header in SIP request.
Use Mac Header	Configures whether to use MAC header for SIP. If set to "No", all SIP REGISTER messages will not contain MAC header. If set to "Only for REGISTER", MAC header will only be included in SIPREGISTER and UNREGISTER messages. If set to "Yes to All SIP", all outgoing SIP REGISTER messages will contain MAC header. Default is No.
Add MAC in User-Agent	Configures whether to add MAC address in User-Agent header. If set to "No", all outgoing SIP messages will not attach MAC address to the User-Agent header; If set to "Yes except REGISTER", all outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header; If set to "Yes to All SIP", all outgoing SIP messages including REGISTER message will attach MAC address to the User-Agent header. Default is No.
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. <ul style="list-style-type: none"> • 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 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 ".

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/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. The default setting 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	<p>Specifies the mechanism to transmit DTMF (Dual Tone Multi-Frequency) signals. There are 3 supported modes:</p> <ul style="list-style-type: none"> • In audio, which means DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs); • RFC2833, which means to specify DTMF with RTP packet. Users could know the packet is DTMF in the RTP header as well as the type of DTMF. • SIP INFO, which uses SIP INFO to carry DTMF. The defect of this mode is that it is easily to cause desynchronized of DTMF and media packet if the SIP and RTP messages are required to transmitted, respectively. <p>The default setting is "RFC2833".</p>
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.
Preferred Video Codec	
Preferred Video Codec	This parameter is to configure the preferred Video Codec used to receive and display video for SIP calls on WP820. The default setting is H.264.
Enable Video FEC	When enabled, the video sender will temporarily allocate part of the bandwidth to one data channel to send FEC data to system, thus, to improve the video quality the WP820 gets. Enabling this function will take up part of bandwidth and reduce call rate. The default setting is "Yes"
Enable RFC5168 Support	Enables/disables RFC5168 mechanism for video calls to WP820. RFC5168 allows SIP party to request the sender to refresh its video frame in H.264. The default setting is “No”.
FEC Payload Type	Configures FEC payload type. The range is 96-126. Default setting is 120.
H.264 Image Size	Sets the H.264 image size. It can be selected from the dropdown list. <ul style="list-style-type: none"> • 720P • 4CIF



	<ul style="list-style-type: none"> • VGA • CIF • QVGA • QCIF <p>Note: For some network environment, the default setting “720P” might be too high that causes not receiving video or video quality issue during video call to WP820. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower. The default setting is 720P.</p>
Use H.264 Constrained Profiles	<p>Configures that whether to set H.264 constrained profiles to use H.264 CBP to establish video call with WebRTC. The function takes effect when H.264 profile setting includes BP type. It is recommended to set to "Yes" when establishing video call with WebRTC</p> <p>The default setting is “No”.</p>
Video Bit Rate	<p>Configures the bit rate for video stream received on the WP820. The default setting is 2048 kbps. The valid range is from 32 – 2048 kbps.</p> <p>Note: The video bit rate can be adjusted based on the network environment. Increasing the video bit rate may improve video quality if the bandwidth is permitted. If the bandwidth is not permitted, the video quality will decrease due to packet loss. For some network environment, the default setting “720P” might be too high that causes no video or video quality issue during video call to WP820. In this case, please change “H.264 Image Size” to “VGA” or “CIF” and change “Video Bit Rate” to “384kbps” or lower.</p>
SDP Bandwidth Attribute	<p>Sets the SDP bandwidth attribute. It can be selected from the drop-down list. The default setting is “Media Level”.</p> <ul style="list-style-type: none"> • Standard: use AS format in session level; use TIAS format in media level • Media Level: use AS format in media level. • Session Level: use AS format in session level. • None: no modifications in the session format. <p>Note: Please do not modify this setting without knowing the session format supported by the server. Otherwise, it might cause video decoding failure.</p>
RTP Settings	
SRTP Mode	<p>Sets if the phone will enable the SRTP (Secured RTP) mode. It can be selected from dropdown list:</p> <ul style="list-style-type: none"> • Disable • Enabled but not forced



	<ul style="list-style-type: none"> • Enabled and forced <p>The default setting is “Disable”.</p> <p>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”.</p> <p>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</p>
SRTP Key Length	<p>Configures all the AES (Advanced Encryption Standard) key size within SRTP. It can be selected from dropdown list:</p> <ul style="list-style-type: none"> • AES128&256 bit • AES 128 bit • AES 256 bit <p>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.</p> <p>The default setting is “AES128&256 bit”.</p>
Enable SRTP Key Life Time	<p>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. The default settings is “Yes”.</p>
RTCP Destination	<p>Configures the server address. When there is a call, the RTCP package sent from the phone will also be sent to this address.</p> <p>Note: The address should contain port number.</p>
Symmetric RTP	<p>Configures if the phone enables the symmetric RTP mechanism.</p> <p>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”.</p>
RTP IP Filter	<p>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”.</p>
RTP Timeout (s)	<p>Configures the RTP timeout setting; If the phone does not receive any RTP packet within the specified RTP time, the call will be automatically disconnected. Default settings is 30s and the supported range is between 0 and 600.</p> <p>The corresponding P-value of this settings for Account 1 and Account 2 are: P29068 and P29168, respectively.</p>



Account/Call Settings

Call Features	
Start Video Automatically	Defines whether to enable video automatically when there is a call from contacts or dialing interface. If set to "Yes", the video call will be started automatically. If set to "No", dial the call via SIP audio.
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 is 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".
Intercept Anonymous Calls	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. The default setting is " Log All ". <ul style="list-style-type: none"> • 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.
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.



Mute on Answer Intercom Call	When enabled, phone will set mute feature upon answering incoming intercom calls. The corresponding P-values for Account1 and Account2 are respectively: P26071 and P26171 with possible values 0 for 'OFF' and 1 for 'ON'.
Transfer on 3-way Conference Hang up	Transfers conference from hosted party when hang up, thus other parties can continue the conference without interruption. The default setting is unchecked.
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.
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. <ul style="list-style-type: none"> • 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



	<p>forward incoming calls to the accounts of In Time Forward to and Out Time Forward to.</p> <ul style="list-style-type: none"> • Others: Set the call forwarding rule based on following account status. <ul style="list-style-type: none"> ✓ 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	<p>Enables/disables the Dial plan mechanism for different cases. If the specific case is checked, the Dial plan mechanism will be disabled.</p> <ul style="list-style-type: none"> • 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. <p>The default setting is unchecking all the cases.</p>
Dial Plan	<p>Dial Plan Rules:</p> <ol style="list-style-type: none"> 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; <ol style="list-style-type: none"> 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
- m. Flag T: when adding a “T” at the end of the dial plan, the phone will wait for 3 seconds before dialing out. This gives users more flexibility on their dial plan setup.

E.g. with dial plan 1XXT, phone will wait for 3 seconds to let user dial more than just 3 digits if needed.

Originally the phone will dial out immediately after dialing the third digit.

- **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:
 - Replace:
 {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+ }



	<p>Example of a simple dial plan used in a Home/Office in the US: <code>{ ^1900x. <=1617>[2-9]xxxxxx 1[2-9]xx[2-9]xxxxxx 011[2-9]x. [3469]11 \+x+ }</code></p> <p>Explanation of example rule (reading from left to right):</p> <ul style="list-style-type: none"> • ^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 <p>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: <code>{ *x+ }</code> which allows the user to dial * followed by any length of numbers.</p>
<h3>Caller IDs</h3>	
<h4>Caller ID Display</h4>	<p>Specifies which header tag will be used from the SIP INVITE message for the Caller ID display.</p> <ul style="list-style-type: none"> • 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". <p>The default setting is "Auto".</p>
<h3>Ring Tones</h3>	
<h4>Account Ringtone</h4>	<p>Allows users to configure the ringtone for the account. Users can choose different ringtones from the dropdown list.</p> <p>Note: User can also choose silent ring tone.</p>
<h4>Ignore Alert-Info Header</h4>	<p>If checked, configured default ringtone will be played by ignoring Alert-Info header.</p>



Match Incoming Caller ID	<p>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:</p> <ul style="list-style-type: none"> • <u>Specific caller ID number</u>. For example, 8321123; • <u>A defined pattern</u> 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. • <u>Alert Info text</u> 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: <i>Alert-Info: <http://127.0.0.1>; info=priority</i> <p>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</p>
---------------------------------	---

Account/Advanced Settings

Security Settings	
Check Domain Certificates	<p>Defines whether the domain certificates will be checked when TLS/TCP is used for SIP Transport.</p> <p>The default setting is "No".</p>
Validate Certification Chain	<p>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.</p> <p>The default setting is "No".</p>
Validate Incoming SIP Messages	<p>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.</p> <p>The default setting is "No".</p>
Allow Unsolicited REFER	<p>Configures whether to dial the number carried by Refer-to after received Out-of-dialog SIP REFER request actively.</p> <ul style="list-style-type: none"> • 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.



	<ul style="list-style-type: none"> 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	<p>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.</p> <p>The default setting is "No".</p>
Check SIP User ID for Incoming INVITE	<p>Configures the phone to check the SIP User ID in the Request URI of the SIP INVITE message from the remote party. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is "No".</p>
Allow SIP Reset	<p>Configures if allow SIP Notification message to perform factory reset.</p> <p>The default setting is "No".</p>
Authenticate Incoming INVITE	<p>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".</p>
SIP Realm Used for Challenge INVITE & NOTIFY	<p>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.</p>
MOH	
Upload Local MOH Audio File	<p>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.</p> <p>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.</p>
Enable Local MOH	<p>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".</p>
Advanced Features	
Special Feature	<p>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".</p>



Feature Key Synchronization	This feature is used for BroadSoft/Metaswitch call feature synchronization. When set to BroadSoft/Metaswitch, DND and Call Forward features can be synchronized with BroadSoft or Metaswitch server. Default settings is “Disable”
Allow Sync Phonebook via SIP Notify	<p>Allows users to synchronize XML phonebook upon receiving SIP NOTIFY message with header <i>Event: sync-contacts</i>.</p> <p>Note: Received SIP NOTIFY will be first challenged for authentication purpose before contacting configured server to download XML phonebook. The parameters used are the ones configured at [Download Contacts]. The authentication can be done either using admin credentials (if no SIP account is configured) or using SIP account credentials. The default setting is “Yes”.</p>

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	<p>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”.</p> <p>Note: This parameter must be set to “No” for Direct IP Calling to work.</p>
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 is required by your ITSP. The default setting is keep the box blank.



Guest Features	
Guest Settings	
Guest Login	Enable/disable guest login. Users should configure SIP domain name when using this function. Users should input SIP username and password on LCD. 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 of 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 Settings	
Call Features	
Enable Video Call	Enables the video call feature.
Default Video Zoom Area	In a video call, the default area which is displayed after press Zoom. The default value is 0 (full screen). Range 0-9.
Enable Transfer	Enable the transfer feature. When " unchecked ", the phone will block the TRANSFER key on the LCD screen. The default setting is " checked ".
Hold Call Before Completing Transfer	If you choose "Yes", the transfer call status will be kept as hold status after Attended transfer operation.
Enable Conference	Enable the conference. When " unchecked ", the phone will block the conference function. The default setting is " checked ".
Enable noise Shield	Configures whether to enable noise shield feature. If enabled, all the background noise will be suppressed except the sound from speaker.
Enable In-call Recording	If set to "Yes", the device can record during a call; if set to "No", this feature is hidden during a call.



Enable Call Waiting	Enables the call waiting feature. If it is unchecked, 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 " checked ".
Enable Call Waiting Tone	Sets the phone to play the call waiting tone if there is another incoming call. If it is " Unchecked ", the phone will only display the indicator on the LCD screen for another incoming call. The default setting is " checked ".
Enable Proximity Sensor	If set to "Yes", the phone will automatically turn the screen off when near the proximity sensor during a call. Note : If proximity sensor is disabled, the LCD screen will not turn off during call when handset is held near the ear.
Incoming/Outgoing Call	
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 " checked ".
Auto Mute on Entry	Configures whether to mute the call on entry automatically. <ul style="list-style-type: none"> • 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.
Rejected Call Notification	Specifies whether to enable Rejected calls notification. When enabled, a missed call notification will prompt on LCD after rejecting an incoming call.
Enable DND Reminder Ring	Enables the DND reminder ring. If set to "Yes", the ring splash that indicates an incoming call when DND is enabled will be played.
Off hook Auto Dial	Configures a User ID/Extension to dial up automatically after the off-hook auto dial delay time ends when the phone is off hook or hands-free. The phone will use the first account to dial out by default.
Off hook Auto Dial Delay (s)	Defines the delay time of Off hook Timeout. Once configured Off hook Timeout, the phone will dial out automatically after the delay time ends. If not configured Off hook Timeout, there will be no delays and the phone will dial up the User ID/Extension automatically.



Off hook/On hook 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 off hook of handset when picked up from cradle.
On-cradle Hang up	Enables on hook of handset when repositioned on cradle.
DND Settings	
DND Mode	Configures the DND mode for the phone. If set to "On", DND feature is effective for the phone system. If set to "Custom", select the account(s) to apply DND feature on. If set to "Off", DND feature will be disabled.
Enable DND Reminder Ring	Enables the DND reminder ring. If set to "Yes", the ring splash that indicates an incoming call when DND is enabled will be played.
Advanced Settings	
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 "checked" .
Notification Tone	Configures the notification tone for new SMS and voicemails.
Contact source priority	Configure the priority of the ID source displayed on the phone when incoming/outgoing calls. Select one ID source and click the Up/Down arrow on the right to adjust the order. Note: If the "Caller ID Display" under the account is configured as "Disabled", the caller number cannot be obtained, the phone will only display "Unavailable".



Phone Settings/Ring Tone

CPT Settings	
Auto Config CPT by Region	Configures whether to choose Call Progress Tone automatically by region. If set to "Yes", the phone will configure CPT (Call Progress Tone) according to different regions automatically. If set to "No", you can manually configure CPT parameters. The default setting is " No ".
Call Progress Tones: <ul style="list-style-type: none"> •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. <ul style="list-style-type: none"> • 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 .
Upload Ringtone	
Upload Ringtone	Users could click on "Upload" button to upload ringtone files in .mp3/.wav/.ogg format and size less than 2M. User can upload up to 10 files.

Phone Settings/Video Settings

Video Frame Rate	Configures video frame rate which needs to be adjustable based on network condition. Increasing the frame rate will significantly increase the amount of data transmitted, therefore consuming more bandwidth. The video quality will deteriorate due to packet loss if extra bandwidth is not allocated.
Video Display	Set the video display mode to: <ul style="list-style-type: none"> • Original proportion • Cut proportionally • Add black margin proportionally



	<p>If set to "Original proportion", the phone displays video in its original proportion. If the video display proportion is different from the one of the phones, the phone will stretch or compress video to display it. If set to "Cut proportionally", the phone will cut video to meet its own display proportion. If set to "Add black margin proportionally", the phone will display video in its original proportion. If it still exists spare space, the phone will add black edge on it.</p>
Enable Frame Skipping in Video Decoder	<p>Enables the phone system for frame skipping in video decoder. If it is enabled, the video decoder will skip the P frame and start decoding from the next I frame. Enabling this option will help reduce flickering in the video when the bandwidth is limited in the network environment.</p> <p>The default setting is "Yes".</p>

Phone Settings/PTT/Multicast Settings

General Settings	
Allow PTT/Paging When Lock Screen Status	<p>If set to "Yes", the device can initiate PTT/Paging in the lock screen status.</p>
IGMP Keep-alive Interval (s)	<p>Specifies how often the phone report IGMP when PTT/ Paging function is turned on. IGMP reporter help to keep PTT/ Paging receivable in dormant state. The interval may take some effect to standby time.</p>
PTT/Group Paging	
Settings	
PTT multicast address	<p>Defines PTT multicast address.</p>
Port	<p>Defines port number for PTT multicast address.</p>
Emergency PTT/paging volume	<p>Set default volume for PTT/paging when emergency channel/group is used.</p>
PTT Config	
PTT	<p>Enable or disable PTT.</p>
Default Channel	<p>Defines default channel for PTT. When pressing and holding the PTT button, PTT will be initiated using the default channel.</p>



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	<p>Defines whether to accept PTT calls while device is in active call.</p> <ul style="list-style-type: none"> • 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. <p>Default is "No"</p>
Caller ID	Set Caller ID displayed on the call interface during a PTT call.
PTime (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.
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	<p>Defines whether to accept paging while device is in active call.</p> <ul style="list-style-type: none"> • 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



	<p>the same priority; If device is in active SIP call, device will accept paging and put the SIP call on hold.</p> <p>Default is “No”.</p>
Caller ID	Set Caller ID displayed on the call interface during paging
PTime (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.

Multicast Paging Function

Settings

Paging Priority Active	<p>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.</p> <p>The default setting is disabled.</p>
Paging Barge	<p>If enabled, during active call, if incoming multicast paging has higher priority (1 is the highest) than this value, the call will be put on hold and multicast paging will be played.</p> <p>Default setting is “Disabled”.</p> <p>Note: The option is displayed if “Paging Priority Active” is enabled.</p>
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 ”.

Multicast Channel Settings

Multicast Paging Function	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 to 239.255.255.255. User can enter up to 10 Multicast paging addresses.



Phone Settings/Wallpaper Setting

WP820 wallpaper is customizable through web GUI and the user can upload up to 10 wallpapers.

Note:

WP820 support JPG, PNG, BMP format, size \leq 2MB (Best Pixel: 240 * 320px)

Wallpaper Setting	
Wallpaper Source	Configures the source of wallpaper, if selected: <ul style="list-style-type: none"> • Default: use the system default wallpaper. • Download: use the wallpaper downloaded from network, a server path must be configured for the Directory or file path of the wallpaper. TFTP, HTTP and HTTPS protocols are supported. • Uploaded: use the wallpaper uploaded from the webpage. <p>For more details on different method to change the wallpaper, please refer to the WP820's User Guide.</p>

Network Settings Page Definitions

Network Settings/Bluetooth

Bluetooth	
Device Name	Display name when paired with other devices.
Bluetooth Headset Mode	Enables/Disables Bluetooth headset mode. The WP820 will become a headset of the paired Bluetooth device, and can answer and dial calls for the paired device after enabled.
Bluetooth	Enables/Disables Bluetooth function. The WP820 can be found by nearby Bluetooth devices after enabled.
Bluetooth Devices	Scan available devices and complete the pairing. After enables Bluetooth function, automatically scan the available Bluetooth devices.



Network Settings/Wi-Fi Settings

Wi-Fi Basics	
IP Mode	<p>Select which Internet protocol to use from dropdown list:</p> <ul style="list-style-type: none"> • Both, prefer IPv4. • Both, prefer IPv6. • IPv4 Only. • IPv6 Only. <p>When both IPv4 and IPv6 are enabled, phone attempts to use preferred protocol first and switches to the other choice if it fails.</p>
Wi-Fi Signal Warning	<p>Selects Wi-Fi warning level. When the Wi-Fi signal strength is lower than the threshold set by this level, the device will warning.</p>
Wi-Fi Function	<p>Enables/disables the Wi-Fi feature.</p> <p>The default setting is "Disable".</p>
Wi-Fi Band	<p>Configures the Wi-Fi frequency band from the dropdown list:</p> <ul style="list-style-type: none"> • 2.4G • 5G • Dual band (2.4 G & 5G)
ESSID	<p>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. User can set the IPv4 and IPv6 type to either DHCP or Static IP when clicking on "Show Advanced Options".</p>
Add Network	
ESSID	<p>Determines the ESSID of the default Wi-Fi network. The default password is "wp!987@dmn" and it uses WPA2PSK security access.</p>
Security Mode for Hidden SSID	<p>This parameter defines the security mode used for the wireless network when the SSID is hidden. 3 Modes are available:</p> <ul style="list-style-type: none"> - WEP - WPA/WPA2 PSK3 - WPA Enterprise: This feature allows using 802.1x WPA2-Enterprise secure network authentication.
EAP Method	<p>When WPA Enterprise is selected, users can choose one of the below EAP methods which can be configured for credential based or certificate authentication.</p>



	<ul style="list-style-type: none"> - PEAP - TLS2 - TTLS - PWD
CA Certificate	Upload the 802.1x CA certificate to the phone; or delete existed 802.1x CA certificate from the phone.
Identity	Enter the Identity information for the 802.1x mode.
Password	Configures the hidden ESSID password.
Advanced Settings	
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.
Channel Mode	"Auto" mode is enabled by default, in this mode, devices will do fully scanning; "Customize" mode is used to specify channels, and only the selected channels will be scanned and used to make network switch and roaming decision.
Wi-Fi Roaming	
Signal Threshold	Sets the Wi-Fi signal threshold. When the Wi-Fi signal strength of the device drops below this configured value, the device will scan for a hotspot above the threshold value and connect to it. The default setting is -70 and the valid range is [-100, -30].
Good Signal Scanning Interval (s)	Sets the time interval for signal scanning when the Wi-Fi signal strength is higher than the signal threshold. Default is 600s, and valid range is from 5 to 600.
Poor Signal Scanning Interval (s)	Sets the time interval for signal scanning when the Wi-Fi signal strength is lower than the signal threshold and there is no hotspot that is higher than the current signal strength. Default is 5s, and valid range is from 5 to 600.

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).
OpenVPN® Mode	Simple mode only supports some basic or common parameters configuration; Professional mode supports configuration file upload in zipped format, which is totally customized by need, please refer to https://openvpn.net for more information.
Enable OpenVPN® Comp-lzo	Enables/disables the LZO compression. When LZO compression is enabled on the OpenVPN server, this option needs to be checked otherwise there will be a network connection failure. The P-value for this functionality is P8508 with two possible values 0 and 1; 0 – OFF/1 - ON. Default setting is NO .
OpenVPN® Server	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).
Additional Options	Configures additional options to include for the OpenVPN feature (optional).



Network Settings/Advanced Network Settings

Preferred DNS 1 Server	Defines the secondary DNS IP address if the static IP is used.
Preferred DNS 2 Server	Configures the secondary alternate DNS IP address to failover during both: the default DNS server and alternate DNS server's outage.
IPv6 Preferred DNS Server	Defines primary choice for IPv6 DNS to handle Internet protocol mapping.
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.
Remote Control	
CSTA Control	Indicates whether CSTA control feature is enabled. This allows third party applications to control the WP820 via uaCSTA standard. Supports 3CX uaCSTA web client call control. Changes made to this parameter will require reboot to take effect.



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. <ul style="list-style-type: none"> • 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.
Select Language File	Allows users to upload custom language file to the phone. Press " Browse " to bring up the file selection menu to select the local .txt file to upload to the phone.



System Settings/Security Settings

Web/SSH Access	
Enable SSH	Enable/Disable SSH access to the phone. The default setting is checked .
SSH Port	Customize the SSH port. The default setting for SSH port is 22.
Access Method	Determines which protocol will be used to access the phone 's Web GUI. It can be selected from HTTP and HTTPS. The default setting is HTTP .
Port	Specifies which port to use to access the phone 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: <ul style="list-style-type: none"> • 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 and to access the Call Settings menu along with the DND toggle function. The default setting is " Unrestricted ".
User Login Timeout	Set login timeout (in minutes) for user. If there is no activity within the specified amount of time, the user will be logged out, and the system will jump to the login page automatically. If set to 0, the user will not be logged out automatically. Default is 15 minutes.
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.
TLS	
Minimum TLS Version	Configures the minimum TLS version supported by the phone. Default is 1.1.
Maximum TLS Version	Configures the maximum TLS version supported by the phone. Default is No limit.
Enable Weak TLS Cipher Suites	<p>Enable or disable weak TLS cipher suites.</p> <ul style="list-style-type: none"> • If set to "Enable Weak TLS Cipher Suites", allows users to encrypt data by weak TLS cipher suites. • If set to "Disable Symmetric Encryption RC4/DES/3DES", allows users to disable weak cipher DES/3DES and RC4.
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.
Custom Certificate	
Screen Lock Function	Enables/Disables screen lock function.
Screen Lock Password	Display current screen lock password.
Lock Screen Settings	
Screen Lock Function	Allows the user to configure lock screen functions on the web UI. The screen lock password was also added to provide additional security. Default Disabled.
Screen Lock Password	Add new digit password, edit current password and it displays the current screen lock password.

System Settings/Preferences

Sound	
Silent Mode	Enables silent mode.
Vibrate Mode	Enables vibrate mode.
Charging Tone	If set to "Yes", it will sound a tone once you start charging.
Low Battery Warning Tone	If set to "Yes", it will sound a tone when LCD prompts low battery.
Voicemail Notification Tone	If set to "Yes", it will sound a tone when LCD prompts unread voicemail message.



Lock Volume	If set to "Yes", volume adjustments on the handset become locked.
Ringtone volume	Configures the volume of ringtone.
Media volume	Configures the volume of media.
Alarm volume	Configures the volume of the alarm.
Default Ringtone	Configure default ringtone for incoming calls.
Notification Tone	Configure notification tone for new SMS, Voicemail etc.

LCD & LED Management

Enable Missed Call Indicator	When " checked ", the LED indicator on the upper right corner of the phone will light up when there is missed call on the phone.
Enable MWI Indicator	When " checked ", the LED indicator on the upper right corner of the phone will light up when there is new voicemail on the phone
Enable New Message Indicator	Turns on the LED indicator at device's upper right corner when there are unread Messages. If it set to "checked", the LED indicator will keep off if the phone has new messages. Otherwise, the LED indicator will be turned on. Default setting is " checked ".
Enable Keypad Backlight	When " checked ", the backlight will light up when the button is pressed. Default setting is " checked ".
Brightness	Configures the Brightness of LCD backlight.
Timeout	Sets the timeout interval of the LCD backlight. If timeout is set to 'never', the screen will always stay on. The value range is between 15s and 30 minutes.
Font Size	Set the font size for the LCD display. Choices are: Standard, Small, and Large.

Gesture Control

Flip phone

Reject incoming call	If set to "Reject", the phone will reject incoming calls if users flip the phone. If set to "Reject with SMS", the phone will reject incoming calls when flipping the phone and send a pre-configured SMS to the caller. The default setting is "Off".
-----------------------------	--

Pick up the phone

Ringtone	If set to "Mute", the ringtone will be muted once users pick up the phone when receiving an incoming call. If set to "Ringing Down", the ringtone's volume will
-----------------	---



	decrease once the phone is picked up when receiving incoming calls. The default setting is “Off”.
Alarm Ringtone	If set to “Mute”, the alarm ringtone will be muted once users pick up the phone during alarm. If set to “Ringing Down”, the alarm ringtone’s volume will decrease once the phone is picked up during alarm. The default setting is “Off”.
Button Customization	
Soft key	
Main Screen Left Softkey	Configures the function of the left softkey when users are on the Main screen. This can be set to “ Call History ”, “ Menu ”, “ Settings ”, “ Contacts ”, “ Voicemail ”, “ DND ”, “ LDAP ”.
Main Screen Center Softkey	Configures the function of the center softkey when users are on the Main screen. This can be set to “ Call History ”, “ Menu ”, “ Settings ”, “ Contacts ”, “ Voicemail ”, “ DND ”, “ LDAP ”.
Main Screen Right Softkey	Configures the function of the right softkey when users are on the Main screen. This can be set to “ Call History ”, “ Menu ”, “ Settings ”, “ Contacts ”, “ Voicemail ”, “ DND ”, “ LDAP ”.
Call Screen Left Softkey	Configures the function of the left softkey when users are on the Call screen. This can be set to “ Option ”, “ Transfer ”, “ Hold ”, “ Mute ”, “ New Call ”, “ Conference ”, “ Record ”.
Call Screen Center Softkey	Configures the function of the center softkey when users are on the Call screen. This can be set to “ Option ”, “ Transfer ”, “ Hold ”, “ Mute ”, “ New Call ”, “ Conference ”, “ Record ”.
Call Screen Right Softkey	Configures the function of the right softkey when users are on the Call screen. This can be set to “ Option ”, “ Transfer ”, “ Hold ”, “ Mute ”, “ New Call ”, “ Conference ”, “ Record ”.
Multi-function Button	
PTT/Paging	If “PTT/Paging” is chosen to be the function for Multi-function button, a short press on the button will take users to PTT/Paging settings. Users can also press and hold the key to initiate PTT/Paging call.
SAFE/Panic Call	If “SAFE/Panic Call” is configured to be the function for Multi-function button, a short press on the key will open status page to make sure that Panic Call is enabled. Users can also press and hold the key to trigger Panic Call.



Mute	If "Mute" is chosen, users will be able to mute incoming calls ringtone by pressing on the key. Also, the key will be performing mute/unmute function during calls.
Speed Dial	Short press to open status page, long press to dial a contact.
Disable	If set to "Disabled", Pressing the multi-function button has no function.

System Settings/TR-069

Enable TR-069	Sets the phone to enable the "CPE WAN Management Protocol" (TR-069). The default setting is "Yes".
ACS URL	Specifies URL of TR-069 ACS (e.g., http://acs.mycompany.com), or IP address. Default setting is https://acs.dgms.cloud
ACS User name	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 User name	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.
Update Detect	Click the "Update Detect" button to check whether the firmware in the firmware server has an updated version, if so, proceed to firmware upgrade immediately.
Config File	
Config File	
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.



Use Grandstream GAPS	<p>Configures the download path and update mode for the configuration file server.</p> <ul style="list-style-type: none"> • If checked, 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 unchecked, then users can manually configure the path and update mode for the configuration file server. The default setting is “Checked”.
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	<p>Includes configured user name and password in HTTP request before receiving authentication challenge from the server.</p> <p>The default setting is “No”.</p>
Config File Prefix	<p>Enables your ITSP to lock configuration updates.</p> <p>If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.</p>
Config File Postfix	<p>Enables your ITSP to lock configuration updates.</p> <p>If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.</p>
Authenticate Conf File	<p>Sets the phone to authenticate configuration file before applying it.</p> <p>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”.</p>
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file is using OpenSSL.
Provision	
Automatic Upgrade	
Automatic Upgrade	<p>Specifies when the firmware upgrade process will be initiated; there are 4 options:</p> <ul style="list-style-type: none"> • 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)” <p>Note: Day of week is starting from Sunday. The default setting is “No”.</p>



Enable Randomized Automatic Upgrade	Configures whether the phone will upgrade automatically at random time point within the configured period. This option is mainly used for multiple phones upgrade at the same time.
Firmware Upgrade and Provisioning	<p>Defines the phone's rules for automatic upgrade. It can be selected from:</p> <ul style="list-style-type: none"> • Always Check at bootup. • Always Check at bootup when Firmware/Config pre/suffix changes. • Skip the Firmware Check. <p>The default setting is "Always Check at bootup".</p>
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, 160 and Option 66 to Override Server	<p>Obtains configuration and upgrade server's information from DHCP server using options 66 and 43.</p> <p>Note: If set to "Yes" on the LAN side, the device will reset the CPE, upgrade, network VLAN tag and priority configuration according to option 43 sent by the server. At the same time, the upgrade mode and server path of the configuration upgrade mode will be reset according to option 160 and 66 sent by the server. If set to "Prefer, fallback when failed", the device can fallback to use the configured provisioning server under its Firmware and Config server path in case the server from DHCP Option fails.</p>
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 ".
Config Provision	
Download and Process All Available Config Files	By default, the device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, and cfg.xml (corresponding to device specific, model specific, and global configs). If set to "Yes", the device will download and apply (override) all available configs in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, cfg.xml.
Config Provision	This feature's purpose is to make the device downloads the configuration files and provision by the configured order.



PNP Feature	
PNP (3CX) Auto Provision	<p>Sets the phone system to broadcast the SIP SUBSCRIBE message during booting up to allow itself to be discovered and be configured by the SIP platform. The default setting is "Checked".</p> <p>Note: This setting requires rebooting the phone to take effect.</p>
Advanced Settings	
Disable SIP NOTIFY Authentication	<p>Disables the SIP NOTIFY Authentication on the phone. If set to "Yes", the phone will not challenge NOTIFY with 401.</p> <p>The default setting is "No".</p>
Validate Certification Chain	<p>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.</p> <p>The default setting is "No".</p>
mDNS Override Server	<p>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".</p> <p>The default setting is "Use Type A".</p>
Factory Reset	<p>Resets the phone to the default factory setting mode.</p>

Maintenance/System Diagnosis

Syslog	
Syslog Protocol	<p>Select the transport protocol over which log messages will be carried.</p> <ul style="list-style-type: none"> • UDP: Syslog messages will be sent over UDP (the default setting). • SSL/TLS: Syslog messages will be sent securely over TLS connection.
Syslog Level	<p>Selects the level of logging for syslog. The default setting is "None".</p> <p>There are 4 levels from the dropdown list: DEBUG, INFO, WARNING and ERROR. The following information will be included in the syslog packet:</p> <ul style="list-style-type: none"> • DEBUG (Sent or received SIP messages).



	<ul style="list-style-type: none"> • 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). <p>Note: Changing syslog level does not require a reboot to take effect.</p>
Syslog Server	Configures the URI which the phone will send the syslog messages to. The default setting is " log.ipvideotalk.com ".
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	<p>Selects the log priority to display. It can be selected from list below:</p> <ul style="list-style-type: none"> • 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 trace, tombstones, ANR log and Battery 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 and click the "Delete" button on the right to delete it.
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.
Ping	
Target Host	Configures the IP address or URL for the Target Host in order to ping it. Press Start to start pinging the configured target host. Press Stop to pinging the configured host.
NSLookup	
Host Name	Enter a host name and find out the corresponding IP address. It will also do reverse name lookup and find the host name for an IP address you specify.

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:

Bootup Completed	Configures the event URL when phone boots up.
Incoming Call	Configures the event URL when phone has an incoming call.
Outgoing Call	Configures the event URL when phone has an outgoing call.
Missed Call	Configures the event URL when the phone has new a missed call.
Connected	Configures the event URL when a call is established.
Disconnected	Configures the event URL when a call is disconnected.



DND On	Configures the event URL when DND is enabled.
DND Off	Configures the event URL when DND is disabled.
Forward On	Configures the event URL when the forward feature is enabled on the phone.
Forward Off	Configures the event URL when the forward feature is disabled on the phone.
Blind Transfer	Configures the event URL when users transfer a call with blind transfer on the phone.
Attended Transfer	Configures the event URL when users transfer a call with attended transfer on the phone.
On Hold	Configures the event URL when users hold a call on the phone.
Unhold	Configures the event URL when users resume a call on the phone.
Log On	Configures the event URL when users log on the phone successfully.
Log Off	Configures the event URL when users log off the phone.
Register	Configures the event URL when an account in the phone is registered successfully.
Unregister	Configures the event URL when an account in the phone is unregistered.
SAFE/Panic Call	Configures the event URL when panic call is made.

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

Contacts	
New contact	<p>Allows users to add a new contact by filling the corresponding contact's information and setting the appropriate account then clicking on OK.</p> <p>Users can modify the contact later by pressing on the Edit icon under Operation section.</p>
Sort Phonebook by	<p>Sets which part of name, first name or last name, will be sorted in alphabetical order to display.</p> <p>The default setting is "Last Name".</p>
Delete	Select the Contacts you want to be deleted and press on Delete .
Add to blacklist	<p>Selects the contacts you want to be Blacklisted and press on Add to blacklist.</p> <p>The blacklisted contact's calls/messages will be blocked.</p>
Groupe	
New Group	<p>Click on New Group and fill the Group name, then select the contacts names you want to be added to this group and press on OK. A new group will be created in the phonebook.</p>
Delete	Select the group you want to be deleted and press on Delete .
Blacklist	
Remove blacklist	Select the blacklist you want to be deleted and press on Remove blacklist .
Import/Export Contacts	
Import	
Clear the Old List	Configure to delete the previous contacts before downloading the new ones.
Clear Old History Mode	<ul style="list-style-type: none"> If set to "Clear all", the phone will delete all previous records before importing the new records.



	<ul style="list-style-type: none"> If set to "Keep Local Contacts", the new-added local new contacts will not be deleted when importing new records. <p>The default setting is "Clear all".</p>
Replace Duplicate Items	<p>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".</p>
Replace Duplicate Entries Mode	<ul style="list-style-type: none"> 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. <p>The default setting is "Replace by name".</p>
File Encoding	<p>Specifies the encoding format for phonebook file importing. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> UTF-8 GBK UTF-16 UTF-32 Big5 Big5-HKSCS Shift-JIS ISO8859-1 ISO8859-15 Windows-1251 EUC-KR <p>The default setting is "UTF-8".</p>
File Type	<p>Sets the type format for phonebook file importing. It can be selected from the dropdown list.</p> <ul style="list-style-type: none"> XML vCard <p>The default setting is "XML".</p>
Import Local File	<p>Uploads the contact file from PC to the phone.</p>



Export	
File Encoding	<p>Specifies the encoding format for phonebook file exporting. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> • UTF-8 • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR <p>The default setting is "UTF-8".</p>
File Type	<p>Sets the type format for phonebook file importing. It can be selected from the dropdown list.</p> <ul style="list-style-type: none"> • XML • vCard <p>The default setting is "XML".</p>
Export	Downloads the phonebook file from the phone to PC.
Download Contacts	
Clear The Old List	<p>Determines if the phone will delete the previous contacts before downloading the new contact file.</p> <p>The default setting is "No".</p>
Clear Old History Mode	<ul style="list-style-type: none"> • 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. <p>The default setting is "Clear all".</p>
Replace Duplicate Items	<p>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.</p> <p>The default setting is "No".</p>



Replace Duplicate Entries Mode	<ul style="list-style-type: none"> • 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. <p>The default setting is "Replace by name".</p>
Download Mode	<p>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".</p>
File Encoding	<p>Selects the encoding format for phonebook file download. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> • UTF-8 (The default settings) • GBK • UTF-16 • UTF-32 • Big5 • Big5-HKSCS • Shift-JIS • ISO8859-1 • ISO8859-15 • Windows-1251 • EUC-KR
Download Server	<p>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 <i>phonebook.xml</i>.</p>
HTTP/HTTPS User Name	<p>Configures user name for HTTP/HTTPS server to download the phonebook file.</p>
HTTP/HTTPS Password	<p>Specifies password for HTTP/HTTPS server to download phonebook file.</p>
Automatic Download Interval	<p>Determines how the phone to send the request to the server to download the phonebook file. It can be selected from the dropdown list:</p> <ul style="list-style-type: none"> • None • 5 minutes • 30 minutes • 1 Hour • 2 Hours • 4 Hours • 6 Hours



	<ul style="list-style-type: none"> • 8 Hours • 12 Hours
Download Now	Starts downloading the XML phonebook to the phone immediately.

Application/LDAP Book

Connection Mode	Selects which protocol will be used for LDAP searching, LDAP or LDAPS.
Server Address	Configures the URI of the LDAP (Lightweight Directory Access Protocol) server.
Port	Configures the LDAP server port. The default LDAP port number is 389.
Base DN	<p>Determines the LDAP search base. This is the location in the directory where the search is requested to begin.</p> <p><u>Example:</u> dc=grandstream, dc=com ou=Boston, dc=grandstream, dc=com</p>
User Name	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	Specifies the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.
LDAP Name Attributes	<p>Configures the "name" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes.</p> <p><u>Example:</u> gn cn sn description</p>
LDAP Number Attributes	<p>Configures the "number" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated number attributes.</p> <p><u>Example:</u> telephoneNumber telephoneNumber Mobile</p>
LDAP Name Filter	<p>Configures the filter used for name lookups.</p> <p><u>Examples:</u> ((cn=%)(sn=%)) returns all records which has the "cn" or "sn" field starting with the entered prefix; (!(sn=%)) returns all the records which do not have the "sn" field starting with the entered prefix; (&(cn=%) (telephoneNumber=*)) returns all the records with the "cn" field starting with the entered prefix and "telephoneNumber" field set.</p>



LDAP Number Filter	Defines the filter used for number lookups. <u>Examples:</u> ((telephoneNumber=%)(Mobile=%) returns all records which has the "telephoneNumber" or "Mobile" field starting with the entered prefix; (&(telephoneNumber=%) (cn=*)) returns all the records with the "telephoneNumber" field starting with the entered prefix and "cn" field set.
Search Field Filter	Configures filters used upon LDAP search. The default settings is "All Filter".
LDAP Display Name Attributes	Configures the entry information to be shown on phone's LCD. Up to 3 fields can be displayed. <u>Example:</u> %cn %sn %telephoneNumber
Max Hits	Specifies the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. Default setting is 50.
Search Timeout (s)	Configures the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 4000 seconds.
LDAP Lookup For Dial	Sets the phone system to do the LDAP number searching when making outgoing calls. The default setting is "No".
LDAP Lookup For Incoming Call	Sets the phone system to do LDAP number searching for incoming calls. The default setting is "No".
LDAP Dialing Default Account	Configures the default account that being used when dialing LDAP contact. Users may choose the Account 1-6; the default setting is "Default".

Application/Recording

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

Application/Call History

Call History	
Call History	Lists the call History content with their Name, Number , Time and Date , and Operation.



Value-added Service Page Definitions

Door System

Door System Type	Configures the door system type.
Door System Name	Display info on LCD when incoming call matches GDS number. This is used to identify door position, e.g.: "east gate" or "3rd floor gate".
System Number Password	Enables open door button display when caller number or IP address matches this setting. e.g: "36311" or "192.168.124.81"
System Password	Configures the access password of the door system. This password corresponds to the system number. When a call comes from the door system, tap on the open button on LCD to send the password to the corresponding door system.
System ringtone	Sets the system ringtone when receiving calls from GDS.

BroadSoft Directories

XSI Service Settings	
Authentication Type	Defines the authentication type to use login credentials or SIP credentials. If set to "Login Credentials", please fill in user name and password in the following options; If set to "SIP Credentials", please fill in user name, user ID, and password.
Server	BroadSoft XSI server address with protocol.
Port	Port of the BroadSoft XSI server.
Action Path	Action path for BroadSoft XSI server.
BroadWorks User ID	User ID for BroadSoft XSI server.
Login Password	Password for BroadSoft XSI server.
BroadSoft Directory & Call Logs Update Interval	Configures the interval to obtain BroadSoft call log and directory data thus to update the matching number data on the dialing interface. Default is 1800s.
BroadSoft Directory Hits	The maximum hits returned from the BroadSoft XSI server directory. The valid range is from 1 to 1000. If set to blank, server's default value will be used.
Associated BroadSoft Account	Configures the associated BroadSoft account when dialing BroadSoft contacts.



BroadSoft Directory Order	Defines the BroadSoft directory order displayed on LCD. Select one item and click the Up/Down arrow on the right to adjust the order.
Network Directories	
Group Directory	Enable/disable the Group directory. Enter a name for this option.
Enterprise Directory	Enable/disable the Enterprise directory. Enter a name for this option.
Group Common	Enable/disable Group Common. Enter a name for this option.
Enterprise Common	Enable/disable Enterprise Common. Enter a name for this option.
Personal Directory	Enable/disable the Personal directory. Enter a name for this option.
Missed Call Log	Enable/disable the Missed Call Log. Enter a name for this option.
Placed Call Log	Enable/disable the Placed Call Log. Enter a name for this option.
Received Call Log	Enable/disable the Received Call Log. Enter a name for this option.

SAFE/Panic Call

SAFE Monitoring Settings	When enabled, the phone can detect personal SAFE state.
No Movement Sensitivity	Configures the sensitivity of “No movement” detection. There are 7 levels available for detection. Choose Disabled to stop No movement detection.
No Movement Timeout	Set the timeout value for “No movement” detection. The phone will start warning if the phone keeps no movement until timeout.
Tilt Sensitivity	Set the sensitivity of Tilt detection. There are 7 levels available for detection. Choose Disabled to stop Tilt detection.
Tilt Timeout	Set the timeout value for Tilt detection. The phone will start warning if the phone keeps tilt until timeout.
Running Sensitivity	Set the sensitivity of Running detection. There are 7 levels available for detection. Choose Disabled to stop Running detection.
Running Timeout	Set the timeout value for Running detection. The phone will start warning if the phone keeps waggle until timeout.
Snooze Timeout	Set the timeout value of snooze. You can choose snooze while in warning/alarm State. After the timeout, the phone will start detecting again.



Warning Timeout	Set the timeout value of warning. The phone will start alarm if the phone keeps warning and not be canceled.
Panic Call Silent Alarm	If set to “Yes”, the alarm triggered by pressing multi-function button will be silent alarm.
Emergency Call	If set to “Yes”, the phone will automatically dial out emergency dial number when into alarm state.
Associated account	Selects the call account for emergency calls.
Emergency Dial Force Speaker	If Set to ‘Yes’, the phone will use the speaker for emergency calls. Default setting is NO.
Emergency Dial Number	Set the number for dial out when into alarm state.
Warning Tone	Set the tone of warning.
Alarm Tone	Set the tone of alarm.



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.

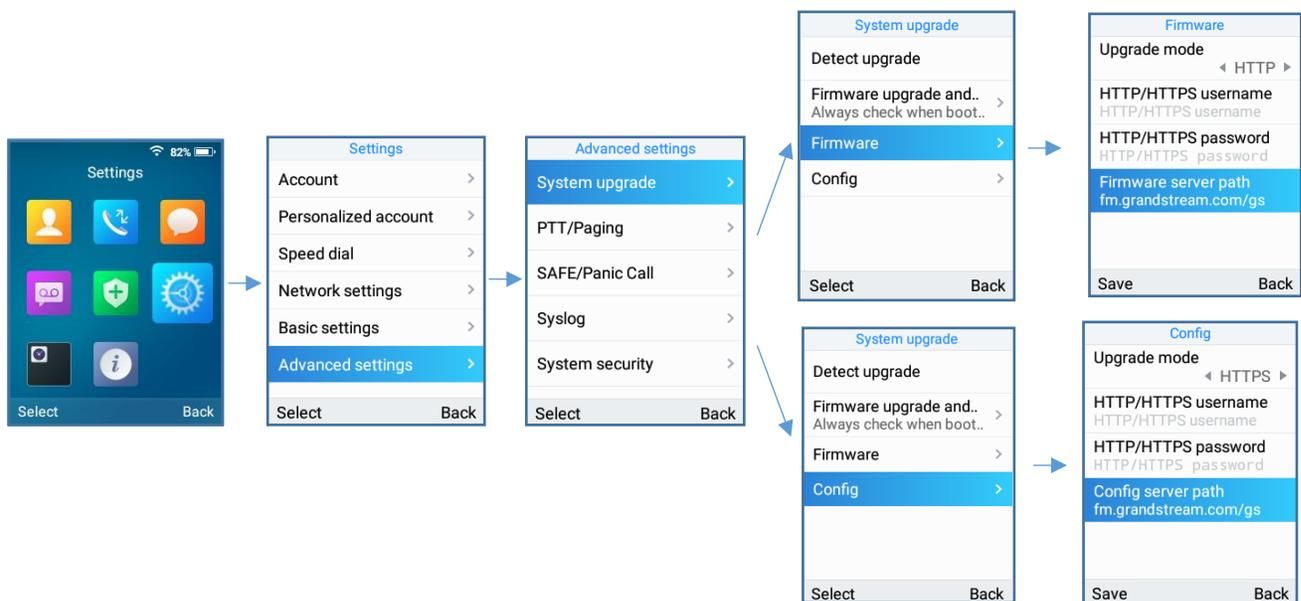


Figure 12: WP820 Upgrade Configuration via Keypad Menu

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 or reboot the phone for the upgrade process to begin.

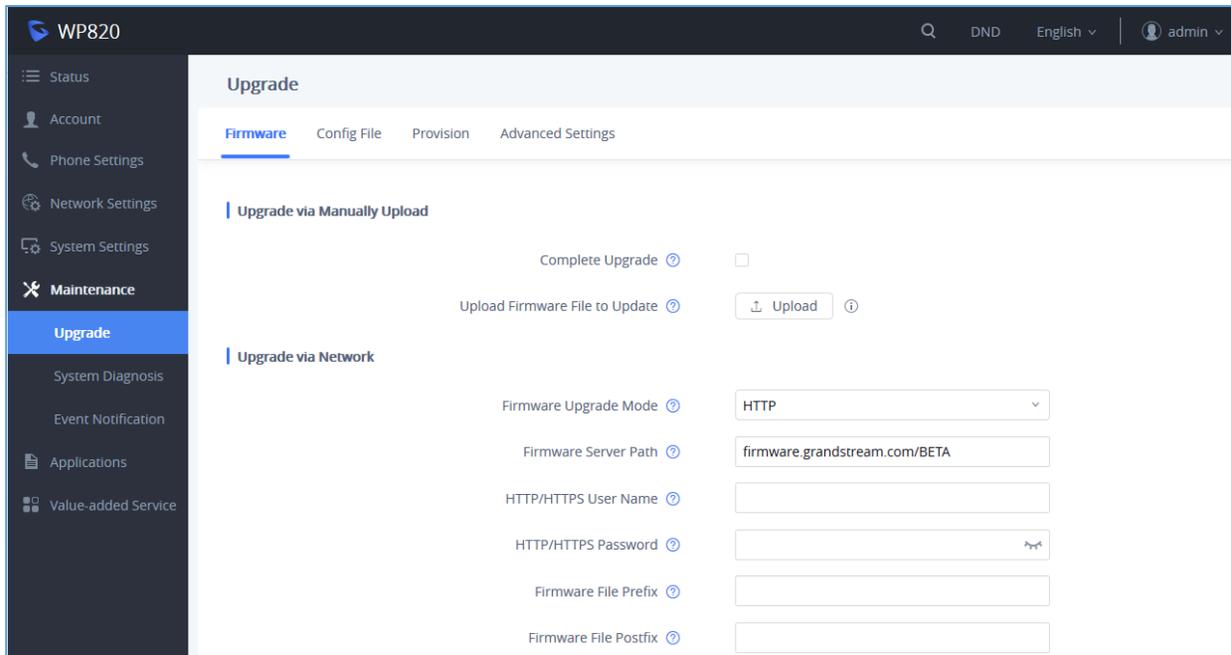


Figure 13: WP820 Upgrade Configuration via Web GUI

Note:

- Please do not power off or unplug the WP820 when the upgrading process is on.
- In case wrong firmware file is uploaded or something goes wrong, an error message will be prompt indicating that the firmware upgrade failed.

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.
<https://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.

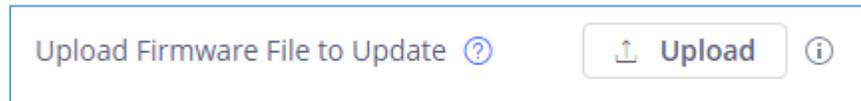


Figure 14: Upload Firmware File to Update

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 <https://www.grandstream.com/support/firmware> for latest firmware.

Instructions for local firmware upgrade via TFTP:

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



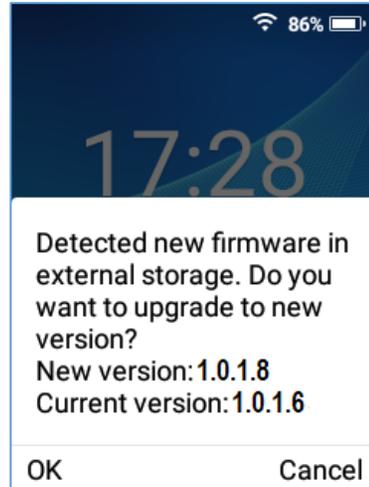


Figure 15: New Firmware Detected

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**

Config Provision via USB

This feature allows the user to place an XML configuration file on a USB drive and upload to WP820.

Note: WP820 will automatically scan the USB drive for `cfg{mac}.xml` files after the connection is established. Please ensure only one instance of the file type is contained in the root directory of the USB drive.

1. Download the Config 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 Config file.

Wi-Fi Provision via USB

This feature allows the user to place a Wi-Fi configuration package on USB and upload to WP820.

Note: Please see the Wi-Fi configuration upload guide on the Grandstream product page for additional details by using the following URL:

https://www.grandstream.com/hubfs/Product_Documentation/WiFi_provision_guide.pdf



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:

<https://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:
https://www.grandstream.com/hubfs/Product_Documentation/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.

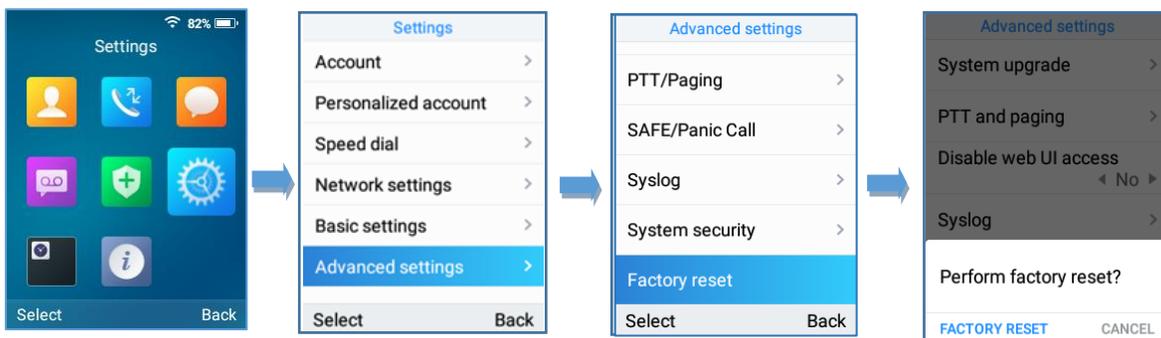


Figure 16: WP820 LCD - Confirm Factory Reset

3. Once confirming the factory 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.

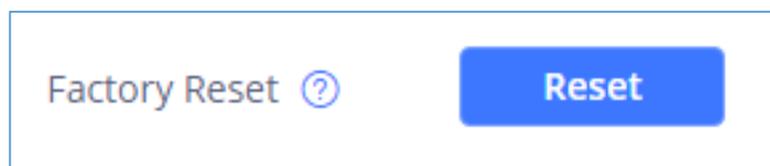


Figure 17: WP820 Web GUI - Factory Reset

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



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

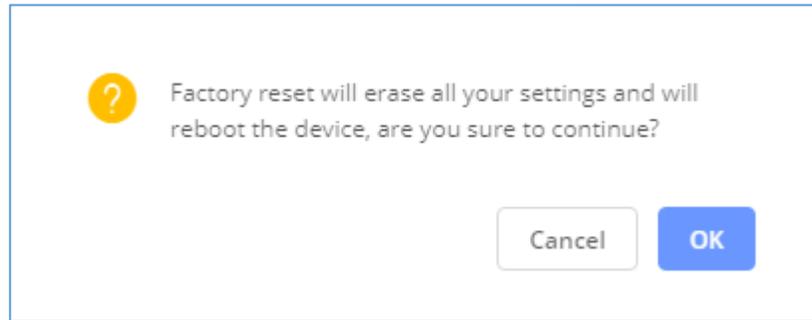


Figure 18: WP820 Web GUI - Confirm Factory Reset

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.

Note: When constraint mode or lock screen is enabled, the user will need to enter the admin password before the device can initiate the factory reset process.

EXPERIENCING WP820 ENTERPRISE PORTABLE WI-FI PHONE

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

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

Our technical support staff is trained and ready to answer all 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.

