Grandstream Networks, Inc.

WP810

Cordless Wi-Fi IP Phone

Administration Guide

COPYRIGHT

CAUTION

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

WARNING

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

Common part:

- This equipment complies with 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.

U.S. FCC Part 68 Regulatory Information

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

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

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

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

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

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

This equipment uses the following USOC jacks: RJ45C.

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

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

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

Company Name: Grandstream Networks, Inc.

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

Tel: 1-617-5669300

Fax: 1-617-2491987

WP810 Administration Guide
Version 1.0.7.7

U.S. FCC Part 15 Regulatory Information

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

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

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

The SAR limit of USA (FCC) is 1.6 W/kg averaged over one gram of tissue. This model (FCC ID: YZZWP810) has also been tested against this SAR limited.
The highest SAR value reported under this standard during product certification for use at the ear is 1.19 W/kg and body is 0.32 W/kg.
Body-worn SAR testing was worn on the belt clip at a separation distance of 0 mm. To meet RF exposure guidelines during body-worn operation, the device should be used with the belt clip.

Canada Regulatory Information

Radio equipment

Operation of 5150-5250 MHz is restricted to indoor use only.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1) L'appareil ne doit pas produire de brouillage.

2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-3 (B)/NMB-3(B)

This radio transmitter [IC: 11964A-WP810] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Terminal equipment

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

Ce produit répond à l'innovation, des sciences et de Développement économique Canada spécifications techniques applicables.

Le nombre équivalent de sonneries (REN) indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison de dispositifs, à la seule condition que la somme des REN de tous les dispositifs ne dépasse pas cinq.

EU Regulatory Information

Support Frequency Bands and Power:

WLAN 2412-2472 MHz < 20 dBm.

WLAN 5150-5250 MHz < 23 dBm.

WLAN 5250-5350 MHz / 5470-5725 MHz < 20 dBm.

Body-worn SAR testing has been carried out at a separation distance of 5 mm. To meet RF exposure guidelines during body-worn operation, the device should be positioned at least this distance away from the body.

The simplified EU declaration of conformity referred to in Article 10(9) shall be provided as follows:

Hereby, [Grandstream Networks, Inc.] declares that the radio equipment type [WP810] is in compliance with Directive 2014/53/EU.

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

GNU GPL INFORMATION

WP810 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL related source code can be downloaded from Grandstream web site from:
http://www.grandstream.com/support/faq/gnu-general-public-license/gnu-gpl-information-download

Table of Contents

WP810 Administration Guide
Version 1.0.7.7

WP810 Administration Guide
Version 1.0.7.7

WP810 Administration Guide
Version 1.0.7.7

Table of Tables

Table of Figures

WP810 Administration Guide
Version 1.0.7.7

DOCUMENT PURPOSE

This document describes how to configure WP810 Cordless Wi-Fi IP 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 WP810, please visit http://www.grandstream.com/support to download the latest "WP810 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.

WP810 Administration Guide
Version 1.0.7.7

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 1.0.7.7

- Added Multicast Listening setting fields for Multicast Paging settings on web UI [Multicast Listening].

Firmware Version 1.0.1.1

- This is the initial version.

GUI INTERFACE EXAMPLES

http://www.grandstream.com/sites/default/files/Resources/wp810_web_gui.zip

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

WELCOME

Thank you for purchasing Grandstream WP810. This powerful Cordless Wi-Fi IP Phone features dual-band 802.11a/b/g/n/ac Wi-Fi and supports Wi-Fi roaming. 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 120 hours standby time and 6 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 WP810:

Table 1: WP810 Features at a Glance

WP810	
	• 2 SIP accounts and 2 lines. • 3-way audio conference calls. • Dual-band 802.11a/b/g/n/ac Wi-Fi. • Wi-Fi roaming. • 120 hours standby time. • 6 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 WP810.

Table 2: WP810 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, 802.1x, TLS, SRTP, IPv6
Voice Codecs and Capabilities	Support for G.711µ/a, G.729A/B, G.722 (wide-band), iLBC, Opus, in-band and out-of-band DTMF (In audio, RFC2833, SIP INFO), VAD, CNG, AEC, PLC, AJB, AGC, ANS
Graphic Display	1.8-inch (128x160) TFT color LCD
Peripherals	2 soft keys, dial, hangup, speakerphone, phonebook, backlit keypad, proximity senor, vibration motor, volume button and navigation keys
Push-to-Talk	Customizable button for push-to-talk.
Auxiliary Ports	3.5 mm headset jack, Micro-USB port for charging, dual-MIC, dual-color MWI LED.
Telephony Features	Hold, transfer, forward, 3-way audio conference, downloadable phonebook XML (up to 500 items), call waiting, call log (up to 100 records), off-hook auto dial, auto answer, flexible dial plan, personalized music ringtones, 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 and Layer 3 (ToS, DiffServ, MPLS) QoS
Multi-language	English, Chinese, German, French, Italian, Portuguese, Russian, Spanish and more
Upgrade/ Provisioning	Firmware upgrade via TFTP/HTTP/HTTPS/FTP/FTPS, mass provisioning using encrypted XML configuration file, manual upload.
Power & Green Energy Efficiency	Universal power adapter included Input: 100-240VAC; Output: +5VDC, 1A (5W) 1500mA Li-ion battery, 120h standby time and 6h talk time
Physical	Handset Dimensions : 158.5 x 50 x 22.5mm Charger cradle dimensions : 81.15 x 75.89 x 36.36mm Handset weight: 120g Handset package weight (not including QIG): 340g
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.
Compliance	FCC, CE, RCM, IC

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining best performance with the WP810.

Equipment Packaging

Table 3: Equipment Packaging

WP810
• 1x Handset unit • 1x Universal power supply 5V • 1x Charging station • 1x Belt clip • 1x Rechargeable battery • 1x Quick Installation Guide
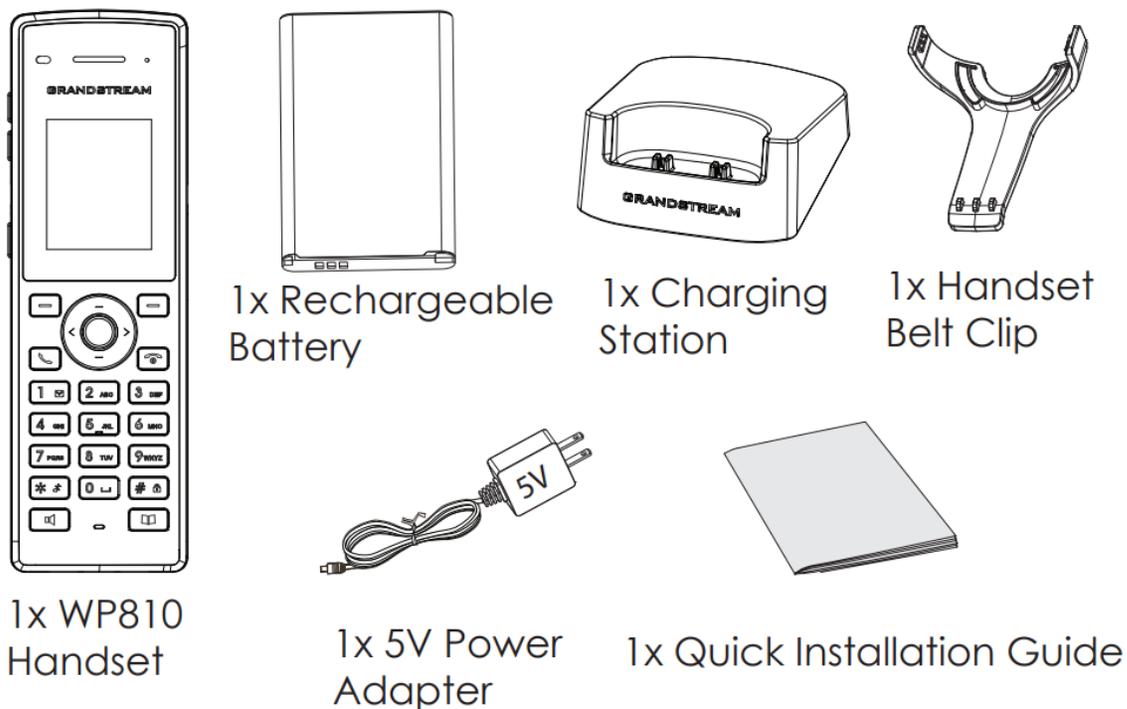
Figure 1: WP810 Package Content

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

Setting up the WP810

Charging Station

Plug the power adapter into a power source socket to start using the charging station.

1: Charging station
2: Power adapter
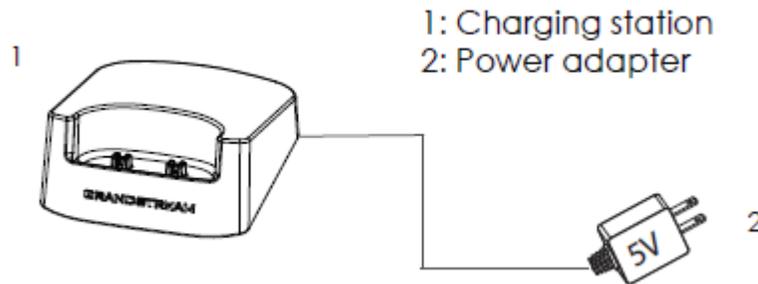
Figure 2: Charging Station

Handset

Please refer to the following steps in order to setup your WP810:
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**.

1: Battery cover
2: Battery
3: Rear of handset
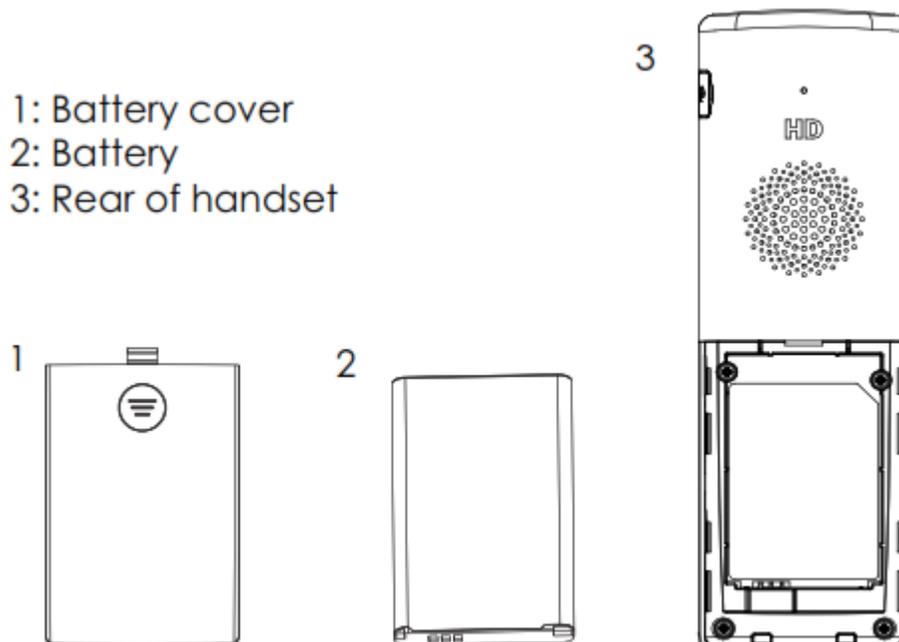
Figure 3: WP810 Handset Setup

WP810 Administration Guide
Version 1.0.7.7

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 120 hours

- **Talk time:** up to 6 hours' active talk time

In order to get the best performance of your WP810, 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.

WP810 Handset Keys Description

The WP810 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 WP810 LCD screen and the main hardware components.
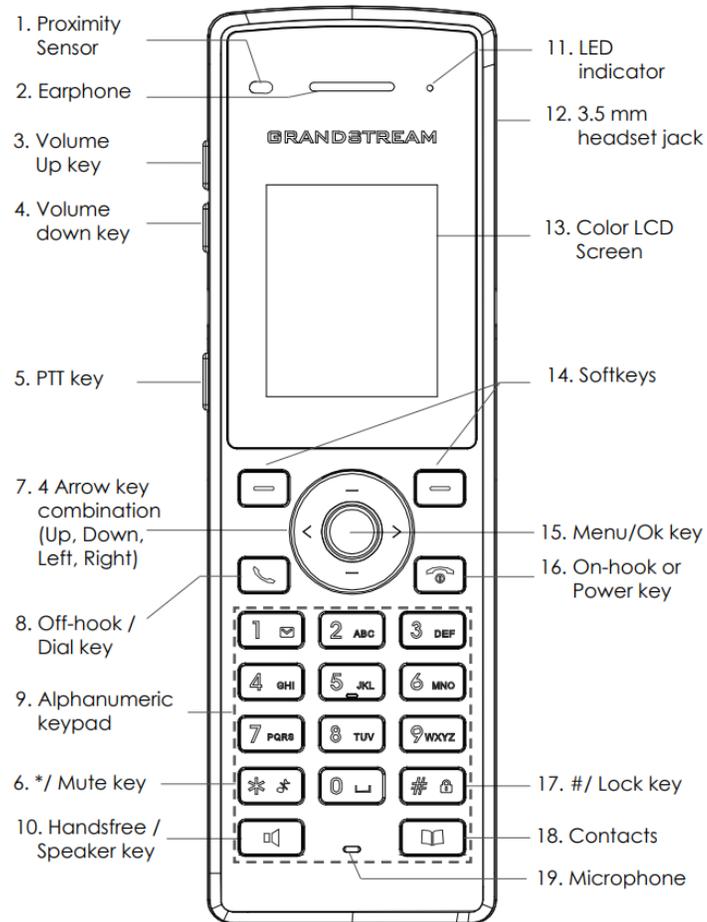
Figure 4: WP810 Description

The following table describe the WP810 keypad keys.

Table 4: WP810 Description

Key	Description
1.	**Proximity sensor**	The proximity senor can detect and measure gravitational acceleration, tilt, vibration, altitude changes, and static position.
2.	**Earphone**	Delivers audio output.
3,4	**Volume up / Down Keys**	Configure the handset and ringtone volume.
5.	**PTT Key**	PTT (Push-to-Talk) button, to initiate PTT call.
6.	*** / Mute key**	Keep pressing on * in idle screen to mute/unmute the ringtone.
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.	**Hands-free / Speaker key**	Activates or deactivates the mute feature when keep pressing on * in idle screen.
11.	**LED indicator**	1dual-color LED indicator indicating power, call, battery, message waiting…
12.	**3.5 mm headset jack**	Phone connector for the headphones/headsets.
13.	**Color LCD Screen**	1.8-inch (128x160) color LCD
14.	**Softkeys**	Correspond to functions displayed on the LCD. These functions change depending on the current context.
15.	**Menu/OK key**	Access to contacts list.
16.	**On-hook or Power key**	Selects the option chosen by the cursor or enters the main menu from the home screen.
17.	**# / Lock key**	Terminates calls or turns the handset on / off.
18.	**Contacts**	Locks keypad against unintentional entries when keep pressing #. • Press and hold # key for approximately 2 seconds to lock the keys. • Press **Unlock** softkey and then **#** to unlock the keys.
19.	**Microphone**	Picks up audio earpiece and hands-free calls.

WP810 Icons Description

Following table contains description of each icon that might be displayed on the screen of the WP810.

Table 5: WP810 Icons Description

	Battery status Charging
	Wi-Fi not enabled/configured
	Wi-Fi signal status
	Outgoing Call notification
	Missed Call notification
	Incoming Call notification
	Mute enabled icon
	DND enabled icon

🔒	**SRTP & TLS enabled icon**
👤	**Contacts**
💬	**SMS**
📞	**Call History**
📼	**Voice Mail**
🛡	**Diagnosis**
⚙	**Settings**
ℹ	**Status**

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

WP810 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.
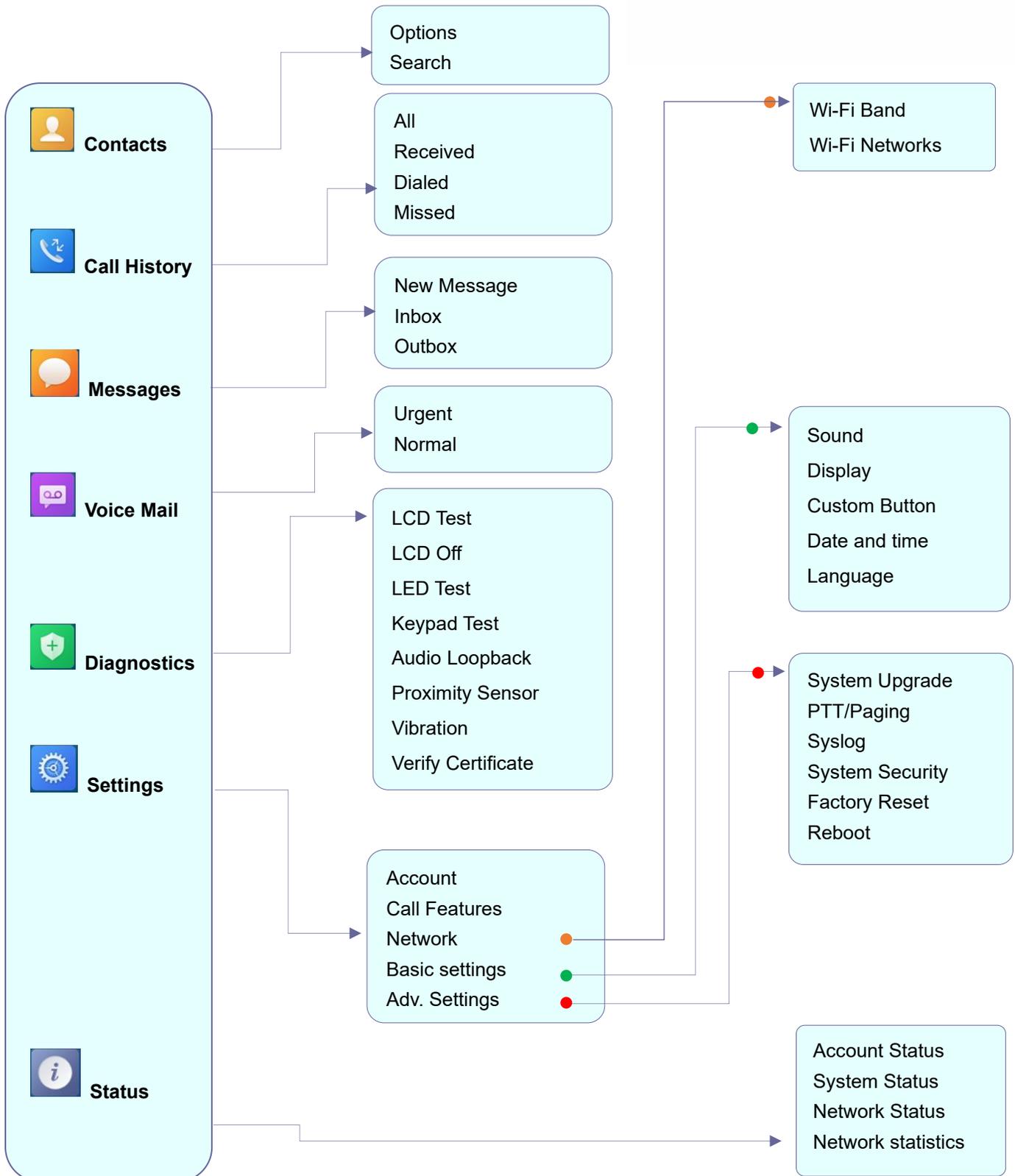
Figure 5: WP810 Menu Structure

WP810 Administration Guide
Version 1.0.7.7

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 Message"** of up to 160 characters to another device or check the received ones.
Voice Mail	• **Select:** Play voice mail messages received. Note: Voicemail ID needs to be configured, otherwise, "select" softkeys will open configuration settings.
Diagnostics	• **LCD Test** • **LCD off** • **LED Test** • **Keypad Test** • **Audio Loopback** • **Proximity Sensor** • **Vibration** • **Verify Certificate**
Settings	• **Account** Configure/View SIP accounts settings and account ringtone. • **Call settings** Configure the account auto answer, call forward, DND and speed dial settings. • **Network Settings** Configure the networks settings including Wi-Fi settings, Bluetooth settings, and additional networks settings. • **Basic Settings** Configure the basic settings including voice settings, display settings, Gestures and button customization, language settings and date/time settings. • **Adv. Settings** Configure the advanced settings including system upgrade, PTT/Paging settings, system security settings, syslog settings and factory reset / reboot.

Status	Displays account status, system info, Network status and network statistics
	    • **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.

Connecting WP810 to Wi-Fi Network

The WP810 supports dual-band 802.11a/b/g/n/ac Wi-Fi, please refer to the following steps in order to connect your WP810 to the Wi-Fi networks:

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

2. Select "Wi-Fi Band" (automatic, 2.4GHz or 5GHz) and navigate to "Wi-Fi Networks". 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)

WP810 will display Wi-Fi icon on the main LCD menu if the connection to the Wi-Fi network is successful.
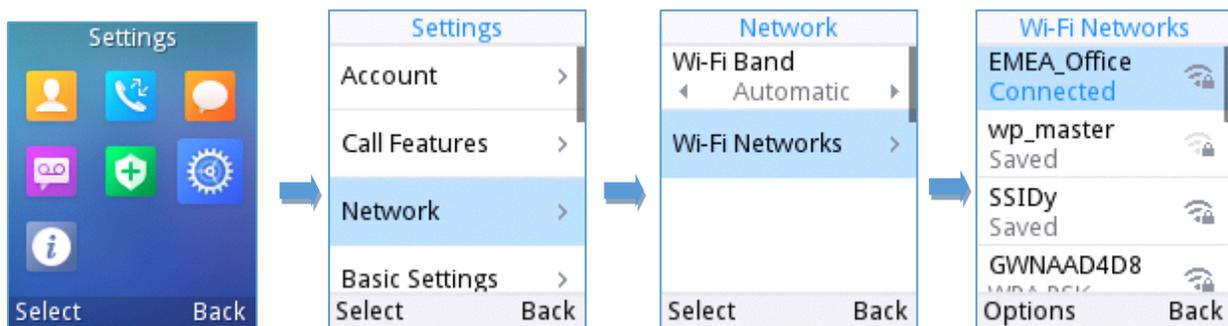
Figure 6 : Connecting to Wi-Fi Network

Notes:

• If 5GHz and 2.4Ghz are both available when "Wi-Fi Band" is set to "Automatic", the WP810 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.

• WP810 supports connection to Wi-Fi with captive portal enabled that requires additional credentials to sign up or login before it is allowed to use Wi-Fi.

Obtain WP810 IP Address

In order to know which IP address is assigned to your WP810, please follow below steps:

1. Unlock first your WP810 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 WP810.
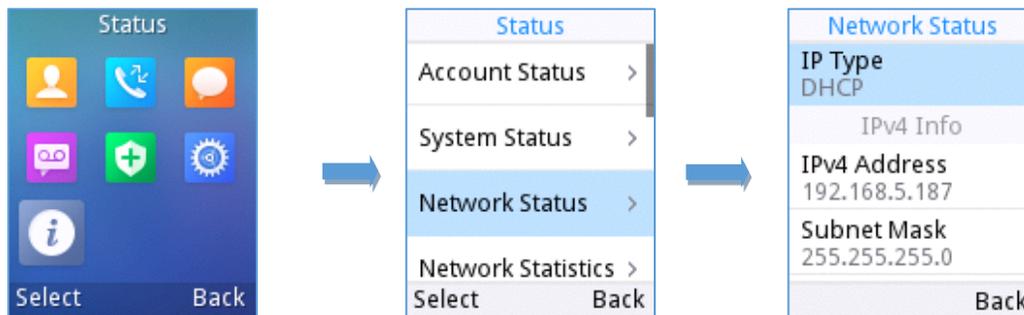
Figure 7: Obtaining IP Address

WP810 Administration Guide
Version 1.0.7.7

WP810 WEB GUI ACCESS CONFIGURATION

The WP810 can be configured using:

- Web GUI embedded on the WP810 using PC's web browser.

- LCD Configuration Menu using the WP810 keypad.

Note: From the Web GUI, you can configure all the functions supported by the WP810; while via keypad menu, you can access limited configuration.

Configuration via Web Browser

The WP810 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the WP810 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 WP810.

2. Make sure the WP810 is booted up and powered correctly.

3. You may check WP810 IP address via a subscribed WP810 on its LCD menu **Status → Network Status.** Please see **Obtain WP810 IP Address**

4. Open Web browser on your computer and enter the WP810 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 WP810. This can be easily done by connecting the computer to the same hub or switch as the WP810.

- The default administrator username is "admin", and the random password can be found on the sticker at the back of the unit. the default end-user username is "user" and the password is "123".

- If **'Web Access'** parameter is set to "Disabled" under **Advanced settings → System security**; web UI access will be disabled.

Web GUI Languages

Users can select the language in web GUI login page, or at the upper right of the web GUI after logging in.
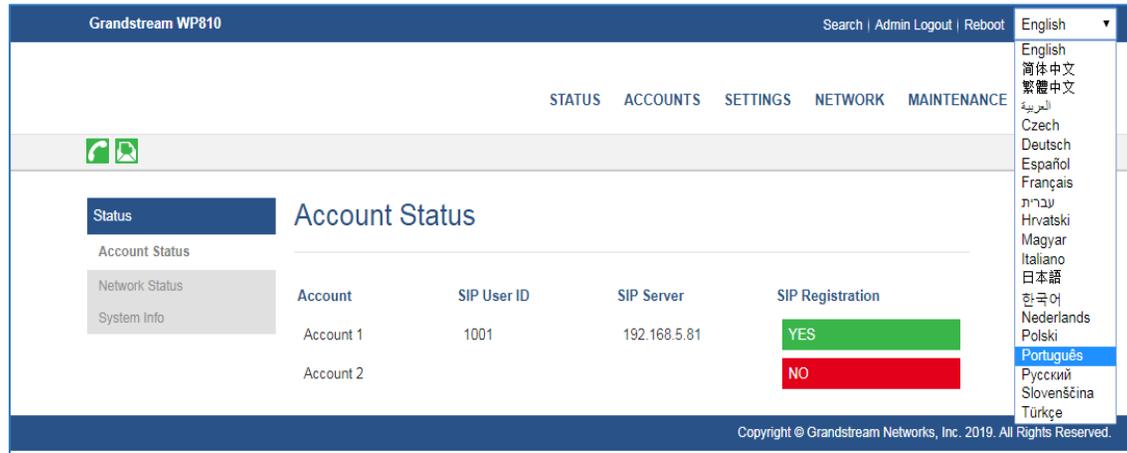
Figure 8: WP810 Web GUI Language

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	Random password available on the sticker at the back of the unit.	All pages

Changing User Level Password

1. Access the Web GUI of your WP810 using the admin's username and password.

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

3. Go to **Maintenance → Web Access.**

4. locate **User Password** section:

WP810 Administration Guide
Version 1.0.7.7

a. Type in your new user password in **New Password** field.

b. Type in again same entered password in **Confirm 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 WP810 using the admin's username and password. (Default username and password is admin/Random Password from the sticker on the back of the unit).

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

3. Go to **Maintenance → Web Access.**

4. locate **Admin Password** section:

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

b. Type in your new admin password in **New Password** field.

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

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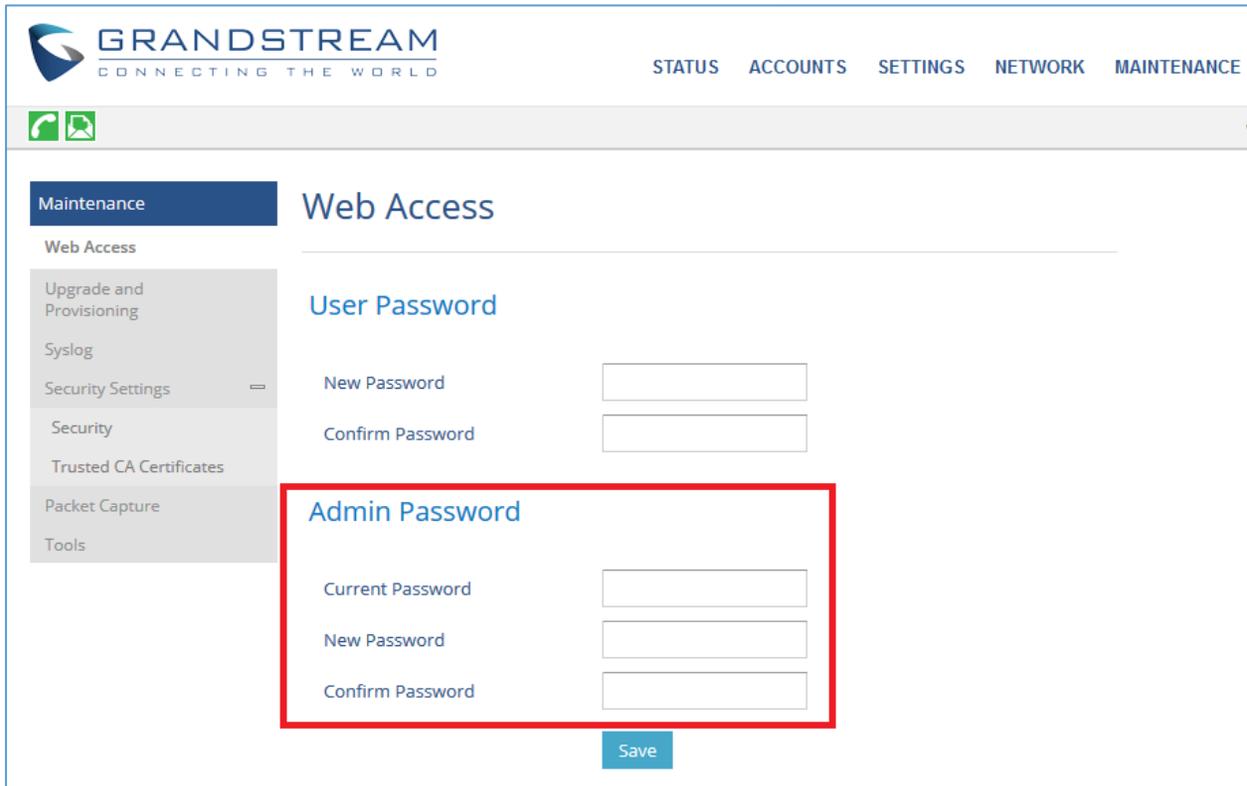
Figure 10: Admin Level Password

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 WP810 using the admin's username and password. (Default username and password are admin/Random password from the sticker on the back of the unit.).

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

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

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

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.
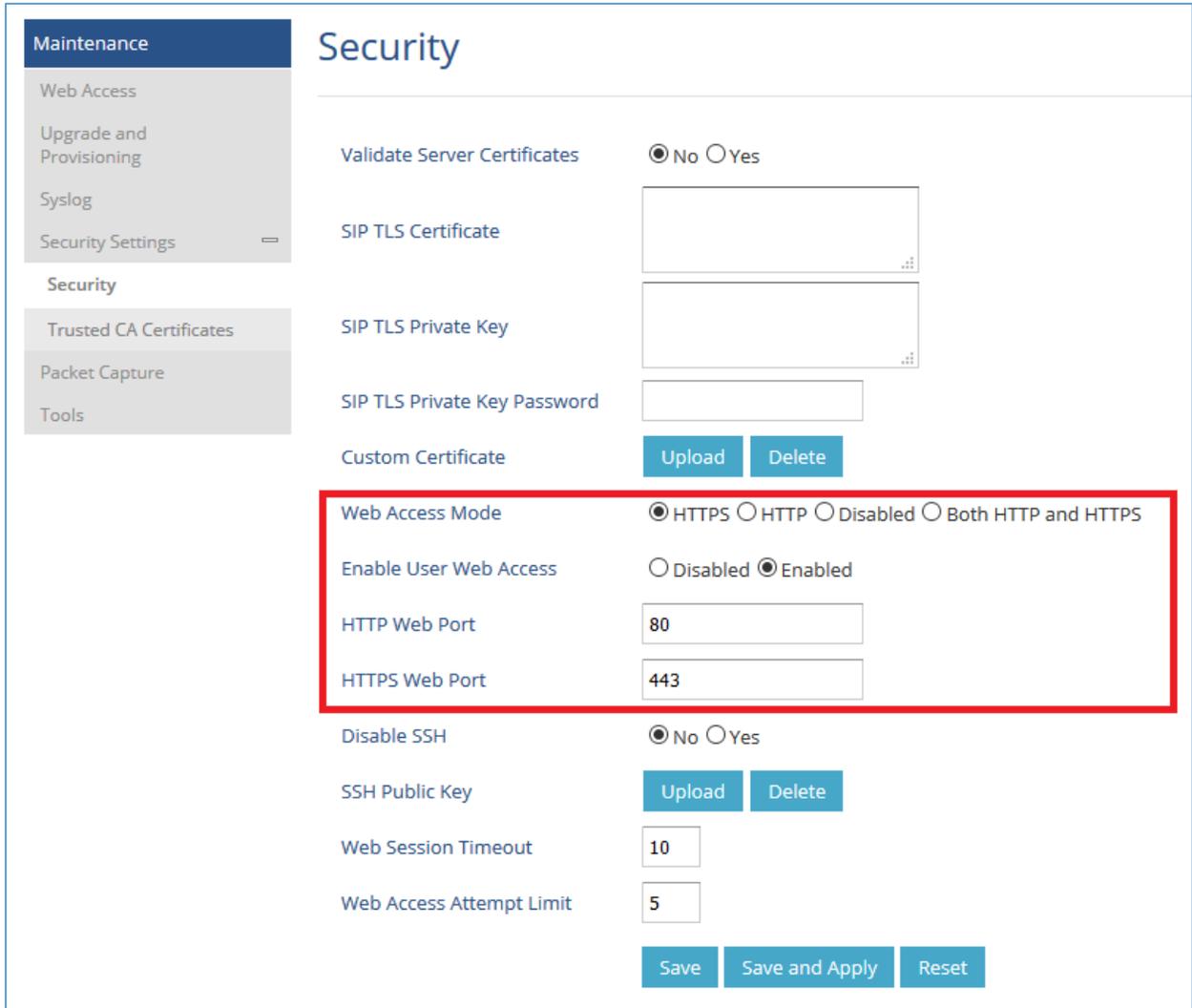
Figure 11: Web Access Port

WP810 WEB GUI SETTINGS

This section describes the options in the WP810 Web UI. As mentioned, you can log in as an administrator or an end user.

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

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

- **Settings:** Configure general settings, call settings, ringtone, Video Settings, Multicast paging

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

- **Maintenance:** Configure upgrade and provisioning settings, system diagnosis, and TR069 settings.

- **Directory:** Configure phonebook settings and Call History

Status Page Definitions

Status/Account Status

Account	Displays list of configured accounts.
SIP user ID	Displays the numbers of the configured accounts.
SIP Server	Displays list of SIP Server user by the configured accounts.
SIP Registration	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.
IPv4 Address Mode	Indicates the configured address mode: 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
Gateway	Displays assigned default gateway. Example: 192.168.5.1

IPv6 Address Mode	Indicates the configured address mode: DHCP or Static IP
IPv6 Address	Displays assigned IP address.
DNS	Shows assigned DNS server address.
NAT Type	Indicates type of NAT for each Profile. (Based on STUN protocol.)
NAT Traversal	
Account 1	Indicates type of NAT for Account 1.
Account 2	Indicates type of NAT for Account 2.

Status/System Info

Product Model	Product model of the phone.
Part Number	Product part number.
Software Version	
Boot	Booting code version.
Manifest	Specifies Manifest version.
Core	Specifies Core version.
Base	Specifies Base version.
IP Geographic Information	
Time Zone	Time Zone information
System Time	
System Up Time	System up time since last reboot.
System Time	Shows actual time and date according to your configuration
Service Status	
gui	Reveals status of GUI
phone	Reveals status of phone
System Information	
Download System Information	Click to "download" the user's configuration file.

User Space	
User Space Used	Reveals status of user space
Database Status	Reveals status of database
Core Dump	
Generate core dump	Generate core dump by killing program.
Core Dump	Core Dump status

Accounts Page Definitions

Account/General 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.
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.
Backup Outbound Proxy	IP address or Domain name of the Secondary Outbound Proxy which will be used when the primary proxy cannot be connected.
SIP User ID	Configures the SIP service subscriber's ID used for authentication. It can be identical to or different from the SIP User ID.
Authenticate ID	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.
Authenticate Password	The account password required for the phone to authenticate with the SIP server before the account can be registered.

Name	Configures the SIP server subscriber's name (optional) that will be used for Caller ID display.
Voice Mail Access Number	Defines the voice mail portal access number to allow users accessing their voice messages.
Account Display	When set to "Username", LCD will display Username if it is not empty; When set to "User ID", LCD will display User ID if it is not empty.

Account/Network Settings

DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. There are four modes: A Record, SRV, NATPTR/SRV, Use Configured IP. The default setting is "A Record". If the user wishes to locate the server by DNS SRV, the user may select "SRV" or "NATPTR/SRV".
	
	If "Use Configured IP" is selected, please fill in the three fields below:
	  - **Primary IP:**
	  - **Backup IP 1.**
	  - **Backup IP 2.**
	If SIP server is configured as domain name, phone will not send DNS query, but use "Primary IP" or "Backup IP x" to send SIP message if at least one of them are not empty.
	Phone will try to use "Primary IP" first. After 3 tries without any response, it will switch to "Backup IP x", and then it will switch back to "Primary IP" after 3 re-tries. If SIP server is already an IP address, phone will use it directly even "User Configured IP" is selected

DNS SRV Fail-over Mode	The option will decide which IP is going to be used in sending SIP packets after IPs for SIP server host are resolved with DNS SRV.
	  - **Default**
	If the option is set with "default", it will again try to send register messages to one IP at a time, and the process repeats.
	  - **Saved one until DNS TTL**
	If the option is set with "Saved one until DNS TTL", it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up.
	  - **Saved one until no responses**
	If the option is set with "Saved one until no responses", it will send register messages to the previously registered IP first, but this behavior will persist until the registered server does not respond.

Primary IP	Configures the primary IP address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP1	Configures the backup IP1 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode
Backup IP2	Configures the backup IP2 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode
NAT Traversal	This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, STUN, Keep-alive, UPnP, Auto or VPN. The default setting is "No". If set to "STUN" and STUN server is configured, the phone will route according to the STUN server. If NAT type is Full Cone, Restricted Cone or Port-Restricted Cone, the phone will try to use public IP addresses and port number in all the SIP&SDP messages. The phone will send empty SDP packet to the SIP server periodically to keep the NAT port open if it is configured to be "Keep-alive". Configure this to be "No" if an outbound proxy is used. "STUN" cannot be used if the detected NAT is symmetric NAT. Set this to "VPN" if OpenVPN is used
Proxy-Require	Adds the Proxy-Required header in the SIP message. It is used to indicate proxy-sensitive features that must be supported by the proxy. Do not configure this parameter unless this feature is supported on the SIP server.

Account/SIP Settings

Basic Settings	
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to "User=Phone". Then a "User=Phone" parameter will be attached to the Request-Line and "TO" header in the SIP request to indicate the E.164 number. If set to "Enable", "Tel:" will be used instead of "SIP:" in the SIP request. The default setting is "Disable".
SIP Registration	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is "Yes".
Unregister On Reboot	Allows the SIP user's registration information to be cleared when the phone reboots. The SIP REGISTER message will contain "Expires: 0" to unbind the connection. Three options are available: The default setting is "No". • If set to "All", the SIP user's registration information will be cleared when the phone reboots. The SIP Contact header will contain "*" to notify the server to unbind the connection.

	• If set to "Instance", the SIP user will be unregistered on current phone only. • If set to "No", the phone will not unregister the SIP account when rebooting.
Register Expiration	Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar. The default value is 60 minutes. The maximum value is 64800 minutes (about 45 days).
Subscribe Expiration	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar. The maximum value is 64800 (about 45 days). The default value is 60 minutes.
Reregister Before Expiration	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default value is 0.
Enable OPTIONS Keep Alive	Enable OPTIONS Keep Alive to check SIP Server.
OPTIONS Keep Alive Interval	Time interval for OPTIONS Keep Alive feature in Second.
OPTIONS Keep Alive Max Lost	Number of max lost packets for OPTIONS Keep Alive feature before the phone re-registration.
Local SIP Port	Defines the local SIP port used to listen and transmit. The default value is 5060 for Account 1, 5062 for Account 2, 5064 for Account 3, 5066 for Account 4, 5068 for Account 5, 5070 for Account 6. The valid range is from 1 to 65535.
SIP Registration Failure Retry Wait Time	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
SIP Transport	Determines the network protocol used for the SIP transport. Users can choose from TCP, UDP and TLS. The default setting is "UDP".
SIP Listening Mode	Based on option "SIP Transport" and this option "SIP Listening Mode", phone will decide which transport protocol it should listening to from the incoming request. The default setting is "Transport Only". • Transport Only • Dual

	• Dual (Secured)
	• Dual (BLF Enforced)

SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	This option is used to control the port information in the Via header and Contact header. If set to No, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. The default setting is "No".
Outbound Proxy Mode	The Outbound proxy mode is placed in the route header when sending SIP messages, or they can be always sent to outbound proxy.
Support SIP Instance ID	Defines whether SIP Instance ID is supported or not. Default setting is "Yes".
SUBSCRIBE for MWI	When set to "Yes", a SUBSCRIBE for Message Waiting Indication will be sent periodically. The phone supports synchronized and non-synchronized MWI. The default setting is "No".
SUBSCRIBE for Registration	When set to "Yes", a SUBSCRIBE for Registration will be sent out periodically. The default setting is "No".
Enable 100rel	The use of the PRACK (Provisional Acknowledgment) method enables reliability to SIP provisional responses (1xx series). This is very important to support PSTN internetworking. To invoke a reliable provisional response, the 100rel tag is appended to the value of the required header of the initial signaling messages. The default setting is "No".
Callee ID Display	When set to "Auto", the phone will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in the 180 Ringing. If "Disabled", callee ID will be displayed as "Unavailable". When set to "To Header", caller ID will not be updated and displayed as To Header.
Caller ID Display	When set to "Auto", the phone will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. When set to "Disabled", all incoming calls are displayed with "Unavailable". When set to "From Header", the phone will display the caller ID based on the From Header in the incoming SIP INVITE. The default setting is "Auto".
Add Auth Header on Initial REGISTER	To define whether authorization Header will be added on initial REGISTER from the first REGISTER. The default setting is "No".
Allow SIP Reset	This is used to perform a factory reset through SIP NOTIFY. When the phone receives the NOTIFY with event: RESET, the phone should perform a factory reset after the authentication. The default setting is "No".

WP810 Administration Guide
Version 1.0.7.7

Ignore Alert-Info header	This option is used to configure default ringtone. If set to "Yes", configured default ringtone will be played. The default setting is "No".
Custom SIP Headers	
Use Privacy Header	Controls whether the Privacy header will present in the SIP INVITE message or not, whether the header contains the caller info. When set to "Default", the Privacy Header will show in INVITE only when "Huawei IMS" special feature is on. If set to "Yes", the Privacy Header will always show in INVITE. If set to "No", the Privacy Header will not show in INVITE. Default setting is "Default".
Use P-Preferred-Identity Header	Controls whether the P-Preferred-Identity Header will present in the SIP INVITE message. The default setting is "default": The P-Preferred-Identity Header will show in INVITE unless "Huawei IMS" special feature is on. If set to "Yes", the P-Preferred-Identity Header will always show in INVITE. If set to "No", the P-Preferred-Identity Header will not show in INVITE.
Use P-Access-Network-Info Header	Enables / disables the use of P-Access-Network-Info header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "No".
Use P-Emergency-Info Header	Enables / disables the use of P-Emergency-Info header in SIP request. When disabled, the SIP message sent from the phone will not include the selected header. Default setting is "No".
Use MAC Header	If Yes except REGISTER, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP messages except REGISTER message will attach the MAC address to the User-Agent header. If Yes to ALL, the sip message for register or unregister will contains MAC address in the header, and all the outgoing SIP message including REGISTER will attach the MAC address to the User-Agent header. If No, neither will the MAC header be included in the register or unregister message nor the MAC address be attached to the User-Agent header for any outgoing SIP message.
Advanced Features	
PUBLISH for Presence	Enables Presence feature on the phone.
Omit charset=UTF-8 in MESSAGE	Omit charset=UTF-8 in MESSAGE content-type

Special Feature	Different soft switch vendors have special requirements. Therefore, users may need select special features to meet these requirements. Users can choose from Standard, Nortel MCS, Broadsoft, CBCOM, RNK, Sylantro, Huawei IMS, PhonePower and UCM Call center depending on the server type. The default setting is "Standard".
Session Timer	
Enable Session Timer	This option is used to enable or disable session timer on the phone side. The default setting is "No".
Session Expiration	The SIP Session Timer extension (in seconds) that enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand. The default setting is 180. The valid range is from 90 to 64800.
Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
Caller Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it makes outbound calls. The default setting is "No".
Callee Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it receives inbound calls. Default setting is "No".
Force Timer	If Force Timer is set to "Yes", the phone will use the session timer even if the remote party does not support this feature. If Force Timer is set to "No", the phone will enable the session timer only when the remote party supports this feature. To turn off the session timer, select "No". The default setting is "No".
UAC Specify Refresher	As a Caller, select UAC to use the phone as the refresher; or select UAS to use the Callee or proxy server as the refresher. The default setting is "Omit".
UAS Specify Refresher	As a Callee, select UAC to use caller or proxy server as the refresher; or select UAS to use the phone as the refresher. The default setting is "UAC".
Force INVITE	The Session Timer can be refreshed using the INVITE method or the UPDATE method. Select "Yes" to use the INVITE method to refresh the session timer. The default setting is "No".
Security Settings	
Check Domain Certificates	Choose whether the domain certificates will be checked or not when TLS/TCP is used for SIP Transport. The default setting is "No".

Validate Certificate Chain	Validate certification chain when TCP/TLS is configured. Default setting is "No".
Validate Incoming Messages	Choose whether the incoming messages will be validated or not. The default setting is "No".
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is "No".
Accept Incoming SIP from Proxy Only	When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is "No".
Authenticate Incoming INVITE	If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. Default setting is "No".

Account/Audio Settings

Preferred Vocoder	Multiple vocoder types are supported on the phone, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message.
Use First Matching Vocoder in 200OK SDP	When it is set to "Yes", the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is "No".
Codec Negotiation Priority	Configures the phone to use which codec sequence to negotiate as the callee. When set to "Caller", the phone negotiates by SDP codec sequence from received SIP Invite. When set to "Callee", the phone negotiates by audio codec sequence on the phone. The default setting is "Callee".
Disable Multiple m line in SDP	When it is set to "No", the device will reply with multiple m lines; Otherwise, it will reply 1 m line. The default setting is "No".
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu. The default setting is "Disabled".
SRTP Key Length	Allows users to specify the length of the SRTP calls. The available options are AES 128&256 bit, AES 128 bit and AES 256 bit. Default setting is AES 128&256 bit
Crypto Lifetime	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. The default setting is "Yes".
Symmetric RTP	Defines whether symmetric RTP is supported or not. Default setting is "No".
Silence Suppression	Controls the silence suppression/VAD feature of the audio codecs except forG.723 (pending) and G.729. If set to "Yes", a small quantity of RTP packets containing comfort noise will be sent during the periods of silence. If set to "No", this feature is disabled. Default setting is "No"

Jitter Buffer Type	Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is "Adaptive".
Jitter Buffer Length	Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is "300ms".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used and the actual frames transmitted during the in-payload call. For end users, it is recommended to use the default setting, as incorrect settings may influence the audio quality. The default setting is 2.
G.726-32 Packing Mode	Selects "ITU" or "IETF" for G726-32 packing mode. The default setting is "ITU".
iLBC Frame Size	This option determines the iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is "30ms".
iLBC Payload Type	This option is used to specify iLBC payload type. Valid range is 96 to 127. The default setting is "97".
OPUS Payload Type	Specifies OPUS payload type. Valid range is 96 to 127. Cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Send DTMF	This parameter specifies the mechanism to transmit DTMF digits. There are 3 supported modes: • In audio: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs). • RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. • SIP INFO uses SIP INFO to carry DTMF. Default setting is "RFC2833".

Account/Call Settings

Call Log	Configures Call Log setting on the phone. You can log all calls, only log incoming/outgoing calls (missed calls will not be logged) or disable call log. The default setting is "Log All Calls".
Send Anonymous	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous, blocking the Caller ID to be displayed. Default is "No".
Anonymous Call Rejection	If set to "Yes", anonymous calls will be rejected. The default setting is "No".

Auto Answer	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep. Default setting is "No".
Refer-To Use Target Contact	If set to "Yes", the "Refer-To" header uses the transferred target's Contact header information for attended transfer. The default setting is "No".
Blind Transfer Wait Timeout	Defines the timeout (in seconds) for waiting SIP frag response in blind transfer. Valid range is 30 to 300.
Key As Send	Allows users to configure either the "*" or "#" keys as the "Send" key. Please make sure the dial plan is properly configured to allow dialing * and # out. The default setting is "Pound (#)".
RFC2543 Hold	Allows users to toggle between RFC2543 hold and RFC3261 hold. RFC2543 hold (0.0.0.0) allows user to disable the hold music sent to the other side. RFC3261 (a line) will play the hold music to the other side.
Disable Call Waiting	Enables / disables the call waiting feature for the current account. When set to "Default", global call feature setting will be used. Default setting is Default.
Ringtone	
Ring Timeout	Defines the timeout (in seconds) for the rings on no answer. The default setting is 60. The valid range is from 10 to 300.

Account /Intercom Settings

Allow Auto Answer by Call-Info/Alert-Info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info/Alert-Info header sent from the server/proxy.
Allow Barging by Call-Info/Alert-Info	When enabled, the phone will automatically put the current call on hold and answer the incoming calls based on the SIP Call-Info/Alert-Info header sent from the server/proxy. However if the current call was answered based on the SIP Call-Info/Alert-Info header, then all other incoming calls with SIP Call-Info/Alert-Info headers will be rejected automatically.
Custom Alert-Info for Auto Answer	Used exclusively to match the contents of the Alert-Info header for auto answer. The default auto answer headers will not be matched if this is defined.

Account /Feature Codes

Enable Local Call Features	When enabled, Do Not Disturb, Call Forwarding and other call features can be used via the local feature codes on the phone. Otherwise, the provisioned feature codes from the server will be used. User configured feature codes will be used only if server provisioned feature codes are not provided. And once feature codes are configured, either via server provisioning or local setting, a Softkey named "Features" will show on the LCD screen. **Note:** If the device is registered with Broadsoft account, it doesn't matter if local call features are enabled or disabled, once the Broadsoft account is set, special feature to Broadsoft and Feature Key Synchronization is enabled, the call feature will be handled by Broadsoft server, not by the phone.

Account Swap

Swap Account Settings	Swap configurations between two accounts

Settings Page Definitions

Settings/General Settings

Local RTP Port	Defines local RTP port used to listen and transmit RTP packets.
Local RTP Port Range	This parameter defines the range of local RTP port from 48 to 10000.
Use Random Port	Forces the phone to use random ports for both SIP and RTP messages. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is "**No**". **Note:** This parameter must be set to "No" for Direct IP Calling to work.
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.
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 keeping the box blank.
STUN server	The IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Delay Registration	Configures specific time that the account will be registered after booting up.
Test Password Strength	Only Allow password with some constraints to ensure better security.

Settings/Call Features

Disable Call Waiting	Disables the call waiting feature. The default setting is "No".
Disable Direct IP Call	Disables Direct IP Call. The default setting is "No".
Do Not Escape # as %23 in SIP URI	Specifies whether to replace # by %23 or not for some special situations. The default setting is "No".
Return Code When Refusing Incoming Call	When refusing the incoming call. The phone will send the selected type of SIP message of the call. Default setting is "Busy 486".
Return Code When Enable DND	When DND is enabled, the phone will send the selected type of SIP message. Default setting is "Busy 486".
Allow Incoming Call Before Ringing	This allows incoming calls after dialed but before ringing. This can be used under custom user configuration based on need. Default setting is No.
User-Agent Prefix	Configure the prefix in the User-Agent header.
Auto Answer Delay	Configure the delay for automatically answering the incoming call. Valid range is 0 to 10 (second).

Settings /Multicast Paging

Allowed In DND Mode	Allow Multicast paging when DND Mode is enabled
Paging Barge	During active call if incoming multicast page is higher priority (1 being the highest) than this value the call will be held, and multicast page will be played.
Paging Priority Active	If enabled, during a multicast page if another multicast is received with higher priority (1 being the highest) that one will be played instead.
Multicast Sender ID	Outgoing caller ID that displays to your page group recipients(for multicast channel 1 - 50).
Multicast Listening	Defines multicast listening addresses and labels. For example: • "Listening Address" should match the sender's Value such as "237.11.10.11:6767" • "Label" could be the description you want to use.

Settings /Preferences

Date and Time	
NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. The default setting is "pool.ntp.org".
Secondary NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. Allow user to configure 2 NTP servers.

NTP Update Interval	Time interval for updating time from the NTP server. Valid time value is in between 5 to 1440 minutes. The default setting is "1440" minutes.
Allow DHCP Option 42 to override NTP server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is "Yes".
Time Zone	Configures the date/time used on the phone according to the specified time zone.
Allow DHCP Option 2 to Override Time Zone Setting	Allows device to get provisioned for Time Zone from DHCP Option 2 in the local server.
Self-Defined Time Zone	This parameter allows the users to define their own time zone. The syntax is: **std offset dst [offset], start [/time], end [/time]** Default is set to: **MTZ+6MDT+5, M4.1.0, M11.1.0 MTZ+6MDT+5** This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east. **M4.1.0, M11.1.0** The 1st number indicates Month: 1,2,3..., 12 (for Jan, Feb, ..., Dec) The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…) The 3rd number indicates weekday: 0,1, 2,....,6 (for Sun, Mon, Tue, … ,Sat) Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.
Date Display Format	Configures the date display format on the LCD.
Time Display Format	Configures the time display in 12-hour or 24-hour format on the LCD. The default setting is in 12-hour format.
Language	
Display Language	Selects display language on the phone. Default is English.
Ringtone	
Call Progress Tones	Configures tone frequencies according to user preference. By default, the tones are set to North American frequencies. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. ON is the period of ringing ("On time" in "ms" while OFF is the period of silence. Up to three cadences are supported. • **Dial Tone** • **Second Dial Tone** • **Message Waiting** • **Ring Back Tone**

	• **Call-Waiting Tone**
Call Waiting Tone Gain	Configures the call waiting tone gain to adjust call waiting tone volume. Default is "Low".

Network Settings Page Definitions

Network /Basic Settings

Host name (Option 12)	Specifies the name of the client. This field is optional but may be required by Internet Service Providers.
Vendor Class ID (Option 60)	Used by clients and servers to exchange vendor class ID.

Network /Advanced Settings

HTTP Proxy	Specifies the HTTP proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Bypass Proxy For	Enter host names that do not require a proxy to reach. Those names should be separated by commas.
Layer 3 QoS for SIP	Defines the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. Default is 26.
Layer 3 QoS for RTP	Defines the Layer 3 QoS parameter for RTP. This value is used for IP Precedence, Diff-Serv or MPLS. Default is 46.

Network /Wi-Fi Settings

SSID 1-10	
SSID	Wi-Fi name
Enabled	Enable/Disable SSID
Hidden	Specifies if it is a Hidden SSID
Security	
Security Type	Wi-Fi encryption type
Password	Password to access Wi-Fi Network
Network	
Internet Protocol	Selects which Internet protocol to use. When both IPv4 and IPv6 are enabled, phone attempts to use preferred protocol first and switches to the other choice if it fails.

IPv4 Address	Select the address mode for the IPv4 Address obtained on the phone. Default is "DHCP". If set to "Static", additional information will be required: • IPv4 Static Address • Subnet Mask • Gateway • DNS server 1 & 2
Preferred DNS Server	Enter the Preferred DNS server.
IPv6 Address	Select the address mode for the IPv6 Address obtained on the phone. Default is "Auto-configured". If set to "Statically configured", additional information will be required: - **Full Static**: Configures IPv6 address using Full Static type. • Static IPv6 Address • IPv6 Prefix length - **Prefix Static**: Configures IPv6 address using Prefix Static type. • IPv6 Prefix (64 bits) • DNS server 1 & 2
Preferred DNS Server	Enter the Preferred DNS server.

Maintenance Page Definitions

Maintenance/Web Access

User Password	
New Password	Set new password for web GUI access as User. This field is case sensitive.
Confirm Password	Enter the new User password again to confirm.
Admin Password	
Current Password	The current admin password is required for setting a new admin password.
New Password	Set new password for web GUI access as Admin. This field is case sensitive.
Confirm Password	Enter the new Admin password again to confirm.

Maintenance/ Upgrade and Provisioning

Upgrade Firmware	Allows users to upload the firmware file locally by pressing Start, after selecting the correct firmware file from the local storage, the phone will start the firmware upgrade automatically.
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent: Always Check for New Firmware, Check New Firmware only when F/W pre/suffix changes, Always Skip the Firmware Check. The default setting is "Always Check for New Firmware".

Always Authenticate Before Challenge	Only applies to HTTP/HTTPS. If enabled, the phone will send credentials before being challenged by the server. The default setting is "No".
Validate Hostname in Certificate	To validate the hostname in the SSL certificate
Allow DHCP Option 43 and Option 66 Override Server	Default setting is "Yes". DHCP option 66 originally was only designed for TFTP server. Later on it was extended to support an HTTP URL. WP phones support both TFTP and HTTP server via option 66. Users can also use DHCP option 43 vendor specific option to do this. DHCP option 43 approach has priorities. The phone is allowed to fall back to the original server path configured in case the server from option 66 fails.
Additional Override DHCP Option	When enabled, users could select Option 150 or Option 160 to override the firmware server instead of using the configured firmware server path or the server from option 43 and option 66 in the local network. Please note this option will be effective only when option "Allow DHCP Option 43 and Option 66 to Override Server" is enabled. The default setting is "None".
Allow DHCP Option 120 to override SIP Server	Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is "No".
Automatic Upgrade	Enables automatic upgrade and provisioning. The default setting is "No".
Randomized Automatic Upgrade	Randomized Automatic Upgrade within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s).
Hour of the Day (0-23)	Defines the hour of the day to check the HTTP/TFTP/FTP server for firmware upgrades or configuration files changes. The default value is 1.
Day of the Week (0-6)	Defines the day of the week to check HTTP/TFTP/FTP server for firmware upgrades or configuration files changes. The default value is 1.
Disable SIP NOTIFY Authentication	Device will not challenge NOTIFY with 401 when set to "Yes". Default setting is "No".
Config	
Config Upgrade Via	Allows users to choose the config upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is "HTTPS".
Config Server Path	Defines the server path for provisioning.
Config Server Username	The username for the config server.
Config Server Password	The password for the config server.
Config File Prefix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.

Config File Postfix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
XML Config File Password	The password for encrypting XML configuration file using OpenSSL. This is required for the phone to decrypt the encrypted XML configuration file.
Authenticate Conf File	Sets the phone system to authenticate configuration file before applying it. When set to "Yes", the configuration file must include value P1 with phone system's administration password. If it is missed or does not match the password, the phone system will not apply it. Default setting is "No".
Download Device Configuration	Click to download phone's configuration file in .txt format. Note: Configuration backup file does not include passwords or CA/Custom certificate
Download Device Configuration (XML)	Click to download the device configuration file in .xml format.
Download and Process All Available Config Files	By default, device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml and cfg.xml (corresponding to device specific, model specific and global configs). If this option is enabled, the phone will inverse the downloading process to cfg.xml > cfgMAC.bin > cfgMAC.xml. The following files will override the files that has already been load and processed.
Download User configuration	This allows users to download part of the configuration that does not include any personal settings like Username and Passwords. Also, it will include all the changes manually made by user from web UI, or config file uploaded from "Upload Device Configuration", but not include the changes from the server provision via TFTP/FTP/FTPS/HTTP/HTTPS.
Upload Device Configuration	Uploads configuration file to phone.
Export backup Package	Export backup package which contains device configuration along with personal data.
Restore from Backup package	Click to upload backup package and restore.
Firmware	
Firmware Upgrade Via	Allows users to choose the firmware upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS. The default setting is "HTTPS".
Firmware Server Path	Defines the server path for the firmware server.
Firmware Server Username	The username for the firmware server.

Firmware Server Password	The password for the firmware server.
Firmware File Prefix	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone.
Firmware File Postfix	Enables your ITSP to lock firmware updates. If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.

Maintenance/Syslog

Syslog Protocol	If set to SSL/TLS, the syslog messages will be sent through secured TLS protocol to syslog server. Default setting is UDP. **Note**: The CA certificate is required to connect with the TLS server.
Syslog Server	The URL or IP address of the syslog server for the phone to send syslog to. **Note**: By adding port number to the Syslog server field (i.e. 172.18.1.1:1000), the phone will send syslog to the corresponding port of that IP.
Syslog Level	Selects the level of logging for syslog. The default setting is "None". There are 4 levels: DEBUG, INFO, WARNING and ERROR. Syslog messages are sent based on the following events: • Product model/version on boot up (INFO level). • NAT related info (INFO level). • sent or received SIP message (DEBUG level). • SIP message summary (INFO level). • inbound and outbound calls (INFO level). • registration status change (INFO level). • negotiated codec (INFO level). • Ethernet link up (INFO level). • SLIC chip exception (WARNING and ERROR levels). • Memory exception (ERROR level).
Syslog Keyword Filtering	Syslog will be filtered based on keywords provided. If you enter multiple keywords, it should be separated by ','. Please note that no spaces are allowed.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages. The default setting is "No". Note: By setting Send SIP Log to Yes, the phone will still send SIP log from syslog even when Syslog Level set to NONE.

Maintenance/Security Settings

Security	
Validate Server Certificates	After enabling this feature, phone will validate the server's certificate. If the server that our phone tries to register on is not on our list, it will not allow server to access the phone.
SIP TLS Certificate	SSL Certificate used for SIP Transport in TLS/TCP.
SIP TLS Private Key	SSL Private key used for SIP Transport in TLS/TCP.
SIP TLS Private Key Password	SSL Private key password used for SIP Transport in TLS/TCP.
Custom Certificate	The uploaded custom certificate will be used for SSL/TLS communication instead of the WP phone default certificate.
Web Access Mode	Sets the protocol for web interface. The default setting is "HTTP".
Enable User Web Access	Administrator can disable or enable user web access. Default is Enabled.
HTTP Web Port	Configures the HTTP port under the HTTP web access mode.
HTTPS Web Port	Configures the HTTPS port under the HTTPS web access mode. Default setting is "443".
Disable SSH	Disables SSH access. The default setting is "No".
SSH Public Key	This option allows you to use authentication keys for SSH access. The public key should be loaded to phone's web UI while the private key should be used in the SSH tool side. Note: This will allow upcoming SSH access without password.
Web Session Timeout	Configures timer to logout web session during idle. Default is 10 min. Range is 2-60 min.
Web Access Attempt Limit	Configures attempt limit before lockout. Default is 5. Range is 1-10.
Trusted CA Certificates	
Trusted CA Certificates	Allows to upload and delete the CA Certificate file to phone. **Note:** Users can either upload the file directly from web or they can choose to provision it from their cfg.xml file.
Load CA Certificates	Users are able to specify which certificate they are going to use: • **All Certificates:** (Default) Both built-in and uploaded Certificates. • **Default Certificates:** Built-in Certificates. • **Custom Certificates:** Uploaded Certificates;

Maintenance/Packet Capture

Capture Location	Location where the capture will be stored. Internal storage or USB.
With RTP Packets	Choose whether the packet capture file contains RTP or not.
USB Filename	Filename of the capture. Only required for USB.

Maintenance/Tools

Provision	Makes the phone trigger an instant provisioning.
Factory Reset	Sets back the phone to the factory default settings.
Ping	Makes the phone ping an URL to check if it has access to it.
Traceroute	Checks the route packets take to the specified URL.

Directory Page Definitions

Directory /Contacts

Search Bar	Allows users searching for phonebook entries.
Add Contact	Specifies Contact's First Name, Last Name, Phone Number, Accounts and Groups Blacklist, Whitelist, Work, Friends and Family) to add one new contact in phonebook. **Note:** If the contact number belongs to Blacklist group, the call from this number will be blocked. If the contact number belongs to Whitelist group, when the phone is on DND mode, the call from whitelist number will be allowed.
Edit Contact	Edits selected contact.
Delete All Contacts	Deletes all contacts from phonebook. **NOTE:** a message prompt will be displayed so that users will confirm to delete or cancel the operation, in order to prevent users from losing contacts when deleting them accidentally.

Directory /Phonebook Management

Download XML Phonebook	Click on "Download" to download the XML phonebook file to local PC
Upload XML Phonebook	Click on "Upload" to upload local XML phonebook file to the phone.
Default search mode	Configures default phonebook search mode. Default setting is "Quick match".

Directory / Call History

Call History	
Delete	Users can select an entry, then click "Delete" to remove it from the list.
Delete all	Click on Delete All in order to remove all Call History stored in the phone. **Note:** Users could use the drop-down list to show only selected call history type (All, Answered, Dialed, Missed, Transferred) and also use navigation keys to browse pages when many entries exist.

UPGRADING AND PROVISIONING

The WP810 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.

Upgrade and Provisioning Configuration

There are two ways to setup upgrade and provisioning on WP810. They are Keypad Menu and Web GUI.

Configure via keypad Menu

1. In WP810 Settings, select **Advanced Settings → System Upgrade**.

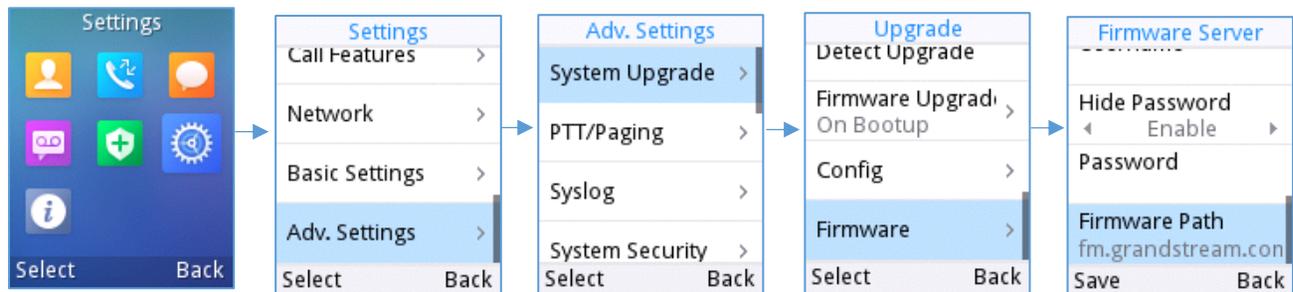2. Navigate to **Firmware** and configure the firmware upgrade server path.

Figure 12: WP810 Upgrade Configuration via Keypad Menu

Configure via Web GUI

Open a web browser on PC and enter the IP address for the WP810. Then login with the administrator username and password. Go to **Maintenance → Upgrade and Provisioning→ Firmware**., 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: WP810 Upgrade Configuration via Web GUI

⚠ **Note:**

-Please do not power off or unplug the WP810 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.

Local Firmware Servers

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 WP810 device to the same LAN segment.

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

4. Configure the Firmware Server Path on your WP810 to the IP address of the PC.

5. Update the changes and reboot the WP810.

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".

WP810 Administration Guide
Version 1.0.7.7

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. For a detailed parameter list, please refer to the corresponding firmware release configuration template in the following link: http://www.grandstream.com/support/tools

When the WP810 boots up, it will issue TFTP or HTTP(S) request to download a configuration XML file named "cfgxxxxxxxxxxxx" followed by "cfgxxxxxxxxxxxx.xml", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If downloading "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file. The configuration file name should be in lower case letters.

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

WP810 Administration Guide
Version 1.0.7.7

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 WP810 to the factory default settings.

1. On WP810 idle screen, go to **Settings → Advanced Settings → Factory reset**.

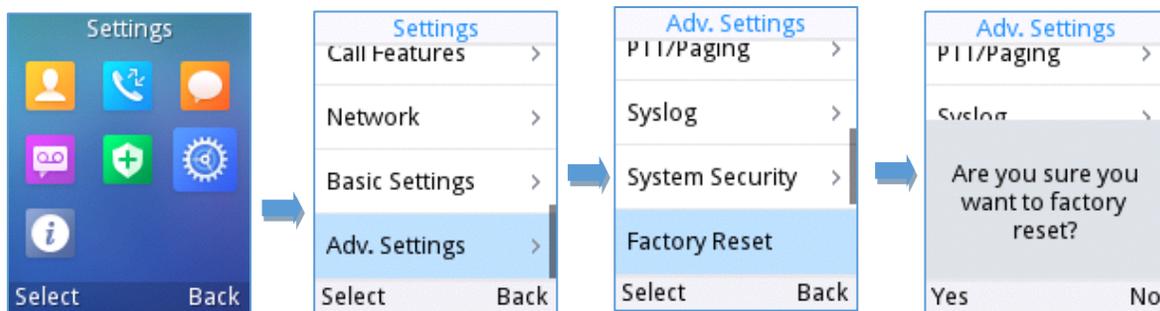2. In the new window, confirm the reset using the left softkey.

Figure 14: WP810 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 WP810 Web GUI and go to **Maintenance → Tools**.
2. Click on the **Start** button in front of **Factory Reset**.

Figure 15: WP810 Web GUI - Factory Reset

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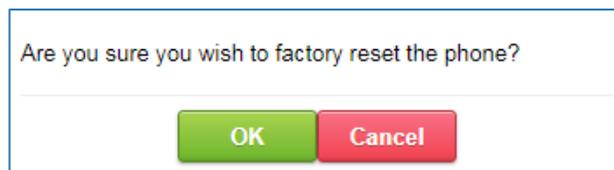4. Click OK to restore the phone to factory settings.

Figure 16: WP810 Web GUI - Confirm Factory Reset

EXPERIENCING WP810 CORDLESS WI-FI IP PHONE

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

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

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

Thank you again for purchasing Grandstream Cordless Wi-Fi IP Phone, it will be sure to bring convenience and color to both your business and personal life.

WP810 Administration Guide
Version 1.0.7.7