Grandstream Networks, Inc.

WP816/WP826/WP836 - Administration Guide

WP816/WP826/WP836 - Administration Guide

WELCOME

The WP816/WP826/WP836 are cordless Wi-Fi IP phones suitable for various enterprise and vertical market applications, including offices, retail, logistics, healthcare, and security. Both models feature integrated dual-band Wi-Fi 6, advanced antenna design, roaming support, and support for the Opus HD voice codec, ensuring high-quality communication. The WP816 supports 3-way voice conferencing, offers 6 hours of talk-time, and 120 hours of standby time (laboratory data) with a 1500mAh battery. In contrast, the WP826 and WP836 support 4-way voice conferencing, provide 240 hours of standby, 12 hours of talk-time for WP826 and 10 hours of talk-time for WP836 (laboratory data) with a 3000mAh battery. WP816/WP826/WP836 phones offer a sleek design, easy-to-use interface, and a variety of practical, customizable features, providing mobility and flexibility to all voice solutions.

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the WP8x6:

 WP816	2 SIP accounts and 2 lines. Configurable button for push-to-talk Dual-band 802.11a/b/g/n/ac/ax Wi-Fi. Wi-Fi roaming. 120 hours standby time. (Laboratory data) 6 hours talk time. (Laboratory data)
 WP826	3 SIP accounts, 3 lines Configurable button for push-to-talk Dual-band 802.11a/b/g/n/ac/ax Wi-Fi. Wi-Fi roaming. 240 hours standby time. (Laboratory data) 12 hours talk time. (Laboratory data)

 WP836	3 SIP accounts, 3 lines Configurable button for push-to-talk. Dual-band 802.11a/b/g/n/ac/ax Wi-Fi. Wi-Fi roaming. 240 hours standby time. (Laboratory data) 10 hours talk time. (Laboratory data) IP67 Rated-Water-proof, dust-proof, cleaning chemical resistant, antibacterial casing.

WP8x6 Features at a Glance

Technical Specifications

The following table summarizes all the technical specifications, including the protocols/standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings.

- **WP816**

Protocol/Standards	SIP RFC3261, DNS (A record, SRV, NATPR), DHCP, SSH, NTP, STUN, LDAP, TR069, SNMP, STRP, RTP/RTCP, RTCP-XR, TFTP, SIMPLE, HTTP/HTTPS, TCP, UDP, TLS, ARP, ICMP, IPv4, IPv6, 802.1x
Voice Codecs and Capabilities	G.729A/B, G.711u/a-law, G.726, G.722(wide-band), G.723,iLBC, Opus, in- band and out-of-band DTMF (in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC, AJB,Headset Noise Shield
Wi-Fi	Yes, integrated dual-band Wi-Fi 6 802.11 a/b/g/n/ac/ax (2.4GHz & 5GHz). 802.11k/r/v Supported
Wi-Fi Encryption	Support WEP, WPA, WPA2, WPA3 (personal)
Graphic	1.77 inch (128x160) color LCD, 1 * Dual color MWI
Bluetooth	Yes, integrated
Peripherals	2 soft keys, navigation keys, confirm key, dial key, hang up key, speaker key, programmable key, quick access and mute key, backlight DTMF keyboard, volume keys, Push-to-Talk key, accelerometer, proximity sensor
Push-to-Talk	Customizable function button for alarm and paging
Auxiliary Ports	3.5mm headphone interface (CTIA cable sequence), Type-C charging interface (supports fast charging)
Telephony	Hold, transfer, forward, 3-way audio conference, call park, downloadable phonebook (XML, LDAP, up to 1000 items), call waiting, call log (up to 200 records), auto answer, click to dial, flexible dial plan, personalized music ringtones, server redundancy and fail-over, push-to-talk
Wall Installation	Base supports wall installation
Security	Ordinary user and administrator level passwords based on MD5 and MD5 sess authentication, SIP authentication algorithms based on SHA-256, SHA-256 sess, SHA-512-256, SHA-512-256 sess, md5 sess. AES security profile, SRTP, TLS call encryption, 802.1x media access control
HD Audio	The earpiece is broadband audio, and the speaker is narrowband audio, supportingHAC and dual Mic.
QoS	Supports Layer 3 QoS (Tos, DiffServ, MPLS, DSCP)

Multi-language	Simplified Chinese, Traditional Chinese, English, Arabic, Catalan, Czech, German, Greek, Spanish, French, Hebrew, Croatian, Magyar, Italian, Japanese, Korean, Latvian, Dutch, Polish, Portuguese, Russian, Swedish, Slovenian, Slovak, Turkish, Ukrainian
Upgrade/Provisioning	Firmware upgrade via FTP/TFTP/FTPS/HTTP/HTTPS, mass provisioning using GDMS/TR069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal power adapter Input: 100-240VAC; Output:+5VDC, 1A (5W) 1500mAh lithium-ion battery, standby time 120h, talk time 6h (laboratory data)
Physical	Handset dimensions: 135.00 x 49.00 x 15.5mm Charger cradle dimensions: 85.00 x 85.00 x 25.8mm Handset weight (not including battery): 82g Handset package weight (not including QIG): 389g
Temperature and Humidity	Operating Temperature: 0oC to 45oC; Operating Humidity: 10-90% (non-condensing) Storage Temperature: -20oC to 60oC; Storage Humidity: 10-90% (non-condensing)
Package Contents	WP816 phone, Type-C power adapter, charger base, belt clip, 1 lithium-ion battery, M3 screw, wall bracket, quick installation guide
Compliance	FCC, CE, RCM, IC

WP816 Technical Specifications

- **WP826**

Protocol/Standards	SIP RFC3261, DNS (A record, SRV, NATPR), DHCP, SSH, NTP, STUN, LDAP, TR069, SNMP, STRP, RTP/RTCP, RTCP-XR, TFTP, SIMPLE, HTTP/HTTPS, TCP, UDP, TLS, ARP, ICMP, IPv4, IPv6, 802.1x
Voice Codecs and Capabilities	G.729A/B, G.711u/a-law, G.726, G.722(wide-band), G.723, iLBC, Opus, in- band and out-of-band DTMF (in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC, AJB,Headset Noise Shield
Wi-Fi	Yes, integrated dual-band Wi-Fi 6 802.11 a/b/g/n/ac/ax (2.4GHz & 5GHz). 802.11k/r/v Supported
Wi-Fi Encryption	Supports WEP, WPA, WPA2, WPA3 (personal)
Graphic	2.4 inch (240x320) color LCD, 1 * Dual color MWI
Bluetooth	Yes, integrated
Peripherals	3 soft keys, navigation keys, confirm key, dial key, hang up key, speaker key, quick access and mute key, backlight DTMF keyboard, volume keys, Push-to-Talk key, accelerometer, proximity sensor
Push-to-Talk	Customizable function button for alarm and paging
Auxiliary Ports	Type-C charging interface (supports fast charging)
Telephony	Hold, transfer, forward, 3-way audio conference, call park, downloadable phonebook (XML, LDAP, up to 1000 items), call waiting, call log (up to 200 records), auto answer, click to dial, flexible dial plan, personalized music ringtones, server redundancy and fail-over, push-to-talk
Wall Installation	Base supports wall installation
Security	Ordinary user and administrator level passwords based on MD5 and MD5 sess authentication, SIP authentication algorithms based on SHA-256, SHA-256 sess, SHA-512-256, SHA-512-256 sess, md5 sess. AES security profile, SRTP, TLS call encryption, 802.1x media access control
HD Audio	The earpiece is broadband audio, and the speaker is narrowband audio, supportingHAC and dual Mic.
QoS	Supports Layer 3 QoS (Tos, DiffServ, MPLS, DSCP)

Multi-language	Simplified Chinese, Traditional Chinese, English, Arabic, Catalan, Czech, German, Greek, Spanish, French, Hebrew, Croatian, Magyar, Italian, Japanese, Korean, Latvian, Dutch, Polish, Portuguese, Russian, Swedish, Slovenian, Slovak, Turkish, Ukrainian
Upgrade/Provisioning	Firmware upgrade via FTP/FTPS/TFTP/HTTP/HTTPS, mass provisioning using GDMS/TR069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal power adapter Input: 100-240VAC; Output:+5VDC, 2A (10W) 3000mAh lithium-ion battery, standby time 240h, talk time 12h (laboratory data)
Physical	Handset dimensions: 135.00 x 49.00 x 15.5mm Charger cradle dimensions: 85.00 x 85.00 x 25.8mm Handset weight (not including battery): 82g Handset package weight (not including QIG): 389g
Temperature and Humidity	Operating Temperature: 0oC to 45oC; Operating Humidity: 10-90% (non-condensing) Storage Temperature: -20oC to 60oC; Storage Humidity: 10-90% (non-condensing)
Package Contents	WP816 phone, Type-C power adapter, charger base, belt clip, 1 lithium-ion battery, M3 screw, wall bracket, quick installation guide
Compliance	FCC, CE, RCM, IC

WP826 Technical Specifications

- **WP836**

Protocol/Standards	SIP RFC3261, DNS (A record, SRV, NATPR), DHCP, SSH, NTP, STUN, LDAP, TR069, SRTP, RTP/RTCP, RTCP-XR, TFTP, SIMPLE, HTTP/HTTPS, TCP, UDP, TLS, ARP, ICMP, IPv4, IPv6, 802.1x
Voice Codecs and Capabilities	G.729A/B, G.711u/a-law, G.726, G.722(wide-band), G.723, iLBC, Opus, in- band and out-of-band DTMF (in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC, AJB, Noise Shield
Wi-Fi	Yes, integrated dual-band Wi-Fi 6 802.11 a/b/g/n/ac/ax (2.4GHz & 5GHz). 802.11k/r/v Supported, 2T2R Supported
Wi-Fi Encryption	Supports WEP, WPA, WPA2, WPA3 (personal)
Graphic	2.8 inch (240x320) color LCD, 1 * Dual color MWI
Bluetooth	Yes, integrated
Peripherals	3 soft keys, navigation keys, confirm key, dial key, hang up key, speaker key, quick access and mute key, backlight DTMF keyboard, volume keys, Push-to-Talk key, accelerometer, proximity sensor
Push-to-Talk	Customizable function buttons such as Alarm and Paging
Auxiliary Ports	Type-C charging interface (supports fast charging)
Telephony	Hold, transfer, forward, 4-way audio conference, call park, downloadable phonebook (XML, LDAP, up to 1000 items), call waiting, call log (up to 200 records), auto answer, click to dial, flexible dial plan, personalized music ringtones, server redundancy and fail-over, push-to-talk
Wall Installation	Base supports wall installation
Security	Ordinary user and administrator level passwords based on SHA-256 and SHA-256 sess authentication, SIP authentication algorithms based on SHA-256, SHA-256 sess, SHA-512-256, SHA-512-256 sess, MD5 sess. AES security profile, SRTP, TLS call encryption, 802.1x media access control.
HD Audio	The handset is broadband audio, supporting HAC and dual Mic
QoS	Supports Layer 3 QoS (Tos, DiffServ, MPLS, DSCP)
Multi-language	Simplified Chinese, Traditional Chinese, English, Arabic, Catalan, Czech, German, Greek, Spanish, French, Hebrew, Croatian, Magyar, Italian, Japanese, Korean, Latvian, Dutch, Polish, Portuguese, Russian, Swedish, Slovenian, Slovak, Turkish, Ukrainian

Upgrade/Provisioning	Firmware upgrade via FTP/FTPS/TFTP/HTTP/HTTPS, mass provisioning using GDMS/TR069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal power adapter Input: 100-240VAC; Output:+5VDC, 2A (10W) 3000mAh lithium-ion battery, standby time 240h, talk time 10h (laboratory data)
Physical	Handset dimensions: 155 x 62 x 19mm Charger cradle dimensions: 95 x 95 x 30.5mm Handset weight (not including battery): 158g Handset package weight (not including QIG): 616g
Weatherproof	IP67 Rated -Water-proof, dust-proof, cleaning chemical resistant, antibacterial casing and 2.0m drop safe
Temperature and Humidity	Operating Temperature: 0oC to 45oC; Operating Humidity: 10-90% (non-condensing) Storage Temperature: -20oC to 60oC; Storage Humidity: 10-90% (non-condensing)
Package Contents	WP836 phone, Type-C power adapter, charger base, belt clip, 1 lithium-ion battery, M3 screw, wall bracket, quick installation guide
Compliance	FCC, CE, RCM, IC

WP836 Technical Specifications

GETTING STARTED

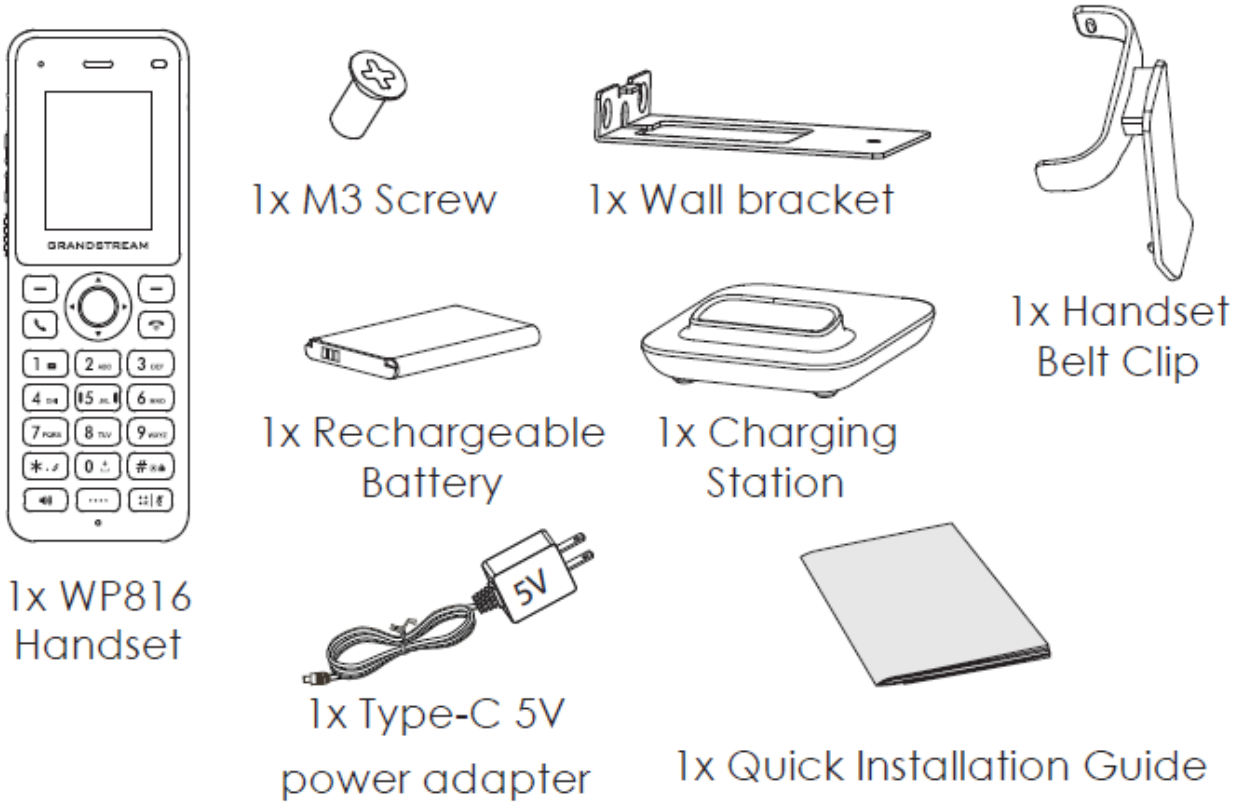
This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the WP8x6

Equipment Packaging

- **WP816**

WP816
1x WP816 Handset 1x Type-C 5V power adapter 1x Rechargeable Battery 1x M3 Screw 1x Wall bracket 1x Charging Station 1x Handset Belt Clip 1x Quick Installation Guide

WP816 Equipment Packaging

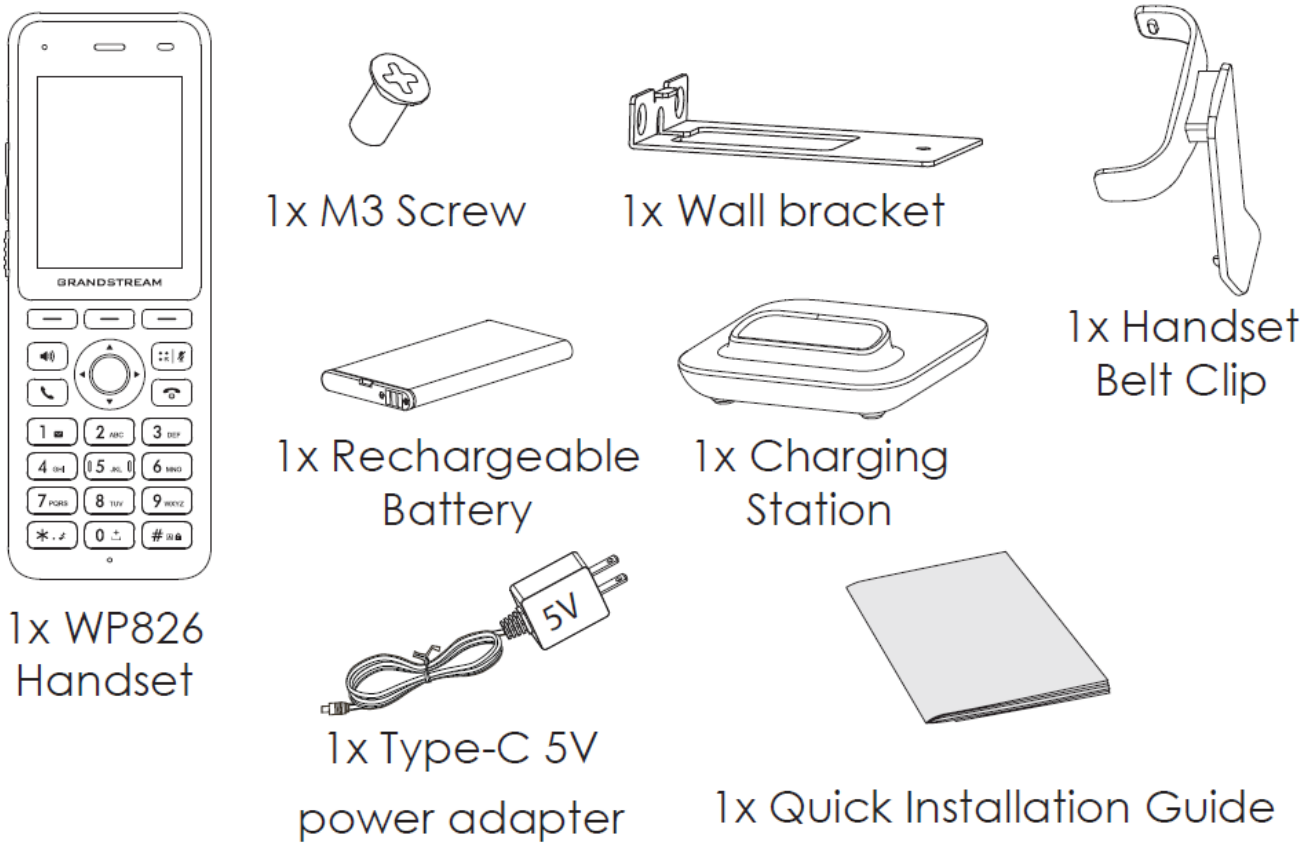


WP816 Package Content

- **WP826**

WP826
1x WP826 Handset 1x Type-C 5V power adapter 1x Rechargeable Battery 1x M3 Screw 1x Wall bracket 1x Charging Station 1x Handset Belt Clip 1x Quick Installation Guide

WP826 Equipment Packaging

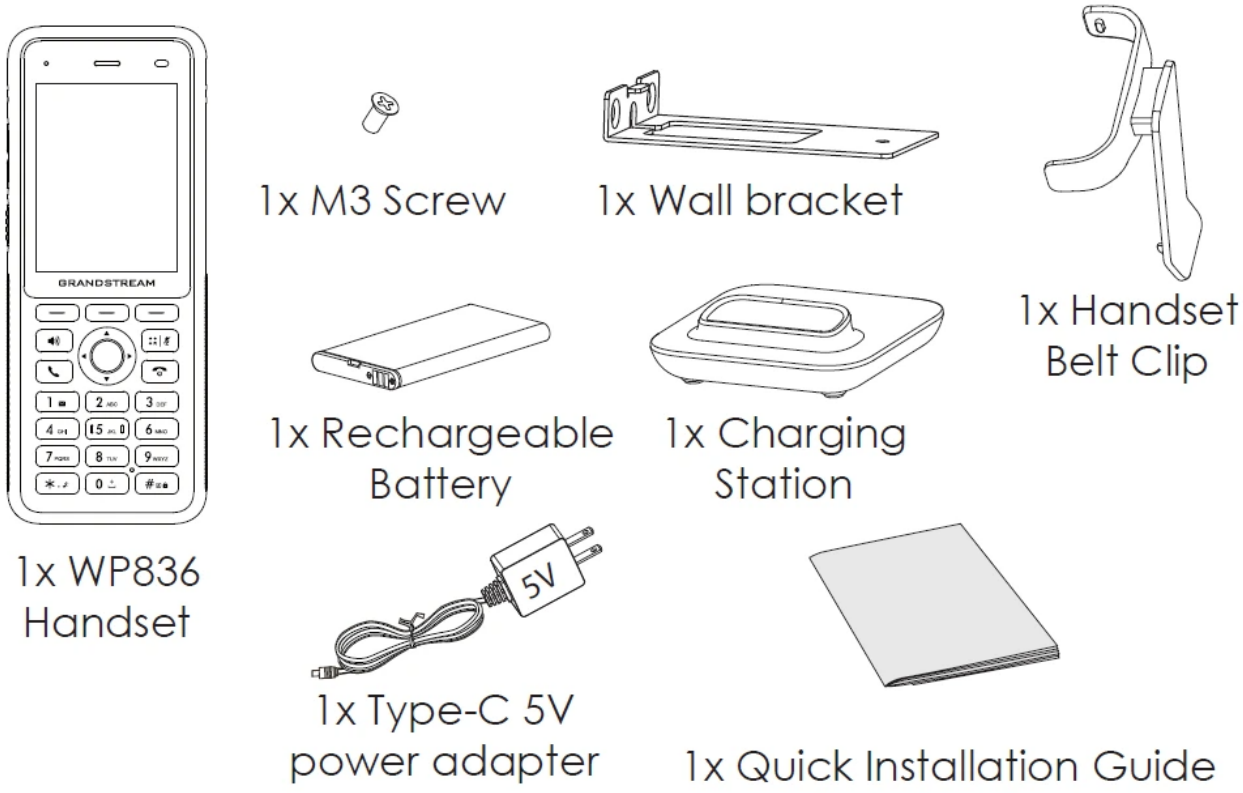


WP826 Package Content

- **WP836**

WP836
1x WP836 Handset 1x Type-C 5V power adapter 1x Rechargeable Battery 1x M3 Screw 1x Wall bracket 1x Charging Station 1x Handset Belt Clip 1x Quick Installation Guide

WP836 Equipment Packaging



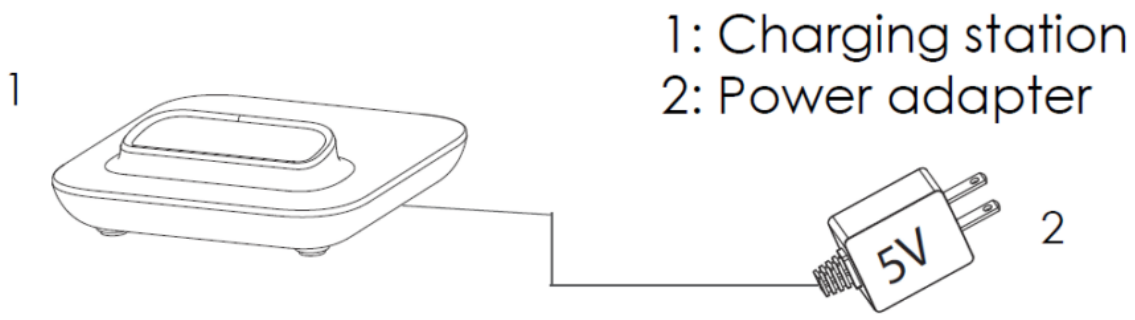
WP836 Package Content

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

Setting up the Phone

Charging Station

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



Charging Station

Handset

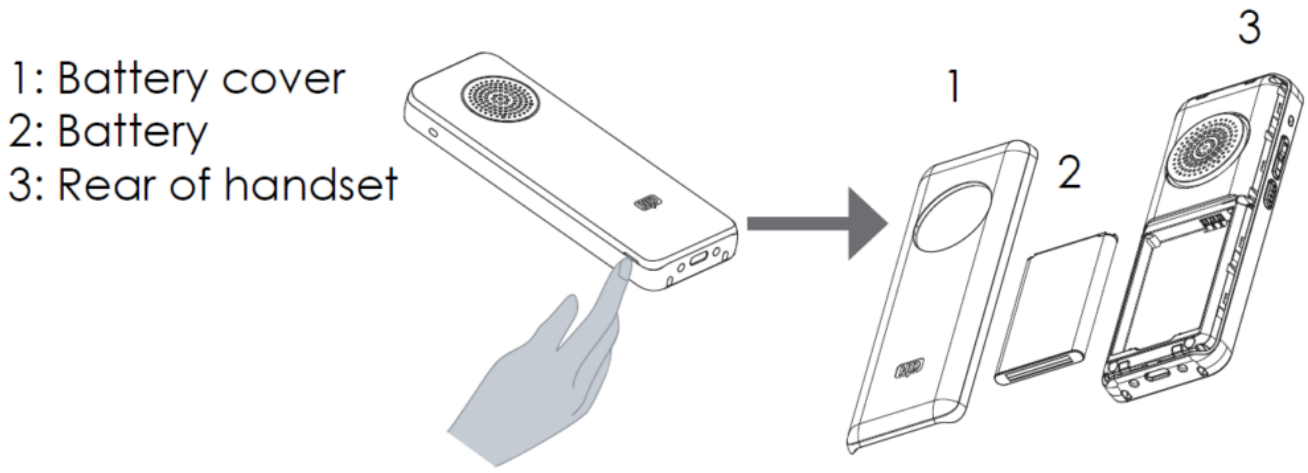
Please refer to the following steps to setup your WP8x6 phone:

1. Open the battery cover from the opening port. Remove the battery door for WP836.
2. Insert the battery with the electrodes in the top right corner for WP816, and the top left corner for

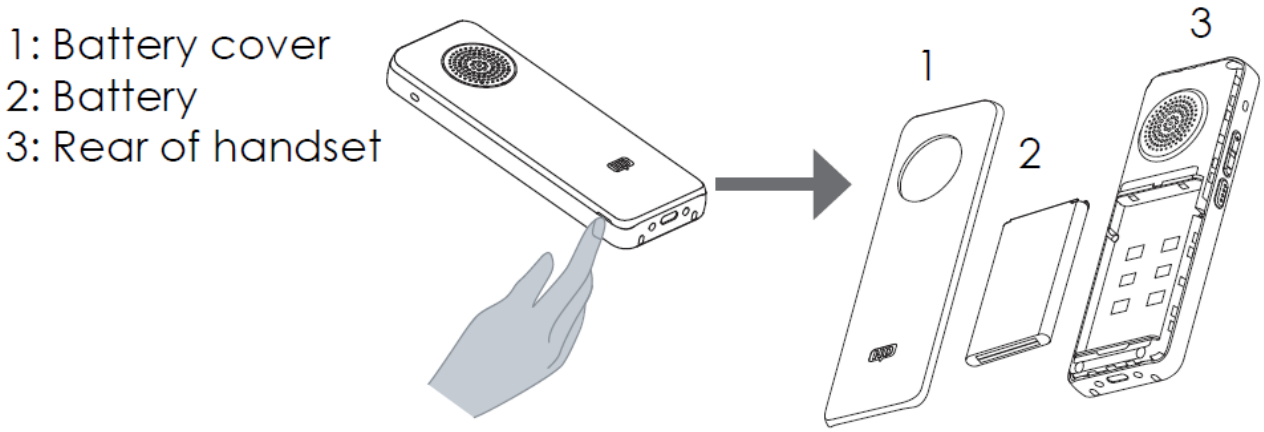
WP826/WP836.

3. Close the battery cover after inserting the battery door for WP836.

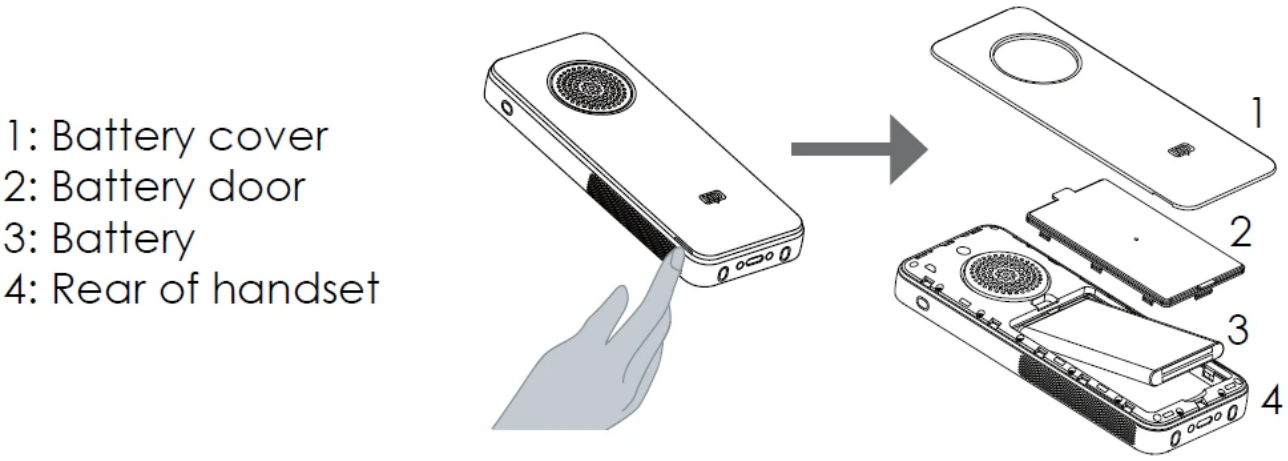
Please charge the battery fully before using the handset for the first time. (For more information about the battery, please refer to **Battery Information**.



WP816 Handset Setup



WP826 Handset Setup



WP836 Handset Setup

Battery Information

WP816

- **Technology:** Rechargeable Li-ion Battery
- **Capacity:** 1500mAh
- **Standby time:** up to 120 hours (laboratory data)
- **Talk time:** up to 6 hours of active talk time (laboratory data)

WP826

- **Technology:** Rechargeable Li-ion Battery
- **Capacity:** 3000mAh
- **Standby time:** up to 240 hours (laboratory data)
- **Talk time:** up to 12 hours of active talk time (laboratory data)

WP836

- **Technology:** Rechargeable Li-ion Battery
- **Capacity:** 3000mAh
- **Standby time:** up to 240 hours (laboratory data)
- **Talk time:** up to 10 hours of active talk time (laboratory data)

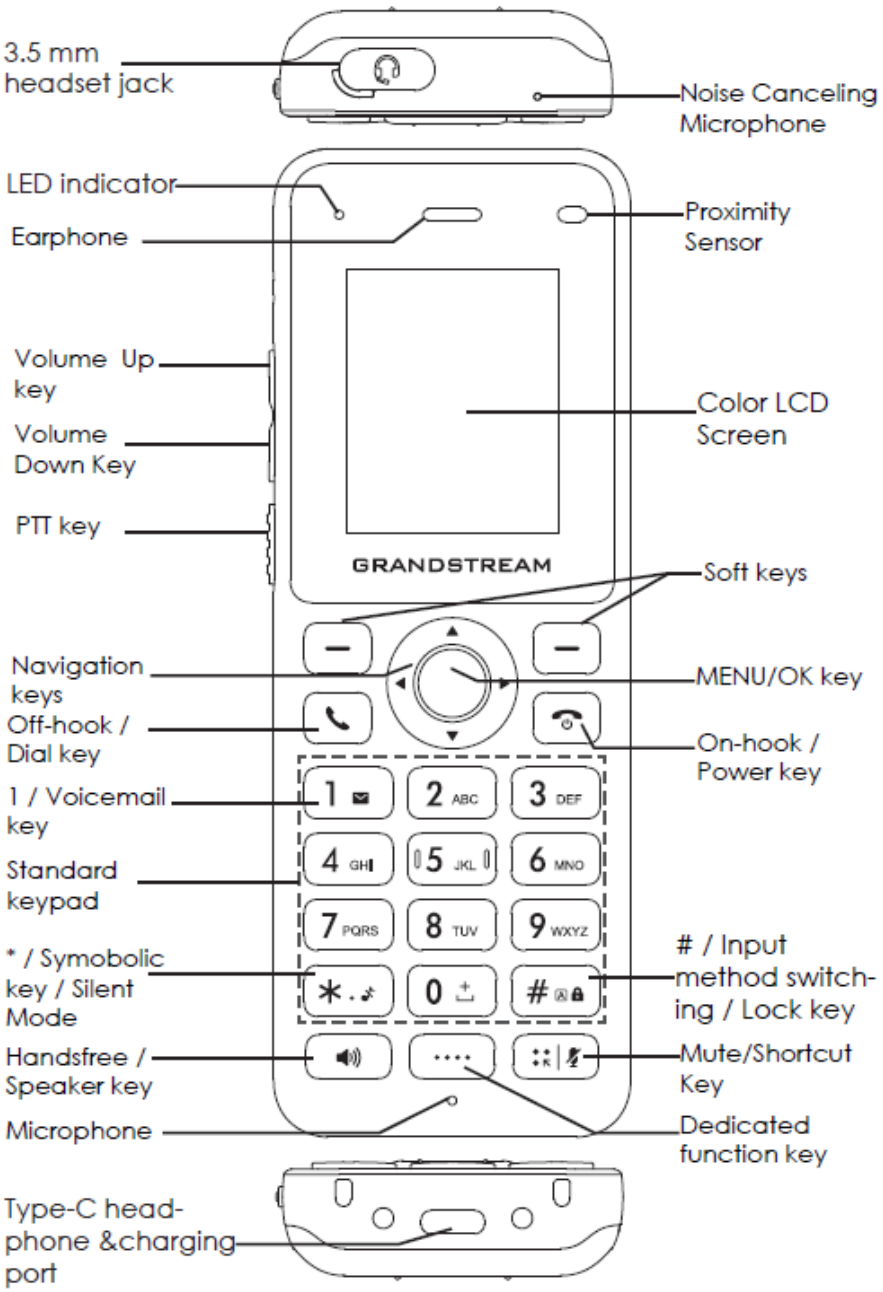
To get the best performance from your WP8x6, we recommend using the original battery provided in the package. The specifications may differ depending on the age and capacity of the battery used.

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

Handset Keys Description

The WP8x6 Wireless IP phone enhances communication and combines usability and scalability in industries such as warehousing, catering, and retail, as well as in factory settings. The following screenshot describes the handset LCD screen and the main hardware components.

- **WP816**



WP816 Description

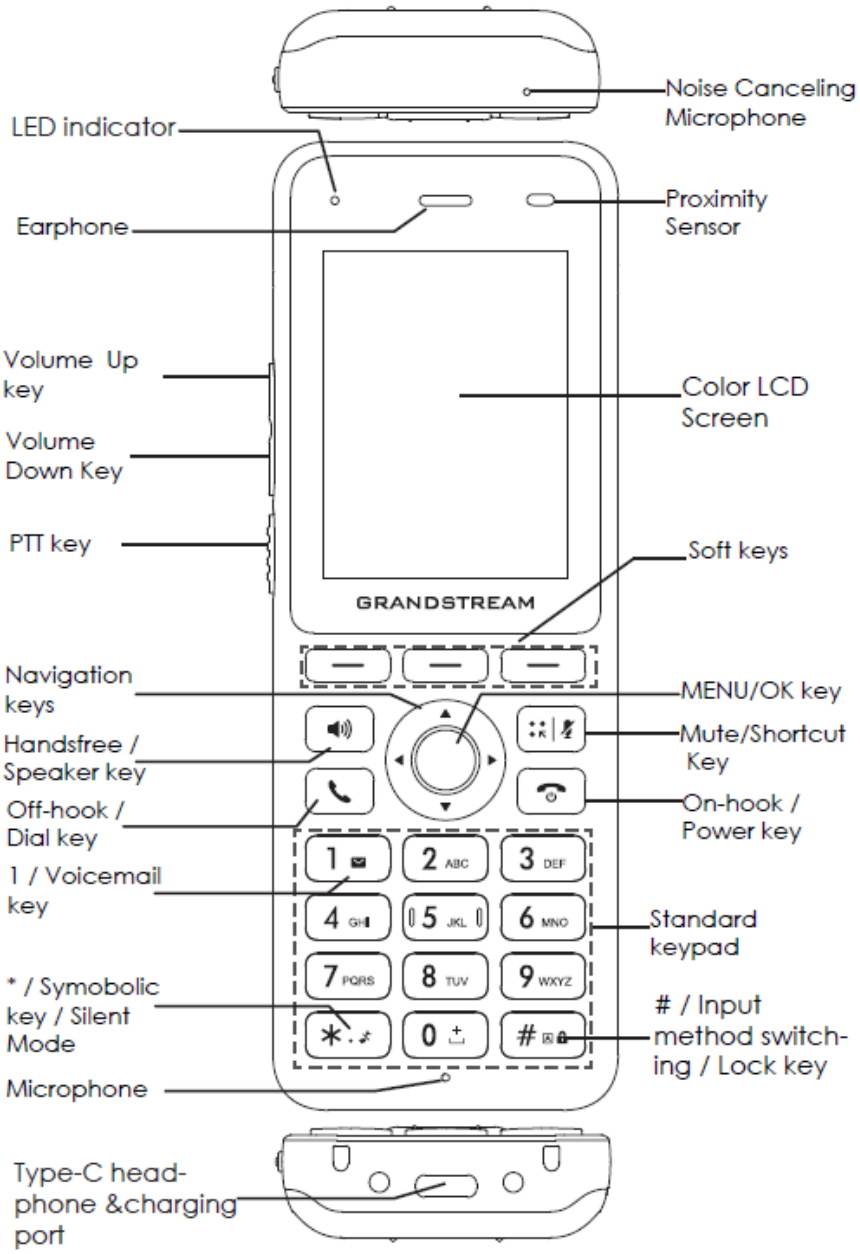
The following table describes the WP816 keypad keys.

Key	Description
3.5 mm headset jack	This port allows you to connect headphones or external speakers to the phone for audio output.
LED indicator	A small light that provides visual notifications for various events like incoming calls, messages, or charging status.
Earphone	Delivers audio output.
Volume Up key	A button used to increase the volume of audio output.
Volume Down Key	A button used to decrease the volume of audio output
PTT Key	PTT (Push-to-Talk) button, to initiate PTT call. This button can also be configured to trigger Alarm.
Navigation keys	Buttons used to navigate through menus, apps, and interfaces.
Off-hook / Dial key	Initiates or answers calls when pressed, and also used to dial numbers when making outgoing calls.

1 / Voicemail key	Long pressing this key initiates a call to your voicemail service, allowing you to check for new messages or manage voicemail settings.
Standard keypad	A grid of numeric keys used for dialing phone numbers, entering text, and navigating through menus by inputting numbers or letters associated with options.
* / Symobolic key / Silent Mode	This key is used to toggle the phone's silent mode on and off, muting all incoming call and message notifications.
Handsfree / Speaker key	Pressing this key enables the phone's speakerphone function, allowing for hands-free communication during calls.
Microphone	Picks up audio earpiece and hands-free calls
Type-C headphone &charging port	This port serves a dual purpose, allowing you to connect Type-C headphones for audio output and charging the phone using a compatible Type-C cable.
Dedicated function key	This button is assigned a specific function or shortcut, such as launching a specific app, activating a feature, or performing a predefined action.
Mute/Shortcut Key	A button that quickly silences incoming calls or notifications when pressed, and may also be customizable to serve as a shortcut for accessing frequently used features.
# / Input method switching / Lock key	Does one of the following: When pressing #: Redials the last dialed number, for this to work the Key As Send option under Account settings => Call settings should be set to # Lock key: Long press to lock keypad against unintentional entries, for this to work enable lock screen from LCD settings under System settings => Security Settings => Screen Lock Input method switching: Allows switching between different input methods (like keyboards types)
On-hook /Power key	This key serves a dual purpose, ending calls or switching off the phone when pressed for a longer duration, and turning on the phone or waking it from sleep mode when pressed briefly.
MENU/OK key	This key serves a dual purpose, opening the menu interface or confirming selections, such as when navigating through apps or options.
Softkeys	Correspond to functions displayed on the LCD. These functions change depending on the current context.
Color LCD Screen	1.77 inch (128x160) IPS color LCD screen
Proximity sensor	The proximity sensor detects when the phone is close to the caller's face, turning off the display to prevent accidental touches and save battery life.
Noise Canceling Microphone	A microphone equipped with technology to reduce background noise, resulting in clearer audio during calls by minimizing unwanted sounds from the surrounding environment.

WP816 keypad keys Description

- **WP826**



WP826 Description

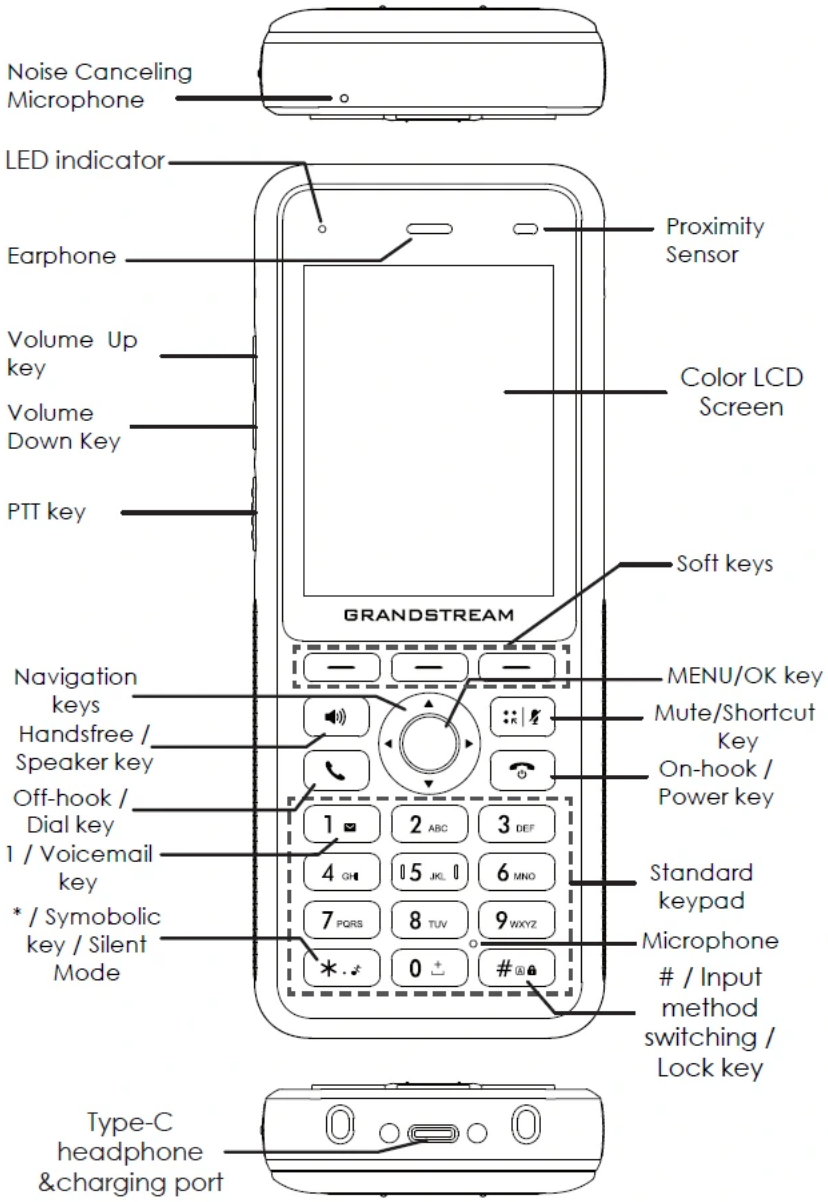
The following table describes the WP826 keypad keys.

Key	Description
LED indicator	A small light that provides visual notifications for various events like incoming calls, messages, or charging status.
Earphone	Delivers audio output.
Volume Up key	A button used to increase the volume of audio output.
Volume Down Key	A button used to decrease the volume of audio output
PTT Key	PTT (Push-to-Talk) button, to initiate PTT call. This button can also be configured to trigger Alarm.
Navigation keys	Buttons used to navigate through menus, apps, and interfaces.
Off-hook / Dial key	Initiates or answers calls when pressed, and also used to dial numbers when making outgoing calls.
1 / Voicemail key	Long pressing this key initiates a call to your voicemail service, allowing you to check for new messages or manage voicemail settings.

Standard keypad	A grid of numeric keys used for dialing phone numbers, entering text, and navigating through menus by inputting numbers or letters associated with options.
* / Symobolic key / Silent Mode	This key is used to toggle the phone's silent mode on and off, muting all incoming call and message notifications.
Handsfree / Speaker key	Pressing this key enables the phone's speakerphone function, allowing for hands-free communication during calls.
Microphone	Picks up audio earpiece and hands-free calls
Type-C headphone &charging port	This port serves a dual purpose, allowing you to connect Type-C headphones for audio output and charging the phone using a compatible Type-C cable.
Softkeys	These buttons are assigned a specific function or shortcut, such as launching a specific app, activating a feature, or performing a predefined action.
Mute/Shortcut Key	A button that quickly silences incoming calls or notifications when pressed, and may also be customizable to serve as a shortcut for accessing frequently used features.
# / Input method switching / Lock key	Does one of the following: When pressing #: Redials the last dialed number, for this to work the Key As Send option under Account settings => Call settings should be set to # Lock key: Long press to lock keypad against unintentional entries, for this to work enable lock screen from LCD settings under System settings => Security Settings => Screen Lock Input method switching: Allows switching between different input methods (like keyboards types)
On-hook /Power key	This key serves a dual purpose, ending calls or switching off the phone when pressed for a longer duration, and turning on the phone or waking it from sleep mode when pressed briefly.
MENU/OK key	This key serves a dual purpose, opening the menu interface or confirming selections, such as when navigating through apps or options.
Softkeys	Correspond to functions displayed on the LCD. These functions change depending on the current context.
Color LCD Screen	2.4 inch (240x320) IPS color LCD screen
Proximity sensor	The proximity sensor can detect when the phone is close to the caller's face, turning off the display to prevent accidental touches and save battery life.
Noise Canceling Microphone	A microphone equipped with technology to reduce background noise, resulting in clearer audio during calls by minimizing unwanted sounds from the surrounding environment.

WP826 keypad keys

- **WP836**



WP836 Description

The following table describes the WP836 keypad keys.

Key	Description
LED indicator	A small light that provides visual notifications for various events like incoming calls, messages, or charging status.
Earphone	Delivers audio output.
Volume Up key	A button used to increase the volume of audio output.
Volume Down Key	A button used to decrease the volume of audio output
PTT Key	PTT (Push-to-Talk) button, to initiate PTT call. This button can also be configured to trigger Alarm.
Navigation keys	Buttons used to navigate through menus, apps, and interfaces.
Off-hook / Dial key	Initiates or answers calls when pressed, and also used to dial numbers when making outgoing calls.
1 / Voicemail key	Long pressing this key initiates a call to your voicemail service, allowing you to check for new messages or manage voicemail settings.
Standard keypad	A grid of numeric keys used for dialing phone numbers, entering text, and navigating through menus by inputting numbers or letters associated with options.

* / Symobolic key / Silent Mode	This key is used to toggle the phone's silent mode on and off, muting all incoming call and message notifications.
Handsfree / Speaker key	Pressing this key enables the phone's speakerphone function, allowing for hands-free communication during calls.
Microphone	Picks up audio earpiece and hands-free calls
Type-C headphone &charging port	This port serves a dual purpose, allowing you to connect Type-C headphones for audio output and charging the phone using a compatible Type-C cable.
Softkeys	These buttons are assigned a specific function or shortcut, such as launching a specific app, activating a feature, or performing a predefined action.
Mute/Shortcut Key	A button that quickly silences incoming calls or notifications when pressed, and may also be customizable to serve as a shortcut for accessing frequently used features.
# / Input method switching / Lock key	Does one of the following: When pressing #: Redials the last dialed number, for this to work the Key As Send option under Account settings => Call settings should be set to # Lock key: Long press to lock keypad against unintentional entries, for this to work enable lock screen from LCD settings under System settings => Security Settings => Screen Lock Input method switching: Allows switching between different input methods (like keyboards types)
On-hook /Power key	This key serves a dual purpose, ending calls or switching off the phone when pressed for a longer duration, and turning on the phone or waking it from sleep mode when pressed briefly.
MENU/OK key	This key serves a dual purpose, opening the menu interface or confirming selections, such as when navigating through apps or options.
Softkeys	Correspond to functions displayed on the LCD. These functions change depending on the current context.
Color LCD Screen	2.8 inch (240x320) IPS color LCD screen
Proximity sensor	The proximity sensor can detect when the phone is close to the caller's face, turning off the display to prevent accidental touches and save battery life.
Noise Canceling Microphone	A microphone equipped with technology to reduce background noise, resulting in clearer audio during calls by minimizing unwanted sounds from the surrounding environment.

WP836 Keypad Keys

Icons Description

The following table contains a description of each icon that might be displayed on the screen of the WP8x6.

	Battery statusCharging
	Wi-Fi connected on 5G band

	Wi-Fi connected on 2.4G band
  	Wi-Fi signal status for threshold alarm
	Outgoing Call notification
	Missed Call notification
	Rejected Call notification
	Incoming Call notification

	Auto-Answer feature enabled icon
	Mute enabled icon
	Silent mode enabled icon
	Warning icon
	DND enabled icon
	Bluetooth enabled icon
	Bluetooth connected icon

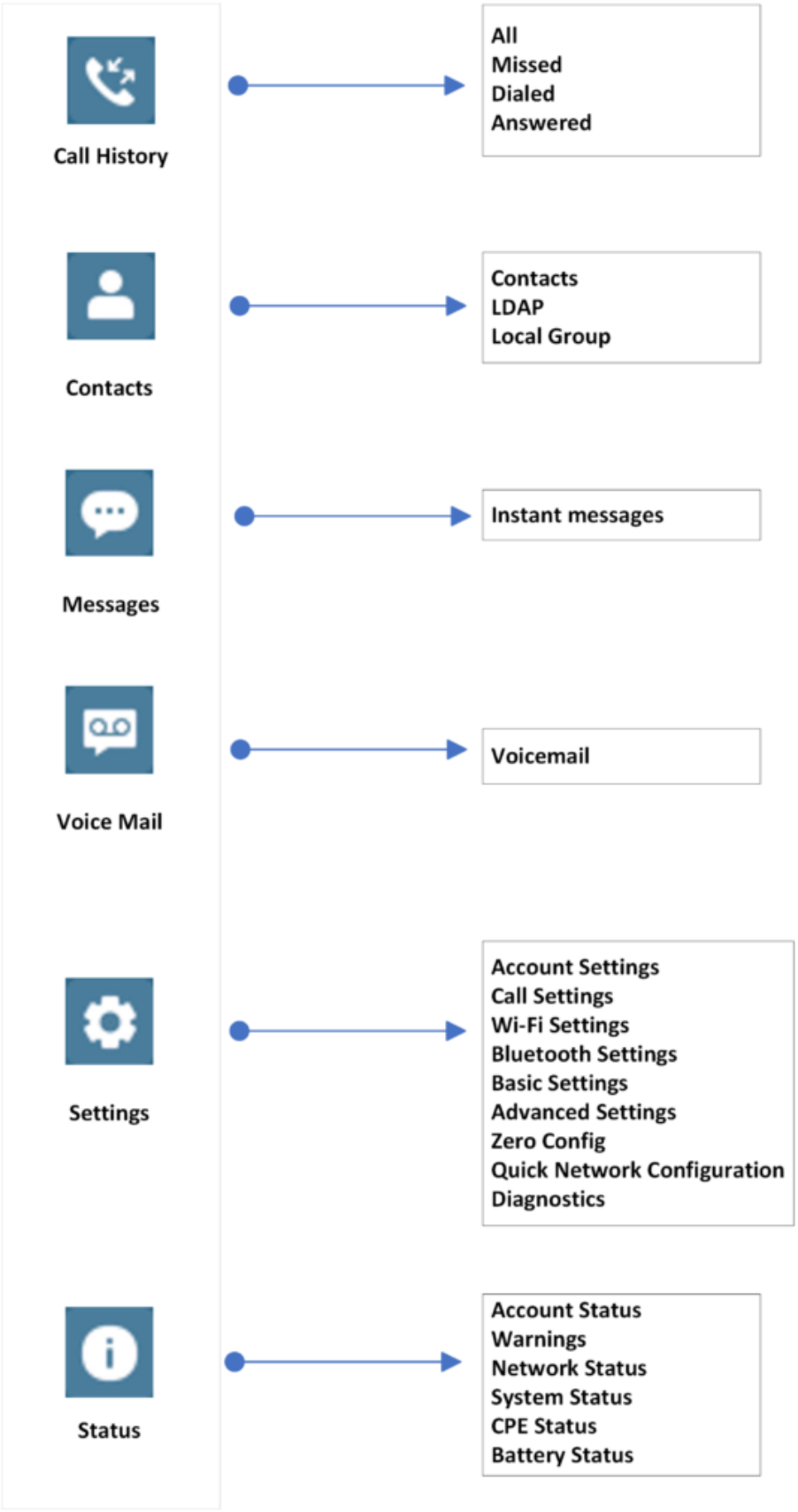
	Call connected through Bluetooth icon		
	Call Forward Enabled		Call Forward Destination Number (shows up to 5 digits)
	Call on HD quality icon		
	Call on Noise Shield		
	Call on AI Noise Reduction		
	Call on both Noise Shield and AI Noise Reduction		
	Call in Recording Mode		
	Contacts		
	Instant Messages		
	Call History		
	Voice Mail		

	Settings
	Status

Icons Description

Handset Menu

The handset has an easy-to-use menu structure. Every menu opens a list of options. To open the main menu, unlock the handset first and press "Menu" (softkey on the left). Press the Arrow keys to navigate to the menu option you require. Then press the OK/Selection key to access further options or confirm the setting displayed. To go to the previous menu item, press the **On-hook /Power key**.



Menu Structure

Call History	Display the call history: Missed Calls, Answered Calls, Dialed Calls or All Calls. You can save dialed numbers on the call log to your contacts.
Contacts	Display the list of the registered contacts and also the LDAP contacts and the local group contacts, with the ability of searching, adding or editing the entries and also deleting the selected contacts.

Messages	With message, you can send a message by pressing "New ", then write a message of up to 200 characters to another device or check the received ones.
Voice Mail	This option alows to view the recieved voicemails with both categories, Normal and Urgent , of both accounts of the WP phone. Note: Voicemail ID needs to be configured, otherwise, "select" softkeys will open configuration settings.
Settings	Account Settings: Configure/View SIP accounts settings and account ringtone.Call settings: Configure the account auto answer, call forward, DND and call waiting 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, Alarm setting, system security settings, syslog settings and factory reset / reboot.Zero Config: This setting configurs the parameters used when adding the WP phone with GCC Fast provisioning service. Wi-Fi Settings: Enables/Disables Wi-Fi service, it can also Configure the Wi-Fi connection parameters, such as the Wi-Fi band, Alarm Threshold... Quick Network Configuration: Quickly set up your phone's Wi-Fi using two methods: access via mobile browser or adjust settings directly on the device for a local solution. Bluetooth Settings: Configures the bluetooth pairing settings. Diagnostics: Displays a set of different device and system diagnostic tools, including the LCD, LED diagnostic tests, ping and traceroute tests, as well as Sensor Data tests.
Status	Account status: Displays account status whether it is registered or not.Warnings: Displays the current alert messages for the phone, this can be messages about failed configuration downloads, Low Battery warning... Network status: Press to enter the sub menu for MAC address, IP Mode (DHCP), IPv4 address, IPv6 address, Subnet Mask, Gateway, DNS server, network statistics... System Status: 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.CPE status: CPE status includes signal strength and network connection stability indicators, such as CPE link, CPE STUN etc., it also contains a tool to run a global CPE diagnosis Battery Status: includes information such as the remaining battery percentage and charging status indicator...

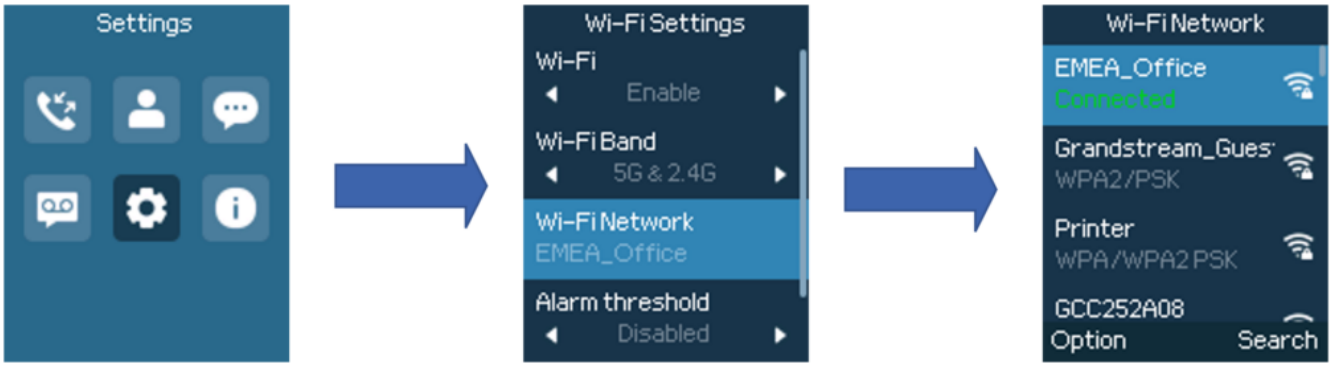
Handset Menu

Connecting the Handset to Wi-Fi Network

The WP8x6 phone supports dual-band 802.11a/b/g/n/ac/ax Wi-Fi. Please refer to the following steps to connect your handset to the Wi-Fi networks:

1. On the LCD menu, press the Menu key and navigate to **Settings** -> **Wi-Fi Settings**.
2. Enable Wi-Fi feature.
3. Select "Wi-Fi Band" (automatic, 2.4GHz or 5GHz) and navigate to "Wi-Fi Network". A list of Wi-Fi networks will be displayed.
4. Select the desired network to connect to. (Enter the correct password to connect if requested)

The handset will display a Wi-Fi icon on the main LCD menu if the con?nection to the Wi-Fi network is successful.



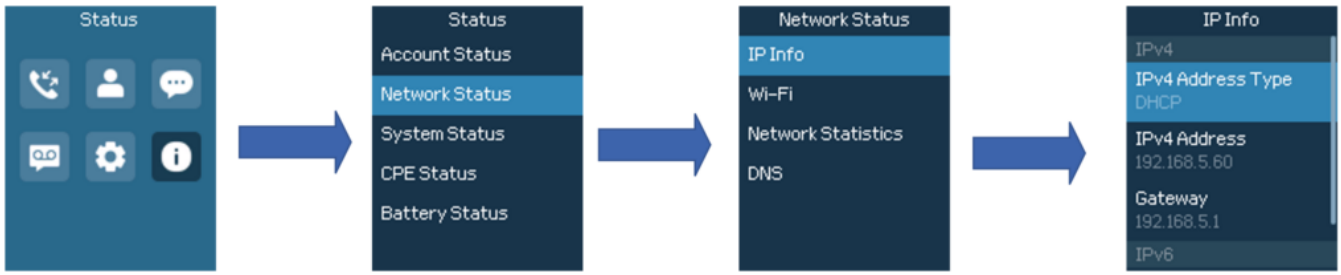
Connecting to Wi-Fi Network

- If 5GHz and 2.4GHz are both available when "Wi-Fi Band" is set to "Automatic", the WP8x6 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 to fix it or to keep it Dual Band.
- The user has the option to enable an alarm threshold to be triggered when the Wi-Fi strength goes below a certain defined network strength threshold.

Obtain IP Address

To know which IP address is assigned to your handset, please follow the steps below:

1. Unlock your phone first and press the "Menu" (Middle softkey) or **OK** button to view the operation menu.
2. Press the Arrow (Up, Down, Left, Right) keys to move the cursor to the Status icon then press "Select" (left softkey) or the **OK** button.
3. Access **Network Status -> IP-info** menu to obtain the IP address of the WP8x6.

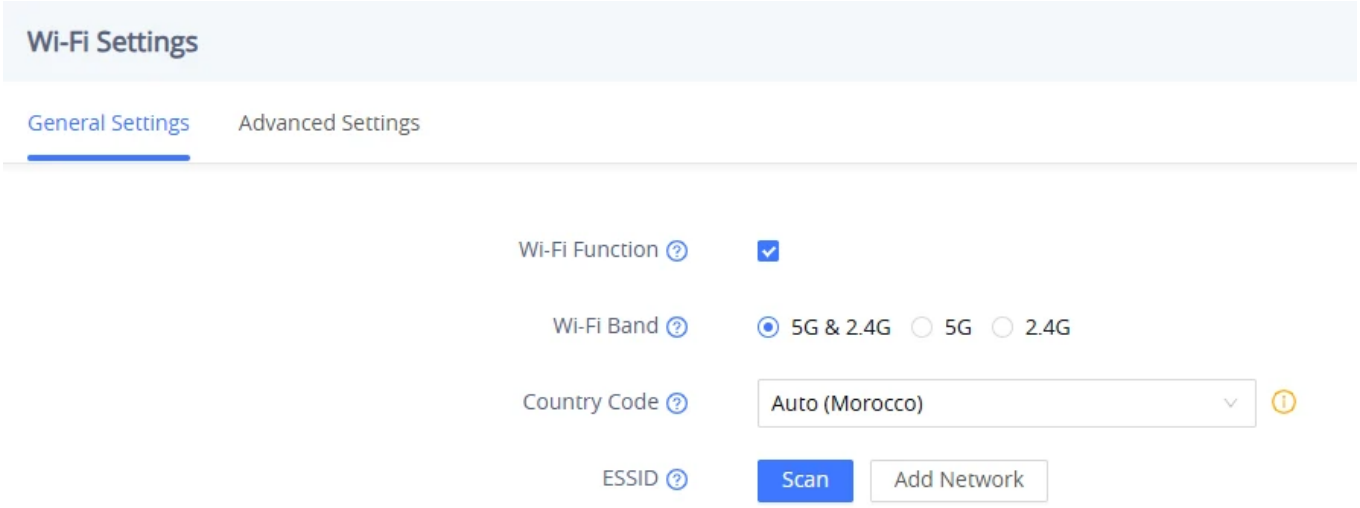


Network Status

Adding a Network via Web UI

After accessing the Web UI as described in the below section, new Wi-Fi networks can be added by navigating to **Network Settings -> Wi-Fi Settings -> General Setting**, then following these steps:

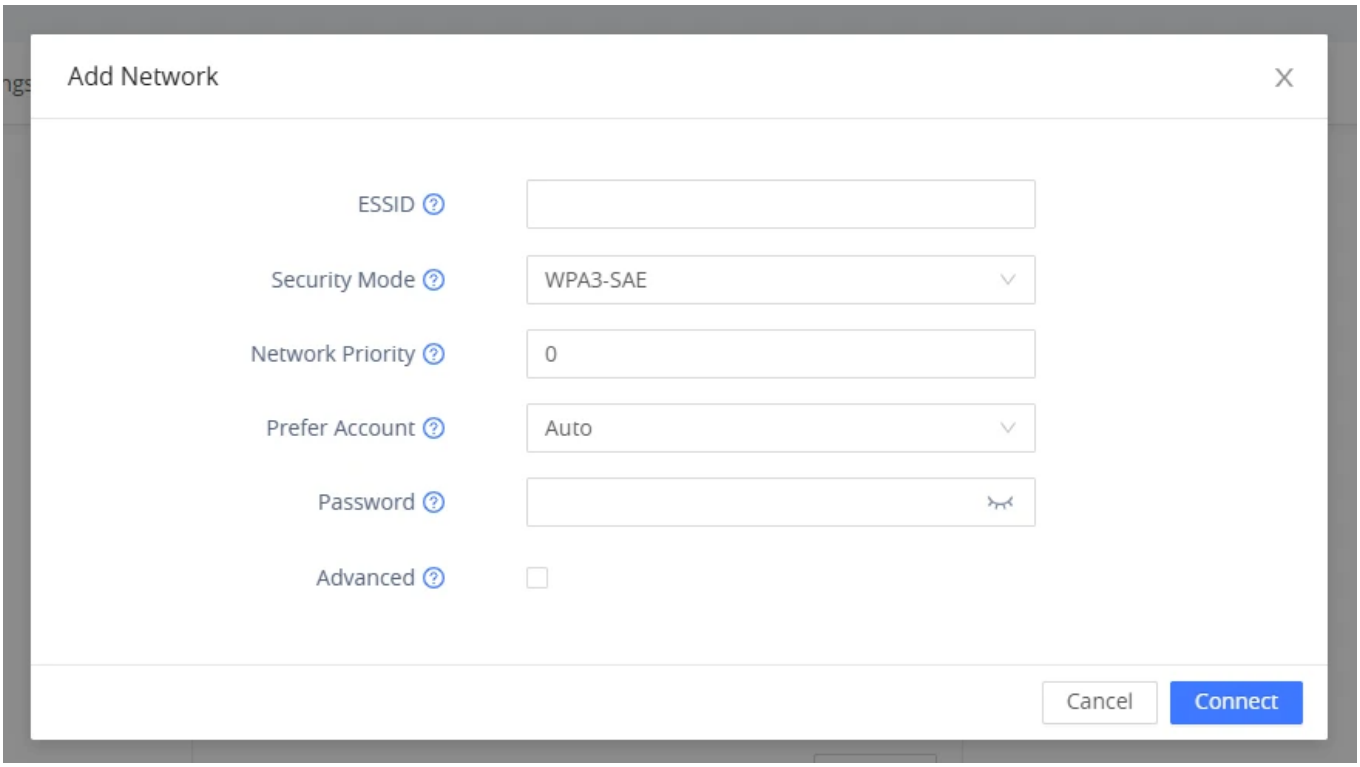
- Enable Wi-Fi by checking Wi-Fi Function
- Select the appropriate Wi-Fi Band
- Set the Country Code
- Press Add Network



WP816/WP826/WP836 Wi-Fi Settings Page

On the Add Network form, enter the following:

- ESSID
- Security Mode
- Network Priority
- Preferred Account
- Password
- Advanced Settings



WP816/WP826/WP836 Add Network Form

The configuration of a Wi-Fi network with **WPA-802.1X**, **WPA3-802.1X**, or **WPA3-192** Security Mode depends on the selected EAP Method. If the chosen method is **EAP-TLS**, **EAP-PEAP**, or **EAP-TTLS**, authentication can be performed via a CA Certificate, and the configuration differs depending on the selected **CA Certificate Type**.

Please refer to the **CA Certificate Type Guide** for more information.

WEB GUI ACCESS CONFIGURATION

The WP8x6 can be configured using:

- The embedded Web GUI on the handset via the PC's web browser.
- LCD Configuration Menu using the WP8x6 keypad.

From the Web GUI, you can configure all the functions supported by the WP8x6, while via the keypad menu, you can access limited configuration.

Configuration via Web Browser

The WP8x6 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the handset through a Web browser such as Google Chrome or Mozilla Firefox.

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.

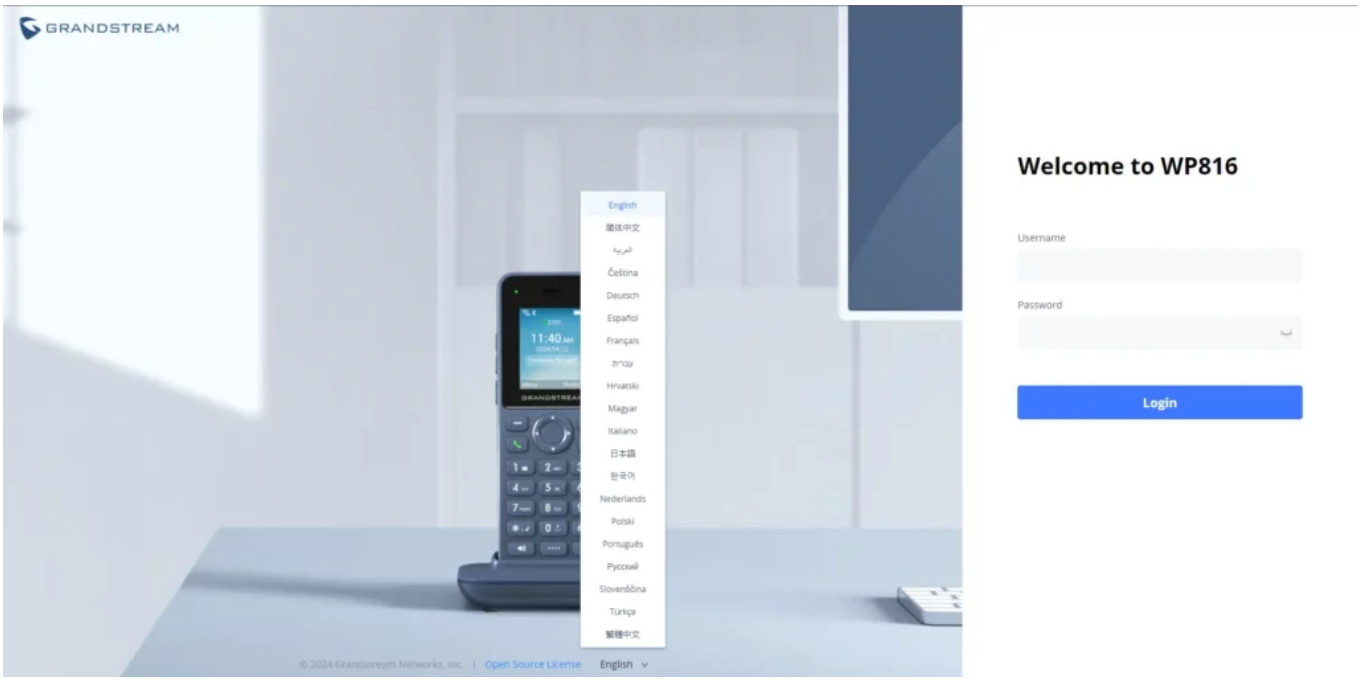
Accessing the Web UI

1. Connect the computer to the same network as WP8x6.
2. Make sure the handset is booted up and powered correctly.
3. You may check the IP address on the phone LCD menu **Status** -> **Network Status -> IP-info.** Please see **Obtain IP Address**
4. Open the Web browser on your computer and enter the WP8x6 IP address in the address bar of the browser.
5. Enter the administrator's username and password to access the Web Configuration Menu.

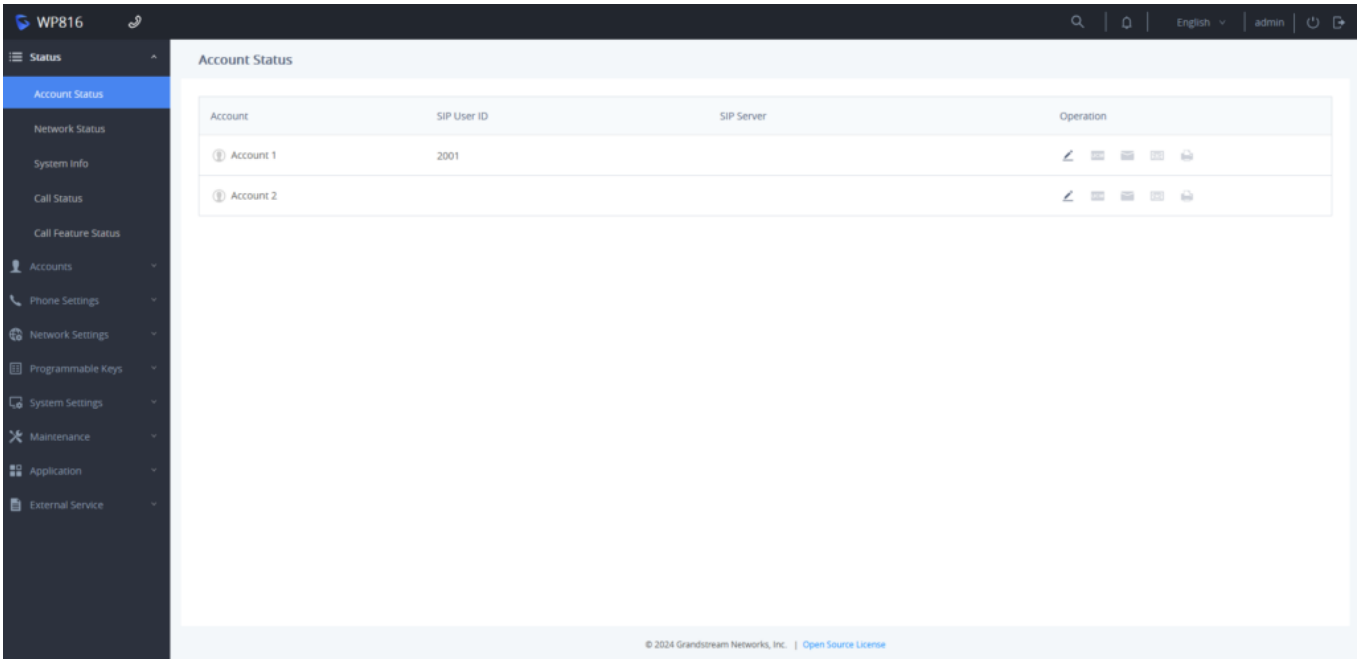
- The computer must be connected to the same sub-network as the phone. This can be easily done by connecting the computer to the same hub or switch as the phone.
- The default administrator username is "admin", for the password, a random code will appear on the web UI, enter this code on your phone. Once verified, you'll proceed to change the default password.
- The default end-user username is "user" and the initial password is "123", you will be prompted to change the user password immediately after providing the initial password. The user access is disabled by default
- If the **'Web Access Mode'** parameter is set to "Disabled" under **Security Settings -> Web/SSH Access**; web UI access will be disabled.

Web GUI Languages

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



Web GUI Language login page



Web GUI Language

Saving the Configuration Changes

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

First Time Login

When setting up your WP8x6 device and connecting to its web UI for the first time after a factory reset, you will be prompted by a digit combination that you need to enter on the keypad of your phone to automatically open the change password page on your browser.



Digits to be entered on the phone keypad



Changing the password

Web UI Access Level Management

There are two default passwords for the login page:

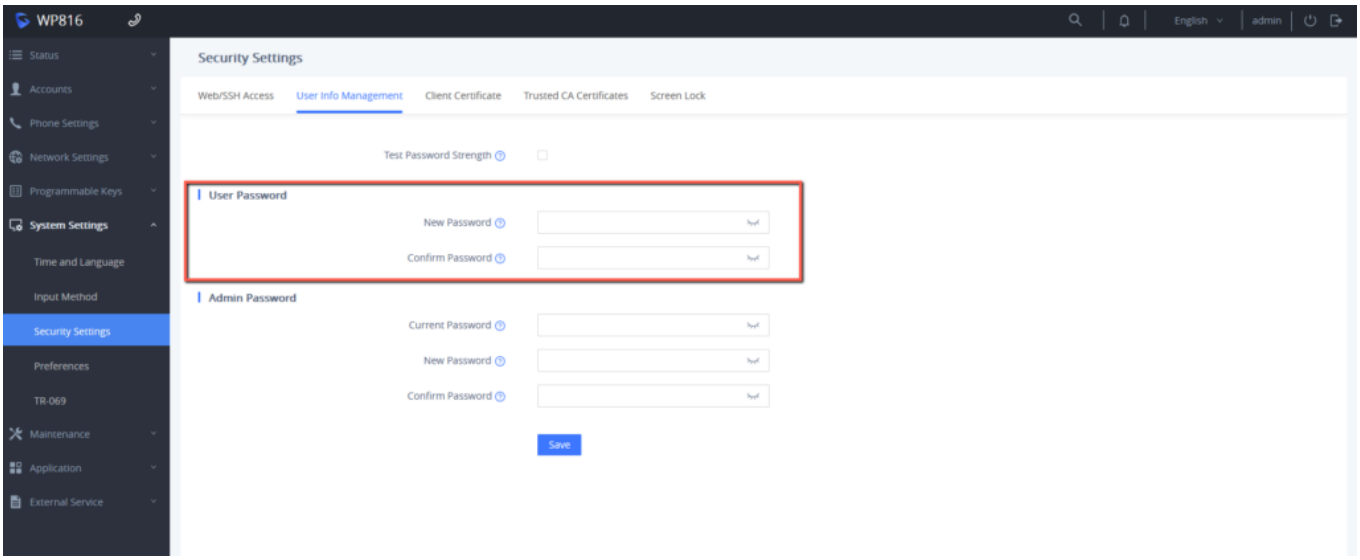
User Level	User Name	Password	Web Pages Allowed
End User Level	user	123	Only Status, Phone Settings, System Settings, Maintenance and System Application with limited options.
Administrator Level	admin	Random password generated after entering a numbers combination on the keypad	All pages

Web UI Access Level

Changing User Level Password

1. Access the Web GUI of your phone using the admin's username and password.
2. Press **Login** to access your settings.
3. Go to **System Settings** -> **User Info Management.**
4. Locate **User Password** section:

   - Type in your new user password in the **New Password** field.
   - Type in again same entered password in the **Confirm Password** field.
5. Press the **Save** button to save your new settings.



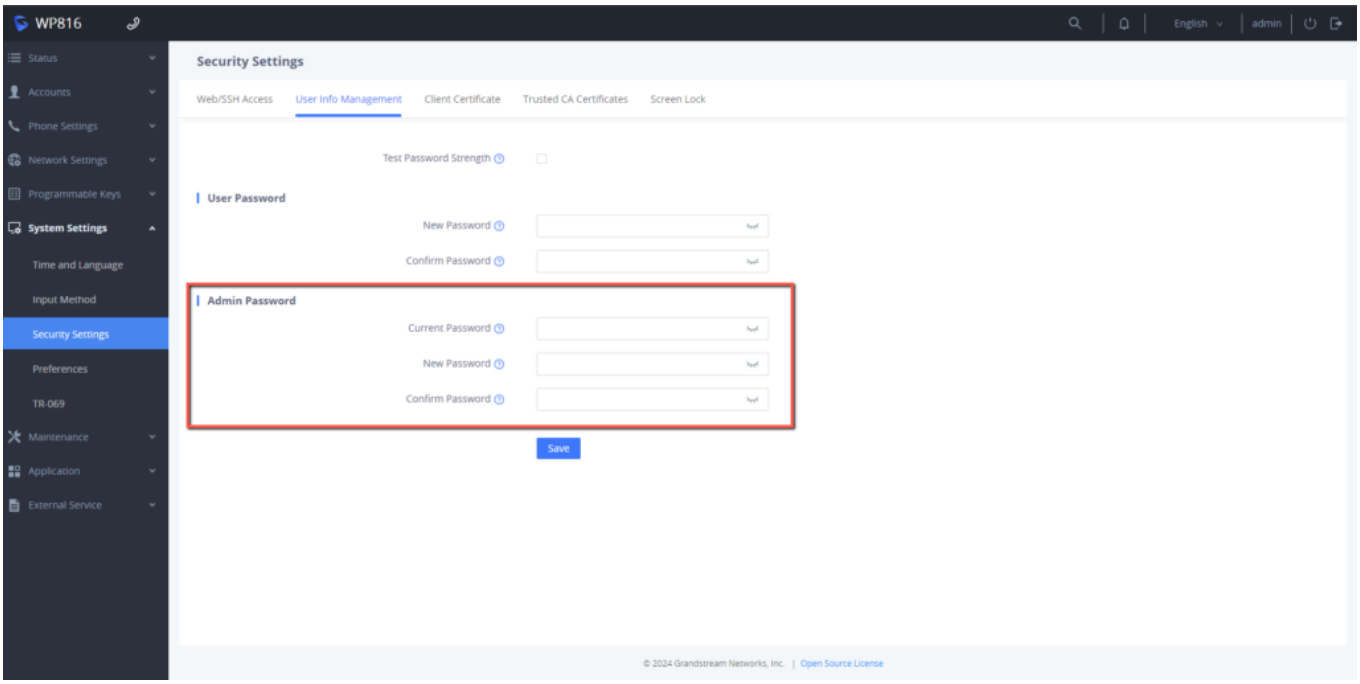
Changing User Level Password

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

Changing Admin Level Password

1. Access the Web GUI of your WP8x6 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 **System Settings -> User Info Management**.
4. Locate **Admin Password** section:

   1. Type in the admin password in the **Current Password** field
   2. Type in your new admin password in the **New Password** field.
   3. Type in again same entered password in the **Confirm Password** field.
5. Press the **Save** button to save your new settings.



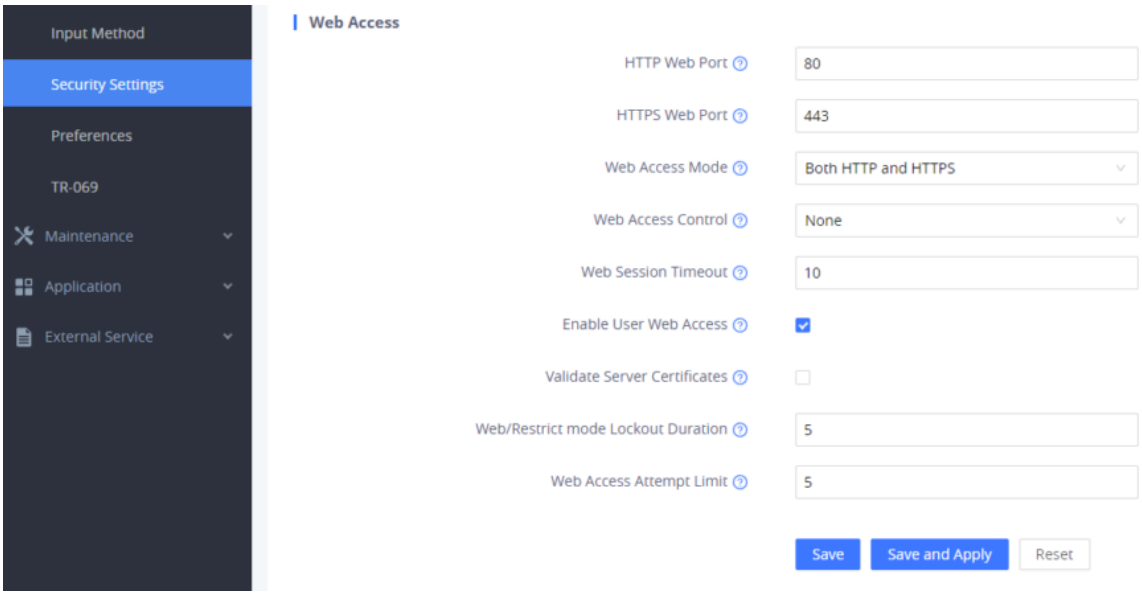
Admin Level Password

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

Changing HTTP/HTTPS Web Access Port

1. Access the Web GUI of your handset 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 **Security Settings -> Web/SSH Access**
4. In Web Access Mode, select the access method depending on the desired protocol (HTTP, HTTPS, or Both)
5. Locate the **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 the **Save** button to save your new settings.

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



Web Access Port

WEB GUI SETTINGS

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

- **Status:** Displays the Account status, Network status, and System Info of the phone.
- **Account:** To configure the SIP account.
- **Phone Settings:** To configure phone general settings, Call Settings, Ringtone, and Multicast Paging.
- **Network Settings:** To configure network settings.
- **Programmable keys:** Configures idle Screen Softkeys, Call Screen Softkeys, Number Keys, Navigate Keys Side Key, and much more.
- **System Settings:** Configures Time and Language settings, Security Settings, Preferences, TR-069.
- **Maintenance:** To configure upgrading and provisioning, System Diagnostics, Outbound Notifications, and Voice monitoring.
- **Application:** Configures Web Service settings, Contacts, LDAP, and Call History.
- **External Service:** Configures GDS Settings and E911 Services.

Status Page Definitions

Status -> Account Status	
Account	Account index, shows a list of : Two Accounts for the WP816. Three Accounts for WP826 and WP836.
SIP User ID	Displays the configured SIP User ID for the account.
SIP Server	Displays the configured SIP Server address, URL or IP address, and port of the SIP server.
Operation	Displays the different types of operations that can be performed on each SIP account, including editing the account, accessing the voicemail....
Status -> Network Status	
WLAN MAC Address	The WLAN MAC Address is a unique identifier assigned to the Wi-Fi interface of the WP phone, facilitating network communication and device recognition within the WLAN (Wireless Local Area Network).

SSID	The SSID (Service Set Identifier) is the name of the Wi-Fi network broadcasted by the access point, allowing devices like the WP phone to identify and connect to the correct network.
BSSID	BSSID is the MAC address of the access point (AP) or router that is providing the Wi-Fi network.
Band Width	The "band" refers to the frequency range at which the Wi-Fi network operates, typically either 2.4 GHz or 5 GHz, determining the speed and coverage of the WP phone's wireless connection.
Channel	The "channel" refers to a specific frequency within the band that the Wi-Fi network uses for communication. Selecting the appropriate channel helps optimize performance and reduce interference for the WP phone's wireless connection.
RSSI	Received Signal Strength Indicator measures the signal strength of the Wi-Fi connection on the WP phone, indicating the quality of the wireless signal received from the access point.
Security Mode	Security Mode indicates the encryption method used to protect data transmitted over the Wi-Fi network on the WP phone, ensuring secure communication between devices and preventing unauthorized access.
Highest Technical Standards	Displays the Highest Wi-Fi version supported by the WP phone
Current Technical Standards	Displays the Wi-Fi version currently used by the WP phone
Country Code	Displays the country where the WP phone is deployed
IPv4 Address Type	Displays how the WP phone have had its IPv4 address assigned
IPv4 Address	Displays the IPv4 address with its corresponding subnet mask
Gateway	Displays the IP address of the gateway
IPv4 NAT Type	Displays the type of NAT used in the IPv4 network
IPv6 Address Type	Displays how the WP phone have had its IPv6 address assigned
Global Unicast Address	Displays the IPv6 Global Unicast Address
Link-Local Address	Displays the Link-Local Address
IPv6 Static Gateway	Displays the IPv6 gateway address
IPv6 DUID	Displays the DHCP Unique Identifier
IPv6 NAT Type	Displays the IPv6 NAT Type used
DNS Server	Displays the Primary and secondary DNS servers used
DNS Mode	Displays the DNS mode used by each account
NAT Traversal	Displays the NAT traversal mode used
Status -> System Info	
Product Model	Product model of the phone.
Part Number	Product part number.
Serial Number	Displays the serial number of the unit
Certificate Type	Displays the certificate type used
Software Version	Boot: boot version number.Core: core version number.Base: base version number.Prog: program version number. This is the main firmware release number, which is always used for identifying the software system of the phone.Locale: locale version number.Res: Resolution version number.
IP Geographic Information	Language: displaying language.Recommend Time Zone: represent the time zone detected by IP address
System Up Time	System up time since the last reboot.
System Time	Current system time on the phone system.

System Time-Zone	Displays the time zone that is configured by user
System Information	Download system information
Service Status	GUI, Phone and CPE service status.
User Space	Shows the percentage of the user space used and the status of the Database
Core Dump	Shows the status of the core dump and the core dump files generated if any. It also gives the ability to generate GUI/Phone core dump files manually.
Special Feature	OpenVPN(R) Support: displaying if the phone supports OpenVPN(R).
Call Status	This tab displays different call informations to monitor and view the call status, information mentioned include the call quality, basic Call info , such as the extensions used , the IP address of the endpoints and the codecs used
Call Feature Status	This tab shows whether the call features for each account, such as DND, Auto Answer, Forward All, Busy Forward, and No Answer Forward, are enabled or disabled.

Accounts Page Definitions

Account x -> General Settings	
Account Register	
Account Active	Indicates whether the account is active.The default setting is "No".
Account Name	The name associated with each account to be displayed on the LCD. (e.g., MyCompany)
SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (e.g., sip.mycompany.com, or IP address)
Secondary SIP Server	The URL or IP address, and port of the SIP server. This will be used when the primary SIP server fails
Outbound Proxy	Defines IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller.
Secondary Outbound Proxy	Defines secondary outbound proxy that will be used when the primary proxy cannot be connected.
SIP User ID	User account information, provided by your VoIP service provider.
SIP Authentication ID	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	The account password required for the phone to authenticate with the SIP server before the account can be registered.After it is saved, this will appear as hidden for security purpose.
Name	The SIP server subscriber's name (optional) that will be used for Caller ID display (e.g., John Doe).
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to "user=phone". A "user=phone" parameter will be attached to the Request-URI and "To" header in the SIP request to indicate the E.164 number. If set to "Enable", "tel:" will be used instead of "sip:" in the SIP request.
Voice Mail Access Number	Allows users to access voice messages by pressing the MESSAGE button on the phone. This value is usually the VM portal access number.
Account Display	When set to "Username", the LCD will display the Username if it is not empty and when set to "User ID", the LCD will display the User ID if it is not empty.
UCM User Password	Input UCM user login password to connect UCM user settings.
Network Settings	

DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. If "Use Configured IP" is selected, please fill in Primary IP, Backup IP 1 and Backup IP 2.A RecordSRVNAPTR/SRVUse Configured IP
Max Number Of Sip Request Retries	Sets the maximum number of retries for the device to send requests to the server. In DNS SRV configuration, if the destination address does not respond, all request messages are resent to the same address according to the configured retry times. Valid range: 1-10.
DNS SRV Failover Mode	Configures the preferred IP mode for DNS SRV. If set to "default", the first IP from the query result will be applied. If set to "Saved one until DNS TTL", previous IP will be applied before DNS timeout is reached. If set to "Saved one until no response", previous IP will be applied even after DNS timeout until it cannot respond.DefaultIf 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 TTLIf 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 responsesIf the option is set with "Saved one until no responses", it will send registered messages to the previously registered IP first, but this behavior will persist until the registered server does not respond.Failback follows failback expiration timer If "Failback follows failback expiration timer" is selected, the device will send all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires.
Failback Expiration (m)	Specifies the duration (in minutes) since failover to the current SIP server or Outbound Proxy before making failback attempts to the primary SIP server or Outbound Proxy.
Register Before DNS SRV Failover	Configures whether to send REGISTER requests to the failover SIP server or Outbound Proxy before sending INVITE requests in the event of a DNS SRV failover.
Primary IP	Configures the primary IP address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 1	Configures the backup IP 1 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 2	Configures the backup IP 2 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
NAT Traversal	Controls whether and how the NAT traversal mechanism is enabled.No: Disables NAT traversal.STUN: Enables NAT traversal using a STUN server. When selected, the device detects its public IP address and port via the configured STUN server.Keep-Alive: Periodically sends UDP keep-alive packets to the SIP server to maintain the NAT binding and prevent port expiration.OpenVPN(R): Uses the OpenVPN tunnel for NAT traversal. Select this option when OpenVPN(R) is enabled.WireGuard(R): Uses the WireGuard tunnel for NAT traversal. Select this option when WireGuard(R) is enabled.Default value is set to "Auto"
Media NAT Traversal	Specifies how media streams handle NAT traversal.No: Disables media NAT traversal. Media traffic is sent using local network information only.Auto: Automatically applies the same behavior defined in NAT Traversal (STUN).STUN: Uses a shared STUN server to discover the device's public IP address and port after NAT.TURN: Relays media streams through a TURN server to ensure connectivity when direct peer-to-peer communication is not possible.ICE: Gathers local addresses, STUN-discovered public addresses, and TURN relay addresses, then dynamically selects the best available media path.Defautl value is set to "Auto"
Enable Trickle ICE	Configure whether to enable Trickle ICE. If enabled, it allows the ICE agent to send candidate addresses as they are collected, rather than waiting for all candidate addresses to be collected before sending them. This can accelerate the connection establishment process. This option is enabled by default when ICE is selected for the Media NAT Traversal.
Candidate Type	Configure the ICE candidate type. If "All" is selected, all address types will be collected. If "Relay Candidates Only" is selected, the candidate addresses will be obtained through a TURN server, which will act as a relay for the media stream.

STUN/TURN Server	Fill in the STUN/TURN server related configurations. You can configure up to three STUN/TURN Servers.
Support rport (RFC3581)	Configures to use symmetric response routing. If it is used, the "rport" field will be added to the Via header field in the SIP Request, and the information will be extracted from the SIP 200OK Response for SIP Register to rewrite the SIP Contact information and apply it in subsequent SIP Requests.
Proxy-Require	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall.
Use SBC	Configures whether a SBC server is used. Note: If enabled, make sure an outbound proxy is set up.
Account x -> SIP Settings	
Basic Settings	
SIP Registration	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is "Enabled".
UNREGISTER on Reboot	If set to "No", the phone will not unregister the SIP user's registration information before new registration.If set to "All", the SIP Contact header will use "*" to clear all SIP user's registration information. If set to "Instance", the phone only needs to clear the current SIP user's info.
REGISTER Expiration	Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
SUBSCRIBE Expiration	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
Re-Register before Expiration	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default value is 0.
Registration Retry Wait Time (s)	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 60 seconds.
Registration Retry Wait Time(s) upon 403 Forbidden	Specifies the interval to retry registration if the process is failed due to 403 Forbidden. Valid range is 0 to 3600 in second. 0 second means stop retry registration. Default value is set to 1200 seconds.
Add Auth Header on Initial REGISTER	If enabled, the phone will add Authorization header in initial REGISTER request. The authorization header contains the authentication credentials.Default is "Disabled".
Add Auth Header on RE-REGISTER	If enabled, the phone will add Authorization header in RE-REGISTER request. The authorization header contains the authentication credentials.Note: By default, this option is enabled.
Enable OPTIONS Keep Alive	Configures whether to enable SIP OPTIONS to track account registration status. If enabled, the phone will send periodic OPTIONS messages to server to track the connection status with the server.Default is "Disabled".
OPTIONS Keep Alive Interval	Configures the time interval the phone sends OPTIONS message to the server. If set to 30 seconds, it means the phone will send an OPTIONS message to the server every 30 seconds.
OPTIONS Keep Alive Max Tries	Configures the maximum number of times the phone will try to send OPTIONS message consistently to server without receiving a response. If set to "3", the phone will send OPTIONS message 3 times. If no response from the server, the phone will re-register.
SUBSCRIBE for MWI	When set to "Yes", a SUBSCRIBE for Message Waiting Indication will be sent periodically.The default setting is "No".
SUBSCRIBE for Registration	When set to "Yes", a SUBSCRIBE for Registration will be sent out periodically.The default setting is "No".

Use Privacy Header	Configures whether the "Privacy Header" is present in the SIP INVITE message.Default: the phone will add "Privacy Header" when special feature is not "Huawei IMS".Yes: the phone will always add "Privacy Header".No: the phone will not add "Privacy Header".The default setting is "default".
Use P-Preferred- Identity Header	Configures whether the "P-Preferred-Identity Header" is present in the SIP INVITE message.Default: the phone will add "P-Preferred-Identity header" when special feature is not "Huawei IMS".Yes: the phone will always add "P-Preferred-Identity header".No: the phone will not add "P-Preferred-Identity header".
Use X-Grandstream-PBX Header	Configures to use X-Grandstream-PBX header in SIP request.Default setting is "Yes".
Use P-Access-Network-Info Header	Configures to use P-Access-Network-Info header in SIP request.Default setting is "Yes".
Use P-Emergency-Info Header	Configures to use P-Emergency-Info header in SIP request.Default setting is "Yes".
Use P-Asserted-Identity Header	Configure whether the "P-Asserted-Identity Header" is present in the SIP REGISTER message.
Use P-Early-Media Header	Configure if the "P-Early-Media Header" support is enabled.
Use Zoom E911 X-switch-info SIP Header	Configure whether the "Zoom E911 X-switch-info SIP Header" is present in the SIP REGISTER message.
Use Accept-Language Header	Specifies whether the phone includes the Accept-Language header in SIP REGISTER messages and SIP responses to SIP INVITE requests. By default, this option is set to Auto, which uses the language configured under System Settings -> Time and Language -> Language -> Display Language. Available options: Disabled: The Accept-Language header is not included.Auto: The header follows the phone's configured display language.Specific Language: Sets the Accept-Language header to the selected language.Supported Languages: Arabic (ar), Catalan (ca), Czech (cz), Danish (da), German (de), Greek (el), English (en), Spanish (es), French (fr), Hebrew (he), Croatian (hr), Hungarian (hu), Italian (it), Japanese (ja), Korean (ko), Latvian (lv), Dutch (nl), Polish (pl), Portuguese (pt), Russian (ru), Swedish (se), Slovenian (sl), Slovakian (sv), and Turkish (tr).
Use MAC Header	If Register Only, all outgoing SIP message will include the MAC header.If Yes to all SIP, all outgoing SIP messages will include the MAC header.If No, the phone's MAC header will not be included in any outgoing SIP messages.The default setting is "No".
Add MAC in User-Agent	If Yes except REGISTER, all outgoing SIP messages will include the phone's MAC address in the User-Agent header, except for REGISTER and UNREGISTER.If Yes to All SIP, all outgoing SIP messages will include the phone's MAC address in the User-Agent header.If No, the phone's MAC address will not be included in the User-Agent header in any outgoing SIP messages.The default setting is "No".
SIP Transport	Selects the network protocol used for the SIP transport.The default setting is "UDP".
Enable TCP Keep-alive	Configures whether to enable TCP Keep-alive for the TCP connection between the terminal and the SIP server.
SIP Listening Mode	Configures whether or not to listen to multiple SIP protocols.If set to "Dual", phone will listen to TCP when UDP is selected.If set to "Dual (Secured)", phone will listen to TLS/TCP when UDP is selected. If "TCP" or "TLS/TCP" is selected, UDP will be listened too.If set to "Dual (BLF Enforced)", phone will try to enforce BLF subscriptions to use TCP protocol by adding 'transport=tcp' to the Contact header.The default setting is "Transport Only".
Local SIP Port	Configures the local SIP port used to listen and transmit.
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	Configures whether the actual ephemeral port in contact with TCP/TLS will be used when TLS/TCP is selected for SIP Transport.The default setting is "No".

Support SIP Instance ID	Configures whether SIP Instance ID is supported or not.The default setting is "Yes".
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
Outbound Proxy Mode	Configures whether to put the Outbound Proxy in the Route header, or if SIP messages should always be sent to Outbound Proxy.In routeNot in routeAlways send toDefault is "in route".
Enable 100rel	When enabled, the 100rel tag is appended to the value of the Supported header of the initial signaling messages.The default setting is "No".
Use Route Set in Notify (Follow RFC 6665)	Configures whether to use route set in NOTIFY (follow RFC 6665).If enabled, the Request URI of the refresh subscription will use the URI in the received NOTIFY Contact (RFC 6665).If disabled, the URI in the previously subscribed 200 OK Contact will be used.
Session Timer	
Enable Session Timer	Configures whether to enable session timer function. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. If set to "Yes", the phone will use the related parameters when sending session timer according to "Session Expiration". If set to "No", session timer will be disabled.The default setting is "No".
Session Expiration	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.The default setting is "No".
Force Timer	If set to "Yes", the phone will use the Session Timer even if the remote party does not support this feature. Otherwise, Session Timer is enabled only when the remote party supports it.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. When set to "Omit", the refresh object is not specified.The default setting is "UAC".
UAS Specify Refresher	As a callee, select UAC to use caller or proxy server as the refresher, or select UAS to use the phone as the refresher.The default setting is "UAC".
Force INVITE	Select "Yes" to force using the INVITE method to refresh the session timer.The default setting is "No".
Account x -> Codec Settings	
Audio	

Preferred Vocoder(Choice 1 - 8)	Multiple vocoder types are supported on the phone, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message. The vocoders supported are: OPUSPCMUPCMAG.723.1G.722 (wide band)G.729A/BiLBCG.726-32G.726-16G.726-24G.726-40
Codec Negotiation Priority	Configures the phone to use which codec sequence to negotiate as the callee. When set to "Caller", the phone negotiates by SDP codec sequence from received SIP Invite. When set to "Callee", the phone negotiates by audio codec sequence on the phone. The default setting is "Callee".
Use First Matching Vocoder in 200OK SDP	When set to "Yes", the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is "No".
iLBC Frame Size	Selects iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is "30ms".
iLBC Payload Type	Specifies iLBC payload type. Valid range is 96 to 127. Cannot be the same as Opus or DTMF payload type. Valid range is 96 to 127. The default setting is "97".
G.726-32 Packing Mode	Selects "ITU" or "IETF" for G.726-32 packing mode.The default setting is "ITU".
G.726-32 Dynamic Payload Type	Specifies G.726-32 payload type. Valid range is 96 to 127. Default is 127.
Opus Payload Type	Specifies Opus payload type. Valid range is 96 to 127. It cannot be the same as iLBC or DTMF Payload Type. Default value is 123.
Send DTMF	Specifies the mechanism to transmit DTMF digits. There are 3 supported modes:In audio: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs).RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.SIP INFO uses SIP INFO to carry DTMF.Default setting is "RFC2833".
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Inbound DTMF Volume	Sets the volume size when using in-audio DTMF transmission mode. The higher the parameter value, the higher the volume value. the valid range is 0-32. The default value is 18.
Enable Audio RED with FEC	If set to "Yes", FEC will be enabled for audio call.
Audio FEC Payload Type	Configures audio FEC payload type. The valid range is from 96 to 126.The default value is 121.
Audio RED Payload Type	Configures audio RED payload type. The valid range is from 96 to 126.The default value is 124.
Silence Suppression	If 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. For codec G.723 and G.729 only.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".
Minimum Jitter Buffer Length	Sets the minimum jitter buffer length based on network conditions.The default value is 0ms. Works over Wi-Fi only.

Voice Frames Per TX	Configures the number of voice frames transmitted per packet. It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120 kbps. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used in the codec table or negotiate the payload type during the actual call. For example, if set to 2 and the first code is G.729, G.711 or G.726, the "ptime" value in the SDP datagram of the INVITE request is 20 ms. If the "Voice Frame/TX" setting exceeds the maximum allowed value, the phone will use and save the maximum allowed value for the selected first codec. It is recommended to use the default setting provided, and incorrect setting may affect voice quality.The default setting is 2.
G.723 Rate	Selects encoding rate for G723 codec.
RTP Settings	
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu.NoEnabled but Not forcedEnabled and ForcedOptionalThe default setting is "No".
SRTP Key Exchange	Select SRTP key exchange method, SDES(Secure Real-time Transport Protocol) or DTLS(Datagram Transport Layer Security)
SRTP Key Length	Allows users to specify the length of the SRTP calls. Available options are:AES 128&256 bitAES 128 bitAES 256 bitDefault setting is AES 128&256 bit
Crypto Life Time	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. The default setting is "Yes".
RTCP Mode	Configure RTCP port negotiation rules.Default: Use the traditional RTCP port, which is "RTP port+1".Negotiate RTCP Port: Use attribute RTCP to negotiate.RTCP Mux: The caller actively negotiates the RTCP port and indicates RTCP Mux at the same time.RTCP Mux Only: The caller forces RTCP Mux, generated by the local media port only apply for RTP port.
RTCP Keep-Alive Method	Configures the RTCP channel keep-alive packet type.Receiver Report: The RTCP channel will sends "receiver report+source description+RTCP extension" as keep-alive data.Sender Report: The RTCP channel will sends "Sender report+source description+ RTCP extension" as keep-alive data.
RTP Keep-Alive Method	Configures the RTP channel keep-alive packet type.No: No data will be sentRTP Version 1: The wrong version infor "1" will be carried when sending RTP data packets.RTP Packet with Silent Payload: If set to "RTP Packet with Silent Payload", the silent payload will be carried when sending RTP format packets.
VQ RTCP-XR Collector Address Selection	When select "Manual", the collector address will be manually configured and transmitted using the SIP Transport protocol. When select "Auto", if the collector address is manually filled in, use this address. If not filled in, use the SIP registered address.
VQ RTCP-XR Collector Name	Configure the host name of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Address	Configure the IP address of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
VQ RTCP-XR Collector Port	Configure the port of the central report collector that accepts voice quality reports contained in SIP PUBLISH messages.
Symmetric RTP	Configures whether Symmetric RTP is used or not. Symmetric RTP means that the UA uses the same socket/port for sending and receiving the RTP stream. The default setting is "No".
RTP IP Filter	Configures whether to filter the received RTP. If set to "Disable", the device will receive RTP from any address; If set to "IP Only", the device will receive RTP from certain IP address in SDP with no port limited; If set to "IP and Port", the device will only receive RTP from IP address & port in SDP. Disabled by Default

RTP Timeout (s)	Configures the RTP timeout of the phone. If the phone does not receive the RTP packet within the specified RTP time, the call will be automatically disconnected. The default range is 0 and 6-600. If set to 0, the phone will not hang up the call automatically.
Account x -> Call Settings	
General	
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 (#)".
No Key Entry Timeout	Configures the timeout (in seconds) for no key entry. If no key is pressed after the timeout, the collected digits will be sent out. The default value is 4 seconds. The valid range is from 1 to 15.
Send Anonymous	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous. Default is "No".
Anonymous Call Rejection	If set to "Yes", anonymous calls will be rejected.The default setting is "No".
Enable Call Waiting	Configures the call waiting function for this account. If set to "Default", it will be configured according to global call waiting function. Default value is "Default".
RFC2543 Hold	Allows users to toggle between RFC2543 hold and RFC3261 hold. RFC2543 hold (0.0.0.0) allows user to disable the hold music sent to the other side. RFC3261 (a line) will play the hold music to the other side. The default setting is "No".
Ring Timeout	Configures the timeout (in seconds) for the phone to ring when an incoming call is not answered. Valid range is 30 to 3600. The default setting is 60.
Call Log	Configures Call Log setting on the phone.Log All CallsLog incoming/Outgoing Only (missed calls NOT recorded)Disable Call LogThe default setting is "Log All Calls".
Auto Answer	
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".
Auto Answer Numbers	Allows the user to configure specific numbers to auto answer. If not set, all numbers will be auto answered If auto answer is enabled. Up to 10 numbers can be configured.
Intercom	
Play warning tone for Auto Answer Intercom	If enabled, phone will play warning tone when auto answering Intercom.
Custom Alert-Info for Auto Answer	Used exclusively to match the contents of the Alert-Info header for auto answer. The default auto answer headers will not be matched if this is defined.
Allow Auto Answer by Call-Info/Alert-Info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info/Alert-Info header sent from the server/proxy.Default is "Yes".
Allow Barging by Call-Info/Alert-Info	When enabled, the phone will automatically put the current call on hold and answer the incoming call based on the SIP Call-Info/Alert-Info header sent from the server/proxy. However, if the current call was answered based on the SIP Call-Info/Alert-Info header, then all other incoming calls with SIP Call-Info/Alert-Info headers will be rejected automatically. Default setting is "No".
Mute on Intercom Answer	If enabled, the phone will mute the mirophone after answer an intercom call via Call-Info/Alert-Info.
Record	

Record Key Default Fuction	Configures whether to turn the recording function on or off when the "Record" key is pressed for the first time in a call using this account. For example, the SIP server can be configured with automatic call recording. In this case, Record key default function should be configured as "Record off".
Call Recording On	Configures the DTMF sequence sent when pressing the Record key during a call on this account. Toggles between this value and the off code if possible; otherwise always sends this code.
Call Recording Off	Configures the DTMF sequence sent when pressing the Recording key during a call on this account when turning recording off.
Transfer	
Transfer on Conference Hangup	Configures whether the call is transferred to the other party if the conference initiator hangs up.The default setting is "No".
Enable Recovery on Blind Transfer	Enable recovery to the call to the transferee on failing blind transfer to the target. The default setting is "Yes".Notes:This feature only applies to blind transfer.This feature depends on how server handles transfer. If there is any NOTIFY from server, this feature will not take effect. If server responds 4xx, phone should try to recover regardless of this option.During blind transfer, after transferor received 200/202 for REFER, but there is no NOTIFY from server after 7 seconds, transferor will decide to recover the call with transferee or not depending on the options. This is the only case that this option will be applied.
Blind Transfer Wait Timeout	Configures the timeout (in seconds) when waiting for sipfrag response in blind transfer. Valid range is 30 to 300. Default setting is "30".
Refer-To Use Target Contact	If set to "Yes", the "Refer-To" header uses the transferred target's Contact header information for attended transfer.
Call Forward	
Enable Forward All	If set to "Yes", all calls will be forwarded to the number specified below. Disabled by Default
All To	Specifies the number to be forwarded to when enabled Forward all.
Enable Busy Forward	If set to "Yes", the call will be forwarded to the number specified below on busy. Disabled by Default
Busy To	Specifies the number to be forwarded to for Call Forward On Busy.
Enable No Answer Forward	If set to "Yes", call will be forwarded to the number specified below on no answer. Disabled by Default
No Answer To	Specifies the number to be forwarded to for Call Forward On No Answer.
No Answer Timeout (s)	Defines the timeout (in seconds) before the call is forwarded on no answer.
Enable Override Forward	If enabled, the local call forward is disabled when an incoming call comes in from the configured override forward number. Disabled by Default
Override Forward Numbers	Configures the number to override the local forward function. The Max number is 10.
Dial plan	
Dial Plan Prefix	Configures a prefix added to all numbers when making outbound calls.
Bypass Dial Plan	Bypass the dial plan when dialing from one of the available items:ContactsCall History Incoming CallCall History Outgoing CallDialing PageMPKAPI

Dial Plan	Configures the dial plan rule. For syntax and examples, please refer to user manual for more details.Dial Plan Rules:Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d;Grammar: x - any digit from 0-9;Grammar: X - any character from 0-9, a-z, A-Z.xx+ - at least 2 digit numbersxx - only 2 digit numbersXX - two characters (AA, Ab, 1C, f5, 68,...)test : only string "test" will pass the dial plan check^ - exclude[3-5] - any digit of 3, 4, or 5[147] - any digit of 1, 4, or 7<2=011> - replace digit 2 with 011 when dialing| - the OR operandExample 1: {[369]11 | 1617xxxxxxx}Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617;Example 2: {^1900x+ | <=1617>xxxxxxx}Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers;Example 3: {1xxx[2-9]xxxxxx | <2=011>x+}Allows any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR Allows any length of numbers with leading digit 2, replacing the 2 with 011 when dialed.Example of a simple dial plan used in a Home/Office in the US: { ^1900x. | <=1617>[2-9]xxxxxx | 1[2-9]xx[2-9]xxxxxx | 011[2-9]x. | [3469]11 }Explanation of example rule (reading from left to right):^1900x. - prevents dialing any number started with 1900;<=1617>[2-9]xxxxxx - allows dialing to local area code (617) numbers by dialing7 numbers and 1617 area code will be added automatically;1[2-9]xx[2-9]xxxxxx |- allows dialing to any US/Canada Number with 11 digits length;011[2-9]x - allows international calls starting with 011;[3469]11 - allows dialing special and emergency numbers 311, 411, 611 and 911.Note: In some cases, where the user wishes to dial strings such as *123 to activate voice mail or other applications provided by their service provider, the * should be predefined inside the dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.Max length of dial plan is up to 1024 characters.
Call Display	
Caller ID Display	When set to "Auto", the phone will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. When set to "Disabled", all incoming calls are displayed with "Unavailable".
Callee ID Display	When set to "Auto", the phone will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in the 180 Ringing. When set to "Disabled", callee id will be displayed as "Unavailable". When set to "To Header", caller id will not be updated and displayed as To Header.
Ringtone	
Ringback Tone at No Early Media	Play ringback tone when there is no receiving early media RTP packets. Disabled by Default
Account RingTone	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu.Note: User can also choose silent ring tone or doorbell.
Ignore Alert-Info header	Configures to play default ringtone by ignoring Alert-Info header.The default setting is "No".
Enable Alert-Info Bellcore Mapping	This option controls how the phone interprets the Alert-Info header. When enabled, values in the format 'Bellcore-dr%N' (N = 1-5) are mapped to predefined Bellcore ring tones. If disabled, the same values trigger custom ring tones instead. A value of 0 results in a silent ringtone, while values between 6-9 always trigger custom ring tones regardless of the setting. Invalid values (less than 0 or greater than 9) default to the standard ringtone.This option is enabled by default.

Match Incoming Caller ID	Specifies matching rules with number, pattern, or Alert Info text (up to 10 matching rules). When the incoming caller ID or Alert Info matches the rule, the phone will ring with selected distinctive ringtone. Matching rules:Specific caller ID number. For example, 8321123.A defined pattern with certain length using x and + to specify, where x could be any digit from 0 to 9. Samples: xx+ : at least 2-digit number.xx : only 2-digit number.[345]xx: 3-digit number with the leading digit of 3, 4 or 5.[6-9]xx: 3-digit number with the leading digit from 6 to 9.Alert Info textUsers could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it. The custom ring tone will be used if the phone receives SIP INVITE with Alert-Info header in the following format: Alert-Info: <http://127.0.0.1>; info=priority When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone. Note: Beginning with firmware version 1.0.3.98, a new feature was introduced that enables the use of a ringtone stream via a remote URL. The functionality of this feature works as follows: the following audio file named test.wav is uploaded onto an HTTP server and the remote URL is "http://192.168.5.165:8080/test.wav;info=ring3", the IP phone then attempts to use the provided URL first to play the ringtone. If the URL is not functional for some reason, it will then use the info=ring3 parameter, as the default ringtone.
Account x -> Advanced Settings	
Security Settings	
Check Domain Certificates	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is "No".
Trusted Domain Name List	Configure the list of trusted domain names, which supports filling in the SAN list used only for domain name verification in TLS to obtain certificates. If it matches any item in the trusted domain name list, the certificate is trusted. By default, the remote proxy domain name and SIP server domain name are trusted. This field allows numbers/letters/-/./*. It supports wildcard domain names, such as "*.mycompany.com", and trusts any domains ending with ".mycompany.com".
Validate Certificate Chain	Validate certification chain when TCP/TLS is configured.The default setting is "No".
Validate Incoming SIP Messages	Specifies if the phone will check the incoming SIP messages Caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
Omit charset=UTF-8 in MESSAGE	Omit charset=UTF-8 in MESSAGE content-type
Allow Unsolicited REFER	Configures whether to dial the number carried by Refer-to header after receiving out-of-dialog SIP REFER request actively.If set to "Disabled", the phone will send error warning and stop dialing.If set to "Enabled/Force Auth", the phone will dial the number after sending authentication. If the authentication fails, it will stop dialing.If set to "Enabled", the phone will dial all numbers carried by SIP REFER.
Accept Incoming SIP from Proxy Only	When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is "No".
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is "No".
Allow SIP Reset	Allow SIP Notification message to perform factory reset.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.The default setting is "No".
MOH	
On Hold Reminder Tone	Configures to play reminder tone when the call is on hold.
Music On Hold URI	Music On Hold URI to call when a call is on hold if server supports it.
Advanced Features	

Special Feature	Different soft switch vendors have special requirements. Therefore, users may need select special features to meet these requirements. Users can choose from Standard, Nortel MCS, Broadsoft, CBCOM, RNK, Sylantro, Huawei IMS, Zoom, PhonePower,UCM Call center, Zoom, and Telestra depending on the server type. The default setting is "Standard".
Feature Key Synchronization	This feature is used for Broadsoft call feature synchronization. When it is enabled, DND, Call Forward features and Call Center Agent status can be synchronized between Broadsoft server and phone. Default is "Disabled".
Conference URI	Configures the conference URI when using Broadsoft N-way calling feature.
Reboot on check-sync event without "reboot="	If option is enabled, the phone will do reboot when receiving SIP NOTIFY check-sync event without "reboot=" header. If the option is disabled, the phone will do provision and not reboot when receiving SIP NOTIFY check-sync event without "reboot=" header. Enabled by default.
PUBLISH for Presence	Enables presence feature on the phone.The default setting is "No".
Call Park	
Call Park Feature Code	Configures the feature access code for parking the current call. Once this parameter is filled, the Call Park feature appears in the Options Menu during an ongoing call. Users can park the call to a specific extension or a parking slot.
Call Park Retrieve Feature Code	Configures the feature access code for retrieving the parked call on accounts.
Account x -> Dial Plan	
Name	Enter the name for the configured rules.
Rule	Enter the rule settings (number pattern, prefix to add ...etc.).
Type	Choose the type of the rule:Pattern: The phone will dial the number matching the entered pattern.Block: The phone will block the number/pattern matching the rule.Dial now: The phone will dial immediately the number once the DTMF matches the dial plan.Prefix: Specify the "Replaced" field to replace by the "Used" field to dial.Second tone: The phone plays the second dial tone when the entered "Trigger" digit is dialed.
Account x ? Hidden Number Plan	
Hidden Number Feature	If set to "Both Direction calls", incoming and outgoing number display will be handled according to hidden number plan. The options are : Incoming Calls Only, Outgoing Calls Only, Both Direction Calls
Hidden Number Plan List	Currently, incoming and outgoing number display will be handled according to hidden number plan. Users are able to configure the hidden number rules, matching their syntax rules from top to bottom as follows:Expression element(element)element (element)element element(element) (element)Element Rules * x:any digit number from 0-9 * +:any length after x(>=1) * [-+...] or *:Escape symbol * ():The part that needs to be hidden, there can only be one hidden part in a ruleExamples x+(xxxx)xxxx: 13705806547 -> 137****6547 xxx(x+)xxxx: 07113705806547 -> 071*******6547 071-x+(xxxx)xxxx: 071-13705806547 -> 071-137****6547
Hidden Number Plan Test	Enter the number to test the hidden rules of the current page. After confirming, please save and apply it.?
Feature Codes	
Enable Local Call Features	When enabled, Do Not Disturb, Call Forwarding and other call features can be used via the local feature codes on the phone. Otherwise, the provisioned feature codes from the server will be used. User configured feature codes will be used only if server provisioned feature codes are not provided.Note: If the device is registered with Broadsoft account, it does not matter if local call features are enabled or disabled, once the Broadsoft account is set, special feature to Broadsoft and Feature Key Synchronization is enabled, the call feature will be handled by Broadsoft server, not by the phone.

DND	
DND Call Feature On	Configures DND feature code to turn on DND.
DND Call Feature Off	Configures DND feature code to turn off DND.
Call Forward Always	
On	Configures Call Forward Always feature code to activate unconditional call forwarding.
Off	Configures Call Forward Always feature code to deactivate unconditional call forwarding.
Target	The extension the call will be forwarded to.
Call Forward Busy	
On	Configures Call Forward Busy feature code to activate busy call forwarding.
Off	Configures Call Forward Busy feature code to deactivate busy call forwarding.
Target	Configures the extension for the call to be forwarded to.
Call Forward No Answer	
On	Configures Call Forward No Answer feature code to activate no answer call forwarding.
Off	Configures Call Forward No Answer feature code to deactivate no answer call forwarding.
Target	The extension the call will be forwarded to.
Call Forward No Answer Timeout (s)	Defines the timeout (in seconds) before the call is forwarded on no answer. valid range is 1 to 120.
Accounts -> Account Swap	
Swap Account Settings	Allows users to swap the two accounts that they have configured. This will Increase the flexibility of account management.Note: Make sure to press "Start" to complete the process.

Phone Settings Page Definitions

Phone Settings > General settings	
Local RTP Port	This parameter defines the local RTP port used to listen and transmit. It is the base RTP port for channel 0. When configured, channel 0 will use this port _value for RTP; channel 1 will use port_value+2 for RTP. Local RTP port ranges from 1024 to 65400 and must be even. Default value is 5004.
Local RTP Port Range	Gives users the ability to define the parameter of the local RTP port used to listen and transmit. This parameter defines the local RTP port from 48 to 10000. This range will be adjusted if local RTP port + local RTP port range is greater than 65486. Default setting is 200.
Use Random Port	When set to "Yes", this parameter will force random generation of both the local SIP and RTP ports. This is usually necessary when multiple phones are behind the same full cone NAT. The default setting is "Yes"Note: This parameter must be set to "No" for Direct IP Calling to work.
Keep-alive Interval	Specifies how often the phone sends a blank UDP packet to the SIP server to keep the "ping hole" on the NAT router to open. The default setting is 20 seconds. The valid range is from 10 to 160.
STUN Server	The IP address or Domain name of the STUN server. STUN resolution results are displayed in the STATUS page of the Web GUI.Only non-symmetric NAT routers work with STUN.

Use NAT IP	The NAT IP address used in SIP/SDP messages. This field is blank at the default settings. It should ONLY be used if it is required by your ITSP.
Delay Registration	Configures specific time that the account will be registered after booting up.
Enable Outbound Notification	Configures whether to enable outbound notifications such as Action URL.
Clean User Data While Different Users Log In	When enabled, if the current login account is different with last one, Device under tesr will delete the contact and call history of the last account.
Custom Filter Warnings Message	Select the event messages which will be notified about when occurred.Note: The strings between the parantheses indicate the name of the module in the configuration file.SystemDatabase Corrupt (sys.db)Capturing Data Packets (sys.pcap)CPE Connection Failed (sys.cpe)Acccount Registration Failed (sys.accts)User Storage Space if Full (sys.user_space)Device Role Downgraded in Account Sharing (sys.account_sharing)The custom client certificate is invalid (sys.cert)Multiple login attempts to admin failedLow batteryUser default passwordNetworkWi-Fi connected to default SSID and password (sys.wifi.default)Wi-Fi disconnected abnormally (sys.wifi.disconnected)Network Error (sys.net)Wi-Fi Signal Issue (sys.wifi.signal.low)UpgradeFailed to download firmware (sys.upgrade.download_fw) Failed to download config file (sys.upgrade.cfg)Please set the URL to where the firmware is located (sys.upgrade.url_fw)Firmware detection failed (sys.upgrade.check_fw)Firmware server auth failed (sys.upgrade.auth_fw)Config server auth failed (sys.upgrade.auth_cfg)Failed to upgrade certificate (sys.upgrade.cert)Upgrade/Config update failed (sys.upgrade.lock)
Phone Settings > Call Settings	
General	
Preferred Default Account	Select the preferred default account for on-hook or off-hook dialing. When the selected account is unavailable, system will use the first available account to dial out.
Long Press Mute Key Functions While Idle DND	Select "Mute" key function while the phone is idle.DND: Pressing the "Mute" key when the phone is idle will enable DND.Idle Mute: Pressing the "Mute" key when the phone is idle will set the phone to be muted when answering incoming calls.Disabled
Last Call Froward Always	If enabled, the number put into the ForwardAll feature will be stored the next time you use the ForwardAll softkey. Note: ForwardAll softkey currently only used for account 1.
Show SIP Error Response	Configures to enable SIP error response information displayed on LCD screen. Enabled by default
Do Not Escape '#' as %23 in SIP URI	Replaces # by %23 for some special situations.
User-Agent Prefix	Configures the prefix in the User-Agent header.
Speaker Key Mode	Specifies how the Speaker key functions on the phone. Select the desired mode to control whether the key can be used for making or answering calls and switching audio channels.Default: The Speaker key can be used to make calls, answer calls, and switch audio channels.Always Disabled: Disables the Speaker key completely.For Switching Channels: The Speaker key can only be used to switch audio channels and cannot be used to answer calls.
Speaker Key Audio Channel Switching Mode	Specifies how the Speaker key switches the audio output channel during call-related states. Speaker Current Channel Toggle: Pressing the Speaker key toggles the speakerphone on or off for the currently active audio channel.Cycle All Channels: Pressing the Speaker key cycles through all available audio output channels.
Enable Use Last Audio Channel	When enabled, the phone remembers the audio channel used during the most recent call and automatically selects it as the default channel for the next call. If the saved channel is no longer available, the phone reverts to its default channel selection logic.

In-call Contact Info Display	Configure the contact information displayed during a call, up to 5 lines to display.The following labels and their combinations can be entered: ? {number} ? {name} ? {title} ? {company} ? {department} ? {email} ? {firstName} ? {lastName}Instance: Line 1:{name} Line 2:{title}-{company} Line 3:{number} / {email}After the configuration, the screen will scroll up and down according to the sequence.
Contact Source Priority	Configure the priority if the ID source displayed on the phone when incming/outgoing calls. Select on ID source and click 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".
Outgoing	
Click-To-Dial Feature	Enables Click-To-Dial feature. If this feature is enabled, user could click the green dial button on left top corner of phone's Web GUI, then choose the account and dial to the target number. The default setting is "Disabled".
Enable Direct IP Call	Enables Direct IP Call feature.
Use Quick IP Call Mode	When set to "Yes", users can dial an IP address under the same LAN/VPN segment by entering the last octet of the IP address.
Predictive Dialing Feature	Configures the predictive dialing feature on the call screen.
Predictive Dialing Source	Predictive dialing feature will sequentially search the number based on the selected sources.
Enable Local Dialing DTMF Tone in Speaker Mode	Configures whether to play local DTMF tone during dialing when using speaker.
Enable Live Keypad	If enabled, phone will automatically dial out and turn on hands-free mode when keypad or softkey is pressed.
Live Keypad Expiration	Configures the expiration time for live keypad. Interval is between 2s and 15s. Default value is 5s.
Enable Auto Redial	Configures to redial automatically at a later time when the dialed number is currently busy.
Auto Redial Times	Configures the total times to redial if "Auto Redial" is enabled.
Auto Redial Interval	Configures the interval between each redial if "Auto Redial" is enabled.
Bypass Dial Plan Through Call History and Directories	Configures hether to check dial plan when dialing from call history and phonebook directories.
Enable Call Completion Service	If enabled, phone will automatically redial the previous failed call when the remote party becomes available.
Incoming	
Enable Incoming Call Popup	If set to "Yes", phone will pop up an incoming call window to notify the call.
Enable Missed Call Notification	If set to "Yes", phone will show a prompt about the missed call information.
Return Code When Refusing Incoming Call	Configures the return code that phone will send to the call when it refuses an incoming call.
Direct IP Call Ringtone	Configure the ringtone for direct IP calls. Default Ring selected is Ring 5.
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.
Enable Call Waiting	Disables the call waiting feature. The default setting is "Yes".
Enable Call Waiting Tone	Enables Call Waiting alert tone when another incoming call is received while a call is in progress.
Ring for Call Waiting	Configures the phone to ring instead of playing call waiting tone when handset or headset is used.
Auto Answer Delay	Configures the delay for automatically answering the incoming call. Valid range is 0 to 10 (seconds)

In Call	
Enable In-call DTMF Display	When set to "No", the DTMF digits entered during a call will not be displayed on LCD. Enabled by Default.
Enable Local In-call DTMF Tone in Speaker Mode	Configures whether to play local DTMF tone during call when using speaker. Enabled by Default
Enable Sending DTMF via Multi-Purpose Keys	Allows multi-function to send DTMF in a call. This option does not affect Dial DTMF. Disabled by Default
Show on Hold Duration	Shows the duration of holding a call on the LCD Enabled by Default.
Enable Auto Unmute	If the option is enabled, automatically unmute the phone when a user unholds the call or establishes a new call. Enabled by Default
Enable Busy Tone on Remote Disconnect	Configures the phone to Play busy tone when call is disconnected remotely. Enabled by Default.
Enable Mute Key In Call	When set to "No", the mute key will not work while on call. Enabled by Default.
Phonebook Matching	
Filter Characters	Filter Characters are used to filter the specific separator characters for Click2Dial or contacts imported from other devices. These specific characters are not part of the actual phone number and needed to filter out. Users could set up multiple characters. For example, if set to "[()-]", when dialing (0571)-8800-8888, the character "()-" will be automatically filtered and dial 057188008888 directly. Initiate calls from other places except dial screen, such as call history and contacts, will automatically filter the characters. Dialing out from Dial screen will not filter any characters.
Enable Phonebook Matching Rules	Enable phonebook matching rules. Multiple options are supported. This function is disabled by default. ? Dial number Indicates the dialing number will be processed. ? Query number Indicates the number for querying contact will be processed. ? Display number Indicates the number displayed ofthe receiver will be processed.
Phonebook Matching Rules	Configure rules for processing numbers. Numbers of 4,7, and 9 digits can be matched from top to bottom. Expression Matching rule/Replacement rule Instance ? 9XXXXXXXX: matches a nine-digit number starting with 9 and is not modified For example: 9XXXXXXXX: 958242234 - >; 958242234 ? (6XXXXXX)/95
Phonebook Matching Rules Test	Enter the number to test the rules. After confirming, please save and apply it.?
Others	
Transfer	
Enable Transfer	Enables Call Transfer feature. Enabled by Default
Hold Call Before Completing Transfer	When set to "No", the phone will not hold the current call or the transfer target for an Attended Transfer.
Default Transfer Mode	Configures the default transfer mode: Blind Transfer, or Attended Transfer. Default is Blind Transfer
Attended Transfer Mode	If set to "Static", attended transfer can only be performed with established calls. If set to "Dynamic", attended transfers can be performed with established calls or be initiated during the transfer process. This option does not affect the user's ability to perform blind transfers.
End Call	
Hang-up Key End Call mode	This feature defines how the Hang-up (End Call) key on the device behaves when terminating a call. Administrators can configure whether a short press or a long press of the key is required to end an active call.Short Press: The call ends immediately when the Hang-up key is briefly pressed.Long Press: The call ends only when the Hang-up key is pressed and held down for a longer duration, reducing the risk of accidental call termination.Set to short press by default
Call Park	

Enable Call Park Softkey	Enable call park service to use call park related softkeys.Enabled by default.
Call Park Softkey Feature Code	Configure the feature access code for parking current call to parking lot or another extension.
Group Call Park Softkey Feature Code	Configure the feature access code for parking current call to the group current user is in.
Call Park Retrieve Softkey Feature Code	Configure the feature access code for retrieving the parked call on accounts or parking lot.
DND	
Enable DND Feature	If disabled, the "Do Not Disturb" switch will not work. Enabled by default. Note: You can Enbale/Disable DND by toggling the DND icon
Return Code Upon DND	Configures the return code that phone will send when it has DND enabled.
Override DND	Configures to override the local DND function. If set to "Off", the local DND function is normal; if set to "Allow All", the local DND function is invalid; if set to "Allow Only Contacts", when the local DND function is enabled, only local contacts and the configured override numbers can call in ; If set to "Allow Override Numbers", when the local DND is turned on, only the configured coverage numbers can call in. The default setting is "Off".
Override DND Numbers	Configure the number to override the local DND function.
Conference	
Enable Conference	Enables the Conference feature. Disabled by default
Hold Call before Adding Conferee	Configures whether to put the current call on hold while adding new members to a conference. If set to "Yes", the current call will be put on hold when the host presses conference or add key to invite new members. When the invited member answers the call and agrees to attend the conference, the host needs to manually resume the conference with the new member added. If set to "No", the current call will not be put on hold and the invited member will join the meeting automatically after answering the call. Disabled by Default
Voicemail	
Enable Voicemail Popup	If enabled, the phone will show a pop-up upon receiving a voicemail. Disabled by default.
IM	
IM Designated Account	Set the default local account for sending instant messages. Users can select a specific local account or choose "Auto", in which case the device follows the "Preferred Account" configured under Phone Settings->Call Settings ->General. The default setting is "Auto".
Enable IM Popup	If enabled, the phone will show a pop up upon receiving an IM.
Instant Message Popup timeout During Call	Configures the timeout period for SMS display during calls (in seconds).
Ring on Receiving IM	Configures whether to ring when the phone receives an IM.
Record	
Enable the Indicator in Recording	When the call is recorded, the recording indicator is displayed on the LCD.
Ringtone	

Call Progress TonesSystem Ring ToneDial ToneSecond Dial Tone Message WaitingRing Back ToneCall-Waiting ToneCall Waiting Tone GainAuto-Answer Tone GainBusy ToneReorder Tone	Configures ring or tone frequencies based on parameters from local telecom. The default value is North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. To set a continuous ring, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported. Call Waiting tone gain can be set to either: Low, Medium, or High, it is set to Low by Default Auto-Answer Tone Gain can be set to either: Low, Medium, or High, Set to Medium by Default
Provision	
Total Number of Custom Ringtone Update	When the call is recorded, the recording indicator is displayed on the LCD.
Video Settings	
Video Display Mode	Configures the video display mode to "Original proportion", "Cut proportionally" or "Add black margin proportionally". 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 phone, 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, but if there are empty spaces, the phone will add black edge to it.
Enable Frame Skipping in Video Decoder	When packet loss occurs, the video decoding will discard the "P" frame of the video and start decoding from the next "I" frame. When the network speed is low, enabling this option would reduce the blurred screen display.
PTT/Paging	
PTT/Group Paging	
General Settings	
PTT/Group Paging Address	Set the PTT/Group Paging address.
Emergency Channel Volume	Set default volume when emergency channel is used.
PTT Config	
PTT	Configures to enable or disable PTT.
Default Channel	Set default channel for PTT. When presing and holding the PTT button, PTT will be initiated using the default channel.
Priority Channel	Set priority channel for PTT. PTT received on priority channel will take precedence over active PTT on normal channel.
Emergency Channel	Set 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	Configures whether to accept PTT while device is in active call. If set to "No", device will ignore PTT while in active call. If set to "Yes", while in active PTT talk, 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. Disabled by default
Caller ID	Set Caller ID displayed on the call interface during a PTT call.
PTime (ms)	Set payload size for PTT.
Audio Codec	Set audio codec for PTT.
Channel	Configures PTT channel. Configures options for the channel such as transport, accept, join PTT and its label. Only available and joined channel will be displayed in PTT channel list. If users need send or receive PTT, "Transport" and "Accept" must be enabled for this channel.

Group Config	
Group Paging	Configures to enable or disable group paging.
Default Group	Set default paging group. When pressing and holding the PTT button, paging will be initiated using the default group.
Priority Group	Configures priority paging group. Paging received on priority group will take precedence over active paging on normal group.
Emergency Group	Set emergency group for paging. Emergency group has the highest priority. Paging using emergency group will take precedence over paging on priority or normal group.
Accept While Busy	Configures whether to accept paging while device is in active call. If set to "No", device will ignore paging while in active call. If set to "Yes", while in active paging call, the device will accept other paging calls if it has the same priority. If device is in an active SIP call, device will accept paging and hang up the SIP call.
Caller ID	Set Caller ID displayed on the call interface during paging. Default is "channel(*)"
PTime (ms)	Set payload size for paging.
Audio Codec	Set audio codec for paging.
Group	Configures paging group. Users can configure whether to use the group to accept and join group, and its label. Only available and joined group will be displayed in paging group list. If users need receive paging, "Subscribe" must be enabled for this group.
Multicast Paging	
Multicast Paging Function	Enable or disable multicast paging.
Allowed in DND Mode	Configures to allow incoming multicast paging when DND Mode is enabled.
Paging Barge	During an active call if incoming multicast page has 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. Enabled by Default.
Multicast Paging Codec	The codec for sending multicast pages.
Multicast Call Timeout(s)	Set multicast based call timeout. When the sender's multicast call exceeds the set time, it will automatically hang up and set to 0 without timeout.multicast.call.ti
Multicast Tone	If enabled, there will be a prompt sound at the beginning and end of the receiver's multicast intercom.
Multicast Listening	Configure the listening address and channel name of multicast paging. You can configure up to 10 Listening Addresses
Settings	
Allow PTT/Paging When Lock Screen Status	If set to "Yes", the device can initiate an PTT/Paging in the lock screen status.
IGMP Keep-alive Interval (s)	Specifies how often the phone reports IGMP when the PTT/Paging function is turned on. IGMP reporter helps to keep PTT/Paging receivable in a dormant state. The interval may have some effect on standby time. The range is 0 or 20-120, where 0 indicates no survival package will be sent.

Network Settings Page Definitions

Network Settings -> Wi-Fi Settings
General Settings

Wi-Fi Function	Enables / Disables the Wi-Fi on the phone. Three options are available:Enable: Enables Wi-Fi to connect to Wi-Fi network.Disable: Disables Wi-Fi. User has ability to enable Wi-Fi from LCD Menu.Disable & Hide Menu from LCD: Disables Wi-Fi and hides "Wi-Fi Settings" menu from phone LCD.
Wi-Fi Band	Set the type of Wi-Fi Band whether its 2G or 5G or 5G&2G.
Country Code	Configures Wi-Fi country code.
ESSID	This parameter sets the ESSID for the Wireless network.Press "Scan" to scan for the available wireless network.Click on "Connect" and enter the authentication credentials of the Wi-Fi network to connect to.Users can connect to hidden networks by pressing on "Add Network" and configure:ESSID: Configure the hidden ESSID name.Security Mode: Select the Security Mode of the configured ESSID from the following options:None: Disables wireless security, allowing open access without encryption.Auto: Automatically selects the most suitable security mode based on device capabilities.WEP: An outdated and insecure security mode, retained only for legacy device support.WPA/WPA2-PSK: Uses a shared password and is commonly deployed in home and small office environments.WPA-802.1X: Provides enterprise-level authentication through a RADIUS server using individual user credentials.WPA3-SAE: A modern and more secure personal mode that replaces WPA2-PSK. WPA3-802.1X: Offers enhanced enterprise security with WPA3 encryption and RADIUS-based authentication.WPA3-192: A high-security enterprise mode featuring 192-bit encryption for sensitive environments.Enhanced Open: Provides encryption without requiring a password, typically used in public networks via OWE.Network Priority: Configure the current network priority within the range of 0-10, with 0 indicating the lowest priority and 10 indicating the highest priority. Default value is 0.Prefer Account: Sets a priority account for this Wi-Fi network; when the device connects to it, the phone automatically switches to that account as the active priority. EAP Method: When the Security Mode is WPA-802.1x, WPA3-802.1x or WPA3-192, select the EAP authentication method from the following options: EAP-PWD, EAP-TLS, EAP-PEAP, EAP-TTLS and EAP-MSCHAPv2. For WPA3-192 security mode, only EAP-TLS is supported.CA Certificate Type: When the EAP Method is EAP-TLS, EAP-PEAP or EAP-TTLS, select the CA Certificate Type from the following options:Skip Verification: No certificate authority verification is performed. System Certificates: Validation is performed using the device's system certificates. The list of trusted certificates is defined under System Settings -> Security Settings -> Trusted CA Certificates -> Load CA Certificates. Trust on First Use: The server certificate is accepted and trusted by the user during the initial connection.Uploaded Certificate: A certificate manually uploaded by the user is used for validation.Domain Name Validation Mode: When the CA Certificate Type is System Certificates or Uploaded Certificates, configure the server's Domain Name Validation Mode, both Suffix Matching and Exact Matching are supported.Domain Name: When the CA Certificate Type is System Certificates or Uploaded Certificates, configure the Domain Name. CA Certificate: When the CA Certificate Type is Uploaded Certificate, optionally upload a CA certificate to verify that the ESSID is trusted. Supports PEM format.Client Certificate: When the EAP Method is EAP-TLS, upload the client certificates and private keys. Supports .p12 and .pfx formats.Client Certificate Password: When the EAP Method is EAP-TLS, cnfigure the private key password. If the private key is encrypted, this is required; otherwise, leave it blank.Phase 2 Authentication: When the EAP Method is EAP-PEAP or EAP-TTLS, configure Phase 2 Identity Authentication Method.EAP-PEAP options: MSCHAPv2, GTC, TLS (displays Client Certificate and Client Certificate Password), None.EAP-TTLS options: MSCHAPv2, MSCHAP, PAP, GTC, None.Anonymous Identity: When the EAP Method is EAP-PEAP or EAP-TTLS, configure anynonmous identity in Phase 1. Supports up to 64 ASCII characters.Identity: Configure the identity. Supports up to 64 ASCII characters.Password: Configure the password. Supports up to 64 ASCII characters. Not displayed if the EAP Method is EAP-TLS or if EAP-PEAP with Phase 2 Authentication is set to TLS.Advanced: Configure IPv4 and IPv6 modes.
Advanced 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.
Wi-Fi Signal Warning	When the WiFi signal strength is lower than the threshold set by this level, the device will warning.
Roaming Signal Threshold	Sets the WiFi signal threshold. When the WiFi signal strength of the device drops below this value, the device will scan for a hotspot above the threshold value and connect to it.
Poor Signal Scan Interval (s)	Sets the time interval for signal scanning when the WiFi signal strength is lower than the signal threshold and there is no hotspot which is higher than the current signal strength.
VoWLAN Target Delay	Selects Low, Medium, or High based on network conditions.
Wi-Fi QR Code Sharing	If enabled, when the Wi-Fi password is selected on the LCD, it will be displayed in plain text and the Wi-Fi QR code will be displayed in the connected Wi-Fi details to share Wi-Fi information.
Wi-Fi Power-Saving Mode	Configure Wi Fi power-saving mode. The options are:DisabledGeneric (PSM)U-APSD
Wi-Fi Roaming Mode	Configures the roaming behavior of the device to optimize Wi-Fi performance and connection stability in different environments. The available options are:Default Mode: This is the default roaming behavior, meaning that the phone will switch to another AP only when the current signal becomes too weak (This is suitable for stable environments where roaming isn't required often)Boost Mode: Enables aggressive roaming, where the phone proactively scans for better APs and switches when a stronger signal is detected (This mode is recommended in enterprise networks where users move frequently between APs and seamless roaming is needed.The default setting for this parameter is "Default Mode".
Enable Roaming Prompt	Configures whether the phone displays a visual text prompt and plays an audible alert tone when Wi-Fi roaming occurs. This setting is disabled by default.
Network Settings -> Bluetooth Settings	
Bluetooth	Enable/Disables Bluetooth
Device Name	Set the name of the local Bluetooth device
Bluetooth Device	Display a list of Bluetooth devices scanned in the surrounding environment.
Network Settings -> OpenVPN(R) Settings	
OpenVPN(R) Enable	Enables/Disables OpenVPN(R) feature. Default is "No".
Import OpenVPN(R) Configuration	Imports the configuration file from the current computer. After importing, the local configuration will be overwritten and OpenVPN(R) function is automatically enabled.
OpenVPN(R) Server Address	Specify the IP address or FQDN for the OpenVPN(R) Server.
OpenVPN(R) Port	Specify the listening port of the OpenVPN(R) server. The valid range is 1 - 65535. The default value is "1194".
OpenVPN(R) Server Secondary Address	Configure OpenVPN(R) server secondary address. This will be used when the primary OpenVPN(R) server fails.
OpenVPN(R) Secondary Port	Specify the listening port of the secondary OpenVPN(R) server. The valid range is 1 - 65535. The default value is "1194".
Randomly Select Server	If enabled, a server will be chosen randomly to handle OpenVPN(R) requests. If disabled, requests will be sent to servers in the order of the configuration.Default setting is "Disabled".
OpenVPN(R) Transport	Specify the Transport Type of OpenVPN(R) whether UDP, TCP, UDP IPV4 Only, TCP IPV4 Only, UDP IPV6 Only, TCP IPV6 OnlyThe default value is "UDP".
OpenVPN(R) CA	Click on "Upload" to upload the Certification Authority of OpenVPN(R). For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.

OpenVPN(R) Certificate	Click on "Upload" to upload OpenVPN(R) certificate. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN(R) Client Key	Click on "Upload" to upload OpenVPN(R) Key. For a new upload, users could click on "Delete" to erase the last certificate, and then upload a new one.
OpenVPN(R) Client Key Password	Allows user to set password for client.key file
OpenVPN(R) TLS Key	Uploads the OpenVPN(R) TLS .key file
OpenVPN(R) TLS Key Type	Selects the encryption type of the OpenVPN(R) TLS key. it can be set to : TLS-Auth, TLS-Crypt, TLS-Crypt V2
OpenVPN(R) Cipher Method	Specifies the encryption algorithms used by the OpenVPN connection. Multiple algorithms can be configured by separating them with colons (:) or by selecting them from the drop-down menu. When multiple algorithms are configured, the algorithm listed highest has the highest priority.Format: AES-128:AES-256:Triple-DES:AES-128-GCM:AES-256-GCM:CHACHA20-POLY1305BlowfishAES-128AES-256Triple-DESAES-128-GCMAES-256-GCMCHACHA20-POLY1305The preffered setting by default is "Blowfish".
OpenVPN(R) Username	Configures the optional username for authentication if the OpenVPN server supports it.
OpenVPN(R) Password	Configures the optional password for authentication if the OpenVPN server supports it.
OpenVPN(R) Comp-lzo	Configures enable/disable the LZO compression. When the LZO Compression is enabled on the OpenVPN server, you must turn on it at the same time. Otherwise, the network will be abnormal. Default value is YES.
Additional Options	Additional options to be appended to the OpenVPN(R) config file, separated by semicolons. For example, comp-lzo no;auth SHA256Note: Please use this option with caution. Make sure that the options are recognizable by OpenVPN(R) and do not unnecessarily override the other configurations above.
Network Settings -> WireGuard(R) Settings	
Enable WireGuard(R)	Enables or disables the WireGuard VPN service on the device. Enabled: The device establishes a WireGuard tunnel using the configured client and peer parameters. Disabled: WireGuard is inactive and all traffic follows the normal network path. Disabled by default.
Import WireGuard(R) Configuration	Allows importing a standard WireGuard .conf configuration file. When a configuration file is imported, the client and peer parameters are automatically populated based on the file contents. Recommended for service-provider or IT-managed deployments to reduce manual configuration errors. Note: After a .conf file is imported, the older configuration will be overwritten
Client Settings	
WireGuard(R) Client Private Key	Specifies the private key used by the WP8x6 device for WireGuard authentication. This key uniquely identifies the device in the VPN tunnel and must remain confidential. Clicking Create generates automatically a private key and its corresponding public key. Note: Only supports Base64-encoded 32-byte keys.
WireGuard(R) Client Public Key	Generates a new private key Displays the public key derived from the client private key..
WireGuard(R) Client IP Address	Defines the virtual IP address assigned to the WP8x6 within the WireGuard tunnel. Example: 10.10.10.2/32 This address is used for routing traffic inside the VPN.
WireGuard(R) Client DNS Address	Configure the DNS address used by the WireGuard(R) client.
WireGuard(R) Client Listening Port	Configure the port that the WireGuard(R) client listens on.

WireGuard(R) Client Maximum Transmission Unit	Configures WireGuard(R)'s maximum transmission unit for client data transmission, in bytes. When set to 0, the MTU value is calculated based on the value configured under:Network Settings -> Advanced Settings -> Advanced Settings -> Maximum Transmission Unit (MTU)The default setting is "0".
Peer Settings	
WireGuard(R) Peer Public Key	Specifies the public key of the WireGuard peer (VPN server). This key is required to authenticate and encrypt communication with the remote peer.
WireGuard(R) Peer Preshared Key	Configure the WireGuard(R) node's pre-shared key (PSK), which is mixed into the Curve25519 key exchange, providing an additional layer of symmetric encryption to enhance confidentiality.
WireGuard(R) Peer Address	Configure the WireGuard(R) peer address, required, can be an IP address or domain name, as well as the port the peer listens on, Format: IP:Port or Hostname:Port Example: 172.0.113.10:51820
WireGuard(R) Allowed IPs	Configure the IP addresses and subnet mask lengths that the WireGuard(R) client can access through the VPN server peer, multiple configurations are allowed, not required (no value means 0.0.0.0/0, no restrictions), e.g., 10.0.0.0/24,10.2.2.2/32. If the subnet mask length is not written, it is considered /32 by default. Note: Up to 10 subnets can be configured.
WireGuard(R) Connection Keep-Alive Interval (seconds)	Configure the client to send a keep-alive message to the server peer every certain number of seconds, default is 25, range is 1-65535.
Network Settings -> Advanced Settings	
Advanced Settings	
Advanced Network Settings	
DNS Refresh Timer (m)	Configures the refresh time (in minutes) for DNS query. If set to "0", the phone will use the DNS query TTL from DNS server response. the Default value is "0"
DNS Failure Cache Duration (m)	Configures the duration (in minutes) of the previous DNS cache when the DNS query fails. If set to "0", the feature will be disabled. Note: Only valid for SIP registration. The Default value is "0"
Layer 3 QoS for SIP	Configures the Layer 3 QoS parameter for SIP. This value is used for IP Precedence, Diff-Serv or MPLS. Default value is 26
Layer 3 QoS for RTP	Configures the Layer 3 QoS parameter for RTP. This value is used for IP Precedence, Diff-Serv or MPLS. Default value is 46
Maximum Transmission Unit (MTU)	Configures the MTU in bytes. Default value is 1500
Release DHCP On Reboot	Configures whether the phone will release DHCP lease on reboot.
Proxy	
HTTP Proxy	Specifies the HTTP proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
HTTPS Proxy	Specifies the HTTPS proxy URL for the phone to send packets to. The proxy server will act as an intermediary to route the packets to the destination.
Bypass Proxy for	Configures the destination IP address where no proxy server is needed. The phone will not use a proxy server when sending packets to the specified destination IP address.
Remote Control	
Action URI Support	Configures whether to enable phone to handle Action URI request.Default is "Enabled".
Remote Control Popup Window Support	Configures whether to enable phone to pop up Allow Remote Control window. Enabled by Default
Action URI Allowed IP List	List of allowed IP addresses from which the phone receives the Action URI

CSTA Control	Configures whether to enable the CSTA (Computer Supported Telecommunications Applications) Control feature.
Static DNS Cache	
NAPTR	NAPTR (Naming Authority Pointer) records are used to specify rules for rewriting one type of domain name to another, typically used for handling Uniform Resource Identifiers (URIs) within the domain, when you configure NAPTR in the static DNS cache, you are specifying custom rules for how specific URIs or domain names should be resolved, the options to configure are : NAPTR DNS Cache Name: The domain name to which this resource record refers. NAPTR DNS Cache Time Interval (s): The time interval that the resource record may be cached before the source of the information should again be consulted, Default value is 300 seconds. NAPTR DNS Cache Order: A 16-bit unsigned integer specifying the order in which the NAPTR records must be processed to ensure the correct ordering of rules. NAPTR DNS Cache Preference: A 16-bit unsigned integer that specifies the order in which NAPTR records with equal "order" values should be processed, low numbers being processed before high numbers. NAPTR DNS Cache Replacement: The next name to query for SRV records. NAPTR DNS Cache Service: Specifies the service(s) available down this SRV record path.
SRV	SRV records are DNS records used to identify servers that provide specific services, such as email, SIP (Session Initiation Protocol) servers, or other services, Configuring SRV in the static DNS cache allows you to specify which servers should be used for particular services, helping ensure that your IP phone connects to the correct servers for specific functions, the available options to configure are: SRV DNS Cache Name: The domain name string with SRV prefix. SRV DNS Cache Time Interval (s): Specifies the time interval that the resource record may be cached before the source of the information should again be consulted. The default value is 300 seconds. SRV DNS Cache Priority: Set the priority of this target host. SRV DNS Cache Weight: Set server selection mechanism. SRV DNS Cache Target: The domain name of the target host. SRV DNS Cache Port: Set the port on the target host of this service.
A	A records are used to map a domain name to an IPv4 address. They are the most common type of DNS record and are used to resolve domain names to IP addresses, Configuring A records in the static DNS cache allows you to manually specify the IP addresses associated with specific domain names, ensuring that your IP phone always connects to the intended destination, the options to configure are: A DNS Cache Name: Set Hostname. A DNS Cache Time Interval: A DNS Cache Time Interval, Default is 300 seconds. A DNS Cache IP Address: A DNS Cache IP Address.

Programmable keys Page Definitions

Programmable Keys -> Idle Screen Softkeys	
Custom Idle Screen Softkey Layout	Enables/disables softkey layout.Default is disabled
Custom Softkey	Press on Add Custom Softkey radio button to add/configure up to 3 custom softkeys. Supported key modes are speed dial, speed dial via active account, and voicemail.Note: The softkey icons have been updated and now have the option to be customized on preference based on the key mode , either speed Dial , speed dial via active, DialDTMF, or voicemail.
Custom Softkey Layout	The softkeys listed under:"Left Softkey - Options" and "Right Softkey - Options" tabs for WP816."Left Softkey - Options", "Middle Softkey - Option" and "Right Softkey - Options" for WP826/WP836 will be displayed on the phone's idle screen, different softkeys are available to be configured. Select the softkey from "Available" list to enable it.
Programmable Keys -> Call screen softkeys	
Custom Call Screen Softkey Layout	Enables/disables custom softkey layout Default is disabled
Custom Softkey	Press on Add Custom Softkey radio button to add/configure up to custom softkeys Supported key modes are speed dial, speed dial via active account, DialDTMF, and voicemail.

Custom Softkey Layout	The softkeys listed under: "Left Softkey - Options" and "Right Softkey - Options" tabs for WP816."Left Softkey - Options", "Middle Softkey - Option" and "Right Softkey - Options" for WP826/WP836 will be displayed on the phone's call screen, depdening on the call status, different softkeys are available to be configured. Select the softkey from "Available" list to enable it.
Number keys	Defines the action that happens after the long press of a number key from 1 to 9 , each key can be configured to do one of the programmable functions:Speed Dial Speed Dial Via Active Account Dial DTMF VoicemailMake sure to provide in addition to the Long Press Function, the account, Value and label for each Number key.
Navigate keys	Defines the action that programmable functions that can be configured for the navigation keys (UP, DOWN, LEFT, RIGHT), two modes are supported: Short Press Function: This will be the action performed when pressing shortly the navigation key Long Press Function: This will be the action performed when long pressing the navigation key , a vibration will be generated to indicate that the long press function is the one activated. The functions that can be defined are : Broadsoft Call Log ContactsMissed Call History Dialed Call History Recieved Call History Account Settings INFO SettingsNext Account Instant Messages Missed notification Remote Phonebook1 Remote Phonebook2 Remote Phonebook3 Remote Phonebook4 Remote Phonebook5 Remote Phonebook Online Contacts Broadsoft Directory Local Phonebook LDAP Search Bluetooth
Multi-Purpose Key	Defines the programmable action of the Multi-function Key, the following parameters needs to be defined: Short Press Function: Defines the programmable action that will be triggered whenmultifunction key is pressed Account: Selects the account on which the multi-function key will take effect Value: Defines the target extension Label: Defines a label for the programmable action
Side Key	The side key is responsible for triggereing functionalities such as the push-to-talk feature, group paging, multicast paging and alarm. Notes:When configured as "PTT/Paging": Short press to open the channel selection page, long press to trigger PTT/Paging When Configured as "Alarm": Short press to enter the alarm function configuration page, long press to initiate active alarm. When configured as "None": the side key button will be disabled The default function for the side key is "PTT/Paging".
Programmable Keys -> Advanced settings	
Allow Programmable Key Configuration via LCD	Enables/disables Programmable Key configuration via LCD by pressing and holding programmable keys(exclude softkey), or entering through the Menu - Settings - Basic Settings - Key Customization path.
Enable Transfer via Non-Transfer Programmable Keys	If enabled, if the programmable key select the dialing out function, it will be used as a transfer during the call.
Transfer Mode via Custom Softkey and Multi-Purpose Keys	Restrict the transfer mode when using custom softkeys and Multi-Purpose Keys as transfers to : Blind transfer, attended transfer, New Call, All for Selection

System Settings Page Definitions

System Settings -> Time and Language	
Date and Time	
NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. The default setting is "pool.ntp.org".
Secondary NTP Server	Defines the URL or IP address of the NTP server. The phone may obtain the date and time from the server. Allow user to configure 2 NTP server domain names. WP phone will loop through all the IP addresses resolved from them.
Enable Authenticated NTP	Configures whether to enable NTP authentication. If enabled, a cryptographic signature appended to each network packet. If the key is incorrectly configured, the phone will refuse to use the time provided by the NTP server.

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.
Authenticated NTP Key ID	Configures the key ID for authenticated NTP. Default value is 1
Authenticated NTP Key	Uploads the key file for authenticated NTP. Note: Only support MD5 key type.
Allow DHCP Option 42 Override NTP Server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is "Yes".
Time Zone	Configures the date/time used on the phone according to the specified time zone. The default setting is "Auto". Note: On firmware release 1.0.3.98, Mexico city Time zone has been added
Allow DHCP Option 2 to Override Time Zone Setting	Allows device to get provisioned for Time Zone from DHCP Option 2 in the local server. The default setting is enabled.
Self-Defined Time Zone	This parameter allows the users to define their own time zone, when "Time Zone" parameter is set to "Self-Defined Time Zone".The syntax is: std offset dst [offset], start [/time], end [/time]Default is set to: MTZ+6MDT+5,M4.1.0,M11.1.0MTZ+6MDT+5This 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,M11.1.0The 1st number indicates Month: 1,2,3.., 12 (for Jan, Feb, .., Dec)The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday...)The 3rd number indicates weekday: 0,1,2,..,6(for Sun, Mon, Tues, ... ,Sat)Therefore, this example is the DST which starts from the First Sunday of April to the 1st Sunday of November.
Date Display Format	Configures the date display format on the LCD. The following formats are supported.yyyy-mm-dd: 2019-03-02mm-dd-yyyy: 03-02-2019dd-mm-yyyy: 02-03-2019dddd, MMMM dd: Saturday, March 02The default setting is yyyy-mm-dd.
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.
System Settings -> Input Method	
Input Method for Contacts	To set the input method for contacts, default value: 123 input method.language.inputMethod.contacts Rule: include:"123","abc","ABC","Ab2","Q9"Default: Q9
Input Method for LDAP	To set the LDAP input method, default value: 123 input method.language.inputMethod.ldap Rule: include:"123","abc","ABC","Ab2","Q9"Default: Q9
System Settings -> Security Settings	
SSH Access	
Enable SSH	Disables SSH access.The default setting is "Yes"
SSH Port	Configures the port for SSH access.Default is 22.
SSH Public Key	Enable the device to use public key authentication as an alternative option to password authentication.
LCD Access	

Configuration via Keypad Menu	Configures access control for keypad Menu settings.Unrestricted: all options on LCD menu can be accessed.Basic settings only: only options for basic setting can be displayed on LCD menu.Constraint Mode: accessing options other than basic settings will require permission. Warning: If the admin password is lost while constraint mode is enabled, your device may become permanently unusable. Remember to be careful when using constraint mode to avoid irreversible damage.Locked Mode: MENU is disabled.Custom Restricted Mode: Customize which settings pages need to be restricted.
Custom Constraint Page	When Configuration via Keypad Menu is set to Custom Constraint Mode, use this option to customize the constraint page displayed on the phone's keypad menu. You can specify which configuration options are available to users and control the settings that can be accessed or modified through the keypad menu. This allows administrators to restrict user access to specific configuration parameters while providing only the required options. Note: When Configuration via Keypad Menu is set to Custom Restricted Mode, the Send Anonymous and Anonymous Call Rejection options can be hidden from the phone's LCD menu.
Factory Reset Security Level	Configure the password inquiry for factory reset.Default: The password is needed when configuration via keypad menu is no UnrestrictedAlways Require Password: The password is needed no matter what configuration via keypad menu mode is.No Password Required: No password is needed no matter what configuration via keypad menu mode is.
Wi-Fi Settings Security Level	Configure the password inquiry for Wi-Fi settings.Default: The password is needed when configuration via keypad menu is no UnrestrictedAlways Require Password: The password is needed no matter what configuration via keypad menu mode is.No Password Required: No password is needed no matter what configuration via keypad menu mode is.
Web Access	
HTTP Web Port	Configures the HTTP port under the HTTP web access mode. The valid range is 80 - 65535. The default value is "80".
HTTPS Web Port	Configures the HTTPS port under the HTTPS web access mode. The valid range is 443 - 65535. The default setting is "443".
Web Access Mode	Sets the protocol for web interface.HTTPSHTTPDisabledBoth HTTP and HTTPS The default setting is "HTTP".
Web Access Control	Web access control by using Blocklist or Allowlist on incoming IP addresses.
Web Access Control List	Only allow the IP address list as a allowlist or restrict the IP address list as a blocklist to access the Web.
Web Session Timeout	Configures timer to logout web session during idle. The valid range is 2-60 min. The default value is 10 min
Enable User Web Access	Administrator can disable or enable user web access.The default setting is "Disabled".
Validate Server Certificates	After enabling this feature, phone will validate the server's certificate. If the server that our phone tries to register on is not on our list, it will not allow server to access the phone.
Web/Restrict mode Lockout Duration	Specifies the time in minutes that the web or LCD login interface will be locked out to user after five login failures. This lockout time is used for web login, and LCD restrict mode admin login. Range is 0-60 minutes.The default setting is "5".
Web Access Attempt Limit	Configure attempt limit before lockout.Default is 5. Range is 1-10.
User Info Management	
Test Password Strength	Checks password strength to ensure better security. Password needs at least 9 characters and 3 of the following options: numerics (0-9)capital letters (A-Z)lower case (a-z)special characters (' ./'`@*-=,|&?!%()~_#')Disabled by Default.
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. The admin password is case sensitive with a maximum length of 25 characters.
Confirm Password	Enter the new Admin password again to confirm.
Client Certificate	
TLS Version	
Minimum TLS Version	Configures the minimum TLS version supported by the phone. The minimum TLS version must be less than or equal to the maximum TLS version. The TLS version can be TLS 1.0, TLS 1.1, TLS 1.2, or TLS 1.3 The Default value is set to "TLS 1.0"
Maximum TLS Version	Configures the maximum TLS version supported by the phone. The maximum TLS version must be greater than or equal to the minimum TLS version. The TLS version can be TLS 1.0, TLS 1.1, TLS 1.2, Unlimited, The Default value is "Unlimited"
Global	
Enable LEGACY_SERVER_CONNECT	If enabled, the parameter SSL_OP_LEGACY_SERVER_CONNECT will be enabled, this option is valid for TLS version 1.2 and below. Option disabled by default.
Enable/Disable Weak Cipher Suites	This feature defines the function for weak cipher suites. If set to "Enable Weak TLS Cipher Suites", allow users to encrypt data by weak TLS cipher suites. If set to "Disable Symmetric Encryption RC4/DES/3DES", allow users to disable weak cipher DES/3DES and RC4.
SIP TLS Certificate	
SIP TLS Certificate	SSL Certificate used for SIP Transport in TLS/TCP.
SIP TLS Private Key	SSL Private key used for SIP Transport in TLS/TCP.
SIP TLS Private Key Password	SSL Private key password used for SIP Transport in TLS/TCP.
DTLS Version	
Minimum DTLS version	Configures the minimum DTLS (Datagram Transport Layer Security) version supported by the phone. The minimum DTLS version must be less than or equal to the maximum DTLS version. The available option are: DTLS 1.0 , DTLS1.2 Default value is DTLS1.0
Maximum DTLS Version	Configures the maximum DTLS version supported by the phone. The maximum DTLS version must be greater than or equal to the minimum DTLS version. The available option are: DTLS 1.0 , DTLS1.2, Unlimited Default value is Unlimited
Custom Certificate	
Custom Certificate	The uploaded custom certificate will be used for SSL/TLS communication instead of the phone default certificate. Note: An invalid Custom certificate will display a warning message
Individual Certificate	
CA Signature Algorithm	This feature allows users to configure CA signature algorithm. Please note that this configuration must be consistent with the root certificate deployed on your server. Otherwise, the TLS communication might fail.
Trusted CA Certificate	
Trusted CA Certificates (1 - 6)	Allows to upload and delete the CA Certificate file to phone.Note: Users can either upload the file directly from web or they can choose to provision it from their cfg.xml file.

Load CA Certificates	Phone will verify the server certificate based on the built-in, custom or both trusted certificates list.The default setting is "Default Certificates".
SCEP	
Basic Settings	
Enable SCEP	Enables or disables the SCEP (Simple Certificate Enrollment Protocol) service on the device. Disabled by default.
SCEP Server URL	Fill in the SCEP server URL(CA URL or RA URL), the protocol header must be included in the URL. Only 'HTTP' URL is supported. Example: http://ca.example.com/scep This server issues certificates to the device after successful authentication.
CA FingerPrint Infomation	Defines the fingerprint of the CA certificate. This ensures the device only trusts the specified Certificate Authority and prevents man-in-the-middle attacks during enrollment.
Challenge Password	Enter the Challenge Password to be sent along with the CSR while applying for a certificate. This value is provided by the CA administrator and is used for initial authentication.
Local Configuration	
Local Public and Private Key Length	Specifies the cryptographic key length used when generating the local key pair. The available options are: 1024 bit, 2048 bit, 3072 bit, 4096 bit Default value is set to 2048 bit.
The Name of Certificate Applicant	Fill in the name of the certificate applicant, which is a required field.
The Country of Certificate Applicant Located	Select the country of the certificate applicant.
The State of Certificate Applicant Located	Specifies the state or province (ST) of the certificate subject.
The Locality of Certificate Applicant Located	Specifies the city or locality (L) of the certificate subject.
The Organization of Certificate Applicant Located	Specifies the organization name (O) associated with the certificate subject.
The organization unit of Certificate Applicant	Specifies the organizational unit (OU) associated with the certificate subject.
HTTP Authentication	
User ID	Defines the HTTP authentication username used to access the SCEP server.
Password	Defines the HTTP authentication password used to access the SCEP server.
Certificates and Updates	
CA Certificate	Displays the currently installed CA certificate obtained via SCEP.
Enable Trust CA Certificate	When enabled, the organizational CA certificate obtained via the SCEP server will be automatically added as a custom certificate into the device's trusted CA list under System Settings -> Security Settings -> Trusted CA Certificates.
Client Certificate	Displays the client certificate issued to the WP8x6 device.
Client Certificate Alternative Name	Specifies Subject Alternative Name (SAN) entries included in the client certificate. Example: $MAC.local Multiple alternative names can be added as required. Up to 5 enteries.
Update Interval before Certificate Expiration	Defines the number of days before certificate expiration when the device automatically attempts renewal. Example: 20 days
Scope of Use	Defines which services use the SCEP-issued certificate. Supported scopes: SSL/TLS communicationOpenVPNTR069SIPOnly the selected services will use the enrolled certificate.
Screen Lock	
Enable Screen Lock Function	If set to "Yes", the keypad can be locked by pressing and holding the STAR * key for about 4 seconds. And will also allow automatic locking.

Lock Screen in Call	Configure the screen lock behavior during active calls. The options are:Disabled: Screen remains unlocked during calls.Manual: User must press and hold the lock key (#) to lock the screen.Auto: Screen automatically locks after 30 seconds of inactivity during a call. The user can also manually lock the screen by pressing and holding the lock key (#).The default settings is "Disabled. Note: To unlock the screen, press the "Unlock" softkey and then press #.
Locked Screen Display	Configure label or call forward information displayed on the locked screen.
Function to Lock when in call	Customize the locking function during phone calls without unlocking.
Lock Screen Password	Password to Lock/Unlock
Emergency	Defines emergency call numbers. If multiple emergency call numbers are entered, they should be separated by ','.
System Settings -> Preferences	
Audio Settings	
Ring	
Incoming Call Ring Mode	Configures the incoming call ring mode: enabling ringing, enabling ringing without fade-in, or disabling the ring entirely.Enabled by default.
Notification Ring	Configures ringing or muting for notification. Disabled by default
Message Ringtone	Configure Short Message and Voicemail ringtone music.
Volume	
Speaker Volume	Configures speaker volume, range 1-8
Receiver Volume	Configures receiver volume, range 1-8
Ringtone and Notification Volume	Configures ringtone and notification volume, range 0-10
Lock Volume	Lock volume adjustment when the option is enabled
Call Tone Volume	Call Tone Volume used for configure the tones level in dB. Value range from -15 to 15.
Tone	
Enable Charging Tone	If set to "Yes" , it will sound a tone once you start charging. Enabled by default
Enable Warning Tone	Configures whether to enable the warning tone of the phone.. If disabled, the network disconnected, the voltage is too high or too low, and voicemail will have no tone Enabled by default.
Headset	
Always Ring Speaker	Configures enabling/disabling the speaker to ring when the headset is used on "Toggle Headset/Speaker" mode. it can be set to "No", "Yes, Both" or "Yes, Speaker Only", The Default Value is "Yes, Both"
Headset TX Gain (dB)	Configures the transmission gain of the headset.
Headset RX Gain (dB)	Configures the receiving gain of the headset.
Enable Headset Noise Shield	When enabled, the remote party will not hear the environmental noise during a call using the headset. Choose according to the TX loudness of the earphone. When the TX loudness of the headset is loud, please select the "Loud Headset", and when the TX loudness of the headset is soft, please select the "Thin Headset". This options is disabled by default.
Headset Type	Select the headset type. When PTT intercom dedicated headset is selected, press and hold the headset's PTT button to initiate a PTT intercom call, and release the button to stop transmitting.
Receiver	
Receiver TX Gain (dB)	Configures the transmission gain of the Receiver.

Enable Receiver Noise Shield 2.0	When Receiver Noise Shield feature is enabled, the remote party will hear less environmental noise during a call. If set to "High Shielding", most of the environmental noise can be shielded. If set to "Soft Shielding", some environmental comfort noise will remain for the remote party.
Receiver Sidetone Volume	Configures Receiver sidetone volume. The valid range is 0 to 30.
Enable HAC	If enabled,the phone will compatible with nearby hearing AIDS.
Other Noise Cancellation	
Priority Noise Cancellation Method	Allows to choose the priority method for built-in noise cancellation on the phone. The options are: AI Noise Cancellation: this will automatically enable and prioritize AI Noise Cancellation during calls. Traditional Noise Cancellation: this will prioritize Noise Shield 2.0 during calls . Note: please make sure that the "Enable Receiver Noise Shield 2.0" option is checked when prioritizing traditional noise cancellation. By default, this parameter is set to "AI Noise Cancellation".
Display Settings	
Brightness	
LCD Brightness	Configure the backlight brightness of the phone when the LCD is active, with an effective value range of 10 to 100 (taking a multiple of 10).
Enable Keypad Backlight	If set to "On", the keypad backlight will light up. When set to "Auto", the button backlight switch will intelligently judge based on ambient light.
Button Backlight Brightness	Set the brightness of the button backlight.
Indicator Light	
Enable Incoming Call Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is incoming call on the phone.
Enable Missed Call Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is new voicemail on the phone.
Enable MWI Indicator	If set to "Yes", 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	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when there is new message on the phone.
Enable Charging Completed Indicator	If set to "Yes", the LED indicator on the upper right corner of the phone will light up when the phone is charged.
Enable Phone Ready Indicator	If set to "Yes," when the screen is off and the device has a registered account and is connected to Wi-Fi, the LED indicator will fast-flash green twice every 5 seconds in the following pattern: Green 100 ms -> fade out 10 ms -> off 100 ms -> green 100 ms -> fade out 10 ms -> off 5 s, then repeat. Disabled by default.
Others	
Display Battery Percentage	Configures whether the battery level is displayed within the battery icon. Set to "Do not Display" by default
Idle Display Mode	Configures the display mode of the idle page. The available options are: Concise, or normal
Label	Sets label text for LCD screen.
Backlight Timeout(s)	Configures LCD screen backlight timeout.
LCD Backlight when Missed Calls during Charging	When the phone is charging and there are missed calls popup, if "Always On" is selected, the screen will remain on without any operation; If "Timeout Screen Shutdown" is selected, the screen will automatically shut down according to the Timeout Screen Shutdown configuration time; if "Dim Always On" is selected, the screen will remain constantly on at a very low brightness without any operation.

Off Screen Indicator Pattern	Configures the Message Waiting Indicator (MWI) LED behavior when the screen is off. This allows users to define a custom flash pattern to suit their preferences, provided the device is operating normally. Default behavior: The green LED lights up for 100ms, fades over 10ms, turns off for 100ms, lights up again for 100ms, fades over 10ms, then turns off for 5000ms (5 seconds). The pattern repeats continuously. Pattern Syntax: c=color,t=on1/off1/change1[-on2/off2/change2[-on3/off3/change3]...]c: LED color (red, green, or yellow)on/off: Duration (in milliseconds) the LED remains on or offchange: Transition time (in milliseconds) for fade in/outExample: c=green,t=100/100/10-100/5000/10 Note: Using a custom pattern may significantly reduce the device's standby time.
LCD Backlight Always On Scene	Specifies conditions under which the LCD screen remains continuously on, ensuring users are notified by critical events. The options are:Network Error: When enabled, the backlight stays on if a network connection error occurs.Account Registration Failed: When enabled, the backlight remains on if any SIP account fails to register.Both options are enabled by default.
Vibration Settings	
Vibrate Mode	Configure whether to enable the phone's vibration mode. Once enabled, the incoming call vibration and notification vibration can be configured separately
Incoming Call Vibration	This configuration is valid when the vibration mode is enable. Configure whether to vibrate during an incoming call.
Notification vibration	This configuration is valid when the vibration mode is enable. Configure whether to vibrate during when the phone has new nonification.
Wallpaper Settings	
Wallpaper Source	Configure the source of wallpaper, if select "default", use the system default wallpaper; if select "download", use the wallpaper downloaded from Network, you need to configure the server path; if select "uploaded", use the wallpaper uploaded locally.
Wallpaper Server Path	Directory or file path of wallpaper, Only HTTP/HTTPS/TFTP protocol headers are supported, please specify the path to the image file name, only PNG format images are supported.
Other Settings	
Answer Mode	Select the answer mode for incoming calls. If you select the "call key", the call-related buttons are allowed to answer; If "any key" is selected, any button pressed will allow answering.
Off-cradle Pickup	If enabled, if only one incoming line is occupied, the call will be automatically answered when the handle is picked up from the charging stand.
Call Setting when Returns to Cradle	Configure the call-related behavior when the phone returns to the cradle. If configured to Hangup Current Line, hang up the current line when the phone returns to the cradle. If configured to Speaker when Calling, it will automatically switch to the speaker sound channel when the phone returns to the cradle, provided that the current channel is not the headphone channel during the call.
Enable Silent Charging	Configure whether the device automatically switches to silent mode whenever it is placed on a charging station or connected to a charger. This setting is disabled by default.
Enable Star Key Silent Mode	Configures whether silent mode can be enabled and disabled by long pressing the * key.
System Settings -> TR-069	
Enable TR-069	Enables TR-069
ACS URL	URL for TR-069 Auto Configuration Servers (ACS).Default setting is: https://acs.gdms.cloud
TR-069 Username	ACS username for TR-069.
TR-069 Password	ACS password for TR-069.

Periodic Inform Enable	Enables periodic inform. If set to "Yes", device will send inform packets to the ACS. The default setting is "Yes".
Periodic Inform Interval	Sets up the periodic inform interval to send the inform packets to the ACS.Default is 86400.
Connection Request Username	The username for the ACS to connect to the phone.
Connection Request Password	The password for the ACS to connect to the phone.
Connection Request Port	The port for the ACS to connect to the phone.
CPE SSL Certificate	The Cert File for the phone to connect to the ACS via SSL.
CPE SSL Private Key	The Cert Key for the phone to connect to the ACS via SSL.
Start TR-069 at Random Time	When enabled, TR-069 will send out first INFORM message to server on randomized timing between 1 to 3600 seconds after phone boots up.

Maintenance Page Definitions

Maintenance -> Upgrade and Provisioning	
Firmware	
Upgrade via Manually Upload	
Upload Firmware File to Update	Upload and start upgrade firmware.
Upgrade via Network	
Firmware Upgrade via	Allows users to choose the firmware upgrade method via TFTP, HTTP, HTTPS, FTP, FTPS Note: DHCP Option 150 provides the TFTP server address for provisioning. By default, it no longer overrides the manually configured provisioning server.
Firmware Server Path	Defines the server path for the firmware server.
Firmware Server Username	The username for the firmware server.
Firmware Server Password	The password for the firmware server.
Firmware File Prefix	If configured, only the firmware with the matching encrypted prefix will be downloaded and flashed into the phone.
Firmware file Postfix	If configured, only the firmware with the matching encrypted postfix will be downloaded and flashed into the phone.
Upgrade Detection	
Upgrade	Press to start upgrade process.
Config File	
Configure Manually	
Download Device Configuration	Click to download phone's configuration file in .txt format.Note Configuration file does not include passwords or CA/Custom certificateYou have the possibility to download all the configuration, or just the changed configuration
Download Device Configuration (XML)	Click to download phone's configuration file in .xml format.Note: Configuration file does not include passwords or CA/Custom certificate. You can download a help template by clicking on the "XML Help document" link.You have the possibility to download all the configuration, or just the changed configuration
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.Note: You have the possibility to download all the configuration, or just the changed configuration

Upload Device Configuration	Uploads configuration file to phone.
Export backup Package	Export backup package which contains device configuration along with personal data.
Restore from Backup package	Click to upload backup package and restore.
Configure via Network	
Config Upgrade Via	Allows users to choose the config upgrade method: TFTP, FTP, FTPS, HTTP or HTTPS.The default setting is "HTTPS".
Config Server Path	Defines the server path for provisioning. Note: Protocol header can be added in the Config Server path (Eg:https://) without the need to configure it on the "Config Upgrade via" parameter.
Config Server Username	The username for the HTTP/HTTPS server.
Config Server Password	The password for the HTTP/HTTPS server.
Always Authenticate Before Challenge	Only applies to HTTP/HTTPS. If enabled, the phone will send credentials before being challenged by the server.
Config File Prefix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
Config File Postfix	Enables your ITSP to lock configuration updates. If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Authenticate Conf File	Authenticates configuration file before acceptance.
XML Config File Password	The password for encrypting XML configuration file using OpenSSL. This is required for the phone to decrypt the encrypted XML configuration file.
Provision	
Auto Upgrade	
Automatic Upgrade	Enables automatic upgrade and provisioning.The default setting is "No".
Start Upgrade at Random Time	Configures whether the phone will upgrade automatically at a random time within the configured time interval.The default setting is "No"
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent: AlwaysCheck for New Firmware, Check New Firmware only when F/W pre/suffixChanges, Always Skip the Firmware Check.The default setting is "Always Check for New Firmware".
Firmware Upgrade Confirmation	If set to "Yes", the phone will ask the user to upgrade. If there is no response, the phone will proceed with the upgrade.If set to "No", the phone will automatically upgrade without user input.Default setting is Yes.
DHCP Option	
Allow DHCP Option 43 and Option 66 Override Server	DHCP option 66 originally was only designed for TFTP server. Later, it was extended to support an HTTP URL. 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. The default setting is "Yes".
Allow DHCP Option 120 to override SIP Server	Enables DHCP Option 120 from local server to override the SIP Server on the phone. The default setting is "No".
Additional Override DHCP Option	When enabled, users could select Option 150 or Option 160 to override the firmware server instead of using the configured firmware server path or the server from option 43 and option 66 in the local network. Please note this option will be effective only when option "Allow DHCP Option 43 and Option 66 to Override Server" is enabled. The default setting is "None".
Config Provision	

Download and Process ALL Available Config Files	By default, device will provision the first available config in the order of cfgMAC, cfgMAC.xml, cfgMODEL.xml, cfg.xml and devMAC.cfg (corresponding to device specific, model specific, and global configs). If set to Yes, device will download and apply (overwrite) all available configs in the same order.
User Protection	When user protection is on, pvalues that user sets will not be changed by provision or provider.
Auto Provision	When enabled, the phone sends SUBSCRIBE in multicast mode. If 3CX, UCM and other IPPBX servers are used as SIP servers, the phone can be automatically configured.
Advanced Settings	
Validate Hostname in Certificate	To validate the hostname in the SSL certificate
Enable SIP Notify Authentication	Device will challenge NOTIFY with 401 when set to Yes
Factory reset	Press Start to begin Factory Reset of the phone.
Maintenance -> System Diagnosis	
One-click Debug	
Output to Local Device	
Timeout	Configures the timeout period for file writing from 1 day to 14 days. The default value is 1 Day.
Automatic Stop Event	Specifies a condition to automatically stop the debug. The supported events are:Account Registration FailureWi-Fi Disconnected AbnormallyPhone Process Crash
Debug Mode	Choose the diagnostic mode. The available options are:Separate Mode: log and packet capture files are each limited to 10MB. If the "File Write Method" stops at 10MB, logging stops when the log file is full, but packet capture continues. Merge Mode: the log and packet capture files share a 20MB limit.
File Write Method	With "10MB Stop," writing stops after 10MB. With "10MB Coverage," the oldest data is overwritten after 10MB.
Start	Start the one-click debug.
Stop	Stop the one-click debug.
Download	Download the one-click debug.Note: the One-Click Debug package includes an sslkeylogfile.txt for decrypting TLS-encrypted SIP/RTP traffic.
Delete	Delete the one-click debug.
Output to Server (Log Only)	
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 Keyword Filter	Syslog will be filtered based on keywords provided. If you enter multiple keywords, it should be separated by ','. Please note that no spaces are allowed.
Send SIP Log	Enables/Disables sending the SIP log in the syslog messages.Enabled by default.
General	

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 Header Format	Configures the preferred header format for Syslog. The options are:Legacy (Default setting)RFC3164 CompliantThe RFC3164 compliant header begins with "PRI" which represent both the Facility (0 - 23) and severity level (0 - 7) of the event. The message includes the timestamp, hostname, process id and the log message. For more information regarding the representation of the numerical values for the facility and severity, please refer to RFC3164.
Include Kernel Logs	Enable/disable the inclusion of kernel messages in the output syslog. Disabled by default.
With RTP Packets	Defines whether the packet capture file contains RTP or not. The default setting is "No".
Generate WLAN Session Keys File	After this configuration is enabled, the DEBUG package will carry the WLAN session key file, named 80211_keys, which records the WLAN session keys that the device has gone through from the start to the end of the One-click DEBUG process. Disabled by default.
Maintain System Log Information after Factory Reset	If Enabled, syslog settings and internal logs will be saved across a factory reset. Disabled by default.
Key Log	
One-Click Export	Exports the current Key Log records into a downloadable .log file for offline analysis or for sharing with technical support. For example: Collect logs before factory reset or when submitting a support ticket.
Clear	Clears all existing Key Log entries from the device. Note: This action does not disable logging. New events will continue to be recorded if logging is enabled.
Enable Key Log Writing and LCD Display	Enables the logging mechanism and allows key events to be shown on the device LCD.ON: New system events are recorded in the Key Log, Key log entries can be displayed on the phone screenOFF: No new log entries are written, Key log information is hidden from the LCDAfter turning off the device (power off), new logs will no longer be written, and LCD key log display will be disabled.
Filters and Search	Allows filtering log entries by a specific time window. You can also search for specific keywords within log entries in the search bar (such as Wi-Fi, Account, Provision, IP, etc.).
Event Name	Describes the event that occurred on the device.
Trigger Time	The exact date and time when the event occurred, based on the device system clock.
Type	Categorizes the event based on the subsystem involved.
Level	Indicates the severity or importance of the event.For example:Info - Normal operational eventsWarning - Non-critical issues that may affect functionality
Device Running Time	Shows how long the device had been running (uptime) at the moment the event was triggered.
Operation	Provides access to the detailed log entry for the selected event. Clicking the icon allows administrators to view or extract additional event details such as the event , source trigger time, type, level , and device running time.
Ping	
Ping	Enter Ping target's IP address or URL and click on start.
Traceroute	

Traceroute	Input target's IP address or URL and click on start
Domain Query	
Domain Query	Enter Domain Query URL and click on start.
Remote Diagnostics	
Remote Diagnostics	When enabled, this device will allow remote access and remote collection of logs. It will automatically end when it expires.
Start	to begin the remote diagnostics , click on the "start" button
Access Address	Displays the IP Address and port number of the access address
Expiration Time	Displays the Expiration time of the Remote Diagnostics , The Expiration time is set to 48 hours since the start of the Remote Diagnostics
Maintenance -> Outbound Notification	
Action URL	
Phone Status	
Setup Completed	Configures the Action URL to send when phone finishes setup process.
Registered	Configures the Action URL to send when phone successfully registers a SIP account.
Unregistered	Configures the Action URL to send when phone unregisters a SIP account.
Register failed	Configures the Action URL to send when phone fails to register a SIP account.
Idle to Busy	Configures the Action URL to send when phone's state changes from idle to busy.
Busy to Idle	Configures the Action URL to send when phone's state changes from busy to idle.
Auto Provision Completed	Configures the Action URL to send when phone's auto provisioning process is completed.
IP Change	Configures the Action URL to send when the IP address changes.
Call Operation	
Off-hook	Configures the Action URL to send when phone is in off-hook state.
On-hook	Configures the Action URL to send when phone is in on-hook state.
Incoming Calls	Configures the Action URL to send when phone receives an incoming call.
Outgoing Calls	Configures the Action URL to send when phone places a call.
Missed Call	Configures the Action URL to send when phone has a missed call.
Established Call	Configures the Action URL to send when phone establishes a call.
Forwarded Call	Configures the Action URL to send when phone forwards an incoming call.
Terminated Call	Configures the Action URL to send when phone terminates a call.
Answered Call	Configures the Action URL to send when phone answers an incoming call.
Rejected Call	Configures the Action URL to send when phone rejects an incoming call.
Blind Transfer	Configures the Action URL to send when phone performs blind transfer.
Attended Transfer	Configures the Action URL to send when phone performs attended transfer.

Transfer Completed	Configures the Action URL to send when phone successfully transfers a call.
Transfer failed	Configures the Action URL to send when phone fails to transfer a call.
Hold Call	Configures the Action URL to send when phone places a call on hold.
Unhold Call	Configures the Action URL to send when phone resumes the call on hold.
Mute Call	Configures the Action URL to send when phone mutes a call.
Unmute Call	Configures the Action URL to send when phone unmutes a call.
Call Settings	
Enable DND	Configures the Action URL to send when phone enables DND.
Disable DND	Configures the Action URL to send when phone disables DND.
Enable Call Forward	Configures the Action URL to send when phone enables Call Forward.
Disable Call Forward	Configures the Action URL to send when phone disables call forward.
Open Forward Always	Configures the Action URL to send when phone enables call forward always function.
Close Forward Always	Configures the Action URL to send when phone disables call forward always function.
Open Call Forward Busy	Configures the Action URL to send when phone disables call forward always function.
Close Call Forward Busy	Configures the Action URL to send when phone disables call forward busy function
Open Call Forward No Answer	Configures the Action URL to send when phone enables call forward no answer function.
Close Call Forward No Answer	Configures the Action URL to send when phone disables call forward no answer function.
Destination	
Destination Name	Identify the destination name. It must be unique.
Protocol	Configure the protocol associated with the destination server. Currently XMPP and SMTP are supported.
Enable SSL	Configure whether to use SSL to encrypt for SMTP protocol. This option is not editable for XMPP.
Destination Address	Configure destination server address, e.g., talk.google.com.
Port	Configure destination server port, e.g., 5222.
Domain	Configure the destination server domain for XMPP protocol. This option is not editable for SMTP.
Username	Configure the authorization username of the destination server.
Password	Configure the authorization user password for the destination server.
From	Configure the sender name for SMTP protocol. This option is not editable for XMPP.
To	Configure the receiver's address.
Extra Attribute Name	Configure extra attribute's name reserved for protocol specific attributes such as "jid" for XMPP protocol. If "jid" is specified, username and domain will be overridden.
Extra Attribute Value	Configure extra attribute's value reserved for protocol specific attributes such as "abc@gmail.com" for "jid" of XMPP protocol. If it is specified, username and domain will be overridden.
Notification	
Event	Configures the event, which will trigger an outbound notification.

Destination	Configures the name of the destination where the outbound notification will be sent to.
Subject	Configures the subject of Email notification. This option is only applicable to SMTP protocol and it is not editable for other protocols.
Message	Configures the message body or the outbound notification.
Extra Attribute Name	Configure extra attribute's name reserved for specific attributes for a given notification in the future.
Extra Attribute Value	Configures extra attribute's value reserved for specific attributes for a given notification in the future.
Maintenance -> Voice Monitoring	
Session Report	
VQ RTCP-XR Session Report	When enabled, the phone will send a session quality report to the central report collector at the end of each call.
Interval Report	
VQ RTCP-XR Interval Report	When enabled, phone will send an interval quality report to the central report collector periodically throughout a call.
VQ RTCP-XR Interval Report Period	Configure the interval (in seconds) of phone sending an interval quality report to the central report collector periodically throughout a call.
Alert Report	
Warning Threshold for Moslq	Configure the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a warning alert quality report to the central report collector.
Critical Threshold for Moslq	Configure the threshold value of listening MOS score (MOS-LQ) multiplied by 10. The threshold value of MOS-LQ causes the phone to send a critical alert quality report to the central report collector.
Warning Threshold for Delay	Configure the threshold value of one way delay (in milliseconds) that causes the phone to send a warning alert quality report to the central report collector.
Critical Threshold for Delay	Configure the threshold value of one way delay (in milliseconds) that causes the phone to send a critical alert quality report to the central report collector.
Display Report	
Display Report on Web UI	When enabled, the phone will display the quality report on the Web GUI. Enabled by Default.
Display Report on LCD	When enabled, phone will display the quality report on LCD. Disabled by Default
Custom Display Layout on LCD	Sets available Items to be displayed on LCD report.
Maintenance -> Scheduled Tasks	
Working Time	Configures office hours for the effective time configuration of scheduled tasks. For example: set to lock the phone during non-working hours, set forward during working hours.
Scheduled Tasks	
Add	Configures a new shceduled task based on : Scheduled Tasks Type: Select the type of scheduled task: Scheduled Reboot, Scheduled lock, or Scheduled Forward, Set to Scheduled Reboot by Default. Repetition period: Configures the recurring day of the scheduled task: Every day, Every Week, Every Month, No Repeat, set to no-repeat by Default Effective Time: Configures the effective time or time period of the scheduled task every day. Set to 00:00 by Default
Delete	Deletes the Scheduled Tasks

Application Page Definitions

Application -> Quick Access	
Quick Access Key Long Press Function	Configure the function triggered when long-pressing the Quick Access shortcut key during a call. When set to Favorite, long-pressing the key during a call opens the Favorite Contacts list.
Custom Softkey Layout	
Mode	Quick StartQuick Jump
Quick Jump	This option appears Info Missed Notification UCM Call features Missed Call History Dialed Call History Received Call HistoryBroadsoft Call LogFavoriteContactsLocal Phonebook LDAPRemote Phonebook Remote Phonebook1 Remote Phonebook2 Remote Phonebook3Remote Phonebook4 Remote Phonebook5 Online Contacts Group Block List Broadsoft Directory MessagesVoicemailSettingsBasic SettingsAccount Settings Wi-Fi Settings BluetoothQuick Network ConfigurationDiagnosticsStatusProfile CodeAlarm SettingsStopwatchTimerCalendar
Quick Start	Speed DialBusy Lamp Field (BLF)Speed Dial via Active AccountDial DTMFCall VoicemailCall ReturnCall ParkLDAP SearchConferenceMonitored Call ParkForwardDNDRedialOpen DoorProvisionHTTP CommandCall FlipSend MessageAlarmBlind TransferAttended TransferAway ToggleWi-Fi ToggleBluetooth Toggle
Account	Select an account.
Value	Enter the corresponding value to the setting set in Quick Start.
Label	Enter the label of the quick start option.
Application -> Web Service	
Use Auto Location Service	To enable or disable auto location services on the phone. (Reboot Required)
Application -> Contacts	
Contacts	
Add Contact	Press Add to create a new contact. You can define the following parameters when creating a new contact: First NameLast NameCompanyDepartmentJob TitleNumberPrefer NumberAccounts GroupsRingtoneNote: Contacts can have up to 10 numbers, categorized as Work, Home, Mobile, or Conference. Categories can be used multiple times.
Edit	Edits the contact parameters.
Delete	Deletes a specific contact entry.
Delete All Contacts	Press to delete all contacts.
Group Management	
Add Group	Specifies Group's name to add new group. Up to 50 contact groups can be added.
Edit Group	Edits selected group.
Delete Group	Delete Selected group.
Phonebook Management	
Enable Phonebook XML Download	Configures to enable phonebook XML download. Users could select HTTP/HTTPS/TFTP to download the phonebook file.The default setting is "Disabled".
HTTP/HTTPS Username	The username for the HTTP/HTTPS server.
HTTP/HTTPS Password	The password for the HTTP/HTTPS server.
Phonebook XML Server Path	Configures the server path to download the phonebook XML.This field could be IP address or URL, with up to 256 characters.

Phonebook Download Interval	Configures the phonebook download interval (in minutes).If set to 0, automatic download will be disabled. The default value is 0. Valid range is 5 to 720 minutes.
Remove Manually-edited Entries on Download	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed. The default setting is "Yes".
Import Group Method	When set to "Replace", existing groups will be completely replaced by imported one.When set to "Append", the imported groups will be attended with the current one.The default setting is "Replace".
Sort Phonebook by	Configures to sort phonebook based on the selection of first name, last name or auto. If you select "Last name", the contact's last name will be displayed first, and the phone book will be sorted by last name; if you select "First name", the contact's first name will be displayed first, and the phone book will be sorted by first name; If you select "Auto", the contact will be displayed based on whether the contact contains Chinese, Japanese, and Korean characters. If there are these characters, the contact's last name will be displayed first.The Default setting is "Auto".
Case Sensitive Search	Set whether the contact phonebook search is case-sensitive. This means that the search function will take into consideration uppercase and lowercase letters. Example: "John" and "john" will generate different search results.
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.
Download vCard Phonebook	Click on "Download" to download the vCard phonebook file to local PC
Upload vCard Phonebook	Click on "Upload" to upload local vCard phonebook file to the phone.
Default Search Mode	Configures the default phonebook search mode. Options are "Full Fuzzy Match" and "Exact Match". The default mode is "Full Fuzzy Match."
Application -> LDAP	
Obtain from UCM Server	
Obtain LDAP configuratio file	Sets the option to obtain the LDAP configuration file from the ucm the phone is registered to, if activated, the Original LDAP file will be overwritten.
Enable UCM LDAP Auto-config Feature on LCD	When it is turned off, the setting soft key supporting UCM LDAP automatic configuration will no longer be displayed on the LCD. Enabled by Default.
Manual Import	
Import LDAP configuration file	Sets the option to Import the LDAP configuration file, if activated, The original LDAP file will be overwritten.
Local Configuration	
LDAP Protocol	Configures the LDAP protocol to LDAP or LDAPS. The default setting is "LDAP". LDAPS is a feature to support LDAP over TLS.
LDAP Version	Selects the protocol version for the phone to send the bind requests. The default setting is "Version 3".
Server Address	Configures the IP address or DNS name of the LDAP server.
Port	Configures the LDAP server port. The default port number is "389".
Base DN	Configures the LDAP search base.This is the location in the directory where the search is requested to begin.Example:dc=grandstream, dc=comou=Boston, dc=grandstream, dc=com
Username	Configures the bind "Username" for querying LDAP servers. Some LDAP servers allow anonymous binds in which case the setting can be left blank.
Password	Configures the bind "Password" for querying LDAP servers. The field can be left blank if the LDAP server allows anonymous binds.

LDAP Number Filter	Configures the filter used for number lookups.Examples:(|(telephoneNumber=%)(Mobile=%)) returns all records which has the "telephoneNumber" or "Mobile" field starting with the entered prefix;(&(telephoneNumber=%) (cn=*)) returns all the records with the "telephoneNumber" field starting with the entered prefix and "cn" field set.
LDAP Name Filter	Configures the filter used for name lookups.Examples:(|(cn=%)(sn=%)) returns all records which has the "cn" or "sn" field starting with the entered prefix;(!(sn=%)) returns all the records which do not have the "sn" field starting with the entered prefix;(&(cn=%) (telephoneNumber=*)) returns all the records with the "cn" field starting with the entered prefix and "telephoneNumber" field set.
LDAP Mail Filter	Configures the filter used for email lookups.Examples:(|(mail=%)(mailBox=%)) returns all records which has the "mail" or "mailbox" field containing the entered filter value;(!(mail=%)) returns all the records which do not have the "mail" field containing the entered filter value;(&(mail=%) (cn=*)) returns all the records with the "mail" field containing the entered filter value and "cn" field set
LDAP Mail Attributes	Specifies the "mail" attributes of each record which are returned in the LDAP search result. This field allows users to configure multiple space separated email attributes.
LDAP Name Attributes	Specifies the "name" attributes of each record which are returned in the LDAP search result. This field allows the users to configure multiple space separated name attributes.Example:gncn sn description
LDAP Number Attributes	Specifies the "number" attributes of each record which are returned in the LDAP search result.This field allows the users to configure multiple space separated number attributes.Example:telephoneNumbertelephoneNumber Mobile
LDAP Display Name	Configures the entry information to be shown on phone's LCD. Up to 3 fields can be displayed.Example:%cn %sn %telephoneNumber
Max Hits	Specifies the maximum number of results to be returned by the LDAP server. If set to 0, server will return all search results. The default setting is 50.
Search Timeout	Specifies the interval (in seconds) for the server to process the request and client waits for server to return. The default setting is 30 seconds.
Sort Results	Specifies whether the searching result is sorted or not.Default setting is "No".
Exact Match Search	Search for exact match result Default setting is "No".
LDAP Lookup	Configures to enable LDAP number searching when dialing / receiving calls.
LDAP Dialing Default Account	Configures the default account used when dialing LDAP contact
Lookup Display Name	Configures the display name when LDAP looks up the name for incoming call or outgoing call. This field must be a subset of the LDAP Name Attributes.Example:gncn sn description
Application -> Remote Phonebook	
The user can configure up to 5 XML Remote Phonebooks.	
Display Name	Configures the entry information to be shown on phone's LCD.
URL	Configures the XML Phonebook URL.
Username	The user name for the phonebook.
Password	The password for the phonebook.
Remote Phonebook Update Interval	Configures the Remote Phonebook download Interval (in minutes). If set to 0, automatic download will be disabled. Valid range is 5 to 720.
Application -> Call History	
Delete	Users can select an entry, then click "Delete" to remove it from the list.

Delete All	Click on Delete All to remove all Call History stored in the phone.Note: Users could use the drop-down list to show only selected call history type (All, Answered, Dialed, Missed, and Transferred) and use navigation keys to browse pages when many entries exist.
Application -> Online Contacts	
Contacts Search URL	Configures the URL to search contacts. This field could be protocol,server address,path,or query parameters, with up to 256 characters. Path and query parameters can use built-in variables in the format of {var}. Optional variables include: {localNumber}: Local number {remoteNumber}: Remote number {sipServer}: Account registration server {model}: Phone model {version}: Version number {mac}: Phone MAC address {Exactsearch}:whether to query accurately (0-fuzzy, 1-exact) {Condition}:query criteria (entered number/name, etc.) {Pagecount}:The maximum number of query results displayed on a page {Pagenum}:Number of pages at the beginning of the queryExample: URL="http://ip:port/getUserInfoByNumber/{remoteNumber}"
Contacts search HTTP POST	Configures the HTTP POST to search contacts. This field could be protocol, server address, path, or query parameters, with up to 1024 characters. Path and query parameters can use built-in variables in the format of {var}. Optional variables include: {localNumber}: Local number {remoteNumber}: Remote number {sipServer}: Account registration server {model}:Phone model {version}:Version number {mac}:Phone MAC address {Exactsearch}:whether to query accurately (0-fuzzy, 1-exact) {Condition}: query criteria (entered number/name, etc.) {Pagecount}: The maximum number of query results displayed on a page {Pagenum}: Number of pages at the beginning of the queryWhen the configuration item is empty (including all blank data), the phone sends a get request, otherwise, the phone sends a post request. It Supports XML and JSON data formats.
Contacts Search Auth Username	Sets The username for the Searching HTTP/HTTPS server.
Contacts Search Auth Password	Sets The password for the Searching HTTP/HTTPS server.
Contact Search Response Syntax	Configure contact search response syntax.Response syntax is mandatory. Enter a URL or response content to parse. If you enter a URL and click respond, the system automatically obtains the response content and result. The format of response syntax is key:val[,key:val]. Each line displays one rule. The comma '', ''is a newline character. The key includes: ? success ? reason ? counts ? total ? name ? company ? department ? title ? email ? firstName ? lastName ? extensionCompany ? extensionHome ? extensionMobile
Application -> Calendar	
Import Calendar	Click on Import to open the Import Calendar dialog, the import calendar Allows you to add an external calendar (.ics) to the system, once the calendar becomes active, it affects how the system behaves on certain dates/times.When clicking on "import" users can configure the below options: Calendar Import Mode: Configure the mode for importing schedule files. If URL mode is selected, the files under the address will be checked for updates at 00:00 every day. If upload file mode is selected, user should import a .ics calendar file.URL Address: Specify the calendar's URL to subscribe and automatically synchronize updates from the calendar owner.Username: Enter the username required to access the calendar URL if the calendar is protected. Used when the calendar is hosted on a server that requires login (HTTP/HTTPS authentication). Leave this field empty if the calendar URL is publicPassword: Enter the password corresponding to the username above. Required only for private or restricted calendars. Leave this field empty if no authentication is neededNote: You can import up to 5 calendars at once, and if multiple calendars conflict (same date/time); The one higher in priority (earlier in list) takes effect
Week Start Day	Select which day the calendar treats as the first day of the week. Set to "Sunday" by default.
Export Current Calendar	Export the currently active calendar configuration as an .ics file. Note: Exported calendars follow the standard ICS (iCalendar) format. Please refer to this guide for steps on how to edit and configure an ICS file: WP8x6 - Editing an ICS File
Application -> PNP Service	

Enable PNP	Configures whether to enable the PNP function. After enabling it, the automatic configuration is supported, and up to 100 devices can be configured. Disabled by Default.
PNP URL Mode	Select the PNP URL mode, including local and custom, custom does not support filling in the local machine-related address.
PNP URL	The configuration terminal can take the server address of the configuration file. The server address can be the IP address of the terminal that provides PNP services. It cannot be configured as a locally related parameter.
Template Management	Profile templates can be managed in this module. The current model only supports the management of one profile template. It supports the generation of batch configuration CSV files based on the profile template. You can fill in the relevant parameter values in this file, and start the PNP batch configuration process after the application.
Upload Profile Template	Users can upload a .xml template file downloaded by respecting the following guidelines: Users can upload the configuration file template here and add parameters to define parameter names. Parameter values are different configuration item values of different devices. To specify a device for configuration, add the %%mac_address%% parameter to the filename in the template file. The parameter can be configured in batches in Step 2 (Batch Configure CSV). If the same parameters need to be configured for all devices, delete %%mac_address%% from filename in the template file and assign values to each parameter. Please write configuration file template according to sample file format specification. Any text file format can be placed in <data><![CDATA[-]]></data>.
Batch Configure CSV	Users can upload a .csv template file download while respecting the following guidelines: If there are batch configuration variables in the configuration file template, generate the batch configuration CSV file according to the uploaded configuration file template, and fill in the relevant batch configuration values after exporting the CSV template. After writing the batch configuration CSV template, upload the CSV template file here.
Effects View	Displays the data inserted from the .csv template to the .xml configuration file.
Progress Data	When connected to a network, the phone can automatically identify and configure itself with the appropriate settings for that network. This eliminates the need for manual configuration, making it faster and easier to set up and manage IP phone deployments. the connected networks will be displayed in the list.
MAC Discovery	During the plug-and-play process, the network infrastructure uses the MAC Discovery feature to detect the IP phone's MAC address and automatically configure it with the appropriate settings, such as IP address, subnet mask, default gateway, and other network-related parameters. This eliminates the need for manual configuration and speeds up the deployment of IP phones in large-scale environments. A list of MAC Addresses with their respective IP address, Product models, and operations is displayed, and the actions that can be performed on those IP phones are the following : Download the Configuration file: this option will download the configuration file of the discovered device Redistribution operation: When a new WP phone is added to the network, the PNP service detects the device and automatically retrieves its configuration information from a central configuration server. The PNP service then redistributes this information to all other IP phones in the network, ensuring that all devices are configured in a consistent and efficient manner.
Application -> Account Sharing	
General Settings	
Enable Account Sharing	Select whether to enable Account Sharing.
Role in Account Sharing	Select the role that the current device will play in the network, the guest device role does not need to register an account on IP PBX, and can make calls in and out of the network through the account set by the host device role.

Group Name	Set the group name, in the host-guest mode, devices with the same group name can discover each other.Note: This item is mandatory if using Account Sharing. The verification format is domain type
Group Password	In the host-guest mode, after setting the group password, the guest device with the same group password as the host device can successfully register an account on the host device.Note:This item is mandatory if using Account Sharing.
SIP Server Port	Sets the SIP service port in Account Sharing, where 0 indicates using the random port, The valid range is from 0 to 65535.
Account Settings	
Account	For the host device role, this setting determines which host device account will be used as the guest device outgoing and incoming account for calls outside the Account Sharing. For the guest device role, this setting determines which account the guest device will use to register on the host device.
Account Name	This setting specifies the account name corresponding to the account used by the guest device.
Sync Ringing In Group	Set whether to enable synchronization of all successfully registered guest device ringtones within the group.
Discovered Host Device list	Shows registered devices on the local network for monitoring, it displays the following information about the discovered devices: IP Address MAC Address Registration Status Operation
Application -> Alarm Settings	
Alarm Monitoring	Enable/Disable the alarm feature. By default, this parameter is disabled.
Alarm Monitoring	
Ambient Sound Detection	Allows to set ambient sound detection to three different modes: Instant Detection: the alarm is triggered immediately when the ambient sound level exceeds the configured threshold. Continuous Detection(3s): the alarm is triggered when the ambient sound level exceeds the configured threshold continuously for 3 seconds. Disabled: the ambient sound detection is feature is disabled. The default setting is "Disabled".
Ambient Sound Level	Configures the level for ambient sound detection. The levels are (from lowest to highest):UncomfortableNoisyHarshWhen ambient sound detection is enabled, the default setting for this parameter is "Harsh".
No Movement Alarm	Allows users to adjust the level of sensitivity for the No Movement Alarm using 7 levels, with Level 1 being the lowest and Level 7 being the highest. The default "Disabled" option can be selected to turn off the No Movement Alarm.
No Movement Timeout (s)	Sets the timeout value (in seconds) for the No Movement Alarm. The alarm will trigger if the phone remains stationary for this duration. The valid range is 5 to 300 seconds and the default setting is "5".
Man Down Alarm	Allows users to adjust the level of sensitivity for the Man Down Alarm using 7 levels, with Level 1 being the lowest and Level 7 being the highest. The default "Disabled" option can be selected to turn off the Man Down Alarm.
Man Down Timeout (s)	Sets the timeout value (in seconds) for the Man Down Alarm. The alarm will trigger if the phone remains in the man-down position for the specified duration. The valid range is 5 to 300 seconds and the default setting is "5".
Running Alarm	Allows users to adjust the level of sensitivity for the Running Alarm using 7 levels, with Level 1 being the lowest and Level 7 being the highest. The default "Disabled" option can be selected to turn off the Running Alarm.
Running Timeout (s)	Sets the timeout value (in seconds) for the Running Alarm. The alarm will trigger if the phone detects running for the configured duration. The valid range is 5 to 300 seconds and the default setting is "5".
Alarm Settings	

Snooze Timeout (s)	Sets the snooze timeout value (in seconds). The snooze can be activated during warning/alarm state. The phone will resume detection after the specified duration. The valid range is 0 to 300 seconds and the default setting is "0".
Warning Timeout (s)	Sets the warning timeout value (in seconds). If the phone remains in a warning state without being canceled, the alarm will trigger after the configured timeout. The valid range is 5 to 300 seconds and the default setting is "5".
Mute While Push Button Alarm	If enabled the alarm triggered by pressing the side key will be a silent alarm. Default setting is disabled.
LCD Backlight Behavior after Push Button Alarm Triggered	Configures the behavior of the LCD backlight during a push button (side key) alarm: Maintain Current: The current LCD backlight will be maintained during the alarm. Turn Off Backlight: the backlight will be turned off during the alarm. The default setting is "Maintain Current".
Push Button Alarm Behavior Overridable	Chooses whether the push button (side key) alarm can be overriden by other alarms: Not Be Override: monitored alarms can not override the push button alarm. Be Override: monitored alarms will be able to override the push button alarm; The default setting is "Not Be Override".
Emergency Call	If enabled, the phone will automatically dial out a configured emergency number while in alarm state. This feature is disabled by default.
Alarm Account	Sets the account that will be used for the emergency call: Auto: the phone will automatically choose an account when initiating the emergency call. Account1: the first SIP account will be chosen for the emergency call. Account2: the second SIP account will be chosen for the emergency call. Account3: (WP826/WP836 Only) the third SIP account will be used for the emergency call. The default setting is "Auto".
Emergency Dial Force Speaker	If enabled, the phone will use speaker for emergency call. This feature is enabled by default.
Emergency Dial Number	Configures the emergency number that will be called when the phone is in alarm state.
Emergency Call Way	When Sequential is selected, emergency numbers are dialed one after another in the configured order. When Simultaneously is selected, all configured emergency numbers are dialed at the same time. If the available number of lines is insufficient, the calls are placed sequentially.
Emergency Call Auto Answer	Specifies whether the device automatically answers incoming calls from configured emergency numbers when an alarm is triggered.
Warning Tone	Sets the warning tone. The default one is "Tone 2".
Alarm Tone	Sets the alarm tone. The default one is "Tone 7".
Prompt Sound To Other Lines	If an alarm is triggered during an active call, the phone will automatically play this prompt to warn the person on the other end of the call about the emergency. The default prompt is "Emergency". However users can upload a custom prompt in any audio format and it will be converted to OGG format and used instead.

External Service Page Definitions

External Service -> Door System

Door System	Connect to a GDS37XX or other door systems and send "Open Door" request.Door System Type: Select "GDS" or "Others" as service type.Account: The account to be used on the phone to interact with the door system.Access Number: The SIP extension or the IP address of the door system depending on the deployed scenario, Peering or Registration.Related Display Name1: Configures the display name of the door system. When the call matches the configured system number, the name will be displayed on LCD. Access Password1: The password set on the GDS37XX to unlock the door 1.Related Display Name2: Configures the display name of the door system. When the call matches the configured system number, the name will be displayed on LCD. Access Password2: Configures the access password of the door system 2. 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. Ringtone: Select the system ringtone from the dropdown list to be played when there is an incoming call from the configured system number of the GDS37xx.Note: During a call with the door system, the phone will display a softkey "open door" which allows the user to send the door access password using DTMF. A confrmation prompt will be displayed to complete the open door action
BroadSoft Xsi	
Authentication Login	
Server	Specifies the hostname or IP address of the BroadSoft XSI server. Example: xsi.example.com
Port	Defines the TCP port used to access the XSI service.
Xsi Actions Path	Specifies the XSI request path on the server. This path is required for the phone to issue XSI action requests such as directory queries and call log retrieval. Example: /com.broadsoft.xsi-actions
Xsi Authentication Type	Defines the credential source used for XSI authentication.SIP Credentials - Uses the SIP account credentials configured on the phone for XSI login.Login Credentials - The device authenticates to the BroadSoft XSI server using dedicated XSI login credentials, instead of reusing SIP account credentials.
BroadSoft User ID	Specifies the BroadSoft user ID used for XSI authentication.
Login Password	Configures password for BroadSoft Xsi server
SIP Authentication ID	Defines the SIP authentication username associated with the selected account. This value is reused for XSI authentication when SIP Credentials are selected.
SIP Authentication Password	Specifies the SIP authentication password associated with the account. This password is also used for authenticating XSI requests.
Auto Login	Controls whether the phone automatically logs in to the XSI server.Enabled: The device automatically authenticates to XSI after boot or network recovery.Disabled: Manual login is required.
Login	Manually initiates an authentication attempt to the XSI server using the configured parameters.
Service Settings	
Sort Phonebook by	Defines how XSI directory entries are sorted on the phone.Auto: Sorting behavior is determined automatically by the device based on available fields.Last Name: Sorting is done based on the Last name.First Name: Sorting is done based on the First name.Set to Auto by default.
BroadSoft Directory Update Interval (m)	Specifies how often (in minutes) the phone synchronizes directory data from the XSI server. By default, it is set to : 4320 minutes (72 hours)
BroadSoft Contacts Download Limit	Defines the maximum number of directory contacts that can be downloaded and stored locally. This prevents excessive memory usage on large enterprise directories.
BroadSoft Contacts Search Limit	Defines the maximum number of results returned for a single directory search query. This improves performance and avoids large result sets.
Network Directories	

Type	Enable or disable the directory source, the available options for display are: Group Directory, Enterprise Directory, Group Common, Enterprise Common, Personal Directory, Missed Call Log, Placed Call Log, Received Call Log
Name	Custom display name shown on the phone UI
External Service -> E911 Service	
Enable E911	Enable Enhanced 911 call. Default is disabled
HELD Protocol	Configure HELD transfer protocol. HTTP or HTTPS
HELD Synchronization Interval	The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when the interval is 0.
Location Server	Configure the primary Location Information Server (LIS) address
Location Server Username	Configure the user name of the primary Location Information Server (LIS)
Location Server Password	Configure the password of the primary Location Information Server (LIS)
Secondary Location Server	Configure the seconary Location Information Server (LIS) address
Secondary Location Server Username	Configure the user name of the secondary Location Information Server (LIS)
Secondary Location Server Password	Configure the password of the secondary Location Information Server (LIS)
HELD Location Types	Configure "locationType" element in the location request. "geodetic", "civic" and "location URI"
HELD Use LLDP Information	If "Yes", the information from LLDP-suport switch is used to generate ChassisID and PortID; otherwaise, the mac address of gateway and phone is used as default.
HELD NAI	If "Yes", Network Access Identifier (NAI) is included as a device identity in the location request sent to the Location Information Server (LIS) Up to 10 HELD identities can be configured.
E911 Emergency Numbers	A user can configure multiple emergency numbers separated with the delimiter symbol ";".
Geolocation-Routing Header	If "Yes", E.911 INVITE message includes the "Geolocation-Routing" header with the value "Yes"
Geolocation Header Format	Selects the format used for the SIP Geolocation header when sending emergency calls:Legacy - Sends the Geolocation value as plain text (e.g., Geolocation: 8476BD6B-5FDD-339D-900B-AEAB0AA0429A).RFC6442 - Sends the Geolocation value in RFC6442-compliant format, enclosed in angle brackets (e.g., Geolocation: <8476BD6B-5FDD-339D-900B-AEAB0AA0429A>).Set to "Legacy" by default.
Priority Header	If "Yes", E.911 INVITE message includes the "Priority" header with the value "emergency"

UPGRADING AND PROVISIONING

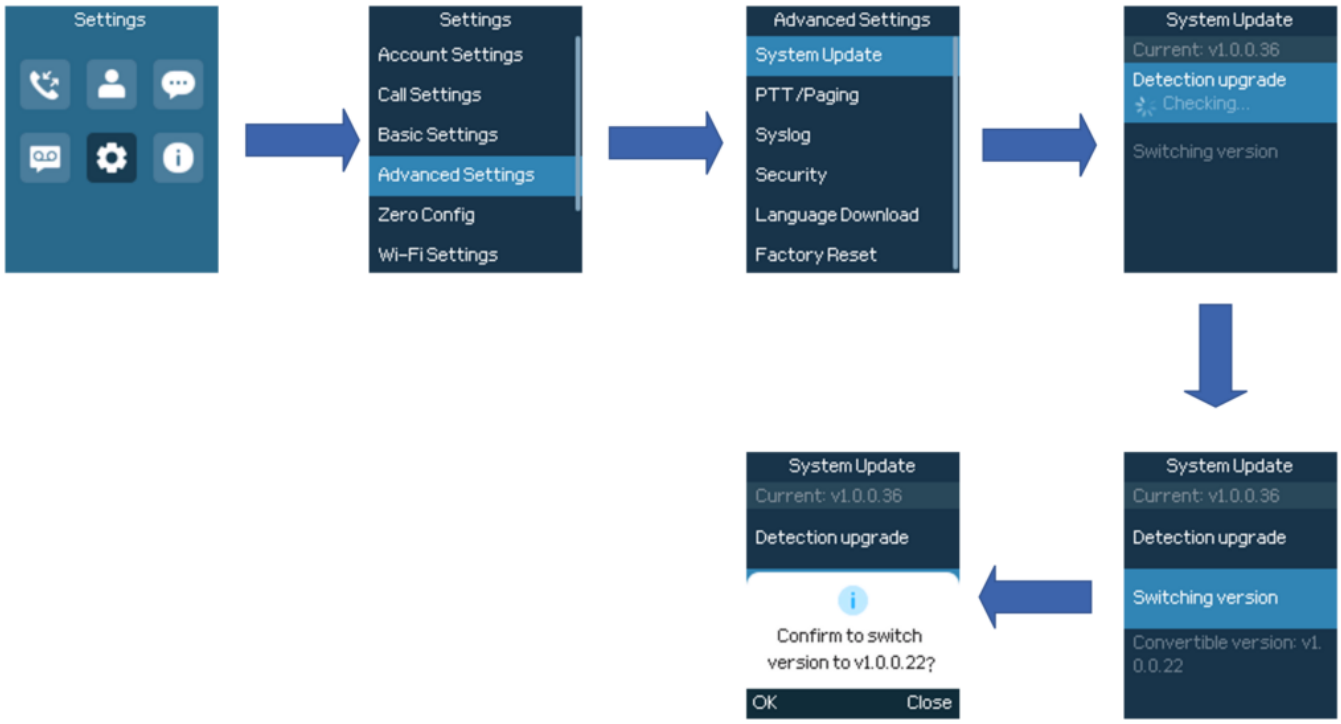
The WP8x6 can be upgraded via TFTP/HTTP/HTTPS/FTP/FTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS/FTP/FTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP, HTTPS, FTP, or FTPS; the server name can be FQDN or IP address.

Upgrade and Provisioning Configuration

There are two ways to set up upgrades and provisioning on WP8x6. They are the Keypad Menu and Web GUI.

Configure via keypad Menu

1. In handset Settings, select **Advanced Settings** -> **System Update**.
2. From here, you will have two options, either to detect if a new firmware is available by choosing the **"detection upgrade"** option or roll back to the previous firmware version by clicking **"Switching version"**

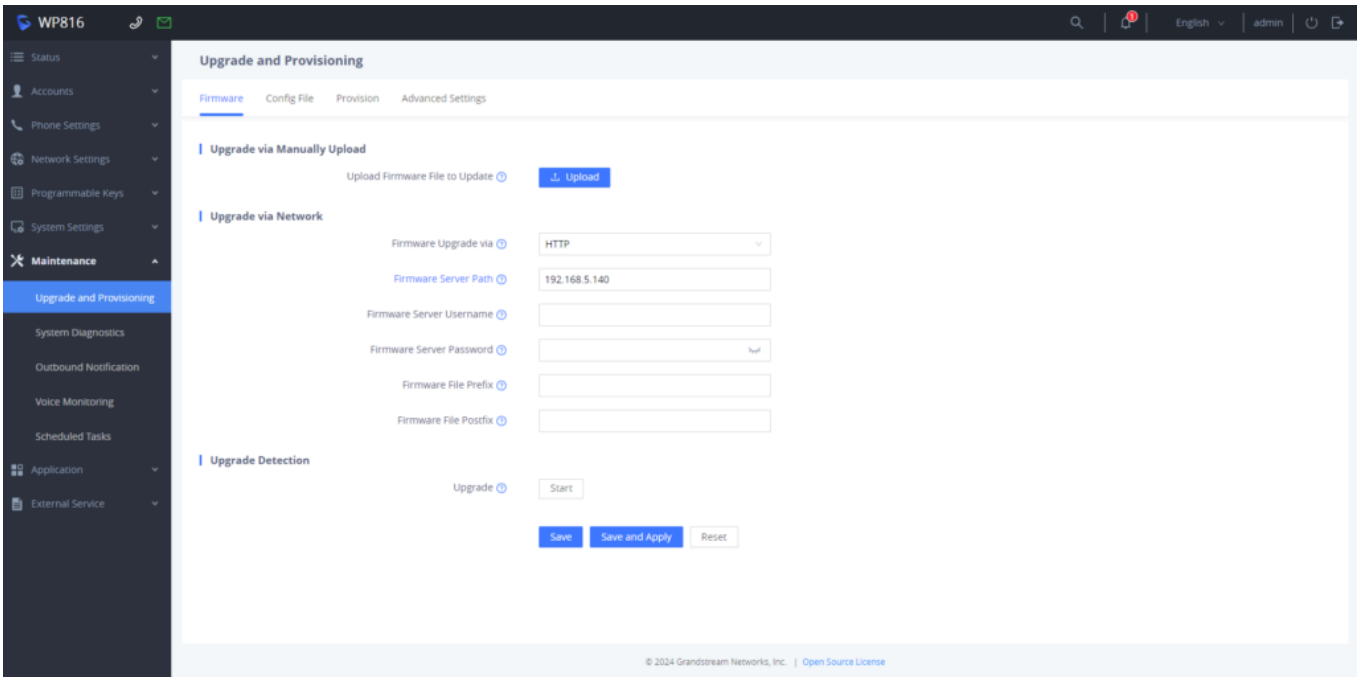


Upgrade detection via Keypad Menu

Configure via Web GUI

Open a web browser on your PC and enter the IP address for the WP8x6. 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, HTTPS, FTP, or FTPS (The default setting is HTTPS). Save and apply the changes or reboot the phone for the upgrade process to begin.

After applying settings, a reboot confirmation pop-up will be displayed for certain configurations



Upgrade Configuration via Web GUI

- Please do not power off or unplug the device when the upgrading process is on.
- In case the wrong firmware file is uploaded or something goes wrong, an error message will be prompted 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 WP8x6 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 WP8x6 to the IP address of the PC.
5. Update the changes and reboot the WP8x6.

Upgrade via Manually Upload

1. Go to **Maintenance** -> **Upgrade and Provisioning -> Firmware -> Upgrade via Manually Upload**, click on the icon .
2. Upload the .bin file downloaded from the official Grandstream firmware website for the corresponding device [WP8x6 in our case]
3. The phone will be rebooted and after that, the new firmware uploaded will be installed.

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, HTTP/HTTPS, or FTP/FTPS. The "Config Server Path" is the TFTP, HTTP, HTTPS, FTP, or FTPS 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. 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 WP8x6 boots up, it will issue a 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 lowercase letters.

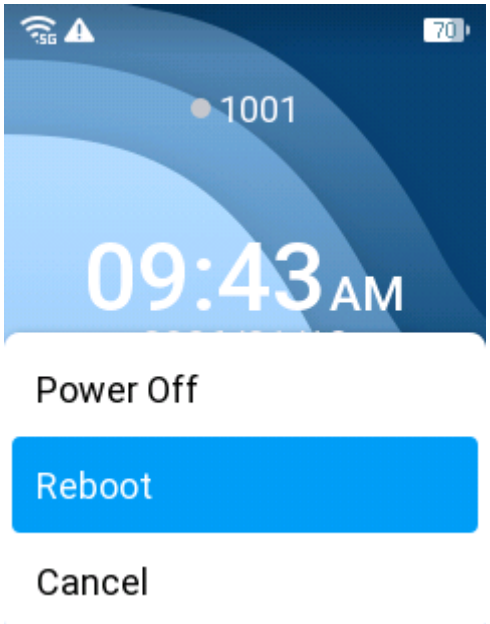
For more details on XML provisioning, please refer to the following document:

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

REBOOT

Reboot through Device keys

To reboot the WP8x6 using the device's touch keys, on idle mode, long press the "offhook" key, until the below menu is displayed, then select the reboot option



Reboot through Device keys

Reboot via SIP NOTIFY

The device supports controlled reboot behavior upon receiving a SIP **NOTIFY** message with the header:

```
Event: Check-Sync
```

This mechanism allows service providers or SIP servers to remotely trigger a reboot for each individual SIP account, enabling account-level management and provisioning synchronization without manual intervention.

When this feature is enabled, the device listens for valid Check-Sync NOTIFY events associated with the configured SIP account and performs a reboot accordingly.

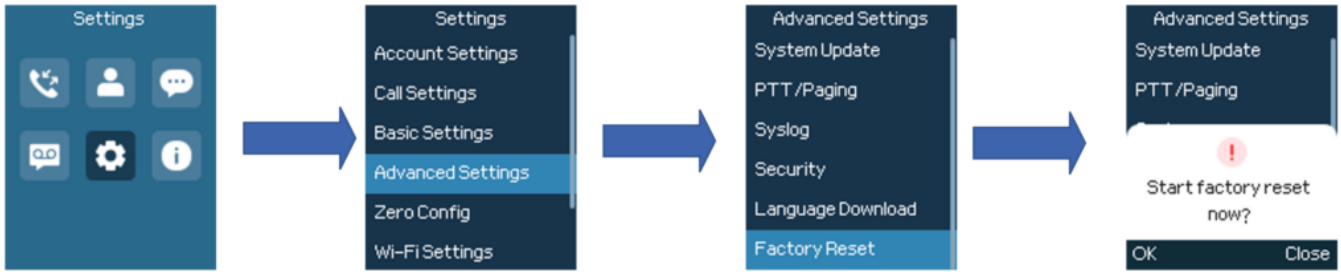
FACTORY RESET

Restore to Factory Default via LCD Menu

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 device to the factory default settings.

1. On the handset idle screen, go to **Settings -> Advanced Settings -> Factory reset**.
2. In the new window, confirm the reset using the left softkey.

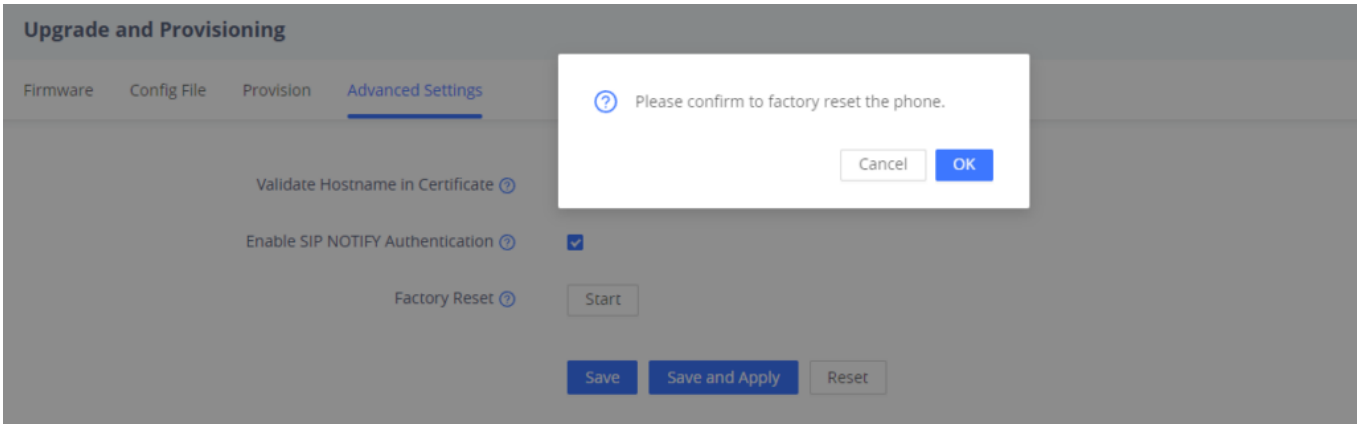


LCD - Confirm Factory Reset

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

Restore to Factory Default via the Web GUI

1. Login to WP8x6 Web GUI and go to **Maintenance -> Tools**.
2. Click on the **Start** button in front of **Factory Reset**.
3. A dialog box will pop up to confirm the factory reset.
4. Click OK to restore the phone to factory settings.



Web GUI - Confirm Factory Reset

ICE Configuration

The ICE (Interactive Connectivity Establishment) feature enables the WP8x6 phone to establish media connections across different network environments by collecting and exchanging candidate addresses during call setup. ICE behavior is configured per account and operates according to the selected media NAT traversal settings and the configured STUN and TURN servers.

The feature supports different candidate collection modes, call fallback behavior, and encrypted media,

depending on configuration and network conditions.

For more information on how the feature works, please visit the guide: **WP8x6 ICE Configuration**

WireGuard Client Configuration

The WireGuard feature enables a the WP8x6 to establish a secure VPN connection to a peer using configured keys, IP addressing, and routing parameters. Once connected, the device can route traffic through the VPN tunnel and reflect the WireGuard client address in system status and application to signal the connection according to the configured settings.

Please refer to the below guide for steps to configure the WP8x6 as WireGuard Client: **WP8x6 WireGuard(R) Client Configuration**

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 1.0.3.40

- Added support for enabling or disabling all configured accounts simultaneously to switch between available and away states. [Quick Start]
- Added support for toggling Away Mode, Bluetooth, and Wi-Fi directly from LCD Quick Access Menu. [Quick Start]

Firmware Version 1.0.3.39

- Added Support of Multicipher Method for OpenVPN. [OPENVPN(R) Cipher Method]
- Added Support Custom Restricted Mode to customize which LCD settings pages need to be restricted. [Custom Restricted Mode] [Custom Constraint Page]
- Added Support to hide 'Send Anonymous' and 'Anonymous Call Rejection' options on LCD menu with Custom Restricted Mode. [Custom Constraint Page]
- Added Support to not allow DHCP Option 150 to override server by default. [Firmware Upgrade via]
- Added Support of "Accept-Language" SIP Header in SIP Message. [Use Accept-Language Header]
- Added Support to configure speaker key audio channel switching mode. [Speaker Key Audio Channel Switching Mode]

Firmware Version 1.0.3.35

- No major changes.

Firmware Version 1.0.3.31

- Added Support to enable or disable trusting CA certificates. [ENABLE TRUST CA CERTIFICATE]
- Added Support to configure the Incoming Call Ring Mode. [INCOMING CALL RING MODE]

Firmware Version 1.0.3.29

- No major changes.

Firmware Version 1.0.3.25

- Added Support for CA Certificate Type. [Network Settings Page Definitions] [Adding a Network via Web UI]

Firmware Version 1.0.3.24

- Added Support to send SIP Log. [SEND SIP LOG]
- Added Support of Phone Ready Indicator. [ENABLE PHONE READY INDICATOR]
- Added the ability to enable or disable the Silent Mode feature activated by long-pressing the * key. [ENABLE

STAR KEY SILENT MODE]

- Added Support of vCard Phonebook. [VCARD PHONEBOOK]
- Added Support of WireGuard(R) Client Maximum Transmission Unit. [WIREGUARD(R) CLIENT MAXIMUM TRANSMISSION UNIT]
- Added Support of WireGuard(R) Peer Preshared Key. [WIREGUARD(R) PEER PRESHARED KEY]
- Added support for up to 10 phone numbers per contact, with multiple entries allowed per category. [Contacts]

Firmware Version 1.0.3.20

- Added support of Enhanced Open (OWE) for Wi-Fi connections. [Enhanced Open]
- Added ability to import and export Calendar from device Web UI. [Calendar]
- Added ability to configure media NAT traversal strategies. [Media NAT Traversal]
- Added support of ICE function. [Enable Trickle ICE] [Candidate Type] [STUN/TURN Server]
- Added support to control the registration retry interval when the server returns 403 Forbidden. [Registration Retry Wait Time(s) upon 403 Forbidden]
- Added support to include Kernel Logs into syslog. [Include Kernel Logs]
- Added support for Key Log functionalities. [Key Log]
- Added support to set Geolocation Header Format.[Geolocation Header Format]
- Added BroadSoft Xsi functionality. [BroadSoft Xsi]
- Added support to set Emergency Call mode. [Emergency Call Way]
- Added support to auto answer emergency call. [Emergency Call Auto Answer]
- Added Support to control reboot when receiving SIP NOTIFY with "Event: Check-Sync" header for each SIP account. [Reboot via SIP NOTIFY] [REBOOT ON CHECK-SYNC EVENT WITHOUT "REBOOT=]
- Added support of WireGuard(R). [WireGuard(R) Settings]
- Added support of PTT headset with for a Type-C interface. [Headset Type]
- Added support of SCEP. [SCEP]
- Added support of DTLS. [DTLS Version]
- Added support of DTLS-SRTP. [SRTP Key Exchange]

Firmware Version 1.0.1.88

- Added support to add Auth Header on Re-register. [Add Auth Header on RE-REGISTER]
- Increased the WPA/WPA2-802.1xand WPA3-802.1x client certificate size limit to 16000 bytes. [ESSID]

Firmware Version 1.0.1.87

- Added Support of Silent Charging. [Enable Silent Charging]
- Added Support to lock the screen during a call. [Lock Screen in Call]
- Added Support to configure IM Designated Account. [IM Designated Account]

Firmware Version 1.0.1.85

- Added Support of Alert-Info Bellcore Mapping. [Enable Alert-Info Bellcore Mapping]
- Added Support to change Hang-up Key End Call mode. [Hang-up Key End Call mode]
- Added Support of Dial DTMF Mode to the custom softkey. [Custom Softkey]

Firmware Version 1.0.1.80

- Added support to filter warning messages. [Custom Filter Warnings Message]

Firmware Version 1.0.1.79

- Added support of WPA3-192 Security mode in Wi-Fi settings. [Security Mode]
- Added support to configure Wi-Fi Roaming Mode. [Wi-Fi Roaming Mode]
- Added support for Roaming Prompt. [Enable Roaming Prompt]
- Increased the contacts group max limit to 50 groups. [Add Group]
- Added support to configure off-screen indicator pattern. [Off Screen Indicator Pattern]
- Added support to have LCD backlight always on under certain situations. [LCD Backlight Always On Scene]

Firmware Version 1.0.1.71

- Added Support of Syslog Header Format. [Syslog Header Format]

Firmware Version 1.0.1.63

- Added Support of SSL Key Log File in One-click debug. [One-click Debug]
- Added Support of OpenVPN failover. [OpenVPN(R) Server Secondary Address][OpenVPN(R) Secondary Port][Randomly Select Server]

Firmware Version 1.0.1.61

- Added support to display call forward destination number on the LCD home screen. [Call Forward Destination Number]
- Added Support to display battery percentage on the LCD. [Display Battery Percentage]
- Added Support to remain LCD backlight at a very low brightness when charging. [LCD Backlight when Missed Calls during Charging]
- Added Support to control the open door prompt confirmation. [Door System]

Firmware Version 1.0.1.52

- Added support of case-sensitive phone book search. [Case Sensitive Search]
- Added support to use "Open Door" Softkey to trigger the DTMF auto-input for other doors. [Door System]
- Added support of Release DHCP On Reboot. [Release DHCP On Reboot]

Firmware Version 1.0.1.44

(This is the initial version for WP836).

- Updated the terms "Blacklist/Whitelist" to "Blocklist/Allowlist" [Web Access Control] [Quick Access]
- Added support to change ringtone for Direct IP call. [Direct IP Call Ringtone]
- Added support for Alarm Settings. [Alarm Settings]
- Added support for AI Noise Cancellation. [AI Noise Cancellation][Icons Description]
- Added option to configure side key as alarm. [Side Key]

Firmware Version 1.0.1.30

- Added Support to disable voicemail pop-up. [Enable Voicemail Popup]

Firmware Version 1.0.1.18

- No major changes.

Firmware Version 1.0.1.14

- No major changes.

Firmware Version 1.0.1.9

- This is the initial version.

(C) 2002-2014 OpenVPN Technologies, Inc. OpenVPN is a registered trademark of OpenVPN Technologies, Inc.