

**Grandstream Networks, Inc.**

---

GHP63x(W)

**Administration Guide**




# GHP63X/W – Administration Guide

## WELCOME

The GHP series of hotel phones feature the GHP630(W) and GHP631(W), easy-to-use IP phones for any hotel room that can be programmed and customized based on the needs of hotels and their guests. The GHP630W and GHP631W models are equipped with integrated dual-band Wi-Fi. The features of the GHP series include an HD speaker, 2 SIP accounts/lines, 6 programmable keys, 10-speed dial keys, 3-way voice conferencing, full band Opus voice codec, and an advanced jitter-resilience algorithm that tolerates up to 30% packet loss without impacting voice quality. The GHP series is supported by the Grandstream Device Management System (GDMS), which provides a centralized interface to configure, provision, manage, and monitor the deployment of Grandstream endpoints. The GHP series IP phones can be installed on a desktop or wall-mounted and can be powered by PoE (GHP630/GHP631), power adapter (GHP630W/GHP631W), and USB Type-C charger. Its elegant and compact design makes it perfect for not only hotels but also hospitals, apartments, dormitories, and much more.

## PRODUCT OVERVIEW

### Feature Highlights

 <p style="text-align: center;"><b>GHP63X/W</b></p>	<ul style="list-style-type: none"> <li>○ 3.5” High-Resolution (480x320) Color LCD Screen</li> <li>○ Integrated dual-band 2.4G/5G 802.11a/b/g/n/ac/ax Wi-Fi 6 (GHP630W &amp; GHP631W only)</li> <li>○ 2 SIP lines with wideband Opus codec.</li> <li>○ 6 programmable keys and 10-speed dial keys to customize different services.</li> <li>○ One 100Mbps network port with PoE (PoE available on GHP630/GHP631).</li> <li>○ Desk/Wall mounted.</li> <li>○ Tolerate up to 30% packet loss without impacting voice quality.</li> <li>○ Supports provision and management via GDMS.</li> <li>○ New voice message and mute LED indicator.</li> <li>○ HAC/VCH (ADA) compliant handset volume boost.</li> <li>○ Magnetic Hook Switch feature.</li> </ul>
---	--

### Technical Specification

- **GHP63X/W**

Protocols/Standards	SIP: SIP RFC3261, TCP/IP/UDP, RTP/RTCP, RTCP-XR, Simple, TLS, SRTP.
Graphic Display	3.5” High-Resolution (480x320) Color LCD
Network Interface	One auto-negotiation 10/100 Mbps ethernet port integrated PoE Class 2
Wi-Fi	GHP630W/GHP631W integrated dual-band 2.4GHz & 5GHz 802.11 a/b/g/n/ac/ax

<b>Keypad</b>	<p>26 keys, including:</p> <ul style="list-style-type: none"> <li>-6 Context-Sensitive Soft keys;</li> <li>-12 Standard Phone Digits keys (0-9: speed dial keys configuration on web page, * , #);</li> <li>-5 Function keys (Flash, Redial, Hands-free, Voice Mail, Hold);</li> <li>-3 Volume Control keys, Up/Down/Mute (with red color LED)</li> </ul>
<b>HD Audio</b>	One HD handset support for wide band audio
<b>Voice Conference</b>	2 SIP accounts and lines, up to 3-way conference
<b>Voice Codecs</b>	Support for G.729A/B, G.711μ/a-law, G.726, G.722 (wide-band), G.723, iLBC, full band Opus, Inband and out-of-band DTMF (in audio, RFC2833, SIP INFO), VAD, AEC, CNG, PLC, AGC, AJB
<b>Voice Capabilities</b>	Dial, Answer, Redial, Flash ,Hands-free, Voice Mail(with the server), Transfer, Conference, Hold/Unhold, Mute /Unmute, flexible dial plan, Speed dial server redundancy & fail-over Call out
<b>Telephony Features</b>	Dial, Answer, Redial, Flash, Hands-free, Voice mail (with the server) Hold/Unhold, Mute/Unmute, flexible dial plan, Speed dial server redundancy, fail-over Call out.
<b>Advanced Features</b>	<p>Support for multicast paging and E911 service.</p> <p>Support GDS Door opening.</p> <p>Support for advanced jitter-resilience algorithm.</p>
<b>USB</b>	USB Type-C port for charging external devices (500mA MAX)
<b>QoS</b>	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
<b>Security</b>	Secure boot, random default password, unique security certificate per device, administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x media access control
<b>Multi-language</b>	English, Spanish, French, Chinese (pending)
<b>Upgrade/Provisioning</b>	Firmware upgrade via FTP / TFTP / HTTP / HTTPS, fast boot in 15 seconds, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
<b>Power &amp; Green Energy Efficiency</b>	<p>Universal power adapter (GHP630W/GHP631W):</p> <p>Input: 100~240Vac 50~60Hz</p> <p>Output: 12V/0.5A(6W)</p>
<b>Temperature and Humidity</b>	<p>Operation: 0°C to 40°C</p> <p>Storage: -10°C to 60°C</p> <p>Humidity: 10% to 90% (Non-condensing)</p>
<b>Package Content</b>	GHP phone, handset with cord, Base Stand, universal power supply (GHP630W, GHP631W), faceplate, Quick Installation Guide
<b>Color</b>	White (GHP630,GHP630W), Black (GHP631,GHP631W)
<b>Physical</b>	<p>Unit size:210mm(L)*147mm(W)*89.8mm(H) (with handset and base stand)</p> <p>Unit weight: 601g (GHP630/GHP631), 658g (GHP630W/GHP631W US), 668g (GHP630W/GHP631W World)</p> <p>Package weight: 824g (GHP630/GHP631), 881g (GHP630W/GHP631W US),891g (GHP630W/GHP631W World)</p>
<b>GHP630 &amp; GHP631 Compliance</b>	<p><b>FCC:</b> Part 15 Subpart B, Class B; Part 68. 316/317.</p> <p><b>CE:</b> EN 55032; EN 55035; EN IEC 61000-3-2; EN 61000-3-3; EN IEC 62368-1.</p> <p><b>UKCA:</b> BS EN 55032; BS EN 55035; BS EN IEC 61000-3-2; BS EN 61000-3-3; BS EN 62368-1.</p>

## GHP630W & GHP631W Compliance

**RCM:** AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004.  
**IC:** ICES-003; CS-03 Part V.

**FCC:** Part 15 Subpart B, Class B; Part 15 Subpart C, 15.247; Part 15 Subpart E, 15.407; Part 68.316/317.

**CE:** EN 55032; EN 55035; EN IEC 61000-3-2; EN 61000-3-3; EN IEC 62368-1; ETSI EN 301489-1-17; ETSI EN 300 328; ETSI EN 301 893; EN IEC 62311.

**UKCA:** BS EN 55032; BS EN 55035; BS EN IEC 61000-3-2; BS EN 61000-3-3; BS EN 62368-1; ETSI EN 301489-1-17; ETSI EN 300 328; ETSI EN 301 893; BS EN IEC 62311.

**RCM:** AS/NZS CISPR32; AS/NZS 4268; AS/NZS 2772.2; AS/NZS 62368.1; AS/CA S004.

**IC:** RSS-247; RSS-Gen; RSS-102; ICES-003; CS-03 Part V.

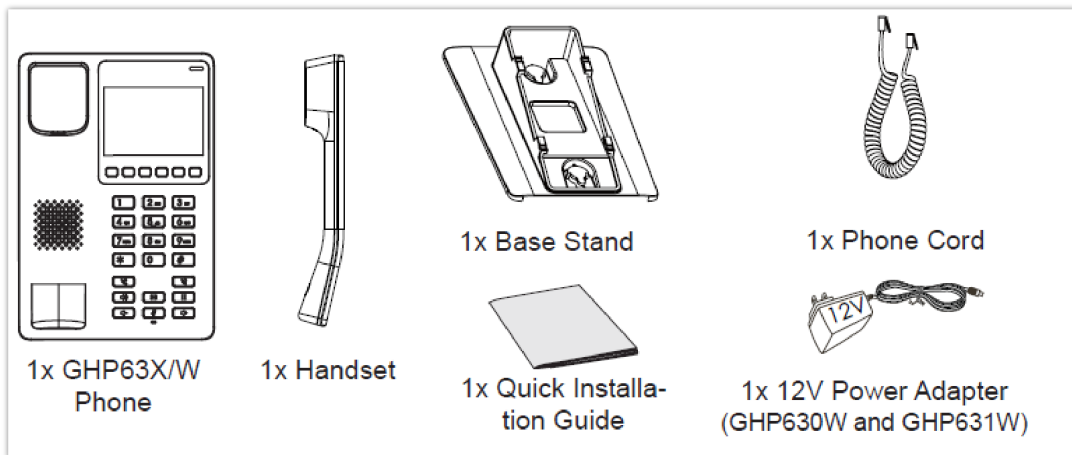
## GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the GHP63X/W.

### Equipment Packaging

#### GHP63X/W

GHP63X/W
<ul style="list-style-type: none"><li>● 1x GHP63X/W Phone</li><li>● 1x Handset</li><li>● 1x Base Stand</li><li>● 1x Quick Installation Guide</li><li>● 1x Phone Cord</li><li>● 1x 12V Power Adapter (GHP630W and GHP631W)</li></ul>



*GHP63x/W Package Content*

#### Note

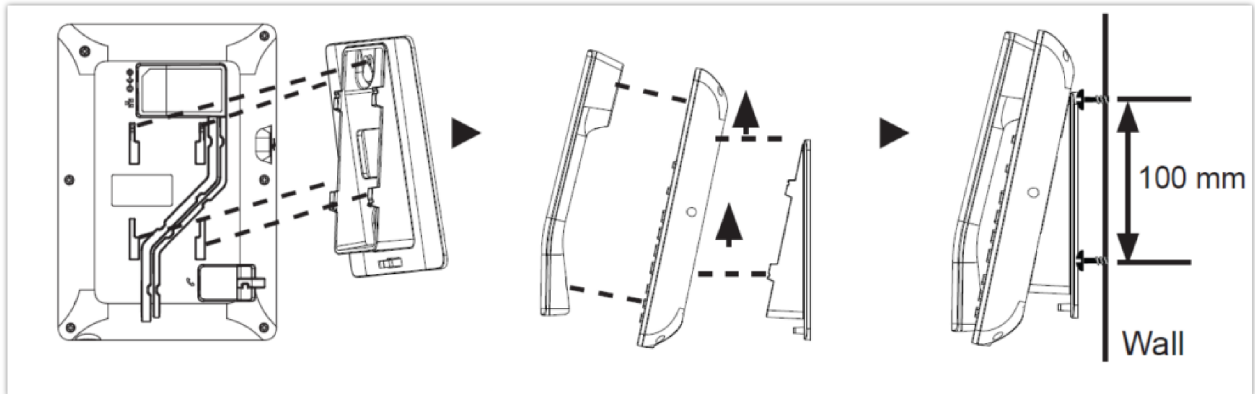
Please check the package before installation. If you find any one of the components missing, please contact your system administrator.

### GHP63X/W Phone Setup

The GHP63X/W can be installed on the desk or can be mounted on the wall. Please follow the instructions below for each installation method

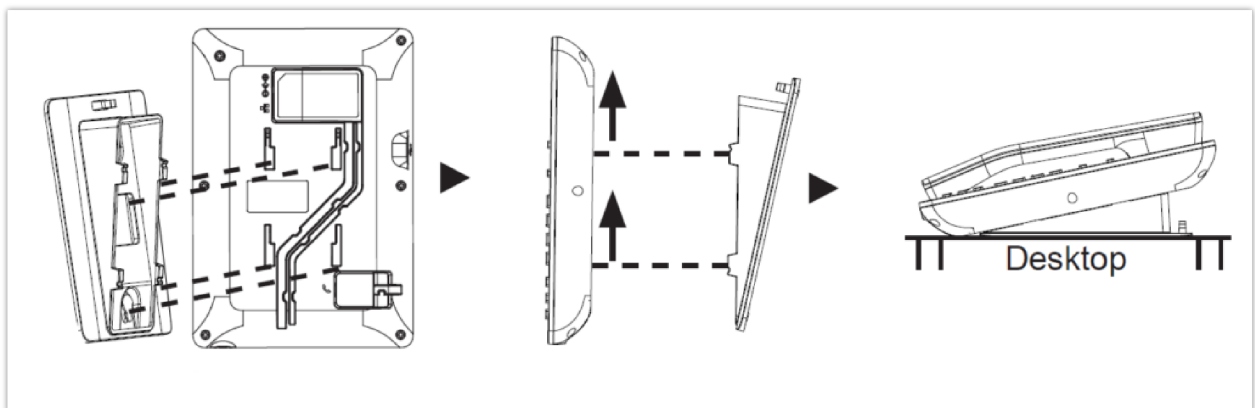
## Wall Mount

1. On the wall where the GHP630/W & GHP631/W will be mounted, mark two dots with 100mm distance in between vertically.
2. Using a drill, make a hole on each marked dot. Put a plastic expansion bolt and screw (not provided) into each hole. Leave enough space on the screws to mount the GHP630/W & GHP631/W.
3. Attach the wall mount spacers to the slot for wall mount spacers on the back of the phone.
4. Mount the GHP630/W & GHP631/W on the screws using its "Wall Mount Slots".



## Desktop Installation

For installing the phone on the table with the phone stand, attach the phone stand to the bottom of the phone where there is a slot for the phone stand.

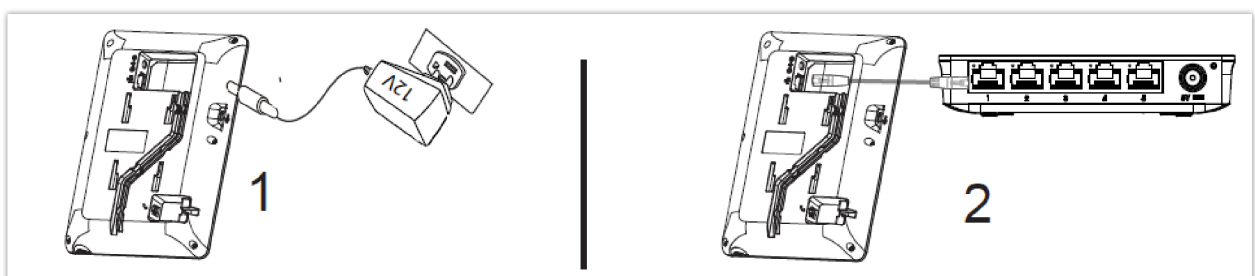


*GHP63X Desktop Mount*

## Power on the phone

To power on the GHP630/W & GHP631/W:

1. For **GHP630W & GHP631W**: Connect the 12V DC output plug to the power jack on the phone; plug the power adapter into an electrical outlet.
2. For **GHP630 & GHP631**: A PoE switch can be used to power up the device without the need of the 12V power adapter.



*Power on the phone*

## Connecting the GHP63X/W

To set up the phone, follow the steps below:

1. Plug in the phone cord to the handset RJ9 port and then connect it to the base.
2. Connect the LAN port of the phone to the RJ45 socket of a hub/switch or a router (LAN side of the router) using the Ethernet cable. This step can be skipped if using GHP630W & GHP631W with Wi-Fi.

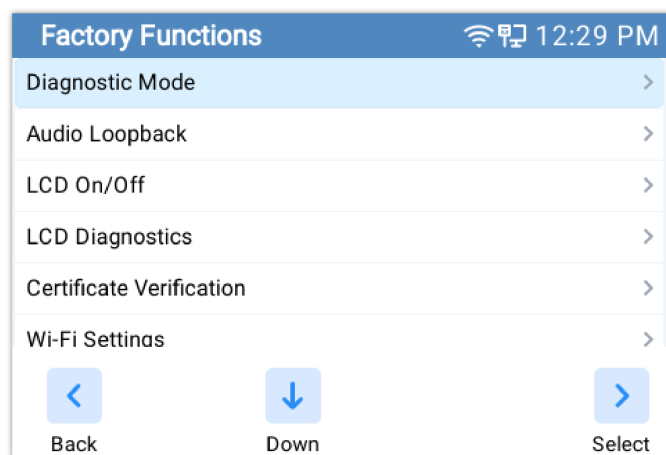
### Note

For easy deployment, the GHP63x/W is out-of-the-box pre-configured to connect to default SSID named **wp\_master** with a password (WPA/WPA2 PSK) equal to **wp!987@dmin**, users can adapt these settings from the web UI as well to make it easier for deployment on a customer's site.

## Display factory functions

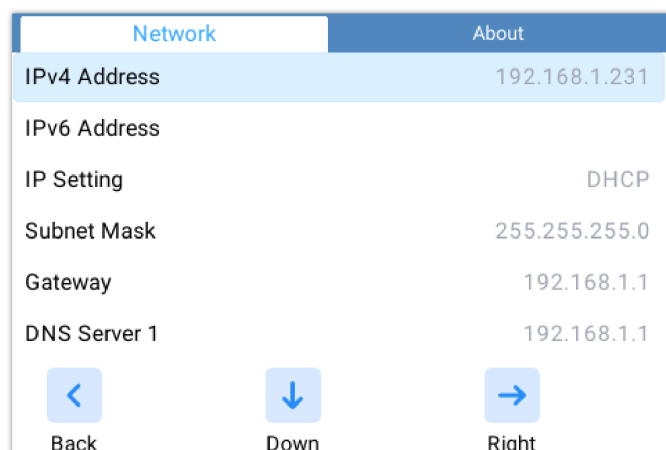
To display factory functions

- o Make sure your phone is powered on
- o Press the **"HOLD" + 2** at the same time, to display the factory functions (including Wi-Fi settings for GHP631W/GHP630W version only)

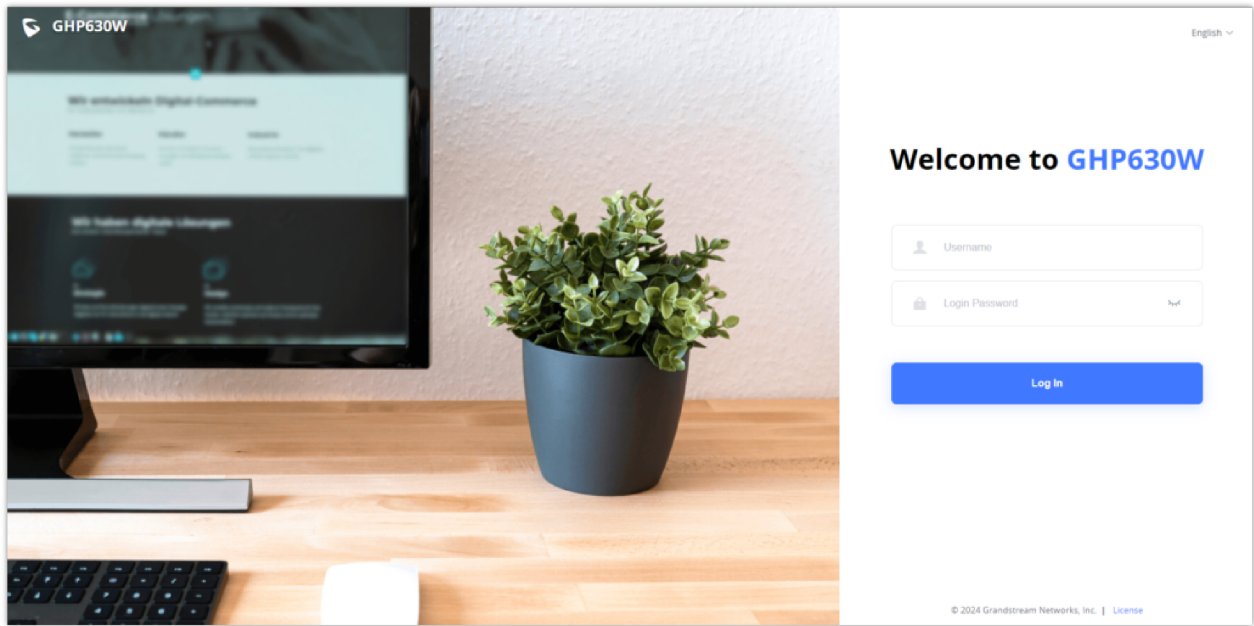


## Phone Configuration Via Web Browser

- o Ensure your phone is powered up and connected to the network.
- o Locate the MAC address on the bottom of the device or the package.
- o From a computer connected to the same network as the GHP63X, Do one of the following:
  1. Type in the following address using the GHP63X's MAC address on your browser: <https://<mac>.local> (Example: <https://c074adffffff.local>)
  2. Press the **"HOLD" + 0** at the same time, to display its local IP address and use it to access the Web UI



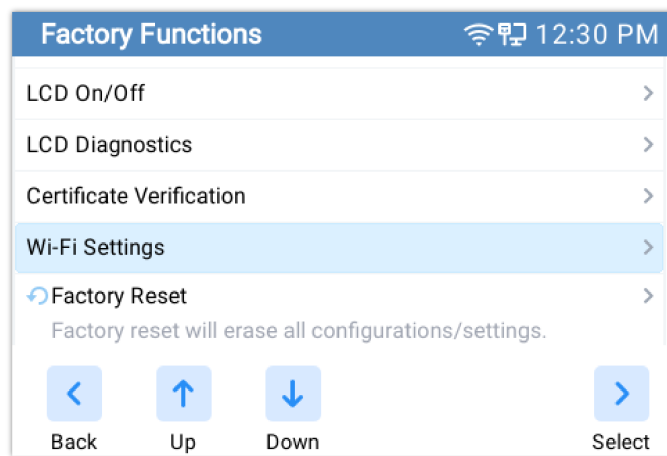
- Enter the admin’s username and password to access the configuration menu. (The factory default username is “admin” while the default random password can be found on the sticker at the back of the unit).



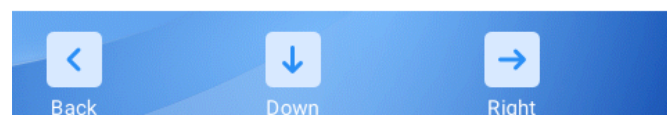
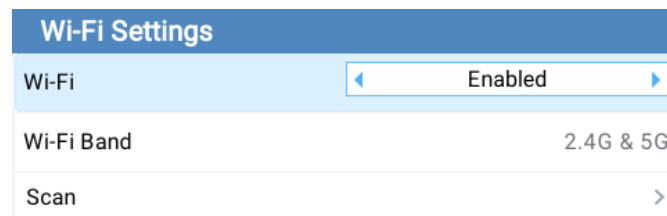
### Connect to Wi-Fi (only for GHP630W/GHP631W)

To connect to Wi-Fi from your GHP63xW device, follow the below steps:

- Press “**HOLD**” + 2 to access the factory functions of the GHP63x/W from the LCD
- Go to **Factory Functions** → **Wi-Fi Settings**



- Enable Wi-Fi, Select the Wi-Fi Band (2.4G, 5G, or both), and scan for nearby networks



- Once the desired network is discovered you can connect to it by providing its password key if available.

# CONFIGURATION GUIDE

## Status Page Definitions

<b>Status → Account Status</b>	
<b>Account Status</b>	This interface indicates the information of the accounts which are configured on the IP phone.
<b>Status → Network Status</b>	
<b>Ethernet</b>	
<b>MAC Address</b>	This field indicates the MAC address of the device.
<b>IPv4 Address Type</b>	This field indicated whether the obtained IP address was configured by DHCP or set statically.
<b>IPv4 Address</b>	This field indicates the IP address allocated to the IP phone.
<b>Gateway</b>	This field indicates the default gateway allocated.
<b>IPv4 NAT Type</b>	This field indicates the type of NAT of the network.
<b>IPv6 Address</b>	This field indicates the IPv6 IP address allocated.
<b>Global Unicast Address</b>	This field indicates the global unicast address.
<b>Link-Local Address</b>	This field indicates the IPv6 unicast address.
<b>IPv6 Static Gateway</b>	This field indicates the IPv6 static gateway address.
<b>IPv6 DUID</b>	This field indicates the DHCP unique identifier.
<b>IPv6 NAT Type</b>	This field indicates the IPv6 NAT type.
<b>Wi-Fi (Only for GHP63xW)</b>	
<b>WLAN MAC Address</b>	This field indicates the WLAN MAC Address.
<b>SSID</b>	This field indicates the SSID that the device is connected to.
<b>Country Code</b>	This field indicates the Country Code.
<b>IPv4 Address Type</b>	This field indicates the IPv4 Address Type, dynamic or static.
<b>IPv4 Address</b>	This field indicates the IPv4 Address.
<b>Gateway</b>	This field indicates the Gateway IP Address.
<b>IPv4 NAT Type</b>	This field indicates the IPv4 NAT Type.



<b>IPv6 Address Type</b>	This field indicates the IPv6 NAT Type.
<b>Global Unicast Address</b>	This field indicates the Global Unicast Address.
<b>Link-Local Address</b>	This field indicates the Link-Local Address, this is an automatically assigned IP address for local network communication without the need for a DHCP server.
<b>IPv6 Static Gateway</b>	This field indicates a manually configured gateway address used for routing traffic on an IPv6 network.
<b>IPv6 DUID</b>	This field indicates the IPv6 DUID, An IPv6 DUID (DHCP Unique Identifier) is a unique identifier assigned to a device by a DHCPv6 server for network configuration and identification purposes.
<b>IPv6 NAT Type</b>	This field indicates the IPv6 NAT Type, IPv6 NAT Type refers to the Network Address Translation (NAT) configuration used for IPv6 connections, which may vary based on the network setup and the type of NAT employed.
<b>DNS &amp; NAT</b>	
<b>DNS Server</b>	Displays the DNS Server and back up DNS server used.
<b>DNS Mode</b>	Displays the DNS Mode used for both accounts.
<b>NAT Traversal</b>	Displays whether NAT Traversal is enabled or not, for both accounts.
<b>Status → System Info</b>	
<b>Information</b>	
<b>Product model</b>	This field indicates the product model.
<b>Part number</b>	This field indicates the part number.
<b>Serial Number</b>	Displays the GHP6xx's Serial Number.
<b>Certificate Type</b>	Displays the certificate type.
<b>Software version</b>	This field indicates the version of the firmware installed.
<b>Language</b>	This field indicates the language used for displaying the web user interface.
<b>Recommended Time Zone</b>	This field indicates the recommended time zone.
<b>System Up Time</b>	This field indicates how long the devices has been turned on.
<b>System Time</b>	This field indicates the time and date set on the system.
<b>System Time Zone</b>	This field indicates the system time zone configured on the device.
<b>Download System Information</b>	This option allows downloading all the the system information.
<b>Capture Screen</b>	Captures a screenshot from the phone LCD, by clicking the start button, once completed, the exact date and time of the screenshot will be displayed along the button that allows the screenshot download

<b>Clear Screenshots</b>	Deletes the latest screenshot taken
<b>Service Status</b>	Displays information about the service status, by displaying parameters such as the gui memory usage, the phone memory usage, and the cpe memory usage
<b>Core Dump</b>	Refers to the process of saving the contents of the phone's memory (RAM) to a storage medium, when a program or the encounters a critical error or crash. Core dumps are useful for developers and system administrators because they provide a snapshot of the program's state at the time of the crash.

## Account Page Definitions

### Basic Settings

<b>Account Register</b>	
<b>Account Active</b>	Indicates whether the account is active. The default setting is "No".
<b>Account Name</b>	The name associated with each account to be displayed on the LCD. (e.g., MyCompany)
<b>SIP Server</b>	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)
<b>Secondary SIP Server</b>	The URL or IP address, and port of the SIP server. This will be used when the primary SIP server fails
<b>Outbound Proxy</b>	IP address or Domain name of the Primary Outbound Proxy, Media Gateway, or Session Border Controller. If a symmetric NAT is detected, STUN will not work and ONLY an Outbound Proxy can provide a solution
<b>Secondary Outbound Proxy</b>	Defines secondary outbound proxy that will be used when the primary proxy cannot be connected.
<b>SIP User ID</b>	User account information, provided by your VoIP service provider.
<b>SIP Authentication ID</b>	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
<b>SIP Authentication Password</b>	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.
<b>Name</b>	The SIP server subscriber's name (optional) that will be used for Caller ID display (e.g., John Doe).
<b>TEL URI</b>	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.
<b>Voice Mail Access Number</b>	Allows users to access voice messages by pressing the MESSAGE button on the phone. This value is usually the VM portal access number.
<b>Network Settings</b>	
<b>DNS Mode</b>	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.  <ul style="list-style-type: none"> <li>● A Record</li> </ul>

	<ul style="list-style-type: none"> <li>• SRV</li> <li>• NAPTR/SRV</li> <li>• Use Configured IP</li> </ul>
<b>Maximum Number of SIP Request Retries</b>	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.
<b>DNS SRV Failover Mode</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> If the option is set with “default”, it will again try to send register messages to one IP at a time, and the process repeats.</li> <li>• <b>Saved one until DNS TTL:</b> If the option is set with “Saved one until DNS TTL”, it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up.</li> <li>• <b>Saved one until no responses:</b> If 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.</li> <li>• <b>Failback follows failback expiration timer:</b> 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.</li> </ul>
<b>Failback Expiration (m)</b>	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.
<b>Register Before DNS SRV Failover</b>	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.
<b>Primary IP</b>	Configures the primary IP address where the phone sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>Backup IP 1</b>	Configures the backup IP 1 address where the phone sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>Backup IP 2</b>	Configures the backup IP 2 address where the phone sends DNS query to when “Use Configured IP” is selected for DNS mode.
<b>NAT Traversal</b>	<p>Set NAT traversal to activate the NAT penetration mechanism.</p> <p>options to be chosen are No, STUN, or Keep-Alive.</p> <ul style="list-style-type: none"> <li>• When set to "STUN" and the STUN server address is specified, detection will be based on the STUN server.</li> <li>• When set to "Keep-alive", messages can be configured to be sent at regular intervals, such as every few minutes, and can be customized with specific packet content and timing parameters to optimize performance in different network environments.</li> </ul> <p>The Default value is set to "No".</p>
<b>Support rport (RFC3581)</b>	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.
<b>Proxy-Require</b>	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall.

## SIP Settings

<b>Basic Settings</b>	
<b>SIP Registration</b>	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is “Enabled”.
<b>UNREGISTER on Reboot</b>	<ul style="list-style-type: none"> <li>• If set to “<b>No</b>”, the phone will not unregister the SIP user’s registration information before new registration.</li> <li>• If set to “<b>All</b>”, the SIP Contact header will use “*” to clear all SIP user’s registration information.</li> <li>• If set to “<b>Instance</b>”, the phone only needs to clear the current SIP user’s info.</li> </ul>
<b>REGISTER Expiration</b>	<p>Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar.</p> <p>The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.</p>
<b>SUBSCRIBE Expiration</b>	<p>Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar.</p> <p>The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.</p>
<b>Re-Register before Expiration</b>	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default value is 0.
<b>Registration Retry Wait Time</b>	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
<b>Add Auth Header on Initial REGISTER</b>	If enabled, the phone will add Authorization header in initial REGISTER request. Default is “Disabled”.
<b>Enable OPTIONS Keep Alive</b>	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”.
<b>OPTIONS Keep Alive Interval</b>	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.
<b>OPTIONS Keep Alive Max Tries</b>	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.
<b>SUBSCRIBE for MWI</b>	When set to “Yes”, a SUBSCRIBE for Message Waiting Indication will be sent periodically. The default setting is “No”.
<b>SUBSCRIBE for Registration</b>	When set to “Yes”, a SUBSCRIBE for Registration will be sent out periodically. The default setting is “No”.
<b>Use Privacy Header</b>	<p>Configures whether the “Privacy Header” is present in the SIP INVITE message.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> the phone will add “Privacy Header” when special feature is not “Huawei IMS”.</li> <li>• <b>Yes:</b> the phone will always add “Privacy Header”.</li> <li>• <b>No:</b> the phone will not add “Privacy Header”.</li> </ul> <p>The default setting is “default”.</p>
<b>Use P-Preferred- Identity Header</b>	<p>Configures whether the “P-Preferred-Identity Header” is present in the SIP INVITE message.</p> <ul style="list-style-type: none"> <li>• <b>Default:</b> the phone will add “P-Preferred-Identity header” when special feature is not “Huawei IMS”.</li> <li>• <b>Yes:</b> the phone will always add “P-Preferred-Identity header”.</li> <li>• <b>No:</b> the phone will not add “P-Preferred-Identity header”.</li> </ul>

<b>Use X-Grandstream-PBX Header</b>	Configures to use X-Grandstream-PBX header in SIP request. Default setting is “Yes”.
<b>Use P-Access-Network-Info Header</b>	Configures to use P-Access-Network-Info header in SIP request. Default setting is “Yes”.
<b>Use P-Emergency-Info Header</b>	Configures to use P-Emergency-Info header in SIP request. Default setting is “Yes”.
<b>Use MAC Header</b>	<ul style="list-style-type: none"> <li>• If <b>Register Only</b>, all outgoing SIP message will include the MAC header.</li> <li>• If <b>Yes to all SIP</b>, all outgoing SIP messages will include the MAC header.</li> <li>• If <b>No</b>, the phone’s MAC header will not be included in any outgoing SIP messages.</li> </ul> <p>The default setting is “No”.</p>
<b>Add MAC in User-Agent</b>	<ul style="list-style-type: none"> <li>• If <b>Yes except REGISTER</b>, all outgoing SIP messages will include the phone’s MAC address in the User-Agent header, except for REGISTER and UNREGISTER.</li> <li>• If <b>Yes to All SIP</b>, all outgoing SIP messages will include the phone’s MAC address in the User-Agent header.</li> <li>• If <b>No</b>, the phone’s MAC address will not be included in the User-Agent header in any outgoing SIP messages.</li> </ul> <p>The default setting is “No”.</p>
<b>SIP Transport</b>	Selects the network protocol used for the SIP transport. The default setting is “UDP”.
<b>Enable TCP Keep-alive</b>	Configures whether to enable TCP Keep-alive for the TCP connection between the terminal and the SIP server.
<b>SIP Listening Mode</b>	Configures whether or not to listen to multiple SIP protocols. <ul style="list-style-type: none"> <li>• If set to “<b>Dual</b>”, phone will listen to TCP when UDP is selected.</li> <li>• If set to “<b>Dual (Secured)</b>”, phone will listen to TLS/TCP when UDP is selected. If “TCP” or “TLS/TCP” is selected, UDP will be listened too.</li> <li>• If set to “<b>Dual (BLF Enforced)</b>”, phone will try to enforce BLF subscriptions to use TCP protocol by adding ‘transport=tcp’ to the Contact header.</li> </ul> <p>The default setting is “Transport Only”.</p>
<b>Local SIP Port</b>	Configures the local SIP port used to listen and transmit.
<b>SIP URI Scheme when using TLS</b>	Specifies if “sip” or “sips” will be used when TLS/TCP is selected for SIP Transport. The default setting is “sips”.
<b>Use Actual Ephemeral Port in Contact with TCP/TLS</b>	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”.
<b>Support SIP Instance ID</b>	Configures whether SIP Instance ID is supported or not. The default setting is “Yes”.
<b>SIP T1 Timeout</b>	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.
<b>SIP T2 Timeout</b>	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.

<b>Outbound Proxy Mode</b>	<p>Configures whether to put the Outbound Proxy in the Route header, or if SIP messages should always be sent to Outbound Proxy.</p> <ol style="list-style-type: none"> <li>1. <b>In route</b></li> <li>2. <b>Not in route</b></li> <li>3. <b>Always send to</b></li> </ol> <p>Default is “in route”.</p>
<b>Enable 100rel</b>	<p>When enabled, the 100rel tag is appended to the value of the Supported header of the initial signaling messages.</p> <p>The default setting is “No”.</p>
<b>Use Route Set in Notify (Follow RFC 6665)</b>	<p>Configures whether to use route set in NOTIFY (follow RFC 6665).</p> <ul style="list-style-type: none"> <li>• If enabled, the Request URI of the refresh subscription will use the URI in the received NOTIFY Contact (RFC 6665).</li> <li>• If disabled, the URI in the previously subscribed 200 OK Contact will be used.</li> </ul>
<b>Session Timer</b>	
<b>Enable Session Timer</b>	<p>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.</p> <p>The default setting is “No”.</p>
<b>Session Expiration</b>	<p>Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand.</p> <p>The default setting is 180. The valid range is from 90 to 64800.</p>
<b>Min-SE</b>	<p>The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.</p>
<b>Caller Request Timer</b>	<p>If set to “Yes” and the remote party supports session timers, the phone will use a session timer when it makes outbound calls.</p> <p>The default setting is “No”.</p>
<b>Callee Request Timer</b>	<p>If set to “Yes” and the remote party supports session timers, the phone will use a session timer when it receives inbound calls.</p> <p>The default setting is “No”.</p>
<b>Force Timer</b>	<p>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.</p> <p>The default setting is “No”.</p>
<b>UAC Specify Refresher</b>	<p>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.</p> <p>The default setting is “UAC”.</p>
<b>UAS Specify Refresher</b>	<p>As a callee, select UAC to use caller or proxy server as the refresher, or select UAS to use the phone as the refresher.</p> <p>The default setting is “UAC”.</p>
<b>Force INVITE</b>	<p>Select “Yes” to force using the INVITE method to refresh the session timer.</p> <p>The default setting is “No”.</p>

## Codec Settings

<b>Audio</b>	
<b>Preferred Vocoder (Choice 1 – 8)</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• Opus</li> <li>• G722</li> <li>• PCMU</li> <li>• PCMA</li> <li>• G.723.1</li> <li>• G.729.1</li> <li>• iLBC</li> <li>• G.726-32</li> </ul>
<b>Codec Negotiation Priority</b>	<p>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”.</p>
<b>Use First Matching Vocoder in 200OK SDP</b>	<p>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”.</p>
<b>iLBC Frame Size</b>	<p>Selects iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is “30ms”.</p>
<b>iLBC Payload Type</b>	<p>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”.</p>
<b>G.726-32 Packing Mode</b>	<p>Selects “ITU” or “IETF” for G726-32 packing mode. The default setting is “ITU”.</p>
<b>G.726-32 Dynamic Payload Type</b>	<p>Specifies G.726-32 payload type. Valid range is 96 to 127. Default is 127.</p>
<b>Opus Payload Type</b>	<p>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.</p>
<b>Send DTMF</b>	<p>Specifies the mechanism to transmit DTMF digits. There are 3 supported modes:</p> <ol style="list-style-type: none"> <li>1. <b>In audio</b>: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs).</li> <li>2. <b>RFC2833</b> sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed.</li> <li>3. <b>SIP INFO</b> uses SIP INFO to carry DTMF.</li> </ol> <p>Default setting is “RFC2833”.</p>
<b>DTMF Payload Type</b>	<p>Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.</p>
<b>Enable Audio RED with FEC</b>	<p>If set to “Yes”, FEC will be enabled for audio call. If set to “Yes”, FEC will be enabled for audio call.</p>
<b>Silence Suppression</b>	<p>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”.</p>
<b>Jitter Buffer Type</b>	<p>Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is “Adaptive”.</p>
<b>Jitter Buffer Length</b>	<p>Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is</p>

	“300ms”.
<b>Voice Frames Per TX</b>	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.
<b>G.723 Rate</b>	Selects encoding rate for G723 codec.
<b>RTP Settings</b>	
<b>SRTP Mode</b>	Enable SRTP mode based on your selection from the drop-down menu. <ul style="list-style-type: none"> <li>• No</li> <li>• Enabled but Not forced</li> <li>• Enabled and Forced</li> <li>• Optional</li> </ul> The default setting is “No”.
<b>SRTP Key Length</b>	Allows users to specify the length of the SRTP calls. Available options are: <ul style="list-style-type: none"> <li>• <b>AES 128&amp;256 bit</b></li> <li>• <b>AES 128 bit</b></li> <li>• <b>AES 256 bit</b></li> </ul> Default setting is AES 128&256 bit
<b>Crypto Life Time</b>	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”.
<b>RTCP Mode</b>	Configure RTCP port negotiation rules. <ul style="list-style-type: none"> <li>• <b>Default:</b> Use the traditional RTCP port, which is "RTP port+1".</li> <li>• <b>Negotiate RTCP Port:</b> Use attribute RTCP to negotiate.</li> <li>• <b>RTCP Mux:</b> The caller actively negotiates the RTCP port and indicates RTCP Mux at the same time.</li> <li>• <b>RTCP Mux Only:</b> The caller forces RTCP Mux, generated by the local media port only apply for RTP port.</li> </ul>
<b>RTCP Keep-Alive Method</b>	Configures the RTCP channel keep-alive packet type. <ul style="list-style-type: none"> <li>• <b>Receiver Report:</b> The RTCP channel will sends "receiver report+source description+RTCP extension" as keep-alive data.</li> <li>• <b>Sender Report:</b> The RTCP channel will sends "Sender report+source description+ RTCP extension" as keep-alive data.</li> </ul>
<b>RTP Keep-Alive Method</b>	Configures the RTP channel keep-alive packet type. <ul style="list-style-type: none"> <li>• <b>No:</b> No data will be sent</li> <li>• <b>RTP Version 1:</b> The wrong version infor "1" will be carried when sending RTP data packets.</li> </ul>
<b>Symmetric RTP</b>	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”.
<b>RTP Timeout (s)</b>	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 Call Settings

General	
<b>Key as Send</b>	Pressing the selected key will immediately dial out.
<b>No Key Entry Timeout</b>	Configures the timeout (in seconds) for no key entry. If no key has been pressed after the timeout, the collected digits will be sent out.
<b>Send Anonymous</b>	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous.
<b>Anonymous Call Rejection</b>	If set to "Yes", anonymous calls will be rejected.
<b>Enable Call Waiting</b>	Enables the call waiting feature. If set to "No", new incoming calls will be rejected after the call is established.
<b>RFC2543 Hold</b>	If set to "Yes", c=0.0.0.0 will be used in INVITE SDP for hold.
<b>Ring Timeout</b>	Configures the timeout (in seconds) for the phone to ring when an incoming call is not answered. Valid range is 30 to 3600.
Auto Answer	
<b>Auto Answer</b>	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".
<b>Auto Answer Numbers</b>	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	
<b>Play warning tone for Auto-Answer Intercom</b>	If enabled, phone will play warning tone when auto answering intercom.
<b>Custom Alert-Info for Auto Answer</b>	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.
<b>Allow Auto Answer by Call-Info/Alert-Info</b>	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".
<b>Allow Barging by Call-Info/Alert-Info</b>	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".
<b>Mute on Intercom Answer</b>	If enabled, the phone will mute the microphone after answering an intercom call via Call-Info/Alert-Info.
Transfer	
<b>Transfer on Conference Hangup</b>	Configures whether the call is transferred to the other party if the conference initiator hangs up.

<b>Enable Local Call Features</b>	When enabled, the phone will use the local call function, dial *87 plus number to use local blind forwarding; When disable, the server-side call function code will be used. Enabled by Default.
<b>Enable Recovery on Blind Transfer</b>	Enable Recovery to the call to the transferee on failing blind transfer to the target.
<b>Blind Transfer Wait Timeout</b>	Configures the timeout (in seconds) when waiting for sipfrag response in blind transfer. Valid range is 30 to 300
<b>Refer-To Use Target Contact</b>	If enabled, the "Refer-to" hear uses the transferred target's Contact header information for attended transfer.
<b>Dial plan</b>	
<b>Dial Plan Prefix</b>	Configures a prefix added to all numbers when making outbound calls.
<b>Bypass Dial Plan</b>	<p>Bypass the dial plan when dialing from one of the available items:</p> <ul style="list-style-type: none"> <li>• <b>Contacts</b></li> <li>• <b>Call History Incoming Call</b></li> <li>• <b>Call History Outgoing Call</b></li> <li>• <b>Dialing Page</b></li> <li>• <b>MPK</b></li> <li>• <b>API</b></li> </ul>
<b>Dial Plan</b>	<p>Configures the dial plan rule. For syntax and examples, please refer to user manual for more details. Dial Plan Rules:</p> <ol style="list-style-type: none"> <li>1. Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d;</li> <li>2. Grammar: x – any digit from 0-9;</li> <li>3. Grammar: X – any character from 0-9, a-z, A-Z.</li> <li>4. xx+ – at least 2 digit numbers</li> <li>5. xx – only 2 digit numbers</li> <li>6. XX – two characters ( AA, Ab, 1C, f5, 68,...)</li> <li>7. test : only string “test” will pass the dial plan check</li> <li>8. ^ – exclude</li> <li>9. [3-5] – any digit of 3, 4, or 5</li> <li>10. [147] – any digit of 1, 4, or 7</li> <li>11. &lt;2=011&gt; – replace digit 2 with 011 when dialing</li> <li>12.   – the OR operand</li> </ol> <ul style="list-style-type: none"> <li>• Example 1: {[369]11   1617xxxxxxx}</li> </ul> <p>Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617;</p> <ul style="list-style-type: none"> <li>• Example 2: {^1900x+   &lt;=1617&gt;xxxxxxx}</li> </ul> <p>Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers;</p> <ul style="list-style-type: none"> <li>• Example 3: {1xxx[2-9]xxxxxx   &lt;2=011&gt;x+}</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• Example of a simple dial plan used in a Home/Office in the US: { ^1900x.   &lt;=1617&gt;[2-9]xxxxxx   1[2-9]xx[2-9]xxxxxx   011[2-9]x.   [3469]11 }</li> </ul> <p>Explanation of example rule (reading from left to right):</p> <ul style="list-style-type: none"> <li>• ^1900x. – prevents dialing any number started with 1900;</li> <li>• &lt;=1617&gt;[2-9]xxxxxx – allows dialing to local area code (617) numbers by dialing 7 numbers and 1617 area code will be added automatically;</li> <li>• 1[2-9]xx[2-9]xxxxxx  - allows dialing to any US/Canada Number with 11 digits length;</li> <li>• 011[2-9]x – allows international calls starting with 011;</li> </ul>

	<ul style="list-style-type: none"> <li>• [3469]11 – allows dialing special and emergency numbers 311, 411, 611 and 911.</li> </ul> <p><b>Note:</b> 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.</p> <p>Max length of dial plan is up to 1024 characters.</p>
<b>Ringtone</b>	
<b>Account Ring Tone</b>	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu.
<b>Ignore Alert-Info header</b>	Configures to play default ringtone by ignoring Alert-Info header. The default setting is “No”.
<b>Match Incoming Caller ID</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Specific caller ID number. For example, 8321123.</li> <li>• 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.</li> <li>• Alert Info text</li> </ul> <p>Users could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it. The custom ring tone will be used if the phone receives SIP INVITE with Alert-Info header in the following format: Alert-Info: &lt;http://127.0.0.1&gt;; info=priority</p> <p>Selects the distinctive ring tone for the matching rule. When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone.</p>

## Account Advanced Settings

<b>Security Settings</b>	
<b>Check Domain Certificates</b>	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is “No”.
<b>Validate Certificate Chain</b>	Validate certification chain when TCP/TLS is configured. The default setting is “No”.
<b>Validate Incoming SIP Messages</b>	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”.
<b>Allow Unsolicited REFER</b>	<p>Configures whether to dial the number carried by Refer-to header after receiving out-of-dialog SIP REFER request actively.</p> <p>If set to “<b>Disabled</b>”, the phone will send error warning and stop dialing.</p> <p>If set to “<b>Enabled/Force Auth</b>”, the phone will dial the number after sending authentication. If the authentication fails, it will stop dialing.</p> <p>If set to “<b>Enabled</b>”, the phone will dial all numbers carried by SIP REFER.</p>
<b>Accept Incoming SIP from Proxy Only</b>	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”.

<b>Check SIP User ID for Incoming INVITE</b>	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".
<b>Allow SIP Reset</b>	Allow SIP Notification message to perform factory reset. The default setting is "No".
<b>Authenticate Incoming INVITE</b>	If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response. The default setting is "No".
<b>MOH ( Music on Hold )</b>	
<b>On Hold Reminder Tone</b>	Configures to play reminder tone when the call is on hold.
<b>Music On Hold URI</b>	Music On Hold URI to call when a call is on hold if server supports it.
<b>Special Feature</b>	Specifies the server type for special requirements.

## Phone Settings Page Definition

### Basic Settings

<b>Local RTP Port</b>	Configures the local RTP port used to listen and transmit. The valid range is 1024 to 65400 and it must be even.
<b>Local RTP Port Range</b>	Configures the range of local RTP port. Valid value is from 24 to 10000.
<b>Use Random Port</b>	If set to "Yes", the 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. This parameter must be set to "No" for incoming direct IP calls (outgoing IP calls are not affected).
<b>Keep-Alive Interval</b>	Specifies how often the phone sends a blank UDP packet to the SIP server in order to keep "ping hole" on the NAT router to open.
<b>STUN Server</b>	This option sets IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
<b>Use NAT IP</b>	Configures the NAT IP address used in SIP/SDP messages. It should ONLY be used if required by your ITSP.
<b>Delay Registration</b>	Configures the specific time that the account will be registered after booting up.
<b>Enable Outbound Notification</b>	Configures whether to enable outbound notifications such as Action URL.

### Call Settings

<b>General</b>	
<b>Preferred Default Account</b>	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.

<b>Mute Key Functions While Idle</b>	If set to "Idle Mute", clicking the MUTE key while idle will cause the phone to be muted automatically when answering incoming calls.
<b>Do Not Escape '#' as %23 in SIP URI</b>	Replaces # by %23 for some special situations.
<b>User-Agent Prefix</b>	Configures the prefix in the User-Agent header
<b>Outgoing</b>	
<b>Enable Direct IP Call</b>	Enables Direct IP Call feature.
<b>Onhook Dial Barging</b>	When the option is set to "Disabled", onhook dialing won't be interrupted by an incoming call.
<b>Off-hook Auto Dial</b>	Configures the digits to be dialed via the first account when the phone is off-hook.
<b>Off-hook Auto Dial Delay</b>	Configures the timeout (in seconds) for off-hook auto dial. Valid range is 0-10. If set to 0, it will be dialed out immediately. Otherwise, it will be dialed out after the configured timeout.
<b>Off-hook/On-hook Timeout (s)</b>	If configured, when the phone is in the off-hook or on-hook, dialing state, it will go idle after the timeout (in seconds). Valid range is 10 to 60.
<b>Redial Expiration (min)</b>	Sets a timeout in minutes for the redial key, after which the previous callout trace will be cleared and the redial key will be invalid. If set to 0, the previous callout trace will not be removed permanently unless the device is turned off. <b>Note:</b> This configuration item also affects the call return soft key timeout in MPK. The default value is set to 30mins.
<b>Incoming</b>	
<b>Allow Incoming Call before Ringing</b>	This allows incoming calls after dialed but before ringing. This can be used under custom user configuration based on need.
<b>Enable Call Waiting</b>	Enables the call waiting feature. If set to "No", new incoming calls will be rejected after the call is established.
<b>Enable Call Waiting Tone</b>	Enables Call Waiting alert tone when another incoming call is received while a call is in progress.
<b>Auto Answer Delay</b>	Configures the delay for automatically answering the incoming call. Valid range is 0 to 10 (seconds).
<b>In Call</b>	
<b>Enable Auto Unmute</b>	If the option is enabled, automatically unmute phone when a user unholds the call or establishes a new call.
<b>Enable Busy Tone on Remote Disconnect</b>	Playing busy tone when call is disconnected remotely.
<b>Enable Mute Key In Call</b>	When set to "No", the mute key will not work while on call.
<b>Transfer</b>	
<b>Enable Transfer</b>	Enables Call Transfer feature.

<b>Hold Call Before Completing Transfer</b>	When set to "No", the phone will not hold the current call or the transfer target for an Attended Transfer.
<b>Conference</b>	
<b>Enable Conference</b>	Enables the Conference feature.

## Ringtone

This section is used to customize ringtones for each specific phone feature

<b>Call Progress Tones</b>	ON is the period of ringing ("On time" in "ms") While OFF is the period of silence. Up to three cadences are supported.
<b>System Ringtone</b>	
<b>Dial Tone</b>	
<b>Second Dial Tone</b>	
<b>Message Waiting</b>	
<b>Ring Back Tone</b>	
<b>Call Waiting Tone</b>	
<b>Call Waiting Tone Gain</b>	
<b>Busy Tone</b>	
<b>Reorder Tone</b>	

## Multicast Paging

<b>Paging Barging</b>	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.
<b>Paging Priority Active</b>	If enabled, during a multicast page if another multicast is received with higher priority (1 being the highest) that one will played instead.
<b>Multicast Channel Number</b>	Multicast channel number (0-50). 0 for normal RTP packets, 1-50 for Polycom multicast format packets.
<b>Multicast Listening</b>	Secifies the label and multicast listening address, it supports up to 10 multicats addresses

## Network Settings

### Ethernet Settings

<b>Internet Protocol</b>	Select Prefer IPv4 or Prefer IPv6
--------------------------	-----------------------------------

<b>IPv4 Address</b>	
<b>IPv4 Address</b>	The IPv4 address obtained by the phone. <b>Note:</b> If you attempt to set a new IP address with an incorrect format, an error message indicating that the format is invalid will be displayed.
<b>Host name (Option 12)</b>	Specifies the name of the client. This field is optional but may be required by Internet Service Providers.
<b>Vendor Class ID (Option 60)</b>	Used by clients and servers to exchange vendor class ID.
<b>DNS Server 1</b>	Enter DNS Server 1 when static IP is used.
<b>DNS Server 2</b>	Enter DNS Server 2 when static IP is used.
<b>Preferred DNS Server</b>	Enter the Preferred DNS Server.
<b>IPv6 Address</b>	
<b>IPv6 Address</b>	The IPv6 address obtained by the phone.
<b>DNS Server 1</b>	Enter DNS Server 1 when static IP is used.
<b>DNS Server 2</b>	Enter DNS Server 2 when static IP is used.
<b>Preferred DNS Server</b>	Enter the preferred DNS server.

## Advanced Settings

<b>Advanced Network Settings</b>	
<b>DNS Refresh Timer (m)</b>	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.
<b>DNS Failure Cache Duration (m)</b>	Configures the duration (in minutes) of previous DNS query fails. If set to "0", the feature will be disabled. <b>Note:</b> Only valid for SIP registration.
<b>Enable LLDP</b>	Controls the LLDP (Link Layer Discovery Protocol) service.
<b>LLDP TX Interval</b>	Configures LLDP TX Interval (in seconds). Valid range is 1 to 3600.
<b>Enable CDP</b>	If enabled, the device will use the Cisco Discovery Protocol feature.
<b>Layer 3 QoS for SIP</b>	Configures the layer 3 QoS parameter for SIP. This value is used for IP Precedence, DiffServ, or MPLS.
<b>Layer 3 QoS for RTP</b>	Configures the layer 3 QoS parameter for RTP. This value is used for IP Precedence, DiffServ, or MPLS.
<b>Enable DHCP VLAN</b>	Configures to enable or disable auto-configure for VLAN settings via DHCP.
<b>Enable Manual VLAN Configuration</b>	Allow phone to keep the VLAN configuration without applying them.

<b>Layer 2 QoS 802.1Q/VLAN Tag</b>	Assigns the VLAN Tag of the Layer 2 QoS packets.
<b>Layer 2 QoS 802.1p Priority Value</b>	Assigns the priority value of the Layer 2 QoS packets. Valid range is 0 to 7
<b>Maximum Transmission Unit (MTU)</b>	Configures the MTU in bytes
<b>Remote Control</b>	
<b>Action URI Support</b>	Configures whether to enable phone to handle action URI request.
<b>Action URI Allowed IP List</b>	List of allowed IP addresses from which the phone receives the action URI.
<b>CSTA Control</b>	Configures whether to enable the CSTA Control feature.

## Wi-Fi Settings (Only GHP630W )

<b>Wi-Fi Function</b>	This parameter enables/disables the Wi-Fi function.
<b>Wi-Fi Band</b>	Set the type of Wi-Fi band.
<b>Country Code</b>	Configures Wi-Fi Country Code
<b>Available Wi-Fi</b>	Available Wi-Fi

## Programmable Keys

### Multi-Purpose Keys

The admin can customize the multi-purpose keys functionality by accessing the web GUI **Programmable Keys → Multi-Purpose Keys**. The phone will generate a multi-purpose keys label based on the customization made by the administrator, which he/she can print and stick on the front side of the phone.

Multi-Purpose Keys Configuration

### Speed Dial



**GHP630W**

- Status
- Accounts
- Phone Settings
- Network Settings
- Programmable Keys
  - Multi-Purpose Keys
  - Speed Dial
  - Advanced Settings
- System Settings
- Maintenance
- Application

## Speed Dial

Room No.

Remarks

<b>1</b>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>2</b> <small>ABC</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>3</b> <small>DEF</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>
<b>4</b> <small>GHI</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>5</b> <small>JKL</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>6</b> <small>MNO</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>
<b>7</b> <small>PQRS</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>8</b> <small>TUV</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>9</b> <small>WXYZ</small>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>
<b>*</b>	<input type="text"/>	<b>0</b>	<input type="text" value="None"/> <input type="text" value="Dynamic account"/> <input type="text" value="Value (User ID)"/> <input type="text" value="Label"/>	<b>#</b>	<input type="text"/>

*Speed Dial Configuration*

## System Settings

### Time

Date and Time	
<b>NTP Server</b>	Configures the URL or IP address of the NTP server. The phone may obtain the date and time from the server.
<b>Secondary NTP Server</b>	Configures the URL or IP address of the NTP server. The phone may obtain the date and time from the server.
<b>Enable Authenticated NTP</b>	Configures whether to enable NTP authentication. If enabled, a cryptographic signature is appended to each network packet. If the key is incorrectly configured, the phone will refuse to use the time provided by the NTP server.
<b>NTP Update Interval</b>	Configures interval for updating time from the NTP server. The valid value is between 5 and 1440 minutes.
<b>Allow DHCP Option 42 to Override NTP Server</b>	When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN.
<b>Time Zone</b>	Configures the date/time used on the phone according to the specified time zone.
<b>Allow DHCP Option 2 to Override Time Zone Settings</b>	Allows device to get provisioned for Time Zone from DHCP option 2 in the local server
<b>Self-Defined Time Zone</b>	This parameter allows the users to specify their own time zone. For syntax and

examples please refer to user manual.

## Security Settings

### Web/SSH Access

SSH is often used to "log in" and perform operations on remote computers but it may also be used for transferring data.

Parameter	Description
<b>SSH Access</b>	
<b>Enable SSH</b>	If set to "Yes", the phone will allow any SSH access to the phone.
<b>SSH Public Key</b>	If enabled, the phone will use public key authentication as an alternative option to password authentication.
<b>Web Access</b>	
<b>HTTP Web Port</b>	Configures the HTTP port under the HTTP web access mode.
<b>HTTPS Web Port</b>	Configures the HTTPS port under the HTTPS web access mode.
<b>Web Access Mode</b>	Sets the protocol for the web interface.
<b>Web Access Control</b>	Restrict web access by using Whitelist or Blacklist on the incoming IP addresses. If set to "None", the web access is unrestricted.
<b>Web Session Timeout</b>	Configures the timer to log out of the web session when idle. Default is 10 minutes. Range is 2-60 minutes.
<b>Validate Server Certificates</b>	Configures whether to validate the server certificate when downloading the firmware/config file. If set to "Yes", the phone will download the firmware /config file only after the server is validated.
<b>Web/Restrict mode Lockout Duration</b>	Specifies the time in minutes that the web login interface will be locked out to the user after five login failures. This lockout time is used for web login. The range is 0-60 minutes.
<b>Web Access Attempt Limit</b>	Configures the number of failed web access attempts allowed before lockout. Default is 5. Range is 1-10.

### User Info Management

Parameter	Description
<b>Test Password Strength</b>	Checks password strength to ensure better security
<b>Admin Password</b>	
<b>Current Password</b>	The current admin password is required to set a new admin password.
<b>New Password</b>	Set new password for web GUI access as Admin. This field is case sensitive.
<b>Confirm Password</b>	Enter the new Admin password again to confirm.

<b>IVR</b>	
<b>Keypad Password</b>	Configure the keypad password used in the IVR.
<b>Enable IVR</b>	If enabled, IVR is available. If disabled, enable configuration item "Enable Basic Settings in IVR" cannot take effect. Enabled By Default.
<b>Enable Basic settings in IVR</b>	If this option is enabled, IVR can modify the IP, gateway, subnet mask, DNS, profile download protocol and firmware download protocol of the phone. If this option is disabled, the IVR refuses to execute the above instructions. Enabled by Default.

### Client Certificate

Parameter	Description
<b>Minimum TLS Version</b>	Configures the minimum TLS version supported by the phone. Minimum TLS version must be less than or equal to maximum TLS version.
<b>Maximum TLS Version</b>	Configures the maximum TLS version supported by the phone. Maximum TLS version must be greater than or equal to minimum TLS version.
<b>Enable/Disable Weak Cipher Suites</b>	Defines the function for weak cipher suites. If set "Enable Weak TLS Cipher Suites", allow users to encrypt data by weak TLS cipher suites.
<b>SIP TLS Certificate</b>	The Cert File for the phone to connect to SIP Server via TLS.
<b>SIP TLS Private Key</b>	The Cert Key for the phone to connect to SIP Server via TLS.
<b>SIP TLS Private Key Password</b>	SSL Private key password used for SIP Transport in TLS/TCP.
<b>Custom Certificate</b>	The uploaded custom certificate will be used for SSL/TLS communication instead of the phone default certificate.

### Trusted CA Certificate

<b>Load CA Certificates</b>	Phone will verify the server certificate based on the built-in, custom or both trusted certificates list.
-----------------------------	---

### Preferences

#### Display Control

<b>New Message LED Indicator</b>	Configure the behaviour of the LED indicator when there is a new voice mail on the phone. If it is set to "off", the LED will not change in any state when there is a message.
----------------------------------	--

#### Audio Control

Parameter	Description
<b>Speaker Ring Volume</b>	Configures speaker ring volume, the valid range is 1 to 8.

<b>Handset Sidetone Volume</b>	Configures handset sidetone volume. The valid range is 0 to 30.
<b>Lock Speaker Volume</b>	Lock volume adjustment when the option is enabled.
<b>Enable Warning Tone</b>	Configures whether to enable the warning tone of the phone. If disabled, the network disconnection and voicemail will not generate any tone.
<b>Handset TX Gain (dB)</b>	Configures the transmission gain of the handset.
<b>Enable HAC</b>	If enabled, the phone will be compatible with nearby hearing aids.
<b>Enable Bootup Tone</b>	If enabled, the phone will emit a sound effect when it boots up.

## LED

<b>LED Brightness: Active</b>	Configures the LED brightness when the phone is active. Valid range is 0 to 10 where 0 is off and 10 is the brightest.
<b>LED Brightness: Idle</b>	Configures the LED brightness when the phone is idle. Valid range is 0 to 10 where 0 is off and 10 is the brightest.

## TR-069

A TR-069 client is a software application that allows service providers and equipment manufacturers to manage, configure, and update their customers' network-connected devices remotely.

Parameter	Description
<b>Enable TR-069</b>	Enable or disable TR-069
<b>ACS URL</b>	URL of the TR-069 Auto Configuration Servers (e.g., <a href="http://acs.mycompany.com">http://acs.mycompany.com</a> , or IP address).
<b>TR-069 Username</b>	ACS username for TR-069.
<b>TR-069 Password</b>	ACS password for TR-069.
<b>Periodic Inform Enable</b>	Enables periodic inform. If set to "Yes", device will send inform packets to TR-069 Auto Configuration Server.
<b>Periodic Inform Interval</b>	Configures periodic inform interval to send the inform packets to TR-069 Auto Configuration Server.
<b>Connection Request Username</b>	The username for the TR-069 Auto Configuration Server to connect the phone.
<b>Connection Request Password</b>	The password for the TR-069 Auto Configuration Sever to connect to the phone.
<b>Connection Request Port</b>	The port for the TR-069 Auto Configuration Server to connect to the phone.
<b>CPE SSL Certificate</b>	The Cert File for the phone to connect to the TR-069 Auto Configuration Sever via SSL.
<b>CPE SSL Private Key</b>	The Cert Key for the phone to connect to the TR-069 Auto Configuration Sever via SSL

<b>Start TR-069 at Random Time</b>	If enabled, TR-069 will send out the first INFORM message to the server on randomized timing between 1 to 3600 seconds after the phone boots up.
------------------------------------	--

## Maintenance

## Upgrade and Provisioning

### Firmware

Parameter	Description
<b>Upgrade via Manual Upload</b>	
<b>Upload Firmware File to Update</b>	Configures to upload and upgrade firmware.
<b>Upgrade via Network</b>	
<b>Firmware Upgrade via</b>	Configures firmware upgrade method as TFTP, FTP, FTPS, HTTP, HTTPS.
<b>Firmware Server Path</b>	Configures the server path for firmware download.
<b>Firmware Server Username</b>	The username for the firmware server.
<b>Firmware Server Password</b>	The password for the firmware server.
<b>Firmware File Prefix</b>	If configured, only the firmware with the matching prefix will be downloaded and flashed into the phone.
<b>Firmware File Postfix</b>	If configured, only the firmware with the matching postfix will be downloaded and flashed into the phone.
<b>Upgrade Detection</b>	
<b>Upgrade</b>	Start the upgrade.

### Config File

Parameter	Description
<b>Configure Manually</b>	
<b>Download Device Configuration</b>	Click to download the device configuration file in .txt format.
<b>Download Device Configuration (XML)</b>	Click to download the device configuration file in .XML format.
<b>Download User Configuration</b>	Click to download the user's configuration file.
<b>Upload Device Configuration</b>	Upload configuration file to the phone.
<b>Export Backup Package</b>	Export a backup package which contains device configuration and personal data.

<b>Restore from Backup Package</b>	Restore from the uploaded backup package.
<b>Configure via Network</b>	
<b>Configure Upgrade via</b>	Choose the protocol that will be used for upgrading.
<b>Configure Server Path</b>	Defines the server path for provisioning.
<b>Configure Sever Username</b>	The username for the config server.
<b>Configure Sever Password</b>	The password for the config server.
<b>Always Indicate before Challenge</b>	If enabled, the phone will send credentials before being challenged by the server. This option only applies to HTTP/HTTPS.
<b>Config File Prefix</b>	If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
<b>Config File Postfix</b>	If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
<b>Authenticate Conf File</b>	If enabled, the phone will authenticate configuration file before acceptance.
<b>XML Config File Password</b>	Configures the password for encrypting the XML configuration file using OpenSSL. This is required for the phone to decrypt the encrypted XML configuration file.

### Provision

Parameter	Description
<b>Auto Upgrade</b>	
<b>Automatic Upgrade</b>	Enables automatic upgrade and provisioning.
<b>Start Upgrading at Random Time</b>	Configures whether the phone will upgrade automatically at a random time within the configured time interval.
<b>Firmware Upgrade and Provisioning</b>	Specifies how firmware upgrading and provisioning request to be sent.
<b>DHCP Option</b>	
<b>Allow DHCP Option 43 and Option 66 to Override Server</b>	If set to "Yes" on the LAN side, the phone will reset the CPE, upgrade, network VLAN tag and priority configuration according to option 43 sent by the server. At the same time, the upgrade mode and server path of the configuration mode will be reset according to option 66 sent by the server. If set to "prefer, fallback when failed", the phone can fallback to use the configured provisioning server under its Firmware and Config server path in case the server from DHCP Option fails.
<b>Allow DHCP Option 120 to Override SIP Server</b>	Specifies the name of the client. This field is optional but may be required by Internet Service Provider.
<b>Additional Override DHCP Option</b>	Configures additional DHCP Option to be used for firmware server instead of the configured firmware server or the server from DHCP Option 33 and 66. This option will be effective only when "Allow DHCP Option 43 and Option 66 to Override Server" is enabled.

Config Provision	
<b>Download and Process All Available Config Files</b>	By default, the device will follow cfgMAC.xml, cfgMAC, cfgMODEL.xml, cfg.xml, devMAC.cfg sequence searches for the first available configuration file and updates the configuration file, and the subsequent configuration files will be ignored.If this configuration item is enabled, the device will follow cfg.xml, cfgMODEL.xml, cfgMAC, cfgMAC.xml, devMAC.cfg downloads configuration files one by one and loads updates. If the same configuration items exist between files, the configuration items that are later in the download order will overwrite the previous contents.
<b>User Protection</b>	When user protection is on, P-values that the user sets will not be changed by provision or provider.
<b>3CX Auto Provision</b>	If enabled, the phone will send SUBSCRIBE requests to the multicast address in LAN during bootup for the automatic provisioning. This feature requires 3CX server support.

## Advanced Settings

Parameter	Description
<b>Validate Hostname in Certificate</b>	Configures tp validate the hostname in the SSL certificate.
<b>Enable SIP NOTIFY Authentication</b>	Device will challenge NOTIFY with 401 when set to "Yes".
<b>Factory Reset</b>	Initiate factory reset. All the configuration on the device will be erased.

## System Diagnostics

### Syslog

Syslog is a protocol that computer systems use to send event data logs to a central location for storage. Logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT operational tasks

Parameter	Description
<b>Syslog Protocol</b>	Allows sending syslog through secured TLS protocol to the syslog server. <b>Note:</b> CA verification is required.
<b>Syslog Server</b>	The URL/IP address for the syslog server.
<b>Syslog Level</b>	Selects the level logging of syslog.
<b>Syslog Keyword Filter</b>	Syslog will be filtered based on the configured keywords. Multiple keywords can be separated by ",".
<b>Send SIP Log</b>	Configures whether the SIP log will be included in the syslog messages.

## Notification Events

### Action URL

The following section describes how we can use the settings present in the GHP to configure customizable notifications

Parameter	Description
<b>Phone Status</b>	
<b>Setup Completed</b>	Configures the Action URL to send when phone finishes setup process.
<b>Registered</b>	Configures the Action URL to send when phone successfully registers as a SIP account.
<b>Unregistered</b>	Configures the Action URL to send when phone unregisters a SIP account.
<b>Register Failed</b>	Configures the Action URL to send when phone fails to register a SIP account.
<b>Idle to Busy</b>	Configures the Action URL to send when the phone's state changes form idle to busy.
<b>Busy to Idle</b>	Configures the Action URL to send when phone's state changes from busy to idle.
<b>Auto Provision Completed</b>	Configures the Action URL to send when phone's auto provision process is completed.
<b>IP Change</b>	Configures the Action URL to send when the IP address changes.
<b>Call Operation</b>	
<b>Off-hook</b>	Configures the Action URL to send when phone is in off-hook state.
<b>On-hook</b>	Configures the Action URL to send when the phone is on-hook state.
<b>Incoming Call</b>	Configures the Action URL to send when the phone receives an incoming call.
<b>Outgoing Call</b>	Configures the Action URL to send when phone places a call.
<b>Missed Call</b>	Configures the Action URL to send when phone has a missed call.
<b>Established a Call</b>	Configures the Action URL to send when phone establishes a call.
<b>Terminated Call</b>	Configures the Action URL to send when the phone terminates a call.
<b>Answered Call</b>	Configures the Action URL to send when phone answers an incoming call.
<b>Blind Transfer</b>	Configures the Action URL to send when the phone performs blind transfer.
<b>Attended Transfer</b>	Configures the Action URL to send when the phone performs attended transfer.
<b>Transfer Completed</b>	Configures the Action URL to send when the phone successfully transfers a call.
<b>Transfer Failed</b>	Configures the Action URL to send when the phone fails to transfer a call.
<b>Hold Call</b>	Configures the Action URL to send when the phone places a call on hold.
<b>Unhold Call</b>	Configures the Action URL to send when the phone resumes the call on hold.
<b>Mute Call</b>	Configures the Action URL when the phone mutes a call.



<b>Unmute Call</b>	Configures the Action URL when the phone unmutes a call.
--------------------	--

## Application

### Hotel Service

This section contains the basic settings of Hotel Service Management, including the basic general information of the hotel where the GHP hotel phone is deployed and also the assigned room number.

Parameter	Description
<b>Hotel Name</b>	Configures the hotel name.
<b>Hotel Address</b>	Configures the hotel address.
<b>Hotel Phone Number</b>	Configures the hotel phone number.
<b>Hotel Fax Number</b>	Configures the hotel fax number.
<b>Hotel Room Number</b>	Configures the hotel's room number.

### E911 Service

E911 (Enhanced 911) service allows configuring of the GHP6xx to allow emergency calls to be made while providing the location of the user to be known to the call receiver.

Parameter	Description
<b>Enable E911</b>	Enable or disable E911.
<b>HELD Protocol</b>	Configures HELD transfer protocol.
<b>HELD Synchronization Interval</b>	The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when interval is 0.
<b>Location Server</b>	Configures the primary Location Information Server (LIS) address.
<b>Location Server Username</b>	Configures the username of the primary Location Information Server (LIS).
<b>Location Server Password</b>	Configures the password of the primary Location Information Server (LIS).
<b>Secondary Location Server</b>	Configures the secondary Location Information Server.
<b>Secondary Location Server Username</b>	Configure the username of the secondary Local Information Server.
<b>Secondary Location Server Password</b>	Configure the password of the secondary Location Information Server.
<b>HELD Location Types</b>	Configure "locationType" element in the location request.

<b>HELD Use LLDP Information</b>	If set to "Yes", the information from LLDP-support switch is used to generate ChassisID and portID; otherwise
<b>HELD NAI</b>	If set to "Yes", Network Access Identifier (NAI) is included as a device identity in the location request sent to the Location Information
<b>E911 Emergency Numbers</b>	A user can configure multiple emergency numbers separated with the delimiter symbol ";".
<b>Geolocation-Routing Header</b>	If set to "Yes", E.911 INVITE message includes the "Geolocation-Routing" header with the value "Yes".
<b>Priority Header</b>	If set to "Yes", E.911 INVITE messages includes the "Priority" header with the value "emergency".

## Web Service

This section is utilized to enable the location services on the phone.

Parameter	Description
<b>Use Auto Location Service</b>	Configures to enable or disable auto location services on the phone.

## GDS

GHP6XX can be paired with Grandstream's facility access management system GDS to allow two-way communication, open door from the GHP6xx, and define a specific ringtone to be played when the GDS doorbell rings and initiate a call to GHP6XX.

### GDS

<b>GDS</b>	<p>Connect to a GDS37XX and send OpenDoor request.</p> <ul style="list-style-type: none"> <li>● <b>Service Type:</b> Select GDS as service type</li> <li>● <b>Account:</b> The account to be used on the phone to interact with the GDS37XX</li> <li>● <b>System Identification:</b> A name or a number to identify the GDS37XX</li> <li>● <b>System Number:</b> The SIP extension or the IP address of the GDS37XX depending on the deployed scenario, Peering or Registration</li> <li>● <b>Access Password:</b> The password set on the GDS37XX to unlock the door.</li> <li>● <b>System Ringtone:</b> 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</li> </ul>
------------	---

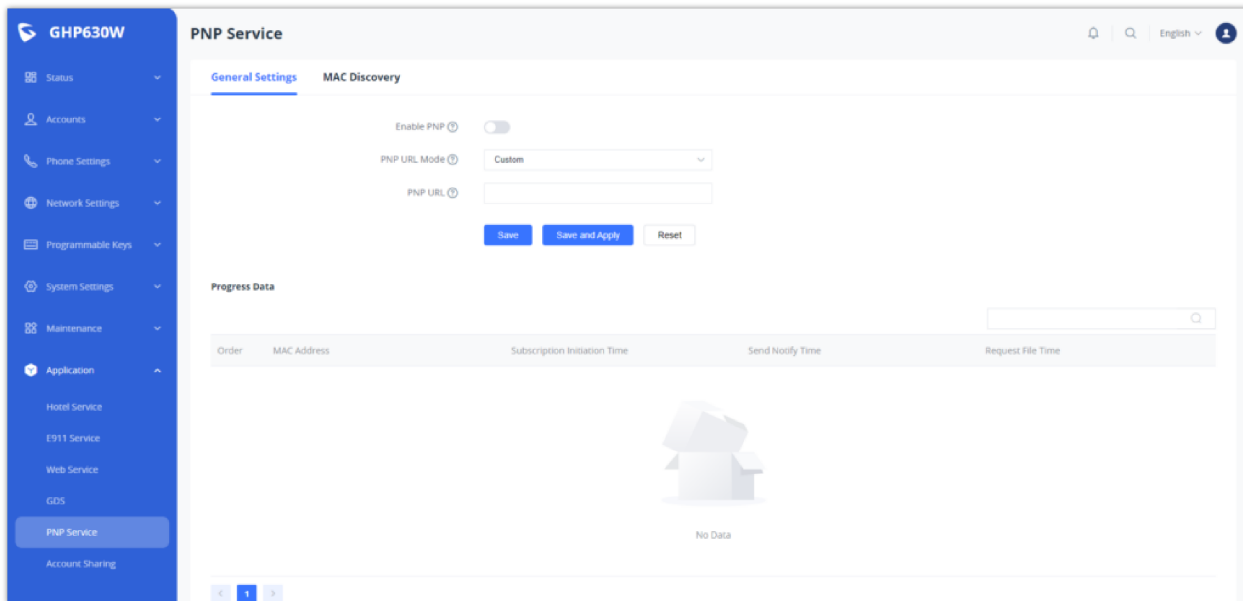
**Notes:**

- When using Peering scenario, on “System Number” field of the GHP6XX specify the IP address of the peered GDS37XX.
- When using Registration scenario and both GHP6XX and GDS37XX are registered on the same SIP server, specify the SIP extension of the GDS37XX on “System Number” field on GHP6XX.

The “Access Password” on GHP6XX should be matching “Remote PIN to Open the door” on GDS37XX.

## PNP Service

Plug and Play (PnP) Service is a feature available on the GHP6xx that allows it to be set as a server terminal for provisioning other IP phones remotely, on the GHP6xx PNP centralized platform, either by setting the configuration locally by uploading local configuration files, or by obtaining the configuration files from a third party HTTP server.



General Settings	
<b>Enable PNP</b>	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.
<b>PNP URL Mode</b>	Select the PNP URL mode, including local and custom, custom does not support filling in the local machine-related address.
<b>PNP URL</b>	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.
<b>Template Management</b>	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.
<b>Upload Profile Template</b>	Users can upload a .xml template file downloaded by respecting the following guidelines: <ul style="list-style-type: none"><li>• 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.</li><li>• 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</li></ul>

	<p>Configure CSV).</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Please write configuration file template according to sample file format specification. Any text file format can be placed in &lt;data&gt;&lt;![CDATA[ --- ]&gt;&lt;/data&gt;.</li> </ul>
<b>Batch Configure CSV</b>	<p>Users can upload a .csv template file download while respecting the following guidelines:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• After writing the batch configuration CSV template, upload the CSV template file here.</li> </ul>
<b>Effects View</b>	Displays the data inserted from the .csv template to the .xml configuration file.
<b>Progress Data</b>	<p>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.</p> <p>the connected networks will be displayed in the list.</p>
<b>MAC Discovery</b>	<p>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.</p> <p>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 :</p> <ul style="list-style-type: none"> <li>• <b>Download the Configuration file:</b> this option will download the configuration file of the discovered device</li> <li>• <b>Redistribution operation:</b> When a new IP 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.</li> </ul>

## Account Sharing

This section is utilized to enable the account-sharing feature.

<b>Basic Settings</b>	
<b>Enable Account Sharing</b>	Select whether to enable Account Sharing.
<b>Role in Account Sharing</b>	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.
<b>Group Name</b>	<p>Set the group name, in the host-guest mode, devices with the same group name can discover each other.</p> <p><b>Note:</b> This item is mandatory if using Account Sharing. The verification format is domain type</p>
<b>Group Password</b>	<p>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.</p> <p><b>Note:</b> This item is mandatory if using Account Sharing.</p>
<b>Account Settings</b>	
<b>Account</b>	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.
<b>Account Name</b>	This setting specifies the account name corresponding to the account used by the guest device.
<b>Sync Ringing In Group</b>	Set whether to enable synchronization of all successfully registered guest device ringtones within the group.
<b>Discovered Host Device list</b>	Shows registered devices on the local network for monitoring, it displays the following information about the discovered devices: <ul style="list-style-type: none"> <li>• IP Address</li> <li>• MAC Address</li> <li>• Registration Status</li> <li>• Operation</li> </ul>

## Contacts

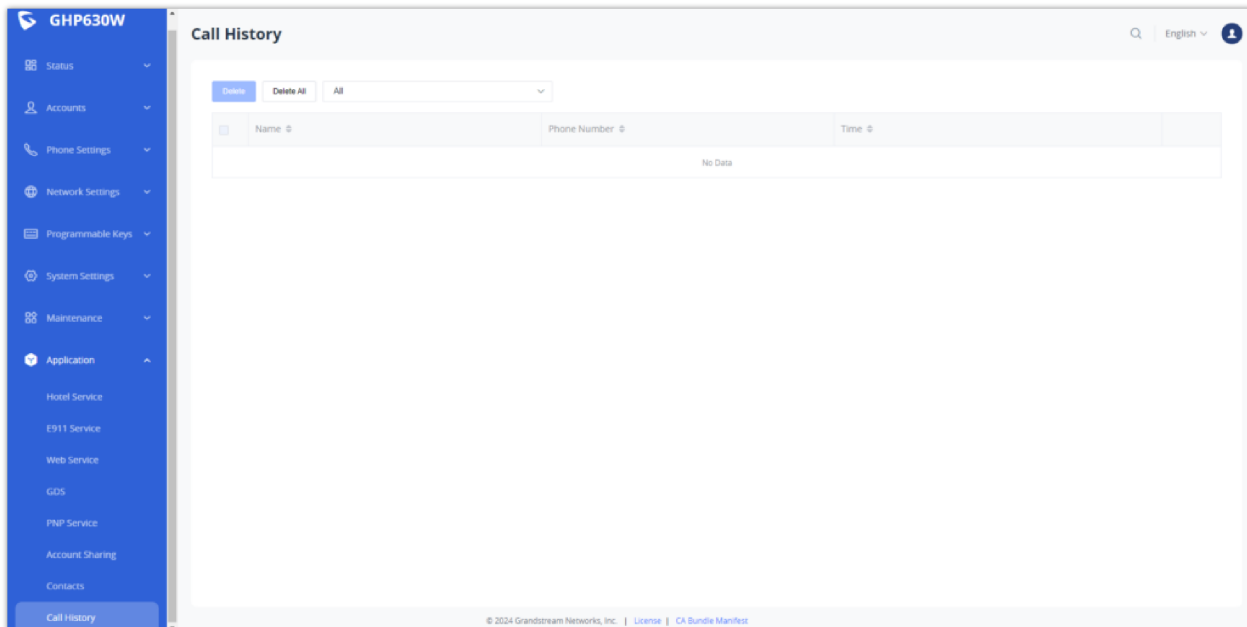
The contacts section allows users to create new contacts, create new groups, or link a remote phone book management using specific credentials and server paths.

<b>Contacts</b>	
<b>Add Contact</b>	The user can add a contact to the phonebook by clicking the "Add Contact" icon, the following parameters can be defined for each contact: <ul style="list-style-type: none"> <li>• First Name</li> <li>• Last Name</li> <li>• Favorite</li> <li>• Company</li> <li>• Department</li> <li>• Job</li> <li>• Job Title</li> <li>• Work</li> <li>• Home</li> <li>• Mobile</li> <li>• Accounts</li> <li>• Groups</li> <li>• Ringtone</li> </ul>
<b>Group Management</b>	
<b>Add Group</b>	The user can create a contacts group by clicking the "Add group" icon, the following parameters can be defined <ul style="list-style-type: none"> <li>• Group Name</li> <li>• Ringtone</li> </ul>
<b>Phonebook Management</b>	
<b>Enable Phonebook XML Download</b>	Enables Phonebook XML download via HTTP, HTTPS, FTP or TFTP.
<b>HTTP/HTTPS Username</b>	Defines the username for the HTTP/HTTPS server.
<b>HTTP/HTTPS Password</b>	Defines the password for the HTTP/HTTPS server
<b>Phonebook XML Server Path</b>	Configures the server path to download XML phonebook file. This field could be IP address or URL, with up to 256 characters.

<b>Phonebook Download Interval</b>	Configures the phonebook download interval (in minutes). If set to 0, automatic download will be disabled. Valid range is 5 to 720.
<b>Remove Manually-edited Entries on Download</b>	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed.
<b>Import Group Method</b>	When set to "Replace", the existing groups will be completely replaced by imported one. When set to "Append", the imported groups will be appended to the current one
<b>Sort Phonebook by</b>	Configures to sort phonebook based on the selection of first name or last name. 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.
<b>Download XML Phonebook</b>	Downloads the XML Phonebook file.
<b>Upload XML Phonebook</b>	Uploads XML Phonebook file to the phone in xml format
<b>Phonebook Key Function</b>	Configures the behavior of the Phonebook key.
<b>Default Search Mode</b>	Configures the default phonebook search mode.
<b>Replace Duplicate Items</b>	Replace duplicate items by name or number

## Call History

The call history tab displays all the answered, dialed, missed, and transferred calls of the registered accounts to the GHP63x IP phone:



## UPGRADING AND PROVISIONING

### Unified Firmware

The GHP610, GHP610W, GHP611, GHP611W, GHP620, GHP621, GHP620W, and GHP621W support unified firmware.

## Firmware Upgrade

The GHP6XX/W series can be upgraded via TFTP / FTP / FTPS / HTTP / HTTPS by configuring the URL/IP Address for the TFTP / HTTP / HTTPS / FTP / FTPS server and selecting a download method. Configure a valid URL for TFTP, FTP/FTPS, or HTTP/HTTPS, the server name can be FQDN or IP address.

### Examples of valid URLs:

[firmware.grandstream.com/BETA](http://firmware.grandstream.com/BETA)

fw.mycompany.com

## Upgrade via Web GUI

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

When upgrading starts, the screen will show the upgrading progress. When done you will see the phone restart again. Please do not interrupt or power cycle the phone during the upgrading process.

Firmware upgrading takes around 60 seconds in a controlled LAN or 5-10 minutes over the Internet. We recommend completing firmware upgrades in a controlled LAN environment whenever possible.

## No Local TFTP/FTP/HTTP Servers

For users who would like to use remote upgrading without a local TFTP/FTP/HTTP server, Grandstream offers a NAT-friendly HTTP server. This lets users download the latest software upgrades for their phones via this server. Please refer to the webpage:

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

Alternatively, users can download a free TFTP, FTP, or HTTP server and conduct a local firmware upgrade. A free windows version TFTP server is available for download from:

[http://www.solarwinds.com/products/freetools/free\\_tftp\\_server.aspx](http://www.solarwinds.com/products/freetools/free_tftp_server.aspx)

<http://tftpd32.jounin.net/>.

Instructions for local firmware upgrade via TFTP:

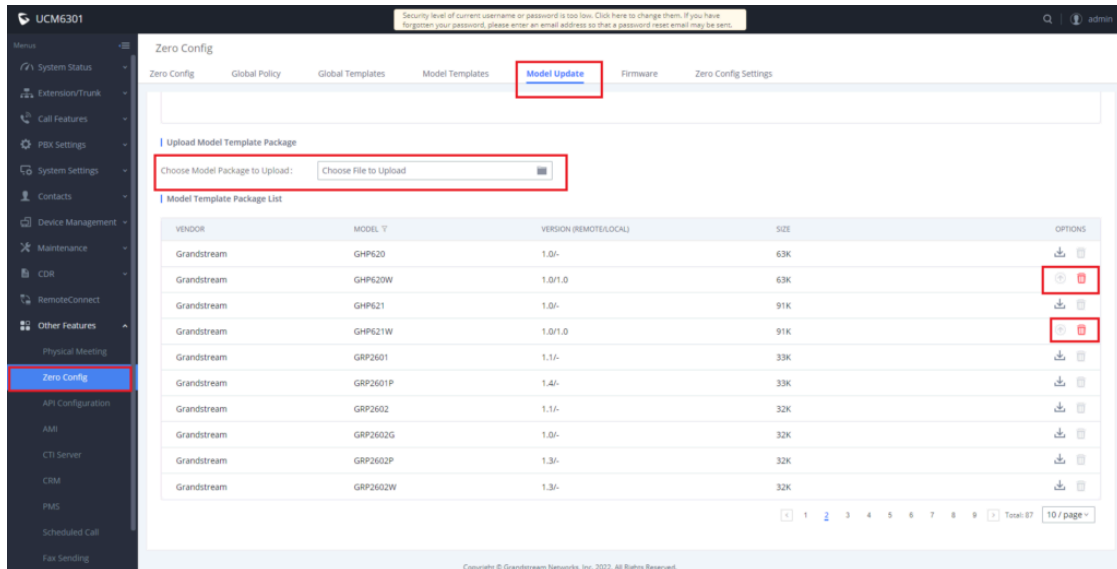
1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the phone to the same LAN segment.
3. Launch the TFTP server and go to the File menu → Configure → Security to change the TFTP server's default setting from "Receive Only" to "Transmit Only" for the firmware upgrade.
4. Start the TFTP server and configure the TFTP server in the phone's web configuration interface.
5. Configure the Firmware Server Path to the IP address of the PC.
6. Update the changes and reboot the phone.

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

## ZERO CONFIG NUMBER SELECTION PROCESS

The Grandstream Zero config tool allows you to automatically provision a range of Grandstream devices without having to configure each UC endpoint manually, this can be helpful in situations that require the mass deployment of UC endpoints, this method will make the provisioning process efficient and optimized, in our GHP63X/W IP hotel phone series, the zero config is used to configure extension selection from a specifically defined range, the process of how to do it is as mentioned below :

1. The administrator needs to log in to the UCM-Web server (SIP server IP address).
2. Select menu "Other Services" – "Zero Configuration" – "Model Update".



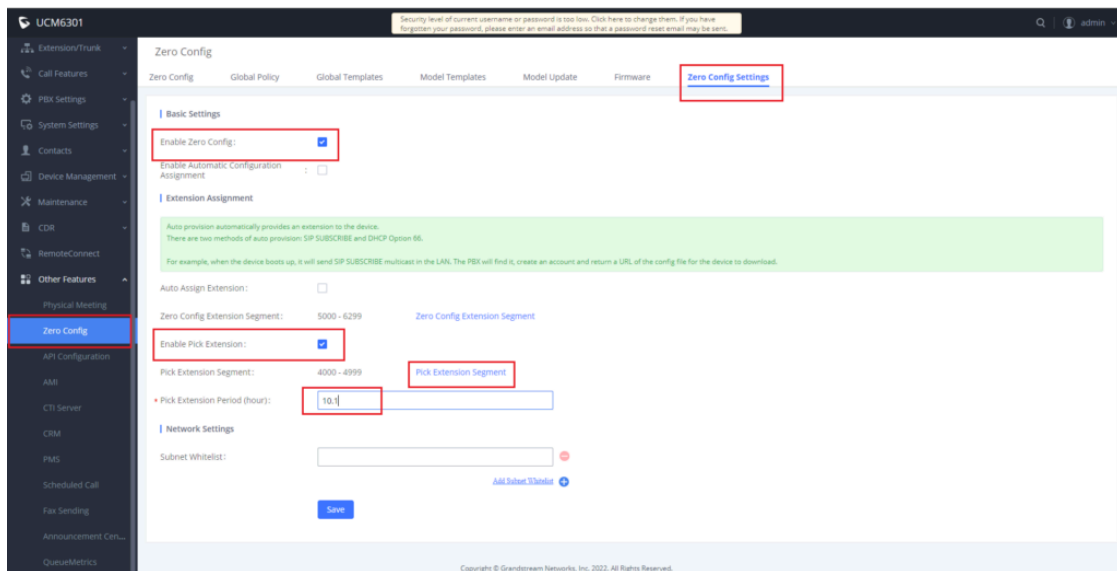
Zero Config – Model Update

- o Select a phone model and click the Download and Install button on the right of the list to download the model configuration file to the UCM.

**Note**

If the corresponding model cannot be downloaded and installed to the UCM local PC due to network reasons, you can upload the file of the UCM zero-configuration template (.pack file) and click the Download and Install button.

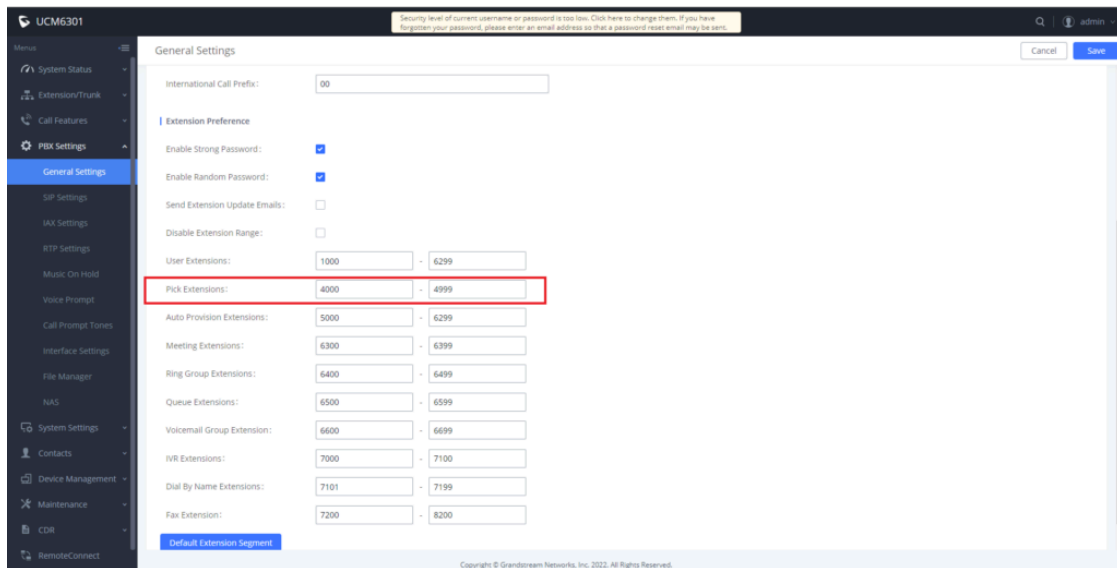
- o Select the menu "Other Services" – "Zero Configuration" – "Zero Configuration Settings", Select "Enable Zero Config" (enabled by default) and "Enable Pick Extension", and click "Pick Extension Segment" to set the optional number segment.



Zero Configuration settings

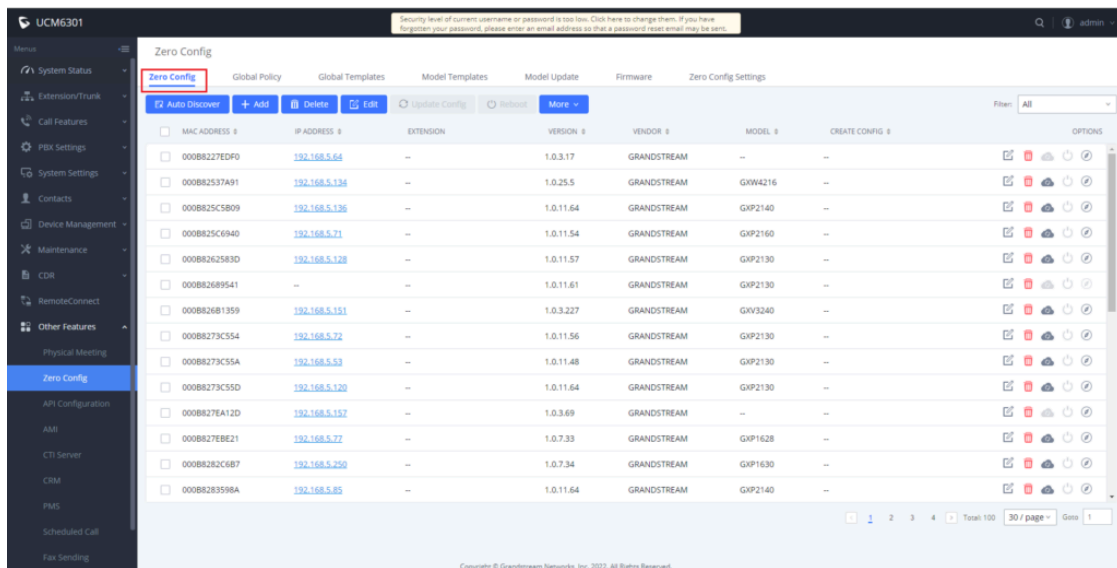
- o Click "Pick Extension Segment" to switch to the menu "PBX Settings" – "General Settings", and enter the corresponding number segment value. Make sure to click save afterward to save the changes.





### Picking Extension Segments

- The UCM6301 automatically discovers and manages device addresses on the same network segment. At the same time, UCM supports manual input of device IP to discover devices.



### Zero Config main page

- Phone users can dial service code **\*\*766\*** + room number to set the room number, and dial service code **\*\*766#** to hear the room number announcement. When the hotel room number is already in use, phone users should dial service code **\*\*766\*** + keypad password + room number + # to reset the room number.
- Phone users can dial **\*\*82#** to enable the UCM zero-configuration number selection process. The UCM sends the room number as the selection number. After receiving the request, the UCM delivers the configuration and sets the room number as the preferred account to complete the selection process.

### Important considerations

1. The extension number cannot be selected when the account number in UCM exceeds the upper limit, and the upper limit of the extension number must be specified.
2. The extension number selection function is not enabled or cannot be selected after the pick extension number selection period has expired.
3. The UCM must contain the template of the target phone and the configuration related to the account in the template.
4. In zero configuration, the total of the selected numbers of extension numbers can be repeatedly selected by multiple phones on the premises, however, it should not exceed the maximum number of registered accounts (concurrent number).

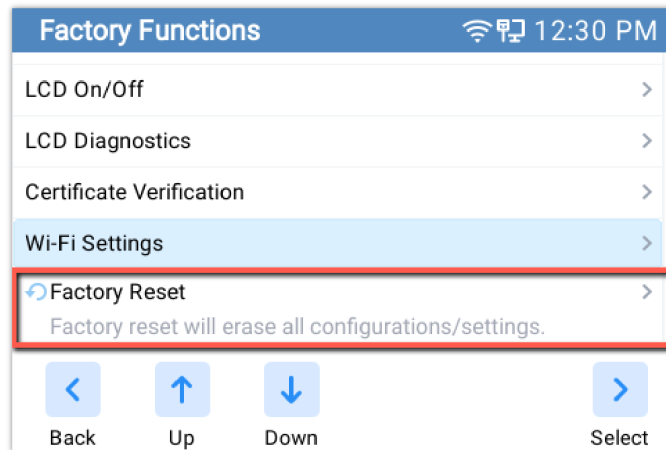
### More on Zero Config

## RESTORE FACTORY DEFAULT SETTINGS

### Restore to Factory Default via LCD menu

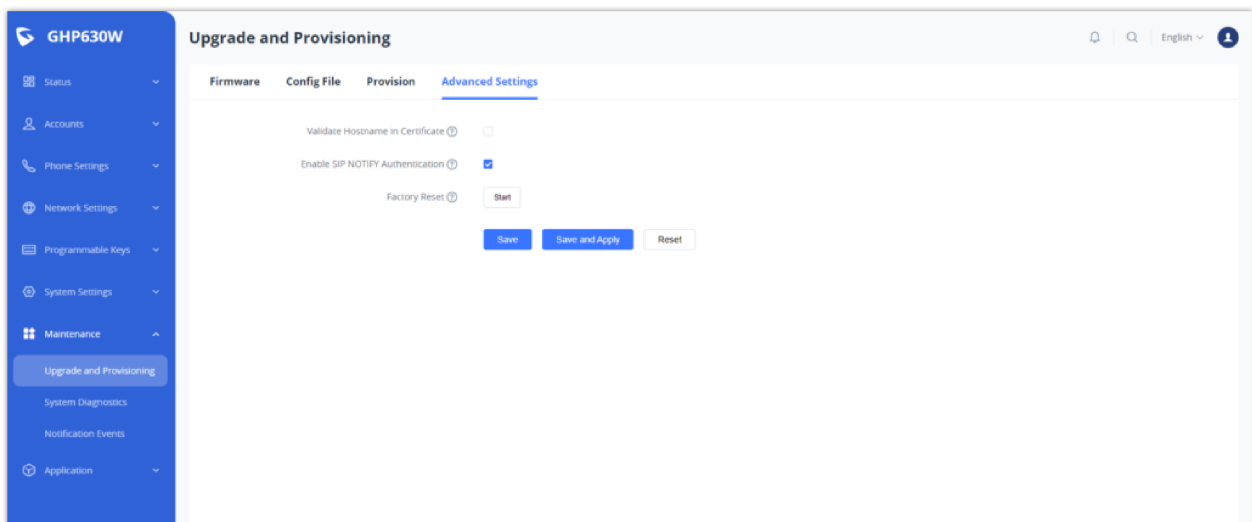
To restore the GHP63x/W to factory settings using the keypad lock :

1. Press “**HOLD**” + 2 to access the factory functions of the GHP63x/W from the LCD
2. From the list of available options, select “Factory Reset” to perform a factory reset to the phone.



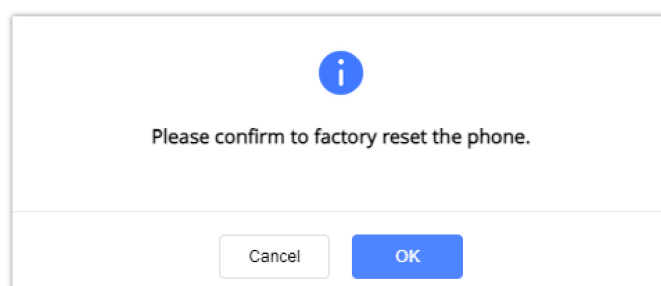
### Restore to Factory Default via Web GUI

To reset the GHP63X to its factory settings using the web GUI, please navigate to **Upgrade and Provisioning** → **Advanced Settings** then click on the **Start** button to start the factory reset process.



*Factory Reset via Web GUI*

The factory reset will immediately start after you click **OK**.



**Warning**

Once the process of resetting to factory settings has started, it cannot be cancelled and all the configuration will be lost. To avoid losing your configuration, please back it up first.

## CHANGELOG

### Firmware 1.0.1.13

- This is the initial firmware.
- 

### COPYRIGHT

©2024 Grandstream Networks, Inc. <https://www.grandstream.com>

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

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

---

### CAUTION

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

### WARNING

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

---

### CERTIFICATION

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

**Company Name:** Grandstream Networks, Inc.

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

**Tel:** 1-617-5669300

**Fax:** 1-617-2491987

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

This equipment uses the following USOC jacks: RJ45C.

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

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

### Caution: Exposure to Radio Frequency Radiation

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.

### CE Authentication



BE	BG	CZ	DK	DE	EE	IE	EL	LI
ES	FR	HR	IT	CY	LV	LT	LU	CH
HU	MT	NL	AT	PL	PT	RO	SI	TR
SK	FI	SE	NO	IS	UK	UK(NI)		

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



Hereby, Grandstream Networks, Inc. declares that the radio equipment GHP63X/W are in compliance with Directive 2014/53/EU.

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

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

---

### GNU GPL INFORMATION

GHP6XX firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

Grandstream GNU GPL-related source code can be downloaded from the Grandstream website:

<https://www.grandstream.com/legal/open-source-software>

---

### Need Support?

Can't find the answer you're looking for? Don't worry we're here to help!

[CONTACT SUPPORT](#)