Grandstream Networks, Inc.

GHP63X/W - Administration Guide

GHP63X/W - Administration Guide

WELCOME

The GHP series of hotel phones features 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, a 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), a power adapter (GHP630W/GHP631W), or a 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

 GHP63X/W	3.5" High-Resolution (480x320) Color LCD Screen Integrated dual-band2.4G/5G 802.11a/b/g/n/ac/ax Wi-Fi 6 (GHP630W &GHP631W only) 2 SIP lines with wideband Opus codec. 6 programmable keys and 10-speed dial keys to customize different services. One 100Mbps network port with PoE (PoE available on GHP630/GHP631). Desk/Wall mounted. Tolerate up to 30% packet loss without impacting voice quality. Supports provision and management via GDMS. New voice message and mute LED indicator. HAC/VCH (ADA) compliant handset volume boost. Magnetic Hook Switch feature.

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
Keypad	26 keys, including: -6 Context-Sensitive Soft keys; -12 Standard Phone Digits keys (0-9: speed dial keys configuration on web page, * , #); -5 Function keys (Flash, Redial, Hands-free, Voice Mail, Hold); -3 Volume Control keys, Up/Down/Mute (with red color LED)
HD Audio	One HD handset support for wide band audio

Voice Codecs	Support for G.729A/B, G.711?/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
Voice Capabilities	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
Telephony Features	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.
Advanced Features	Support for multicast paging and E911 service. Support GDS Door opening. Support for advanced jitter-resilience algorithm.
USB	USB Type-C port for charging external devices (500mA MAX)
QoS	Layer 2 QoS (802.1Q, 802.1p) and Layer 3 (ToS, DiffServ, MPLS) QoS
Security	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
Multi-language	English, Spanish, French, Chinese (pending)
Upgrade/Provisioning	Firmware upgrade via FTP / TFTP / HTTP / HTTPS, fast boot in 15 seconds, mass provisioning using GDMS/TR-069 or AES encrypted XML configuration file
Power & Green Energy Efficiency	Universal power adapter (GHP630W/GHP631W): Input: 100~240Vac 50~60Hz Output: 12V/0.5A(6W)
Temperature and Humidity	Operation: 0°C to 40°C Storage: -10°C to 60°C Humidity: 10% to 90% (Non-condensing)
Package Content	GHP phone, handset with cord, Base Stand, universal power supply (GHP630W, GHP631W), faceplate, Quick Installation Guide
Color	White (GHP630,GHP630W), Black (GHP631,GHP631W)
Physical	Unit size:210mm(L)*147mm(W)*89.8mm(H) (with handset and base stand) Unit weight: 601g (GHP630/GHP631), 658g (GHP630W/GHP631W US), 668g (GHP630W/GHP631W World) Package weight: 824g (GHP630/GHP631), 881g (GHP630W/GHP631W US),891g (GHP630W/GHP631W World)
GHP630 & GHP631 Compliance	FCC: Part 15 Subpart B, Class B; Part 68. 316/317. CE: EN 55032; EN 55035; EN IEC 61000-3-2; EN 61000-3-3; EN IEC 62368-1. UKCA: BS EN 55032; BS EN 55035; BS EN IEC 61000-3-2; BS EN 61000-3-3; BS EN 62368-1. RCM: AS/NZS CISPR32; AS/NZS 62368.1; AS/CA S004. IC: ICES-003; CS-03 Part V.
GHP630W & GHP631W Compliance	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

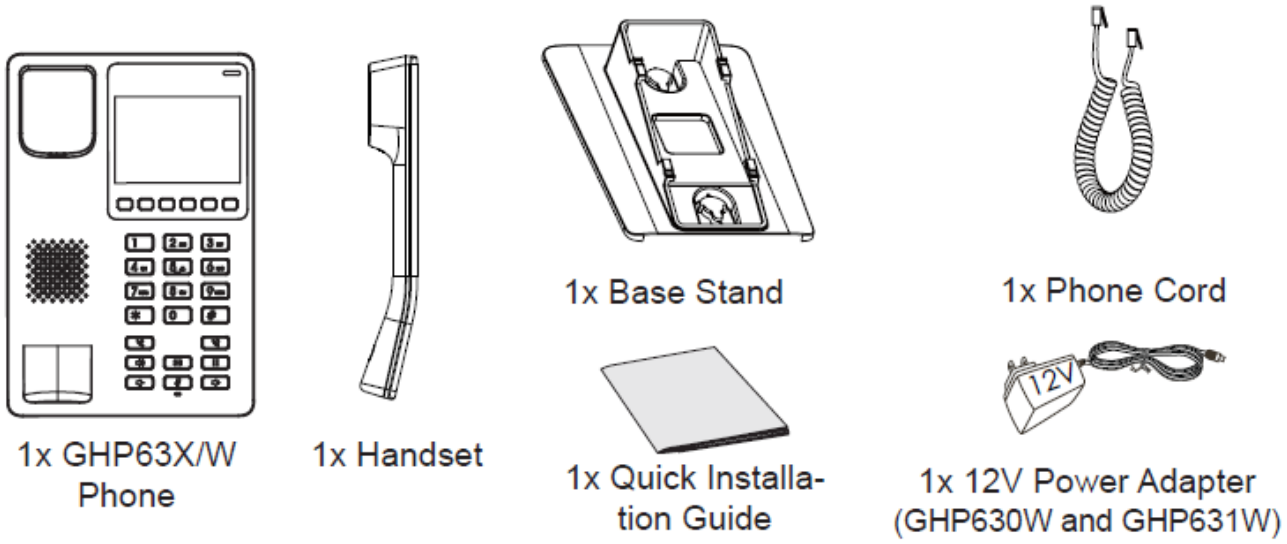
This chapter provides basic installation instructions, including the list of the packaging contents, and also information for obtaining the best performance with the GHP63X/W.

Equipment Packaging

GHP63X/W

GHP63X/W

1x GHP63X/W Phone 1x Handset 1x Base Stand 1x Quick Installation Guide 1x Phone Cord 1x 12V Power Adapter (GHP630W and GHP631W)



GHP63x/W Package Content

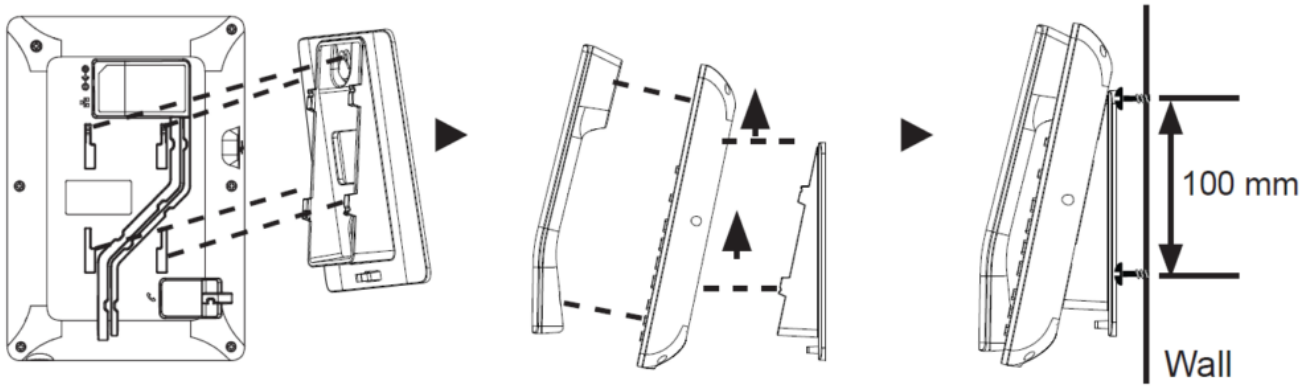
Please check the package before installation. If you find any one of the components missing, please contact your system administrator.

GHP63X/W Phone Setup

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

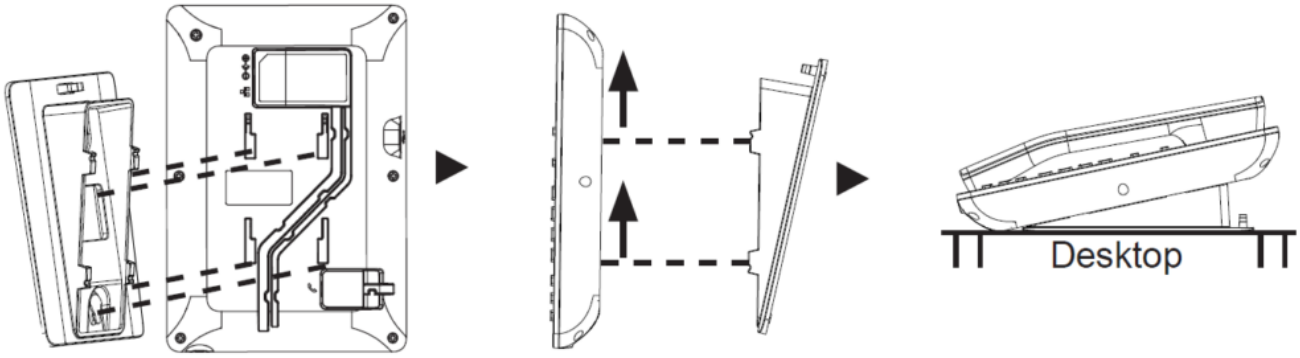
Wall Mount

1. On the wall where the GHP630/W & GHP631/W will be mounted, mark two dots with a 100mm distance in between vertically.
2. Using a drill, make a hole in 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 the wall mount spacers on the back of the phone.
4. Mount the GHP630/W & GHP631/W on the screws using their "Wall Mount Slots".



Desktop Installation

To install 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.

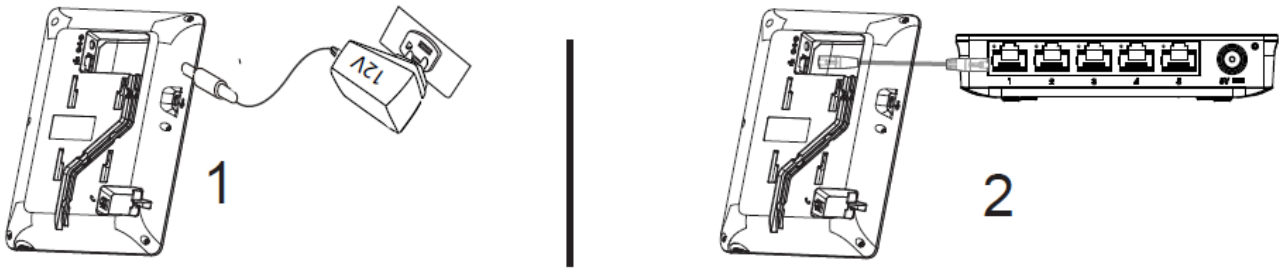


GHP63X Desktop Mount

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 for the 12V power adapter.



Power on the phone

Connecting the GHP63X/W

To set up the phone, follow the steps below:

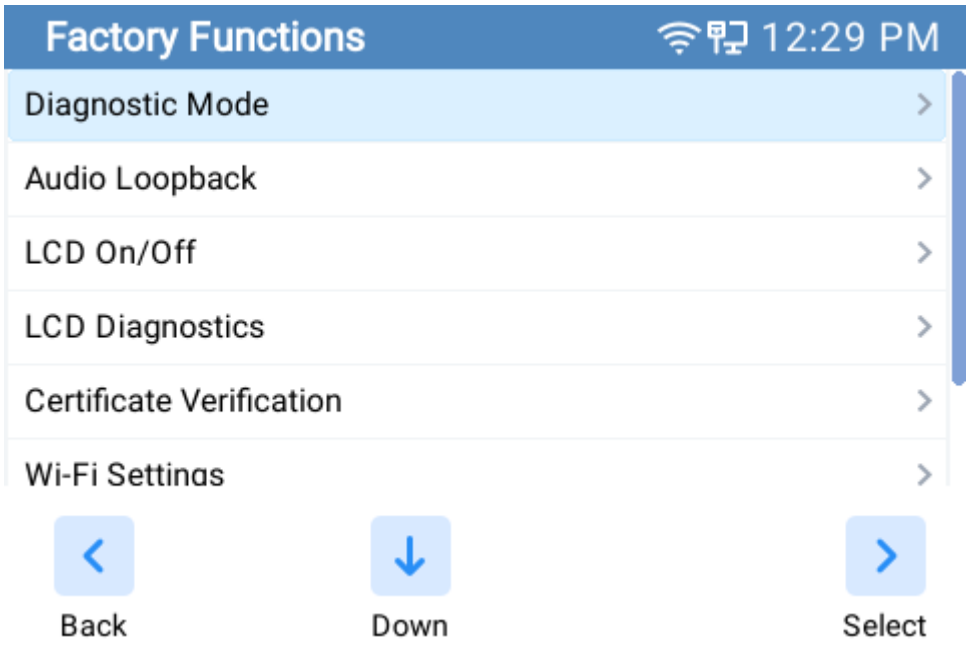
1. Plug in the phone cord to the handset RJ9 port and then connect it to the base.
2. Connect the LAN port of the phone to the RJ45 socket of a hub/switch or a router (LAN side of the router) using the Ethernet cable. This step can be skipped if using GHP630W & GHP631W with Wi-Fi.

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/WPA2PSK) 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

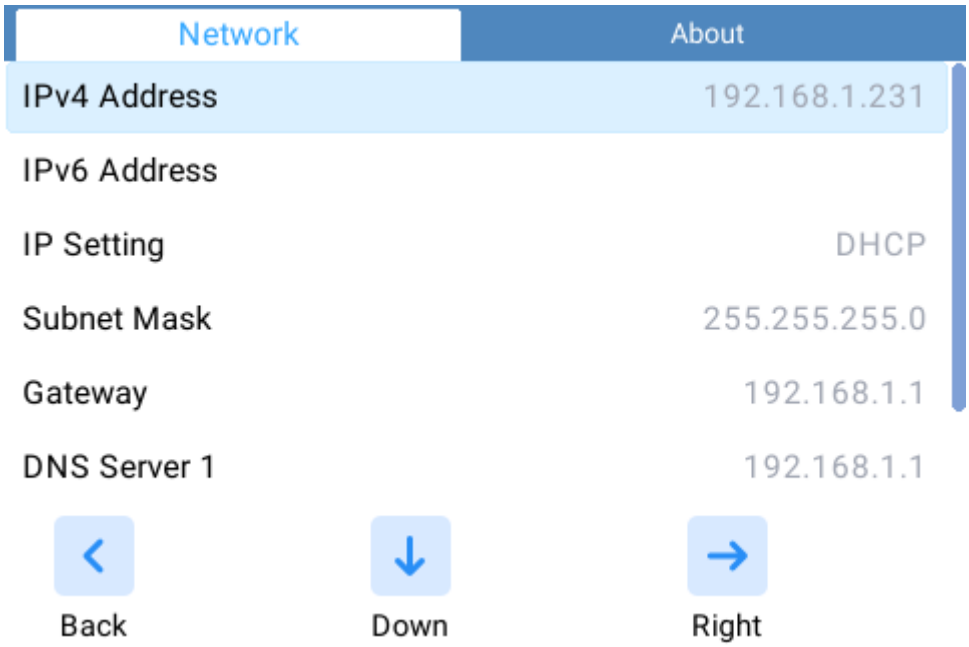
- Make sure your phone is powered on
- Press the **"HOLD" + 2** at the same time, to display the factory functions (including Wi-Fi settings for GHP631W/GHP630W version only)



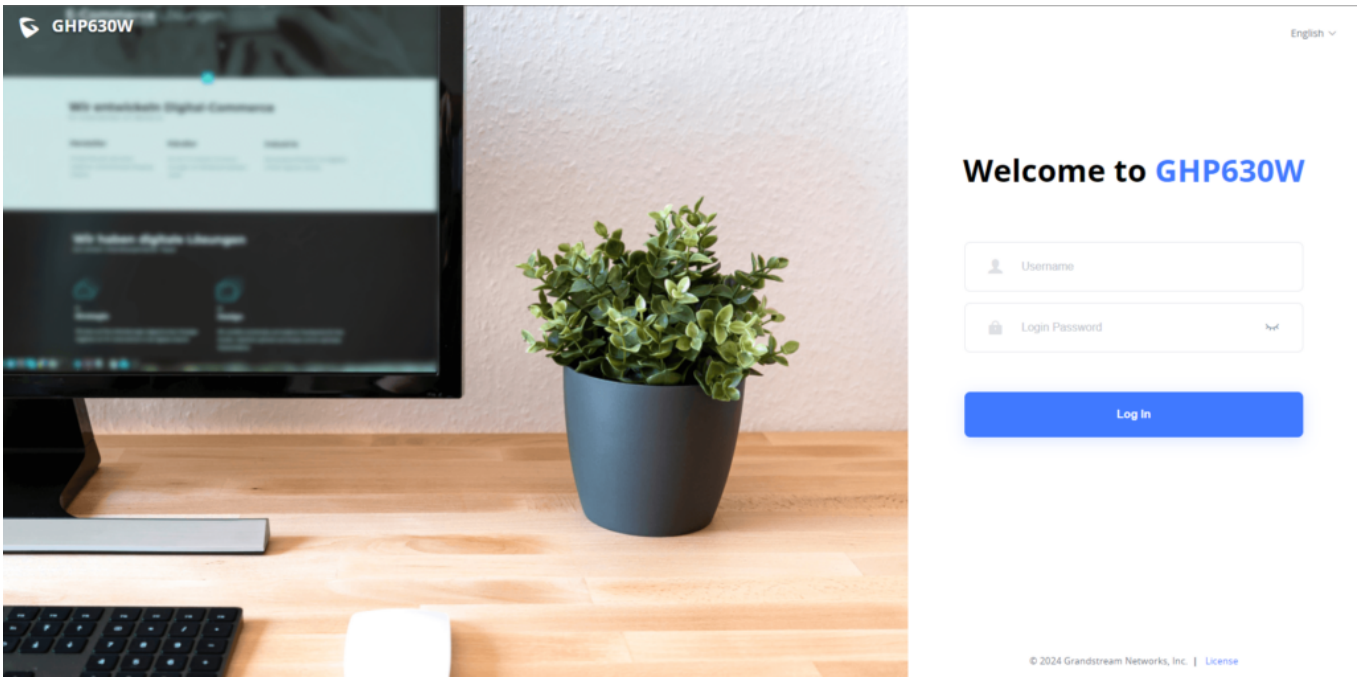
Phone Configuration Via Web Browser

- Ensure your phone is powered up and connected to the network.
- Locate the MAC address on the bottom of the device or the package.
- 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



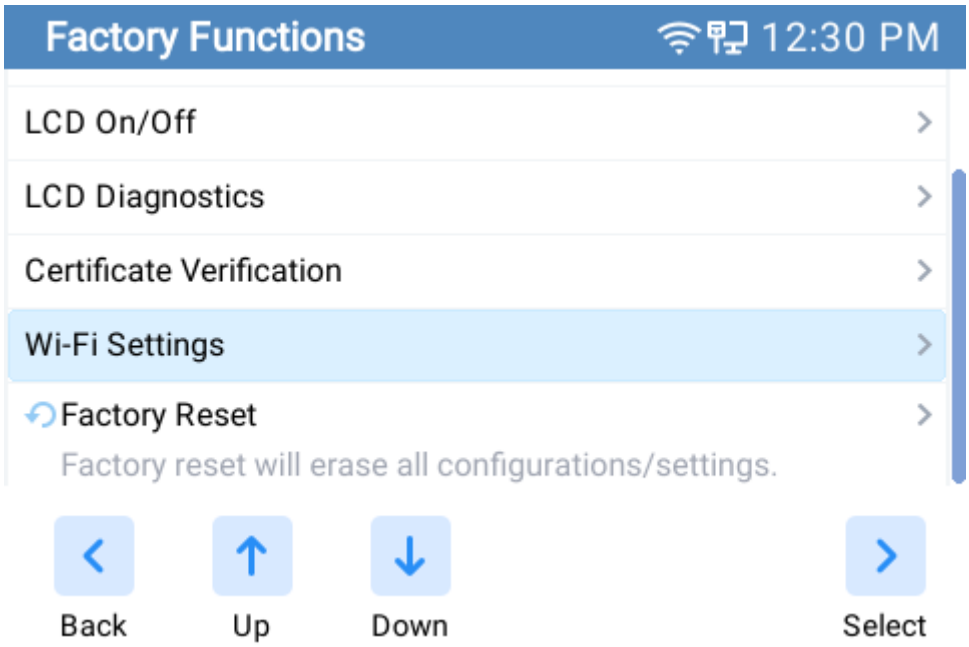
- Enter the admin's username and password to access the configuration menu. (The factory default username is "admin" while the default random password can be found on the sticker at the back of the unit.)



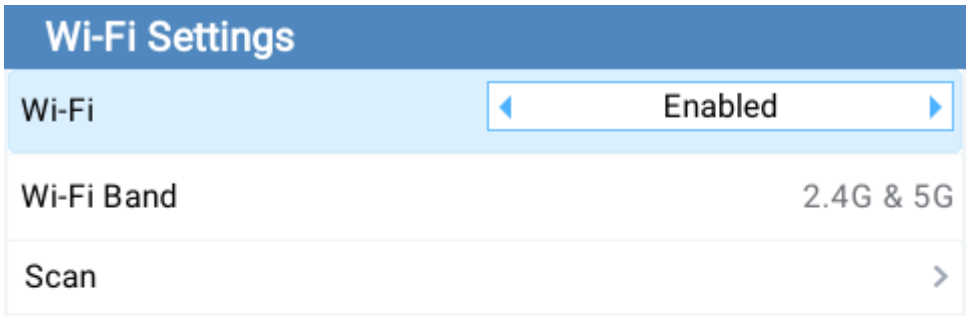
Connect to Wi-Fi (only for GHP630W/GHP631W)

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

- 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.

Screensaver Customization

To customize the GHP63X/W screensaver via the Web UI using an XML file, please refer to the GHP63X(W) - Wallpaper and Screensaver Customization Guide.

CONFIGURATION GUIDE

Status Page Definitions

Status -> Account Status	
Account Status	This interface indicates the information of the accounts which are configured on the IP phone.
Status -> Network Status	
Ethernet	
MAC Address	This field indicates the MAC address of the device.
IP Settings	This field indicated whether the obtained IP address was configured by DHCP or set statically.
IPv4 Address	This field displays the IPv4 address
IPv6 Address	This field displays the IPv6 address, if available
Subnet Mask	This field displays the subnet mask
Gateway	This field indicates the default gateway allocated.
DNS Server 1	This field displays the primary DNS server
DNS Server 2	This field displays the secondary DNS server
NAT Type	This field displays the NAT type used
Wi-Fi (Only for GHP63xW)	
WLAN MAC Address	This field indicates the WLAN MAC Address.
SSID	This field indicates the SSID that the device is connected to.
Country Code	This field indicates the Country Code.

IPv4 Address Type	This field indicates theIPv4 Address Type, dynamic or static.
IPv4 Address	This field indicates the IPv4 Address.
Gateway	This field indicates the Gateway IP Address.
IPv4 NAT Type	This field indicates the IPv4 NAT Type.
IPv6 Address NAT Type	This field indicates the IPv6 NAT Type.
DNS & NAT	
DNS Mode	Displays the DNS Mode used for both accounts.
NAT Traversal	Displays whether NAT Traversal is enabled or not, for both accounts.
Status -> System Info?	
Information	
Product model	This field indicates the product model.
Part number	This field indicates the part number.
Serial Number	Displays the GHP6xx's Serial Number.
Certificate Type	Displays the certificate type.
Security Version	Indicates the version of the security software.
Software version	This field indicates the version of the firmware installed. Including the following types BootBaseProg: This is the main device firmware ResGUI
Language	This field indicates the language used for displaying the web user interface.
Recommended Time Zone	This field indicates the recommended time zone.
System Up Time	This field indicates how long the devices has been turned on.
System Time	This field indicates the time and date set on the system.
System Time Zone	This field indicates the system time zone configured on the device.
Download System Information	This option allows downloading all the the system information.
Capture Screen	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 alows the screenshot download
Clear Screenshots	Deletes the latest screenshot taken
Service Status	Displays information about the service status, by displaying parameters such as the gui memory usage, the phone memory usage, and the cpe memory usage
Core Dump	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

Account Basic Settings

Account Register	
Account Active	Indicates whether the account is active.The default setting is "No".
Account Name	The name associated with each account to be displayed on the LCD. (e.g., MyCompany)

SIP Server	The URL or IP address, and port of the SIP server. This is provided by your VoIP service provider (e.g., sip.mycompany.com, or IP address)
Secondary SIP Server	The URL or IP address, and port of the SIP server. This will be used when the primary SIP server fails
Outbound Proxy	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
Secondary Outbound Proxy	Defines secondary outbound proxy that will be used when the primary proxy cannot be connected.
SIP User ID	User account information, provided by your VoIP service provider.
SIP Authentication ID	SIP service subscriber's Authenticate ID used for authentication. It can be identical to or different from the SIP User ID.
SIP Authentication Password	The account password required for the phone to authenticate with the SIP server before the account can be registered.After it is saved, this will appear as hidden for security purpose.
Name	The SIP server subscriber's name (optional) that will be used for Caller ID display (e.g., John Doe).
TEL URI	If the phone has an assigned PSTN telephone number, this field should be set to "user=phone". A "user=phone" parameter will be attached to the Request-URI and "To" header in the SIP request to indicate the E.164 number. If set to "Enable", "tel:" will be used instead of "sip:" in the SIP request.
Voice Mail Access Number	Allows users to access voice messages by pressing the MESSAGE button on the phone. This value is usually the VM portal access number.
Network Settings	
DNS Mode	This parameter controls how the Search Appliance looks up IP addresses for hostnames. If "Use Configured IP" is selected, please fill in Primary IP, Backup IP 1 and Backup IP 2.A RecordSRVNAPTR/SRVUse Configured IP
Maximum Number of SIP Request Retries	Sets the maximum number of retries for the device to send requests to the server. In DNS SRV configuration, if the destination address does not respond, all request messages are resent to the same address according to the configured retry times. Valid range: 1-10.
DNS SRV Failover Mode	Configures the preferred IP mode for DNS SRV. If set to "default", the first IP from the query result will be applied. If set to "Saved one until DNS TTL", previous IP will be applied before DNS timeout is reached. If set to "Saved one until no response", previous IP will be applied even after DNS timeout until it cannot respond.Default: If the option is set with "default", it will again try to send register messages to one IP at a time, and the process repeats. Saved one until DNS TTL: If the option is set with "Saved one until DNS TTL", it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up. Saved one until no responses: If the option is set with "Saved one until no responses", it will send registered messages to the previously registered IP first, but this behavior will persist until the registered server does not respond. Failback follows failback expiration timer: If "Failback follows failback expiration timer" is selected, the device will send all SIP messages to the current failover SIP server or Outbound Proxy until the failback timer expires.
Register Before DNS SRV Failover	Configures whether to send REGISTER requests to the failover SIP server or Outbound Proxy before sending INVITE requests in the event of a DNS SRV failover.
Primary IP	Configures the primary IP address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 1	Configures the backup IP 1 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.
Backup IP 2	Configures the backup IP 2 address where the phone sends DNS query to when "Use Configured IP" is selected for DNS mode.

NAT Traversal	Set NAT traversal to activate the NAT penetration mechanism. options to be chosen are No, STUN, or Keep-Alive. When set to "STUN" and the STUN server address is specified, detection will be based on the STUN server. 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.The Default value is set to "No".
Support rport (RFC3581)	Configures to use symmetric response routing. If it is used, the "rport" field will be added to the Via header field in the SIP Request, and the information will be extracted from the SIP 200OK Response for SIP Register to rewrite the SIP Contact information and apply it in subsequent SIP Requests.
Proxy-Require	A SIP Extension to notify the SIP server that the phone is behind a NAT/Firewall.

SIP Settings

Basic Settings	
SIP Registration	Selects whether the phone will send SIP Register messages to the proxy/server. The default setting is "Enabled".
UNREGISTER on Reboot	If set to "No", the phone will not unregister the SIP user's registration information before new registration. If set to "All", the SIP Contact header will use "*" to clear all SIP user's registration information. If set to "Instance", the phone only needs to clear the current SIP user's info.
REGISTER Expiration	Specifies the frequency (in minutes) in which the phone refreshes its registration with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
SUBSCRIBE Expiration	Specifies the frequency (in minutes) in which the phone refreshes its subscription with the specified registrar.The maximum value is 64800 minutes (about 45 days). The default value is 60 minutes.
Re-Register before Expiration	Specifies the time frequency (in seconds) that the phone sends re-registration request before the Register Expiration. The default value is 0.
Registration Retry Wait Time	Specifies the interval to retry registration if the process is failed. The valid range is 1 to 3600. The default value is 20 seconds.
Add Auth Header on Initial REGISTER	If enabled, the phone will add Authorization header in initial REGISTER request.Default is "Disabled".
Enable OPTIONS Keep Alive	Configures whether to enable SIP OPTIONS to track account registration status. If enabled, the phone will send periodic OPTIONS messages to server to track the connection status with the server.Default is "Disabled".
OPTIONS Keep Alive Interval	Configures the time interval the phone sends OPTIONS message to the server. If set to 30 seconds, it means the phone will send an OPTIONS message to the server every 30 seconds.
OPTIONS Keep Alive Max Tries	Configures the maximum number of times the phone will try to send OPTIONS message consistently to server without receiving a response. If set to "3", the phone will send OPTIONS message 3 times. If no response from the server, the phone will re-register.
SUBSCRIBE for MWI	When set to "Yes", a SUBSCRIBE for Message Waiting Indication will be sent periodically.The default setting is "No".
SUBSCRIBE for Registration	When set to "Yes", a SUBSCRIBE for Registration will be sent out periodically.The default setting is "No".
Use Privacy Header	Configures whether the "Privacy Header" is present in the SIP INVITE message. Default: the phone will add "Privacy Header" when special feature is not "Huawei IMS". Yes: the phone will always add "Privacy Header". No: the phone will not add "Privacy Header". The default setting is "default".

Use P-Preferred- Identity Header	Configures whether the "P-Preferred-Identity Header" is present in the SIP INVITE message. Default: the phone will add "P-Preferred-Identity header" when special feature is not "Huawei IMS". Yes: the phone will always add "P-Preferred-Identity header". No: the phone will not add "P-Preferred-Identity header".
Use X-Grandstream-PBX Header	Configures to use X-Grandstream-PBX header in SIP request.Default setting is "Yes".
Use P-Access-Network-Info Header	Configures to use P-Access-Network-Info header in SIP request.Default setting is "Yes".
Use P-Emergency-Info Header	Configures to use P-Emergency-Info header in SIP request.Default setting is "Yes".
Use MAC Header	If Register Only, all outgoing SIP message will include the MAC header. If Yes to all SIP, all outgoing SIP messages will include the MAC header. If No, the phone's MAC header will not be included in any outgoing SIP messages. The default setting is "No".
Add MAC in User-Agent	If Yes except REGISTER, all outgoing SIP messages will include the phone's MAC address in the User-Agent header, except for REGISTER and UNREGISTER. If Yes to All SIP, all outgoing SIP messages will include the phone's MAC address in the User-Agent header. If No, the phone's MAC address will not be included in the User-Agent header in any outgoing SIP messages. The default setting is "No".
SIP Transport	Selects the network protocol used for the SIP transport.The default setting is "UDP".
Enable TCP Keep-alive	Configures whether to enable TCP Keep-alive for the TCP connection between the terminal and the SIP server.
SIP Listening Mode	Configures whether or not to listen to multiple SIP protocols. If set to "Dual", phone will listen to TCP when UDP is selected. If set to "Dual (Secured)", phone will listen to TLS/TCP when UDP is selected. If "TCP" or "TLS/TCP" is selected, UDP will be listened too. If set to "Dual (BLF Enforced)", phone will try to enforce BLF subscriptions to use TCP protocol by adding 'transport=tcp' to the Contact header. The default setting is "Transport Only".
Local SIP Port	Configures the local SIP port used to listen and transmit.
SIP URI Scheme when using TLS	Specifies if "sip" or "sips" will be used when TLS/TCP is selected for SIP Transport. The default setting is "sips".
Use Actual Ephemeral Port in Contact with TCP/TLS	Configures whether the actual ephemeral port in contact with TCP/TLS will be used when TLS/TCP is selected for SIP Transport.The default setting is "No".
Support SIP Instance ID	Configures whether SIP Instance ID is supported or not.The default setting is "Yes".
SIP T1 Timeout	SIP T1 Timeout is an estimate of the round-trip time of transactions between a client and server. If no response is received the timeout is increased and request re-transmit retries would continue until a maximum amount of time define by T2. The default setting is 0.5 seconds.
SIP T2 Timeout	SIP T2 Timeout is the maximum retransmit time of any SIP request messages (excluding the INVITE message). The re-transmitting and doubling of T1 continues until it reaches the T2 value. Default is 4 seconds.
Outbound Proxy Mode	Configures whether to put the Outbound Proxy in the Route header, or if SIP messages should always be sent to Outbound Proxy. In route Not in route Always send to Default is "in route".
Enable 100rel	When enabled, the 100rel tag is appended to the value of the Supported header of the initial signaling messages.The default setting is "No".
Use Route Set in Notify (Follow RFC 6665)	Configures whether to use route set in NOTIFY (follow RFC 6665). If enabled, the Request URI of the refresh subscription will use the URI in the received NOTIFY Contact (RFC 6665). If disabled, the URI in the previously subscribed 200 OK Contact will be used.

Session Timer	
Enable Session Timer	Configures whether to enable session timer function. It enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). If there is no refresh via an UPDATE or re-INVITE message, the session will be terminated once the session interval expires. If set to "Yes", the phone will use the related parameters when sending session timer according to "Session Expiration". If set to "No", session timer will be disabled.The default setting is "No".
Session Expiration	Session Expiration is the time (in seconds) where the session is considered timed out, provided no successful session refresh transaction occurs beforehand.The default setting is 180. The valid range is from 90 to 64800.
Min-SE	The minimum session expiration (in seconds). The default value is 90 seconds. The valid range is from 90 to 64800.
Caller Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it makes outbound calls.The default setting is "No".
Callee Request Timer	If set to "Yes" and the remote party supports session timers, the phone will use a session timer when it receives inbound calls.The default setting is "No".
Force Timer	If set to "Yes", the phone will use the Session Timer even if the remote party does not support this feature. Otherwise, Session Timer is enabled only when the remote party supports it.The default setting is "No".
UAC Specify Refresher	As a caller, select UAC to use the phone as the refresher, or select UAS to use the callee or proxy server as the refresher. When set to "Omit", the refresh object is not specified.The default setting is "UAC".
UAS Specify Refresher	As a callee, select UAC to use caller or proxy server as the refresher, or select UAS to use the phone as the refresher.The default setting is "UAC".
Force INVITE	Select "Yes" to force using the INVITE method to refresh the session timer.The default setting is "No".

Codec Settings

Audio	
Preferred Vocoder(Choice 1 - 8)	Multiple vocoder types are supported on the phone, the vocoders in the list is a higher preference. Users can configure vocoders in a preference list that is included with the same preference order in SDP message. Opus G722 PCMU PCMA G.723.1 G.729.1 iLBC G.726-32
Codec Negotiation Priority	Configures the phone to use which codec sequence to negotiate as the callee. When set to "Caller", the phone negotiates by SDP codec sequence from received SIP Invite. When set to "Callee", the phone negotiates by audio codec sequence on the phone. The default setting is "Callee".
Use First Matching Vocoder in 200OK SDP	When set to "Yes", the device will use the first matching vocoder in the received 200OK SDP as the codec. The default setting is "No".
iLBC Frame Size	Selects iLBC packet frame size. Users can choose from 20ms and 30ms. The default setting is "30ms".
iLBC Payload Type	Specifies iLBC payload type. Valid range is 96 to 127. Cannot be the same as Opus or DTMF payload type. Valid range is 96 to 127. The default setting is "97".
G.726-32 Packing Mode	Selects "ITU" or "IETF" for G726-32 packing mode.The default setting is "ITU".
G.726-32 Dynamic Payload Type	Specifies G.726-32 payload type. Valid range is 96 to 127. Default is 127.
Opus Payload Type	Specifies Opus payload type. Valid range is 96 to 127. It cannot be the same as iLBC or DTMF Payload Type. Default value is 123.

Send DTMF	Specifies the mechanism to transmit DTMF digits. There are 3 supported modes: In audio: DTMF is combined in the audio signal (not very reliable with low-bit-rate codecs). RFC2833 sends DTMF with RTP packet. Users can check the RTP packet to see the DTMFs sent as well as the number pressed. SIP INFO uses SIP INFO to carry DTMF. Default setting is "RFC2833".
DTMF Payload Type	Configures the payload type for DTMF using RFC2833. Cannot be the same as iLBC or OPUS payload type.
Silence Suppression	If set to "Yes", when silence is detected, a small quantity of VAD packets (instead of audio packets) will be sent during the period of no talking. For codec G.723 and G.729 only.Default setting is "No".
Jitter Buffer Type	Selects either Fixed or Adaptive for jitter buffer type, based on network conditions. The default setting is "Adaptive".
Jitter Buffer Length	Selects jitter buffer length from 100ms to 800ms, based on network conditions. The default setting is "300ms".
Voice Frames Per TX	Configures the number of voice frames transmitted per packet. It is recommended that the IS limit value of Ethernet packet is 1500 bytes or 120 kbps. When configuring this, it should be noted that the "ptime" value for the SDP will change with different configurations here. This value is related to the codec used in the codec table or negotiate the payload type during the actual call. For example, if set to 2 and the first code is G.729, G.711 or G.726, the "ptime" value in the SDP datagram of the INVITE request is 20 ms. If the "Voice Frame/TX" setting exceeds the maximum allowed value, the phone will use and save the maximum allowed value for the selected first codec. It is recommended to use the default setting provided, and incorrect setting may affect voice quality.The default setting is 2.
G.723 Rate	Selects encoding rate for G723 codec.
RTP Settings	
SRTP Mode	Enable SRTP mode based on your selection from the drop-down menu. No Enabled but Not forced Enabled and Forced Optional The default setting is "No".
SRTP Key Length	Allows users to specify the length of the SRTP calls. Available options are: AES 128&256 bit AES 128 bit AES 256 bit Default setting is AES 128&256 bit
Crypto Life Time	Enable or disable the crypto lifetime when using SRTP. If users set to disable this option, phone does not add the crypto lifetime to SRTP header. The default setting is "Yes".
RTCP Mode	Configure RTCP port negotiation rules. Default: Use the traditional RTCP port, which is "RTP port+1". Negotiate RTCP Port: Use attribute RTCP to negotiate. RTCP Mux: The caller actively negotiates the RTCP port and indicates RTCP Mux at the same time. RTCP Mux Only: The caller forces RTCP Mux, generated by the local media port only apply for RTP port.
RTCP Keep-Alive Method	Configures the RTCP channel keep-alive packet type. Receiver Report: The RTCP channel will sends "receiver report+source description+RTCP extension" as keep-alive data. Sender Report: The RTCP channel will sends "Sender report+source description+ RTCP extension" as keep-alive data.
RTP Keep-Alive Method	Configures the RTP channel keep-alive packet type. No: No data will be sent RTP Version 1: The wrong version infor "1" will be carried when sending RTP data packets.
Symmetric RTP	Configures whether Symmetric RTP is used or not. Symmetric RTP means that the UA uses the same socket/port for sending and receiving the RTP stream. The default setting is "No".
RTP IP Filter	Configures whether to filter the received RTP. If set to "Disable", the device will receive RTP from any address; If set to "IP Only", the device will receive RTP from certain IP address in SDP with no port limited; If set to "IP and Port", the device will only receive RTP from IP address & port in SDP. Disabled by default

Account Call Settings

General	
Key as Send	Pressing the selected key will immediately dial out.
No Key Entry Timeout	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.
Send Anonymous	If set to "Yes", the "From" header in outgoing INVITE messages will be set to anonymous.
Anonymous Call Rejection	If set to "Yes", anonymous calls will be rejected.
Enable Call Waiting	Enables the call waiting feature. If set to "No", new incoming calls will be rejected after the call is established.
RFC2543 Hold	If set to "Yes", c=0.0.0.0 will be used in INVITE SDP for hold.
Ring Timeout	Configures the timeoput (in seconds) for the phone to ring when an incoming call is not answered. Valid range is 30 to 3600.
Call Log	Configures Call Log settings on the phone.
Auto Answer	
Auto Answer	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep. Default setting is "No".
Auto Answer Numbers	Allows the user to configure specific numbers to auto answer. If not set, all numbers will be auto answered If auto answer is enabled. Up to 10 numbers can be configured.
Intercom	
Play warning tone for Auto Answer Intercom	If enabled, phone will play warning tone when auto answering intercom.
Custom Alert-Info for Auto Answer	Used exclusively to match the contents of the Alert-Info header for auto answer. The default auto answer headers will not be matched if this is defined.
Allow Auto Answer by Call-Info/Alert-Info	If set to "Yes", the phone will automatically turn on the speaker phone to answer incoming calls after a short reminding beep, based on the SIP Call-Info/Alert-Info header sent from the server/proxy.Default is "Yes".
Allow Barging by Call-Info/Alert-Info	When enabled, the phone will automatically put the current call on hold and answer the incoming call based on the SIP Call-Info/Alert-Info header sent from the server/proxy. However, if the current call was answered based on the SIP Call-Info/Alert-Info header, then all other incoming calls with SIP Call-Info/Alert-Info headers will be rejected automatically. Default setting is "No".
Mute on Intercom Answer	If enabled, the phone will mute the microphone after answering an intercom call via Call-Info/Alert-Info.
Transfer	
Transfer on Conference Hangup	Configures whether the call is transferred to the other party if the conference initiator hangs up.
Enable Local Call Features	When enabled, the phone will use the local call function. When disabled, the server-side call function code will be used. Default setting is enabled.
Enable Recovery on Blind Transfer	Enable Recovery to the call to the transferee on failing blind transfer to the target.
Blind Transfer Wait Timeout	Configures the timeout (in seconds) when waiting for sipfrag response in blind transfer. Valid range is 30 to 300
Refer-To Use Target Contact	If enabled, the "Refer-to" hear uses the transferred target's Contact header information for attended transfer.
Dial plan	
Dial Plan Prefix	Configures a prefix added to all numbers when making outbound calls.

Bypass Dial Plan	Bypass the dial plan when dialing from one of the available items:ContactsCall History Incoming CallCall History Outgoing CallDialing PageMPKAPI
Dial Plan	Configures the dial plan rule. For syntax and examples, please refer to user manual for more details.Dial Plan Rules:Accepted Digits: 1,2,3,4,5,6,7,8,9,0, *, #, A,a,B,b,C,c,D,d;Grammar: x - any digit from 0-9;Grammar: X - any character from 0-9, a-z, A-Z.xx+ - at least 2 digit numbersxx - only 2 digit numbersXX - two characters (AA, Ab, 1C, f5, 68,...)test : only string "test" will pass the dial plan check^ - exclude[3-5] - any digit of 3, 4, or 5[147] - any digit of 1, 4, or 7<2=011> - replace digit 2 with 011 when dialing| - the OR operandExample 1: {[369]11 | 1617xxxxxxx}Allow 311, 611, and 911 or any 11 digit numbers with leading digits 1617;Example 2: {^1900x+ | <=1617>xxxxxxx}Block any number of leading digits 1900 or add prefix 1617 for any dialed 7 digit numbers;Example 3: {1xxx[2-9]xxxxxx | <2=011>x+}Allows any number with leading digit 1 followed by a 3-digit number, followed by any number between 2 and 9, followed by any 7-digit number OR Allows any length of numbers with leading digit 2, replacing the 2 with 011 when dialed.Example of a simple dial plan used in a Home/Office in the US: { ^1900x. | <=1617>[2-9]xxxxxx | 1[2-9]xx[2-9]xxxxxx | 011[2-9]x. | [3469]11 }Explanation of example rule (reading from left to right):^1900x. - prevents dialing any number started with 1900;<=1617>[2-9]xxxxxx - allows dialing to local area code (617) numbers by dialing7 numbers and 1617 area code will be added automatically;1[2-9]xx[2-9]xxxxxx |- allows dialing to any US/Canada Number with 11 digits length;011[2-9]x - allows international calls starting with 011;[3469]11 - allows dialing special and emergency numbers 311, 411, 611 and 911.Note: In some cases, where the user wishes to dial strings such as *123 to activate voice mail or other applications provided by their service provider, the * should be predefined inside the dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.Max length of dial plan is up to 1024 characters.
Call Display	
Caller ID Display	Auto: The phone will look for the Caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. Disabled: All incoming calls are displayed with "Unavailable" From Header: The caller ID will be retrieved from the From Header in the incoming SIP INVITE.
Callee ID Display	Auto: The phone will update the callee ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and To Header in 180 Ringing.Disabled: Callee ID will be displayed as "Unavailable"To Header: Caller ID will not be updated and displayed as To Header
Ringtone	
Account Ring Tone	Allows users to configure the ringtone for the account. Users can choose from different ringtones from the dropdown menu.
Ignore Alert-Info header	Configures to play default ringtone by ignoring Alert-Info header.The default setting is "No".
Match Incoming Caller ID	Specifies matching rules with number, pattern, or Alert Info text (up to 10 matching rules). When the incoming caller ID or Alert Info matches the rule, the phone will ring with selected distinctive ringtone. Matching rules:Specific caller ID number. For example, 8321123.A defined pattern with certain length using x and + to specify, where x could be any digit from 0 to 9. Samples: xx+ : at least 2-digit number.xx : only 2-digit number.[345]xx: 3-digit number with the leading digit of 3, 4 or 5.[6-9]xx: 3-digit number with the leading digit from 6 to 9.Alert Info textUsers could configure the matching rule as certain text (e.g., priority) and select the custom ring tone mapped to it. The custom ring tone will be used if the phone receives SIP INVITE with Alert-Info header in the following format: Alert-Info: <http://127.0.0.1>; info=prioritySelects the distinctive ring tone for the matching rule. When the incoming caller ID or Alert Info matches one of the 10 rules, the phone will ring with the associated ringtone.

Account Advanced Settings

Security Settings

Check Domain Certificates	Configures whether the domain certificates will be checked when TLS/TCP is used for SIP Transport. The default setting is "No".
Validate Certificate Chain	Validate certification chain when TCP/TLS is configured.The default setting is "No".
Validate Incoming SIP Messages	Specifies if the phone will check the incoming SIP messages Caller ID and CSeq headers. If the message does not include the headers, it will be rejected. The default setting is "No".
Allow Unsolicited REFER	Configures whether to dial the number carried by Refer-to header after receiving out-of-dialog SIP REFER request actively.If set to "Disabled", the phone will send error warning and stop dialing.If set to "Enabled/Force Auth", the phone will dial the number after sending authentication. If the authentication fails, it will stop dialing.If set to "Enabled", the phone will dial all numbers carried by SIP REFER.
Accept Incoming SIP from Proxy Only	When set to "Yes", the SIP address of the Request URL in the incoming SIP message will be checked. If it does not match the SIP server address of the account, the call will be rejected. The default setting is "No".
Check SIP User ID for Incoming INVITE	If set to "Yes", SIP User ID will be checked in the Request URI of the incoming INVITE. If it does not match the phone's SIP User ID, the call will be rejected. The default setting is "No".
Allow SIP Reset	Allow SIP Notification message to perform factory reset.The default setting is "No".
Authenticate Incoming INVITE	If set to "Yes", the phone will challenge the incoming INVITE for authentication with SIP 401 Unauthorized response.The default setting is "No".
MOH (Music on Hold)	
On Hold Reminder Tone	Configures to play reminder tone when the call is on hold.
Music On Hold URI	Music On Hold URI to call when a call is on hold if server supports it.
Advanced Features	
Special Feature	Specifies the server type for special requirements.
Feature Key Synchronization	When enabled, DND and Call Forward features will be synchronized with the SIP server. Disabled by default.
Reboot on check-sync event without "reboot="	When this option is enabled, the phone will reboot when it receives a SIP NOTIFY "check-sync" event that does not include a "reboot=" header. When this option is disabled, the phone will only perform provisioning (without rebooting) when it receives a SIP NOTIFY "check-sync" event without a "reboot=" header. This option is enabled by default.

Account Swap Settings

Swap Account Settings	Allows users to swap the two accounts that they have configured. This will Increase the flexibility of account management.Note: Make sure to press "Start" to complete the process.

Phone Settings Page Definition

Basic Settings

Local RTP Port	Configures the local RTP port used to listen and transmit. The valid range is 1024 to 65400 and it must be even.
Local RTP Port Range	Configures the range of local RTP port. Valid value is from 24 to 10000.
Use Random Port	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).

Keep-Alive Interval	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.
STUN Server	This option sets IP address or Domain name of the STUN server. Only non-symmetric NAT routers work with STUN.
Use NAT IP	Configures the NAT IP address used in SIP/SDP messages. It should ONLY be used if required by your ITSP.
Delay Registration	Configures the specific time that the account will be registered after booting up.
Enable Outbound Notification	Configures whether to enable outbound notifications such as Action URL.

Call Settings

General	
Preferred Default Account	Select the preferred default account for on-hook or off-hook dialing. when the selected account is unavailable, system will use the first available account to dial out.
Mute Key Functions While Idle	If set to 'Idle Mute", clicking the MUTE key while idle will cause the phone to be muted automatically when answering incoming calls.
Do Not Escape '#' as %23 in SIP URI	Replaces # by %23 for some special situations.
User-Agent Prefix	Configures the prefix in the User-Agent header
Outgoing	
Enable Direct IP Call	Enables Direct IP Call feature.This option is enabled by default.
Onhook Dial Barging	When the option is set to "Disabled", onhook dialing won't be interrupted by an incoming call.
Off-hook Auto Dial	Configures the digits to be dialed via the first account when the phone is off-hook.
Off-hook Auto Dial Delay	Configures the timeout (in seconds) for off-hook auto dial. Valid range is 0-30. If set to 0, it will be dialed out immediately. Otherwise, it will be dialed out after the configured timeout.
Off-hook/On-hook Timeout (s)	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.
Incoming	
Enable Missed Call Notification	Enables/Disables missed calls and voicemail LCD screen pop-up notifications. Default setting is enabled.
Allow Incoming Call before Ringing	This allows incoming calls after dialed but before ringing. This can be used under custom user configuration based on need.
Enable Call Waiting	Enables the call waiting feature. If set to "No", new incoming calls will be rejected after the call is established.
Enable Call Waiting Tone	Enables Call Waiting alert tone when another incmong call is received while a call is in progress.
Auto Answer Delay	Configures the delay for automatically answering the incoming call. Valid range is 0 to 10 (seconds).
In Call	
Enable Sending DTMF via specific MPKs	Allows certain MPKs to send DTMF in-call. This option does not affect Dial DTMF
Enable Auto Unmute	If the option is enabled, automatically unmute phone when a user unholds the call or establishes a new call.
Enable Busy Tone on Remote Disconnect	Playing busy tone when call is disconnected remotely.
Enable Mute Key In Call	When set to "No", the mute key will not work while on call.

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

Ringtone

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

Call Progress Tones	Configures ring or tone frequencies based on parameters from local telecom. The default value is North American standard. Frequencies should be configured with known values to avoid uncomfortable high pitch sounds. Syntax: f1=val,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]; (Frequencies are in Hz and cadence on and off are in 10ms) ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. To set a continuous ring, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Up to three cadences are supported. Call Waiting tone gain can be set to either: Low, Medium, or High, it is set to Low by Default
System Ringtone	
Dial Tone	
Second Dial Tone	
Message Waiting	
Ring Back Tone	
Call Waiting Tone	
Call Waiting Tone Gain	
Busy Tone	
Reorder Tone	

Multicast Paging

Multicast Paging Function	Enable or disable multicast paging.
Paging Barging	During an active call if incoming multicast page has higher priority (1 being the highest) than this value, the call will be held and multicast page will be played.
Paging Priority Active	If enabled, during a multicast page if another multicast is received with higher priority (1 being the highest) that one will played instead.
Multicast Listening	Secifies the label and multicast listening address, it supports up to 10 multicats addresses

Network Settings

Ethernet Settings

Internet Protocol	Select Prefer IPv4 or Prefer IPv6
IPv4 Address	
IPv4 Address	The IPv4 address obtained by the phone. Note: 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.
Host name (Option 12)	Specifies the name of the client. This field is optional but may be required by Internet Service Providers.
Vendor Class ID (Option 60)	Used by clients and servers to exchange vendor class ID.
DNS Server 1	Enter DNS Server 1 when static IP is used.
DNS Server 2	Enter DNS Server 2 when static IP is used.
Preferred DNS Server	Enter the Preferred DNS Server.

IPv6 Address	
IPv6 Address	The IPv6 address obtained by the phone. The address can be Prefix static or Full static Prefix static IPv6 address: An IPv6 address configuration where the network portion is manually set, while the interface identifier is generated automatically. Full static IPv6 address: An IPv6 address configuration where both the network portion and the interface identifier are manually set.
Static IPv6 Address	Enter the static IPv6 address when Full Static is used in "Statically configured" IPv6 address type.
IPv6 Prefix length	Enter the IPv6 prefix length when Full Static is used in "Statically configured" IPv6 address type.
DNS Server 1	Enter DNS Server 1 when static IP is used.
DNS Server 2	Enter DNS Server 2 when static IP is used.
Preferred DNS Server	Enter the preferred DNS server.

Advanced Settings

Advanced Network Settings	
DNS Refresh Timer (m)	Configures the refresh time (in minutes) for DNS query. If set to "0", the phone will use the DNS query TTL from DNS server response.
DNS Failure Cache Duration (m)	Configures the duration (in minutes) of previous DNS query fails. If set to "0", the feature will be disabled. Note: Only valid for SIP registration.
Enable LLDP	Controls the LLDP (Link Layer Discovery Protocol) service.
LLDP TX Interval	Configures LLDP TX Interval (in seconds). Valid range is 1 to 3600.
Enable CDP	If enabled, the device will use the Cisco Discovery Protocol feature.
Layer 3 QoS for SIP	Configures the layer 3 QoS parameter for SIP. This value is used for IP Precendence, DiffServ, or MPLS.
Layer 3 QoS for RTP	Configures the layer 3 QoS parameter for RTP. This value is used for IP Precendence, DiffServ, or MPLS.
Enable DHCP VLAN	Configures to enable or disable auto-configure for VLAN settings via DHCP.
Enable Manual VLAN Configuration	Allow phone to keep the VLAN configuration without applying them.
Layer 2 QoS 802.1Q/VLAN Tag	Assigns the VLAN Tag of the Layer 2 QoS packets.
Layer 2 QoS 802.1p Priority Value	Assigns the priority value of the Layer 2 QoS packets. Valid range is 0 to 7
Maximum Transmission Unit (MTU)	Configures the MTU in bytes
Remote Control	
Action URI Support	Configures whether to enable phone to handle action URI request.
Action URI Allowed IP List	List of allowed IP addresses from which the phone receives the action URI.
CSTA Control	Configures whether to enable the CSTA Control feature.

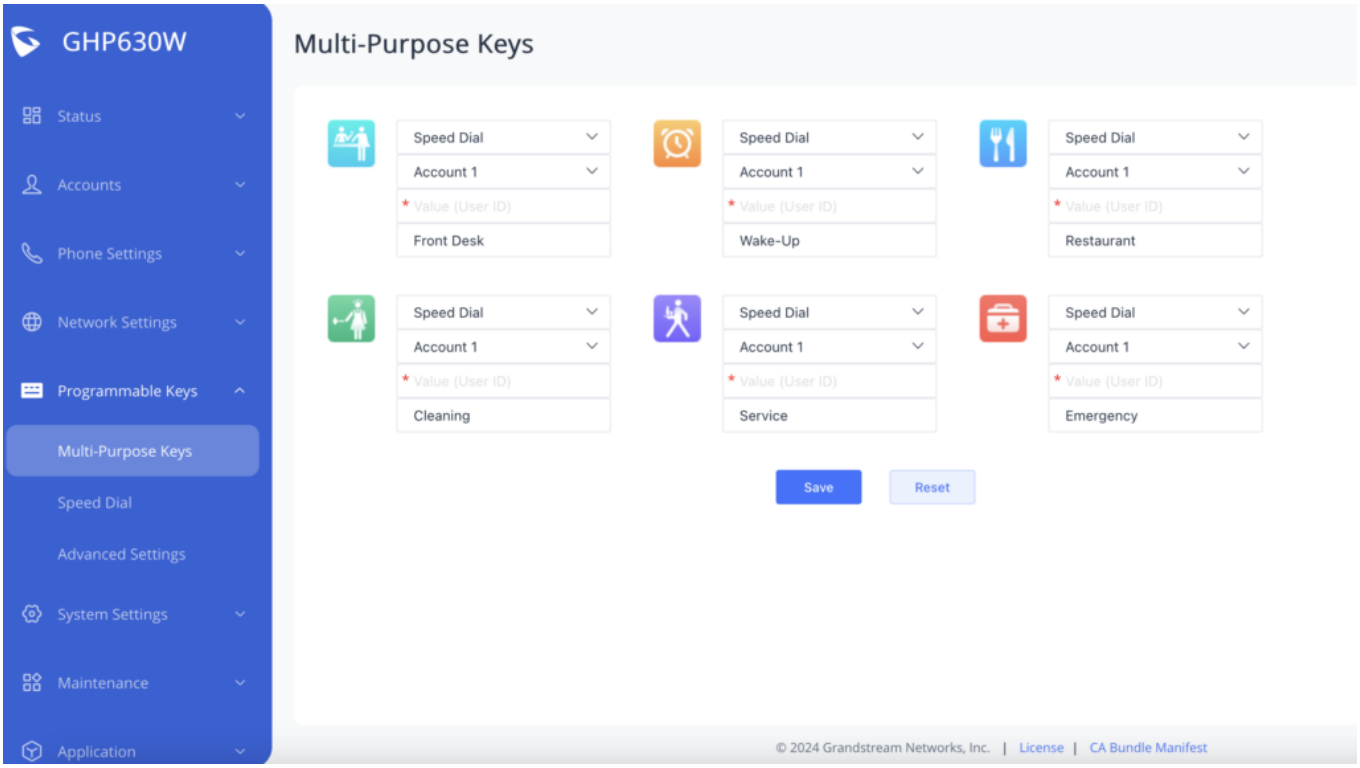
Wi-Fi Settings (Only GHP630W/GHP631W)

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

Programmable Keys

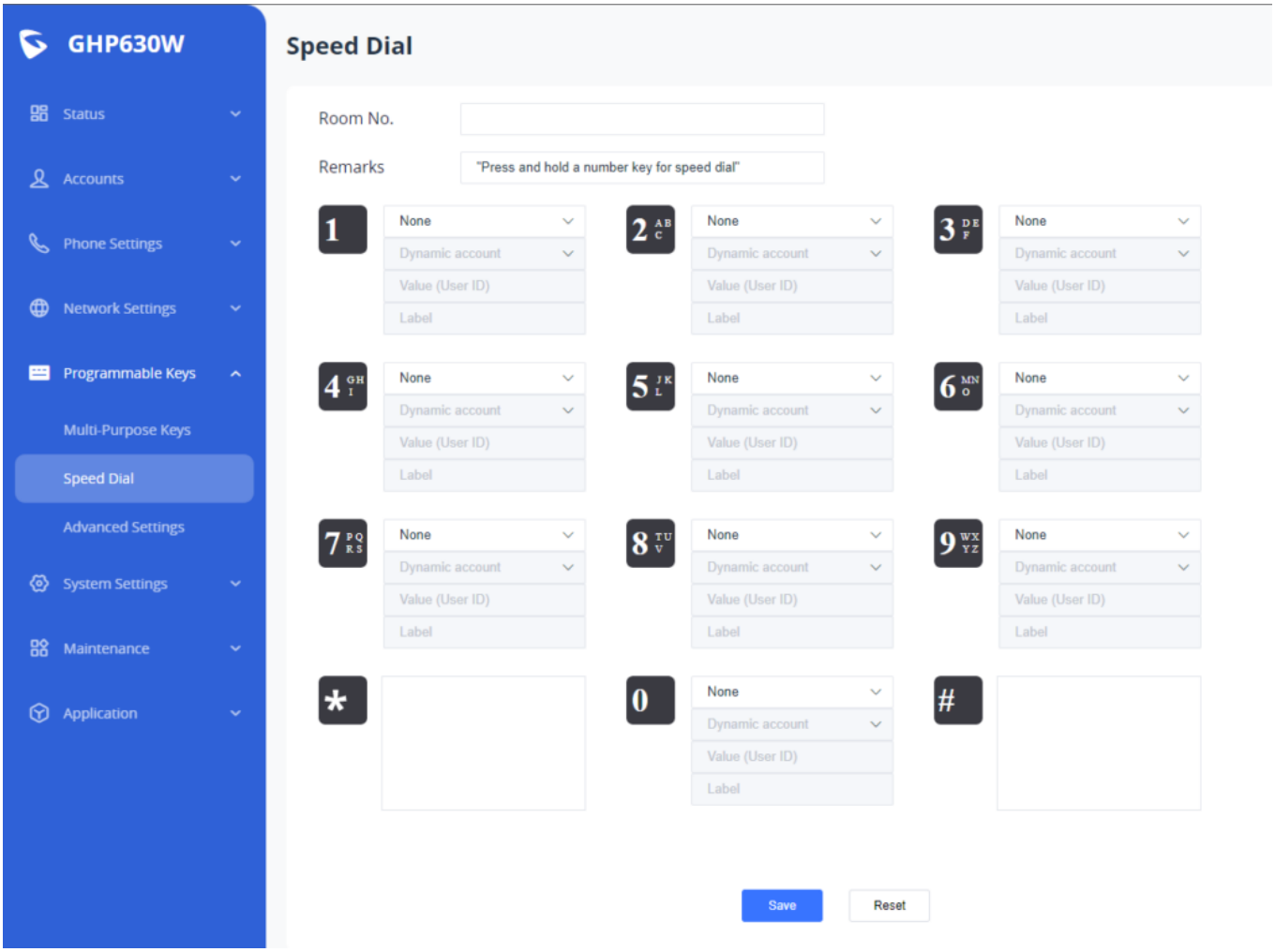
Multi-Purpose Keys

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 key 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



Speed Dial Configuration

Programmable keys advanced settings

Transfer Mode via MPK	Configures the transfer mode to use when pressing the "Transfer" MPK. Choose from Blind Transfer or Attended Transfer. Default is Blind Transfer

System Settings

Time

Date and Time	
NTP Server	Configures the URL or IP address of the NTP server. The phone may obtain the date and time from the server.
Secondary NTP Server	Configures the URL or IP address of the NTP server. The phone may obtain the date and time from the server.
NTP Update Interval	Configures interval for updating time from the NTP server. The valid value is between 5 and 1440 minutes.
Allow DHCP Option 42 to Override NTP Server	When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN.
Time Zone	Configures the date/time used on the phone according to the specified time zone.
Allow DHCP Option 2 to Override Time Zone Setting	Allows device to get provisioned for Time Zone from DHCP option 2 in the local server

Self-Defined Time Zone	This parameter allows the users to specify their own time zone. For syntax and examples please refer to user manual.
Show Clock	Show or hide clock on the idle screen.
Date Display Format	Configures the date display format on the LCD, the options are: yyyy-mm-ddmm-dd-yyyydd-mm-yyyydddd, MMMM dd MMMM dd, dddd Default is yyyy-mm-dd
Language	
Display Language	Selects display language on the phone LCD.
Default Input Selection	Configures the default input selection: Multi-Tap: multi-tap to switch character Shiftable: select input from available characters.
Auto language download	Configures the device to download language files automatically from server.

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.

SSH Access	
Enable SSH	If set to "Yes", the phone will allow any SSH access to the phone.
SSH Public Key	If enabled, the phone will use public key authentication as an alternative option to password authentication.Note: The public key length should be 2048 bits.
Keypad Mode	
Configuration via Keypad Menu	Configures access control for keypad Menu settings.Unrestricted: all options on LCD menu can be accessed;Basic settings only: option for configuration cannot be displayed;Constraint Mode: options for configuration for factory functions and network cannot be displayedLocked Mode: All options from the LCD are disabled.
Web Access	
HTTP Web Port	Configures the HTTP port under the HTTP web access mode.
HTTPS Web Port	Configures the HTTPS port under the HTTPS web access mode.
Web Access Mode	Sets the protocol for the web interface.
Web Access Control	Restrict web access by using Whitelist or Blacklist on the incoming IP addresses. If set to "None", the web access is unrestricted.
Web Session Timeout	Configures the timer to log out of the web session when idle. Default is 10 minutes. Range is 2-60 minutes.
Validate Server Certificates	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.
Web/Restrict mode Lockout Duration	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.
Web Access Attempt Limit	Configures the number of failed web access attempts allowed before lockout. Default is 5. Range is 1-10.

User Info Management

Parameter	Description
Test Password Strength	Checks password strength to ensure better security

Admin Password	
Current Password	The current admin password is required to set a new admin password.
New Password	Set new password for web GUI access as Admin. This field is case sensitive.
Confirm Password	Enter the new Admin password again to confirm.
IVR	
Keypad Password	Configure the keypad password used in the IVR.
Enable IVR	If enabled, IVR is available. If disabled, enable configuration item "Enable Basic Settings in IVR" cannot take effect. Enabled By Default.
Enable Basic settings in IVR	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
Minimum TLS Version	Configures the minimum TLS version supported by the phone. Minimum TLS version must be less than or equal to maximum TLS version. TLS 1.0TLS 1.1TLS 1.2Note: The default setting is TLS 1.2
Maximum TLS Version	Configures the maximum TLS version supported by the phone. Maximum TLS version must be greater than or equal to minimum TLS version.UnlimitedTLS 1.0TLS 1.1TLS 1.2Note: The default setting is Unlimited.?
Enable/Disable Weak Cipher Suites	Defines the function for weak cipher suites. If set "Enable Weak TLS Cipher Suites", allow users to encrypt data by weak TLS cipher suites.Enable Weak TLS Ciphers SuitesDisable Symmetric Encryption RC4/DES/3DESDisable Symmetric Encryption SEEDDisable All Weak Symmetric EncryptionDisable Symmetric Authentication MD5Disable All Weak TLS Ciphers SuitesNote: The default setting is Disable All Weak TLS Ciphers Suites.
SIP TLS Certificate	The Cert File for the phone to connect to SIP Server via TLS.
SIP TLS Private Key	The Cert Key for the phone to connect to SIP Server via TLS.
SIP TLS Private Key Password	SSL Private key password used for SIP Transport in TLS/TCP.
Custom Certificate	The uploaded custom certificate will be used for SSL/TLS communication instead of the phone default certificate.

Trusted CA Certificate

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

Keypad Lock

In this configuration page, the user can configure various parameters related to the keypad lock function.

Parameter	Description
Enable Keypad Locking	If set to enabled, the keypad can be locked by pressing and holding the STAR * key for about 4 seconds. And will also allow automatic locking.
Keypad Lock Type	Select the lock type.All Keys: If set to this option, all keys will be locker and no emergency calls can be made.Functional Keys: If set to this option, only functional keys will be locked but the user can still make emergency calls.
Password to Lock/Unlock	Configures the password to lock/unlock the keypad.

Keypad Lock Timer	Configures the timeout (in seconds) of idle screen for locking keypad . Valid range is 0 to 3600.
Emergency	Defines emergency call numbers. If multiple emergency call numbers are entered, they should be seperated by ','.

Preferences

Display Control	
LCD	
Backlight Brightness: Active	Configures the LCD brightness when the phone is active. Valid range is 10 to 100 where 100 is the brightest.
Backlight Brightness: Idle	Configures the LCD brightness when the phone is idle. Valid range is 0 to 100 where 0 is off and 100 is the brightest.
Active Backlight Timeout	Configures active backlight timeout (in minutes). The valid range is 0 to 90. Default value is 1 minute.
Enable Missed Call Backlight	f set to "Yes", LCD backlight will be turned on when there is a missed call on the phone.
Blank Screen Timeout	Configures how long it waits to turn off LCD automatically during non-office hour under Standard Mode. The valid range is 0 to 90 minutes. 0 means disable Blank Screen feature
Office Hour	Configures office hour for each day of the week.
LED	
New Message LED Indicator	Configure the behavior 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.
Wallpaper	
Wallpaper Source	Configures the location where wallpapers are stored.
Wallpaper Server Path	Configures the directory or file path of wallpaper.
Upload Wallpaper	The uploaded wallpaper must be in JPG or PNG format. 500 KB or smaller.
Color Background	Enter a color to use in HEX format.e.g. #000000Reference: http://htmlcolorcodes.com
Screensaver	
Screensaver	Enables or disables the screensaver feature. Enabled by default.
Screensaver Source	Configures the source location used to load screensaver images. When set to "Default," the device displays the default GHP63x screensaver images. When set to "Download," the device uses a custom XML file to retrieve images from a specified server.
Show Date and Time	Configures whether the date and time are displayed on the screensaver. Enabled by default.
Screensaver Timeout	Configures the idle time before the screensaver is activated. Valid range is 3 to 60 minutes. Default is 3 minutes.
Screensaver Server Path	Configures the server path containing the screensaver XML file. This field is used when Screensaver Source is set to "Download."
Screensaver XML Download Interval	Configures the interval at which the device downloads the screensaver XML file. Valid range is 5 to 720 minutes. Setting this value to 0 disables automatic downloads. Default is 0.
Audio Control	
Speaker Ring Volume	Configures speaker ring volume, the valid range is 1 to 8.
Lock Speaker Volume	Lock volume adjustment when the option is enabled.
Enable Warning Tone	

Handset TX Gain (dB)	Configures the transmission gain of the handset.
Enable HAC	If enabled, the phone will be compatible with nearby hearing aids.

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
Enable TR-069	Enable or disable TR-069
ACS URL	URL of the TR-069 Auto Configuration Servers (e.g., http//acs.mycompany.com, or IP address).
TR-069 Username	ACS username for TR-069.
TR-069 Password	ACS password for TR-069.
Periodic Inform Enable	Enables periodic inform. If set to "Yes", device will send inform packets to TR-069 Auto Configuration Server.
Periodic Inform Interval	Configures periodic inform interval to send the inform packets to TR-069 Auto Configuration Server.
Connection Request Username	The username for the TR-069 Auto Configuration Server to connect the phone.
Connection Request Password	The password for the TR-069 Auto Configuration Sever to connect to the phone.
Connection Request Port	The port for the TR-069 Auto Configuration Server to connect to the phone.
CPE SSL Certificate	The Cert File for the phone to connect to the TR-069 Auto Configuration Sever via SSL.
CPE SSL Private Key	The Cert Key for the phone to connect to the TR-069 Auto Configuration Sever via SSL
Start TR-069 at Random Time	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
Upgrade via Manual Upload	
Upload Firmware File to Update	Configures to upload and upgrade firmware.
Upgrade via Network	
Firmware Uprgade via	Configures firmware upgrade method as TFTP, FTP, FTPS, HTTP, HTTPS. The default setting is HTTP.
Firmware Server Path	Configures the server path for firmware download.
Firmware Server Username	The username for the firmware server.
Firmware Server Password	The password for the firmware server.
Firmware File Prefix	If configured, only the firmware with the matching prefix will be downloaded and flashed into the phone.
Firmware File Postfix	If configured, only the firmware with the matching postfix will be downloaded and flashed into the phone.

Upgrade Detection	
Upgrade	Start the upgrade.

Config File

Parameter	Description
Configure Manually	
Download Device Configuration	Click to download the device configuration file in .txt format.
Download Device Configuration (XML)	Click to download the device configuration file in .XML format.
Download User Configuration	Click to download the user's configuration file.
Upload Device Configuration	Upload configuration file to the phone.
Export Backup Package	Export a backup package which contains device configuration and personal data.
Restore from Backup Package	Restore from the uploaded backup package.
Configure via Network	
Config Uprgade via	Choose the protocol that will be used for upgrading.
Config Server Path	Defines the server path for provisioning.
Config Server Username	The username for the config server.
Config Server Password	The password for the config server.
Always Authenticate before Challenge	If enabled, the phone will send credentials before being challenged by the server. This option only applies to HTTP/HTTPS.
Config File Prefix	If configured, only the configuration file with the matching encrypted prefix will be downloaded and flashed into the phone.
Config File Postfix	If configured, only the configuration file with the matching encrypted postfix will be downloaded and flashed into the phone.
Authenticate Conf File	If enabled, the phone will authenticate configuration file before acceptance.
XML Config File Password	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
Auto Upgrade	
Automatic Upgrade	Enables automatic upgrade and provisioning.NoYes, check for firmware upgrade periodicallyYes, check for upgrade everydayYes, check for upgrade every week
Automatic Upgrade Check Interval (m)	This option appears when Automatic Upgrade is set to "Yes, check for upgrade periodically". It specifies the minutes of the periodic firmware check. The default value is: 10080 minutes.
Hour of The Day (0-23)	This option appears when Automatic Upgrade is set to "Yes, check for upgrade everyday" or "Yes, check for upgrade every week".Configures the hour of the day to check the firmware or config server for firmware upgrade or configuration file changes.
Day of The Week (0-6)	This option appears when Automatic Upgrade is set to "Yes, check for upgrade every week".Configures the day of the week to check the firmware or config server for firmware upgrade or configuration file changes.
Start Upgrade at Random Time	Configures whether the phone will upgrade automatically at a random time within the configured time interval.
Firmware Upgrade and Provisioning	Specifies how firmware upgrading and provisioning request to be sent.

DHCP Option	
Allow DHCP Option 43 and Option 66 to Override Server	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.
Allow DHCP Option 120 to Override SIP Server	Specifies the name of the client. This field is optional but may be required by Internet Service Provider.
Enable DHCP Option 150	It enables DHCP Option 150.
Enable DHCP Option 160	It enables DHCP Option 160.
Enable DHCP Option 161	It enables DHCP Option 161.
Config Provision	
Download and Process All Available Config Files	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.
User Protection	When user protection is on, P-values that the user sets will not be changed by provision or provider.
3CX Auto Provision	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
Validate Hostname in Certificate	Configures tp validate the hostname in the SSL certificate.
Enable SIP NOTIFY Authentication	Device will challenge NOTIFY with 401 when set to "Yes".
Factory Reset	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
Syslog Protocol	Allows sending syslog through secured TLS protocol to the syslog server. Note: CA verification is required.
Syslog Server	The URL/IP address for the syslog server.
Syslog Level	Selects the level logging of syslog.
Syslog Keyword Filter	Syslog will be filtered based on the configured keywords. Multiple keywords can be separated by ",".
Send SIP Log	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
Phone Status	
Setup Completed	Configures the Action URL to send when phone finishes setup process.
Registered	Configures the Action URL to send when phone successfully registers as a SIP account.
Unregistered	Configures the Action URL to send when phone unregisters a SIP account.
Register Failed	Configures the Action URL to send when phone fails to register a SIP account.
Idle to Busy	Configures the Action URL to send when the phone's state changes form idle to busy.
Busy to Idle	Configures the Action URL to send when phone's state changes from busy to idle.
Auto Provision Completed	Configures the Action URL to send when phone's auto provision process is completed.
IP Change	Configures the Action URL to send when the IP address changes.
Call Operation	
Off-hook	Configures the Action URL to send when phone is in off-hook state.
On-hook	Configures the Action URL to send when the phone is on-hook state.
Incoming Call	Configures the Action URL to send when the phone receives an incoming call.
Outgoing Call	Configures the Action URL to send when phone places a call.
Missed Call	Configures the Action URL to send when phone has a missed call.
Established Call	Configures the Action URL to send when phone establishes a call.
Terminated Call	Configures the Action URL to send when the phone terminates a call.
Answered Call	Configures the Action URL to send when phone answers an incoming call.
Blind Transfer	Configures the Action URL to send when the phone performs blind transfer.
Attended Transfer	Configures the Action URL to send when the phone performs attended transfer.
Transfer Completed	Configures the Action URL to send when the phone successfully transfers a call.
Transfer Failed	Configures the Action URL to send when the phone fails to transfer a call.
Hold Call	Configures the Action URL to send when the phone places a call on hold.
Unhold Call	Configures the Action URL to send when the phone resumes the call on hold.
Enable DND	Configures the Action URL to send when DND is enabled on the phone.
Disable DND	Configures the Action URL to send when DND is disabled on the phone.

Scheduled Tasks

Maintenance -> Scheduled Tasks	
Add Task	Adds a specifc task to be exectuted for the GHP63x device, the options to configure are: Task Type: Select what the phone should do automatically. The Task Type defines what action the phone will perform. Scheduled Reboot makes the phone restart at the chosen time, while Scheduled Lock automatically locks the keypad or user interface. Scheduled Unlock does the opposite by unlocking the phone at the specified time, and Scheduled Clear Call Log removes all call history from the device.Repetition Period: Choose how often the task will repeat. The Repetition Period determines how often the scheduled task will run. Choosing No Repeat means the task will execute only once at the specified time. Every Day schedules the task to run daily at the same hour, while Every Week repeats it weekly on the same weekday and time. If Every Month is selected, the task will run once per month on the same date and at the same time.Effective Time: The Effective Time specifies the exact moment when the scheduled task will run. Selecting Custom allows you to manually set a specific date and time for the action. When Office Hours Start Time is chosen, the task will automatically execute at the beginning of the phone's configured office hours. If Non-Office Hours Start Time is selected, the task will run at the start of the non-office period, which is useful for operations that should occur outside working hours to avoid disrupting users. The default value is set to 00:00
Delete Task	Deletes the selected scheduled tasks.

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
Hotel Name	Configures the hotel name.
Hotel Address	Configures the hotel address.
Hotel Phone Number	Configures the hotel phone number.
Hotel Fax Number	Configures the hotel fax number.
Hotel Room Number	Configures the hotel's room number.

E911 Service

E911 (Enhanced 911) service allows configuring 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
Enable E911	Enable or disable E911.
HELD Protocol	Configures HELD transfer protocol.
HELD Synchronization Interval	The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when interval is 0.
Location Server	Configures the primary Location Information Server (LIS) adderss.
Location Server Username	Configures the username of the primary Location Information Server (LIS).
Location Server Password	Configures the password of the primary Location Information Server (LIS).
Secondary Location Server	Configures the secondary Location Information Server.

Secondary Location Server Username	Configure the username of the secondary Local Information Server.
Secondary Location Server Password	Configure the password of the secondary Location Information Server.
HELD Location Types	Configure "locationType" element in the location request.
HELD Use LLDP Information	If set to "Yes", the information from LLDP-support switch is used to generate ChassisID and portID; otherwise
HELD NAI	If set to "Yes", Network Access Identifier (NAI) is included as a device identity in the location request sent to the Location Information
HELD Identity	Specify the identifier to forward in the call information. E.G, mac, ip, uri, etc...
HELD Identity Value	Enter the value corresponding to the identity type. if it's an ip address then the value should be a valid IP address. If it's a URI, then the value provided should be a valid URI.
E911 Emergency Numbers	A user can configure multiple emergency numbers separated with the delimiter symbol ";".
Geolocation-Routing Header	If enabled, the "Geolocation-Routing" header will be included in the E.911 INVITE message.
Geolocation Header Format	The Geolocation Header Format setting defines how the phone includes its location information inside SIP messages for features like emergency calling or location-based routing. Legacy: Uses the older, non-standard geolocation header format meant for compatibility with older PBXs or systems that still rely on the previous method of sending location information.RFC6442: Uses the modern, standardized geolocation header format defined in RFC 6442, providing structured PIDF-LO location data for better accuracy and compatibility with current SIP servers and emergency services.The default value is set to "Legacy"
Priority Header	If set to "Yes", E.911 INVITE messages includes the "Priority" header with the value "emergency".

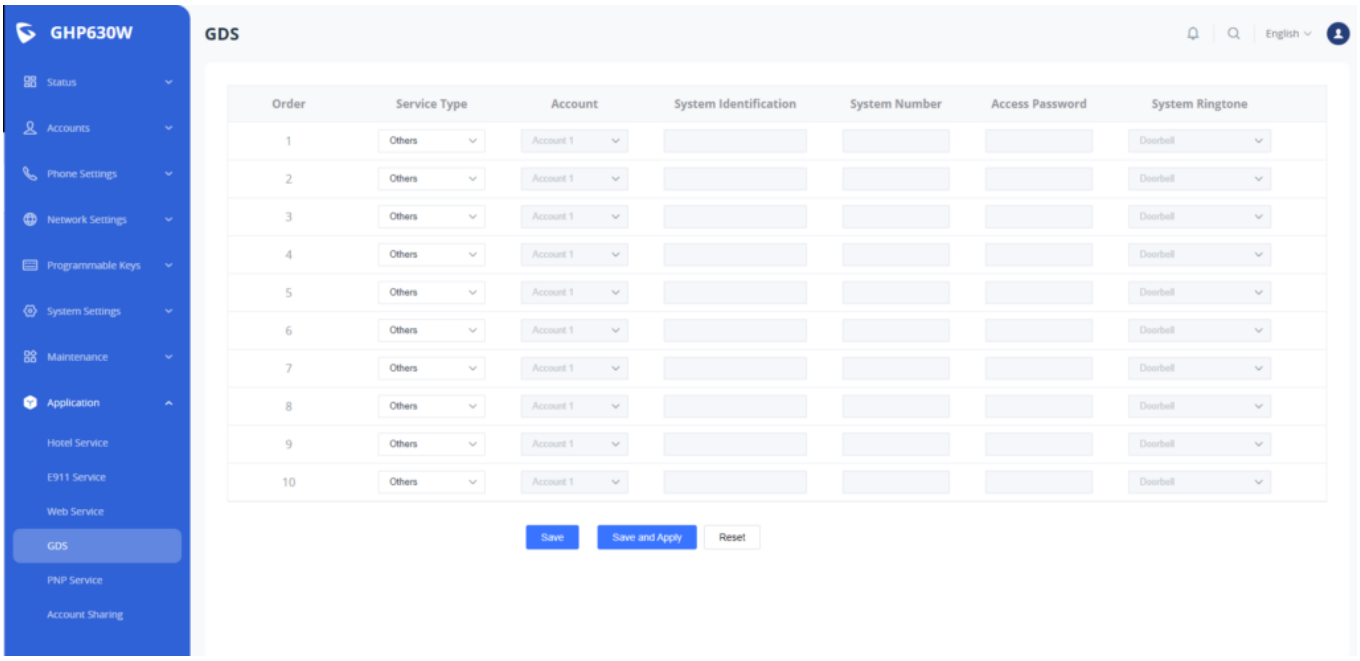
Web Service

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

Parameter	Description
Use Auto Location Service	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, define a specific ringtone to be played when the GDS doorbell rings, and initiate a call to GHP6XX.

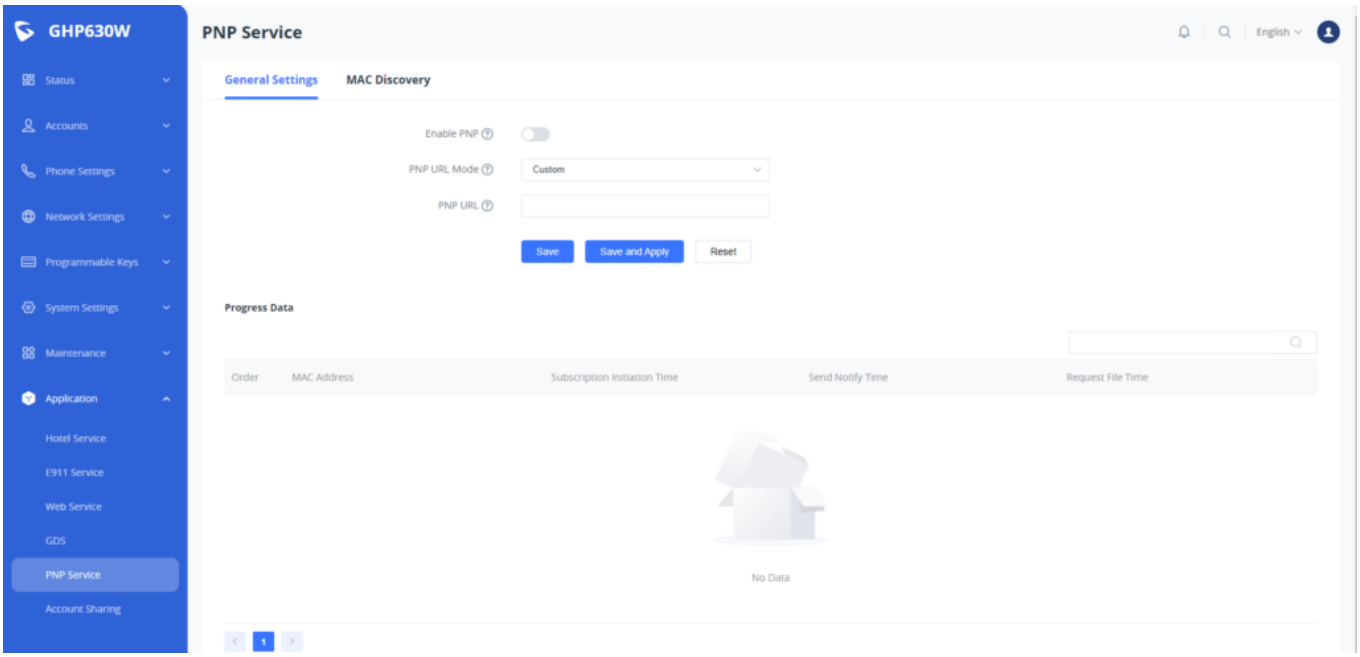


GDS

GDS	Connect to a GDS37XX and send OpenDoor request. Service Type: Select GDS as service type Account: The account to be used on the phone to interact with the GDS37XX System Identification: A name or a number to identify the GDS37XX System Number: The SIP extension or the IP address of the GDS37XX depending on the deployed scenario, Peering or Registration Access Password: The password set on the GDS37XX to unlock the door. System Ringtone: Select the system ringtone from the dropdown list to be played when there is an incoming call from the configured system number of the GDS37xx 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	
Enable PNP	Configures whether to enable the PNP function. After enabling it, the automatic configuration is supported, and up to 100 devices can be configured. Disabled by Default.
PNP URL Mode	Select the PNP URL mode, including local and custom, custom does not support filling in the local machine-related address.
PNP URL	The configuration terminal can take the server address of the configuration file. The server address can be the IP address of the terminal that provides PNP services. It cannot be configured as a locally related parameter.
Template Management	Profile templates can be managed in this module. The current model only supports the management of one profile template. It supports the generation of batch configuration CSV files based on the profile template. You can fill in the relevant parameter values in this file, and start the PNP batch configuration process after the application.
Upload Profile Template	Users can upload a .xml template file downloaded by respecting the following guidelines: Users can upload the configuration file template here and add parameters to define parameter names. Parameter values are different configuration item values of different devices. To specify a device for configuration, add the %%mac_address%% parameter to the filename in the template file. The parameter can be configured in batches in Step 2 (Batch Configure CSV). If the same parameters need to be configured for all devices, delete %%mac_address%% from filename in the template file and assign values to each parameter. Please write configuration file template according to sample file format specification. Any text file format can be placed in <data><![CDATA[-]]></data>.
Batch Configure CSV	Users can upload a .csv template file download while respecting the following guidelines: If there are batch configuration variables in the configuration file template, generate the batch configuration CSV file according to the uploaded configuration file template, and fill in the relevant batch configuration values after exporting the CSV template. After writing the batch configuration CSV template, upload the CSV template file here.
Effects View	Displays the data inserted from the .csv template to the .xml configuration file.
Progress Data	When connected to a network, the phone can automatically identify and configure itself with the appropriate settings for that network. This eliminates the need for manual configuration, making it faster and easier to set up and manage IP phone deployments. the connected networks will be displayed in the list.

MAC Discovery	During the plug-and-play process, the network infrastructure uses the MAC Discovery feature to detect the IP phone's MAC address and automatically configure it with the appropriate settings, such as IP address, subnet mask, default gateway, and other network-related parameters. This eliminates the need for manual configuration and speeds up the deployment of IP phones in large-scale environments. A list of MAC Addresses with their respective IP address, Product models, and operations is displayed, and the actions that can be performed on those IP phones are the following : Download the Configuration file: this option will download the configuration file of the discovered device Redistribution operation: When a new 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.

Account Sharing

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

Basic Settings	
Enable Account Sharing	Select whether to enable Account Sharing.
Role in Account Sharing	Select the role that the current device will play in the network, the guest device role does not need to register an account on IP PBX, and can make calls in and out of the network through the account set by the host device role.
Group Name	Set the group name, in the host-guest mode, devices with the same group name can discover each other.Note: This item is mandatory if using Account Sharing. The verification format is domain type
Group Password	In the host-guest mode, after setting the group password, the guest device with the same group password as the host device can successfully register an account on the host device.Note:This item is mandatory if using Account Sharing.
Account Settings	
Account	For the host device role, this setting determines which host device account will be used as the guest device outgoing and incoming account for calls outside the Account Sharing. For the guest device role, this setting determines which account the guest device will use to register on the host device.
Account Name	This setting specifies the account name corresponding to the account used by the guest device.
Sync Ringing In Group	Set whether to enable synchronization of all successfully registered guest device ringtones within the group.
Discovered Host Device list	Shows registered devices on the local network for monitoring, it displays the following information about the discovered devices: IP Address MAC Address Registration Status Operation

Contacts

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

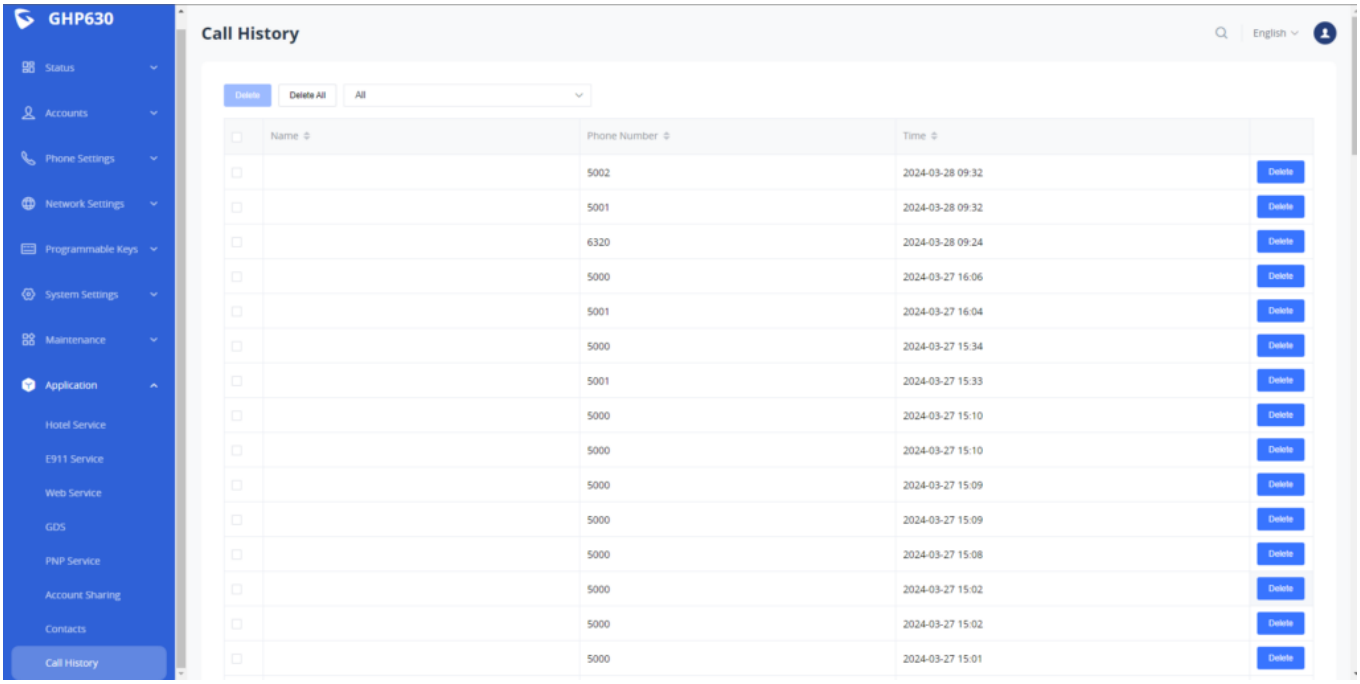
To display the list of contacts from the LCD screen, please press the keys "**HOLD +3**".

Contacts	
Add Contact	The user can add a contact to the phonebook by clicking the "Add Contact" icon, the following parameters can be defined for each contact: First Name Last Name Favorite Company Department Job Job Title Work Home Mobile Accounts Groups Ringtone
Group Management	

Add Group	The user can create a contacts group by clicking the "Add group" icon, the following parameters can be defined Group Name Ringtone
Phonebook Management	
Enable Phonebook XML Download	Enables Phonebook XML download via HTTP, HTTPS, FTP or TFTP.
HTTP/HTTPS Username	Defines the username for the HTTP/HTTPS server.
HTTP/HTTPS Password	Defines the password for the HTTP/HTTPS server
Phonebook XML Server Path	Configures the server path to download XML phonebook file. This field could be IP address or URL, with up to 256 characters.
Phonebook Download Interval	Configures the phonebook download interval (in minutes). If set to 0, automatic download will be disabled. Valid range is 5 to 720.
Remove Manually-edited Entries on Download	If set to "Yes", when XML phonebook is downloaded, the entries added manually will be automatically removed.
Import Group Method	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
Sort Phonebook by	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.
Download XML Phonebook	Downloads the XML Phonebook file.
Upload XML Phonebook	Uploads XML Phonebook file to the phone in xml format
Phonebook Key Function	Configures the behavior of the Phonebook key.
Default Search Mode	Configures the default phonebook search mode.
Replace Duplicate Items	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:

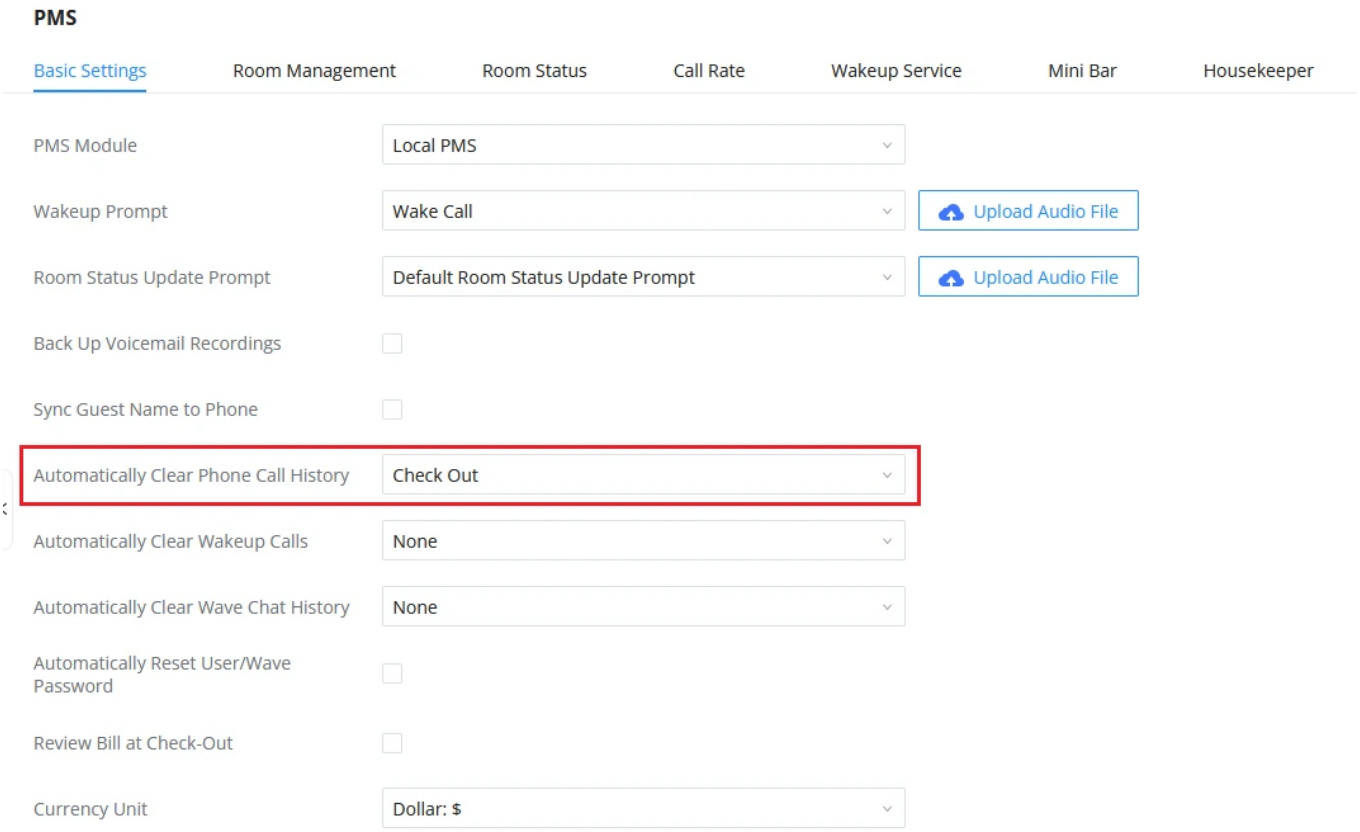


Automatic Call History Clearing with UCM PMS Integration

The GHP63x/W supports automatic clearing of call history when a guest checks out from the UCM PMS. This feature ensures that call logs are removed from the phone after the guest's stay, maintaining privacy and security.

To enable automatic call history clearing, please refer to the steps below:

1. **Log in to the UCM Web Interface** and navigate to **Integrations->PMS->Basic Settings**.
2. Under Basic Settings, set the **"Automatically Clear Phone Call History"** option to **"Check Out"**.



UCM PMS Basic Settings

3. Ensure the GHP63X-W extension is added to the **Room Management** section in the UCM PMS, the Check-in in **Room Status**.
4. After a guest checks out, the call history on the GHP63x/W will be automatically cleared.

If the call history is not cleared after checkout, please verify that the GHP63x/W and UCM firmwares are up to date.

GHP63X/W COMBO KEYS

The table below describes the function of each combination key supported by the GHP63x/W.

Combo Key	Function
HOLD + 0	Device Status Page (IP Address, Account Info)
HOLD + 3	Contacts Display
HOLD + 4	Soft Reboot
HOLD + 5	Screenshot
HOLD + 6	Start Provisioning

HOLD + 8	Force Screensaver

UPGRADING AND PROVISIONING

Unified Firmware

The GHP630, GHP630W, GHP631, and GHP631W 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

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-friendlyHTTP 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://tftpd32.jounin.net/.

Instructions for local firmware upgrade via TFTP:

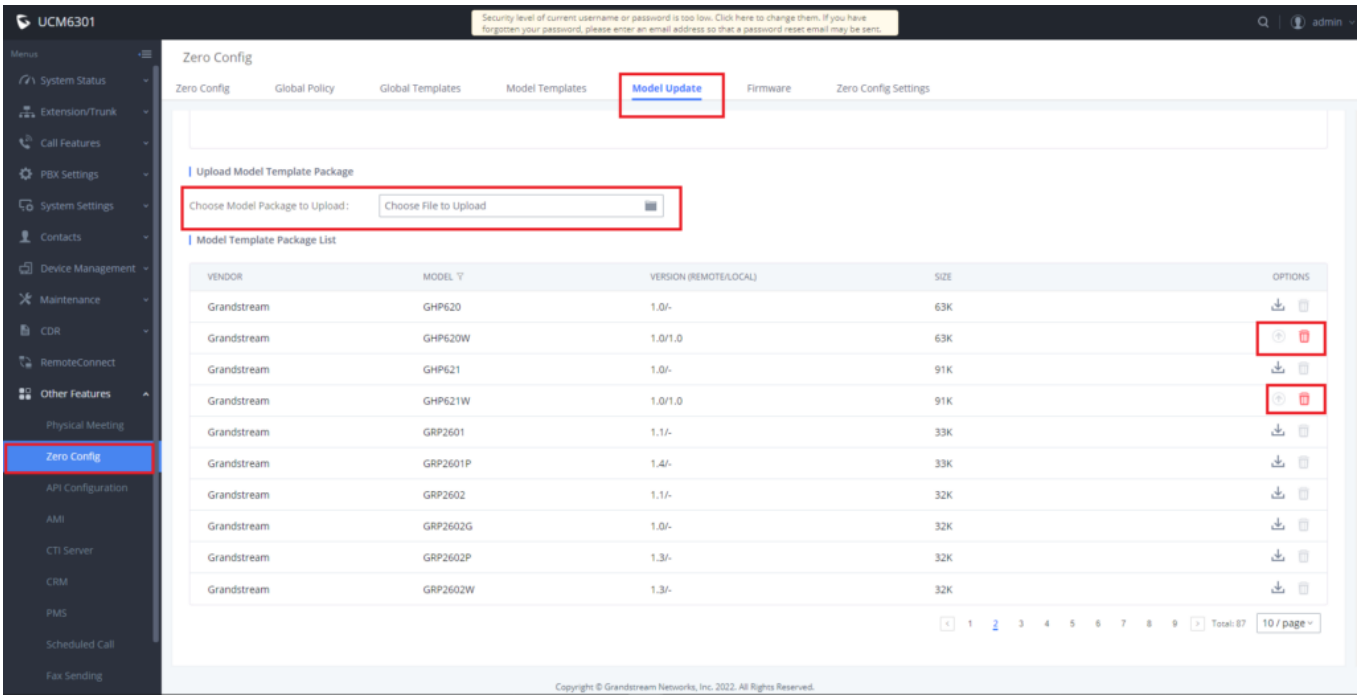
1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the phone to the same LAN segment.
3. Launch the TFTP server and go to the File menu -> Configure -> Security to change the TFTP server's default setting from "Receive 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".

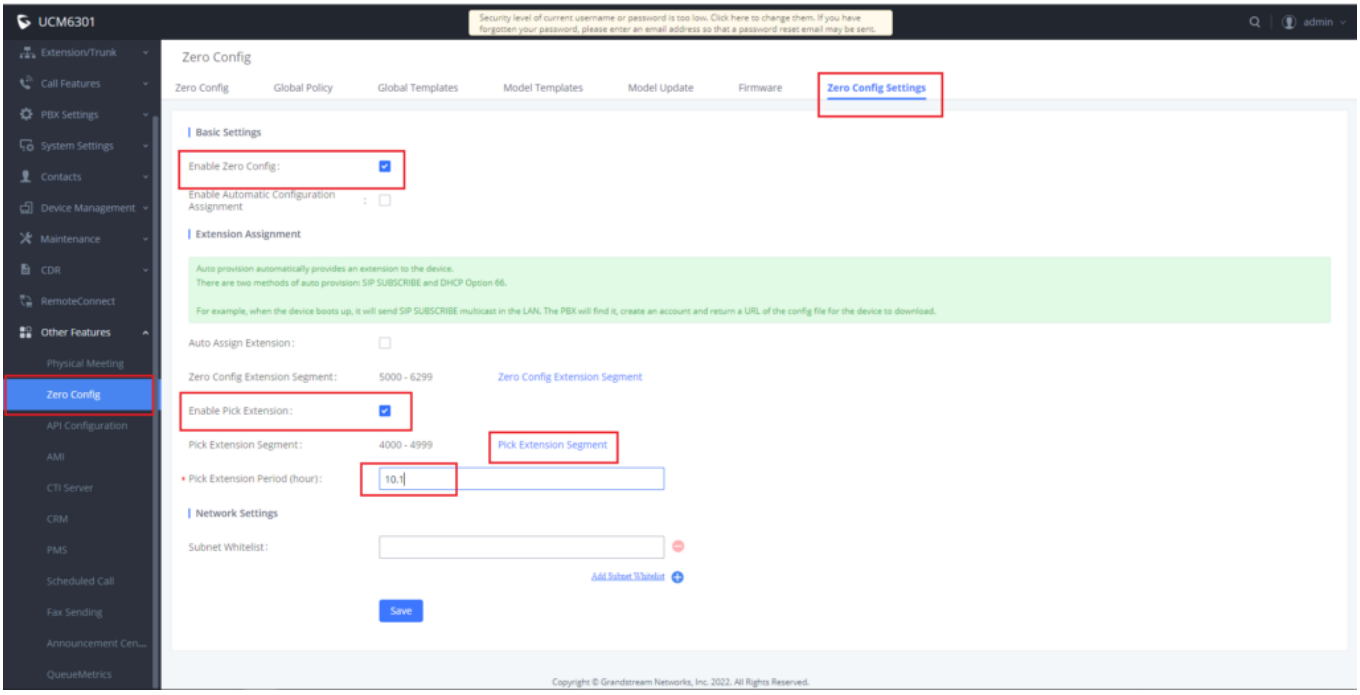


Zero Config - Model Update

- 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.

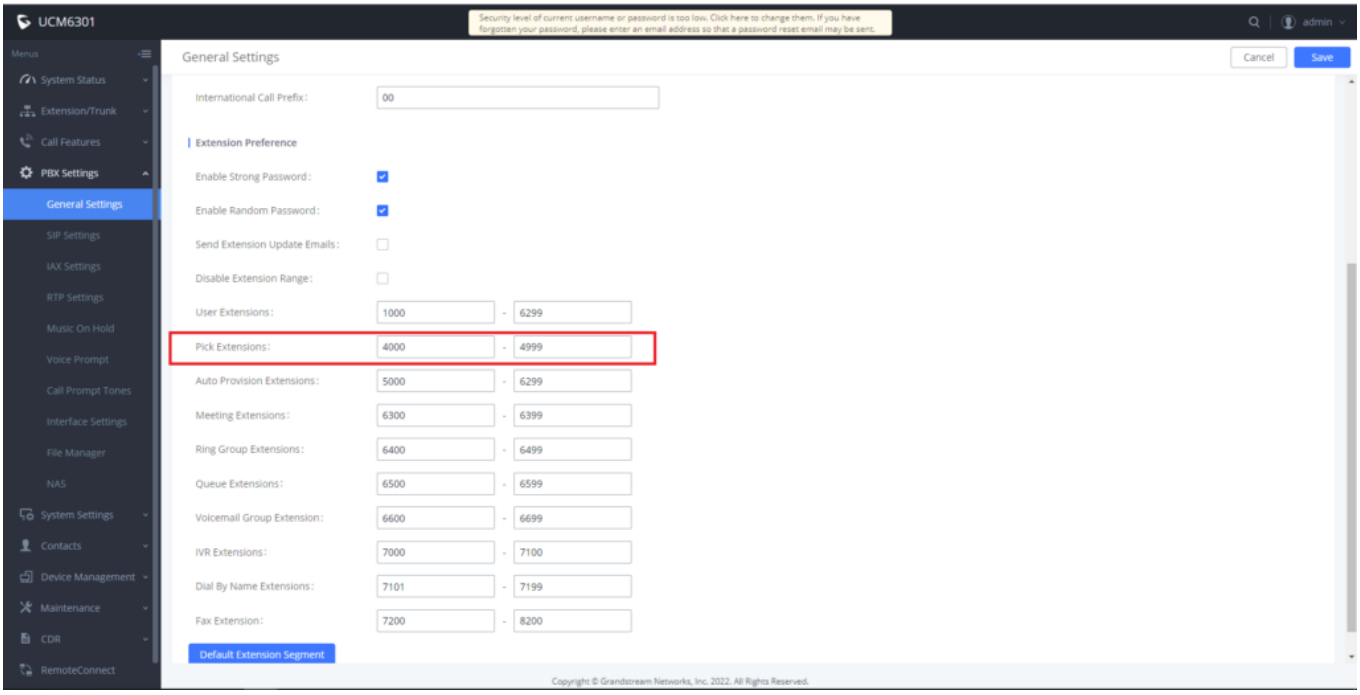
If the corresponding model cannot be downloaded and installed to the UCM local PC due to network reasons, you can upload the file of the UCM zero-configuration template (.pack file) and click the Download and Install button.

- 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.



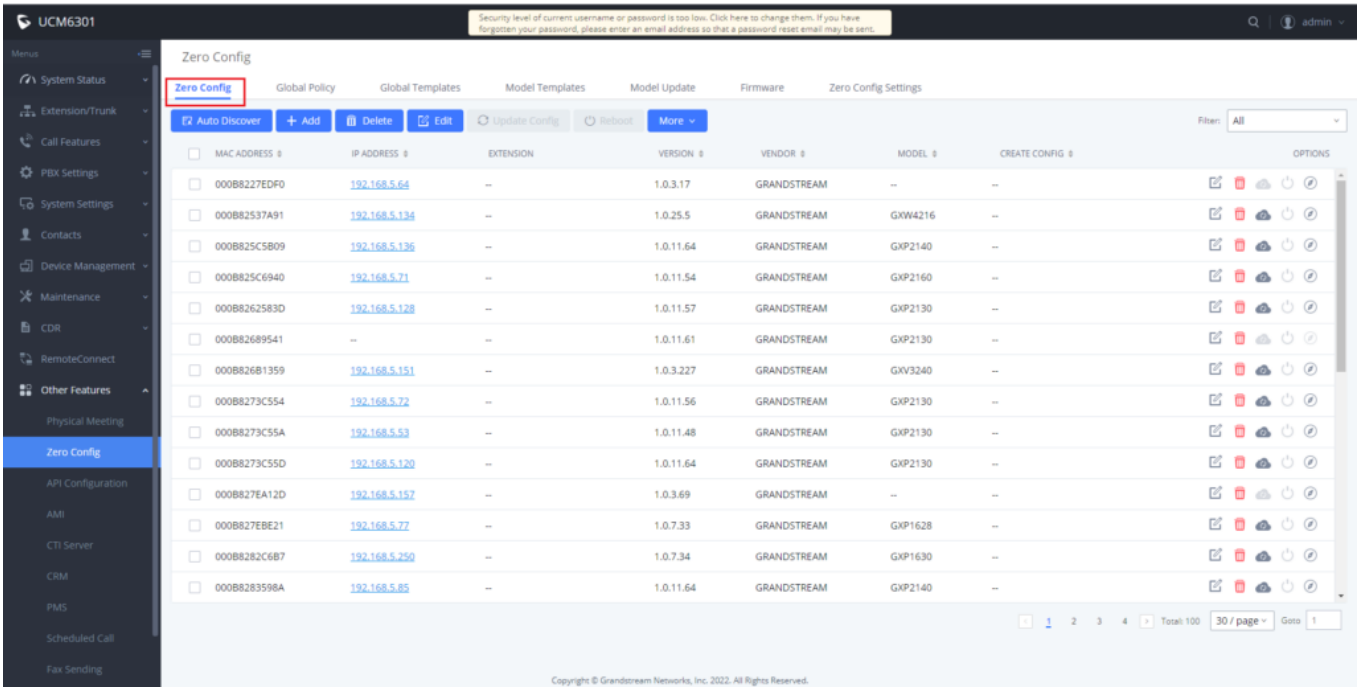
Zero Configuration settings

- 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 UCM630x 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.

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 number of 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).

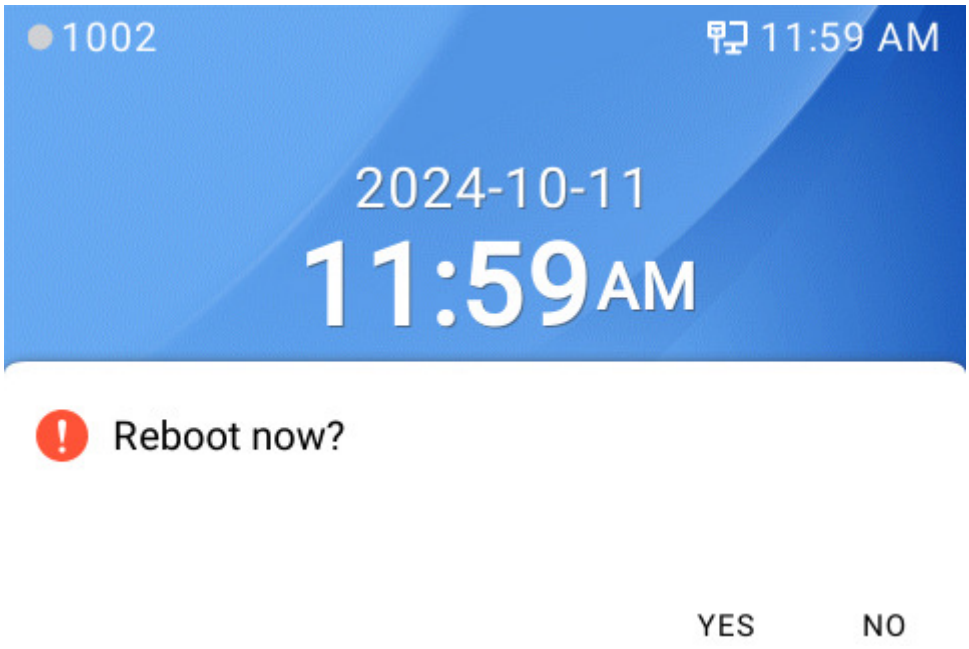
Please refer to the following link for more details on how to use the Zero Config on Grandstream UCMs: https://documentation.grandstream.com/knowledge-base/ucm630x-series-user-manual/#provisioning

REBOOT AND FACTORY RESET SETTINGS

Reboot Device

Users can reboot the GHP63x(W) using the unit's keypad. Please follow the steps below:

1. Press **"HOLD" + 4** on the main screen.
2. The reboot pop-up will appear on the screen. Click on the "yes" key to reboot the device.

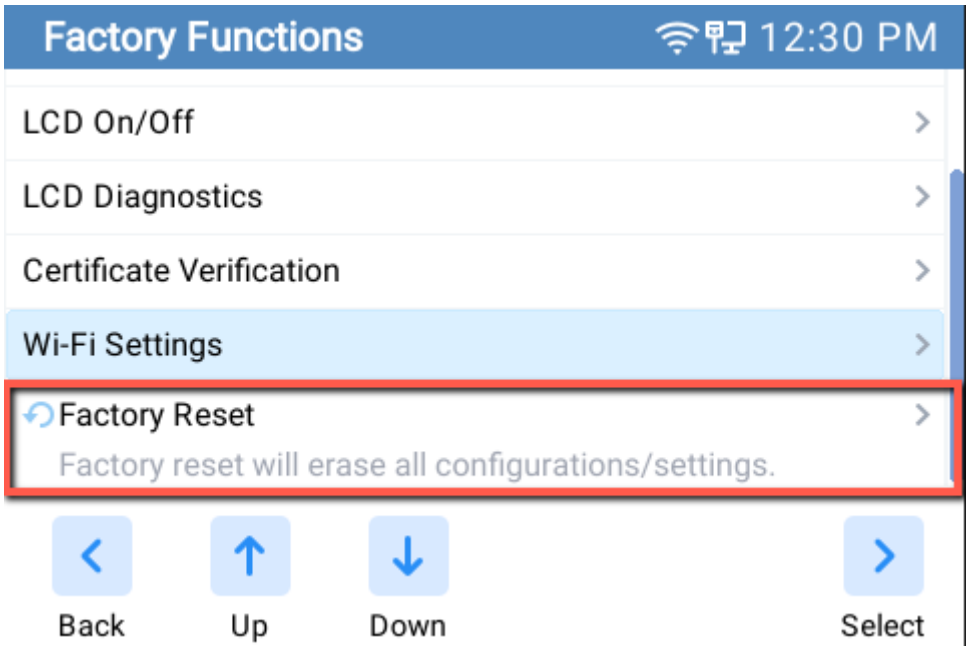


Reboot Device

Restore to Factory Default via LCD menu

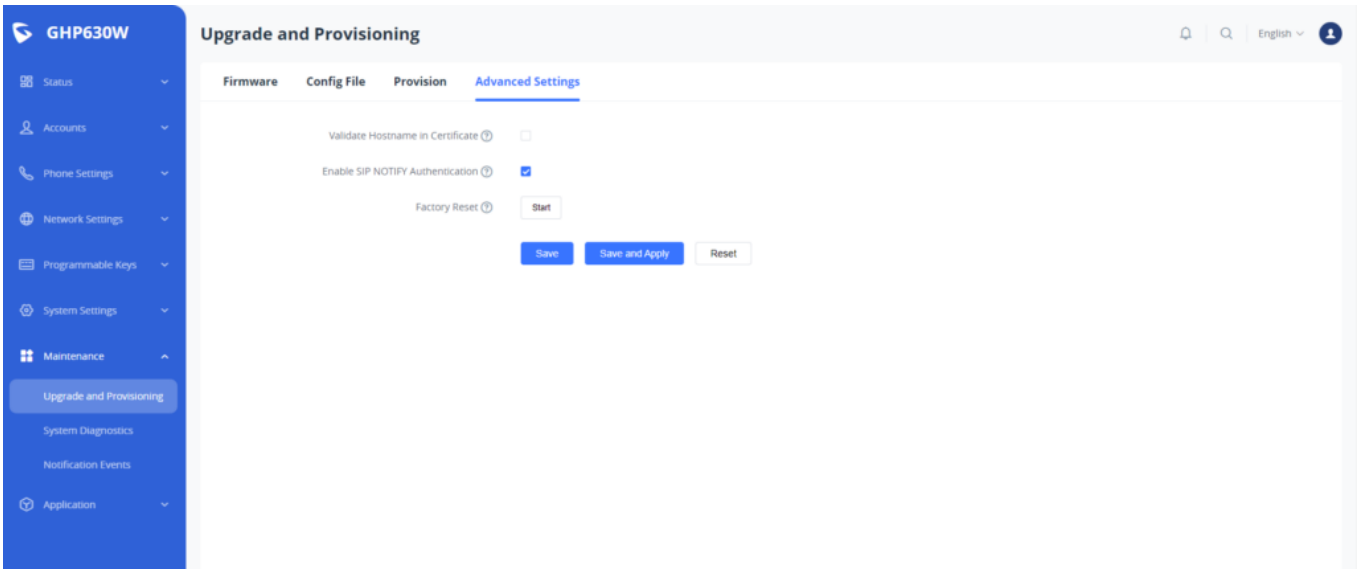
To restore the GHP63x/W to factory settings using the keypad lock :

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 on the phone.



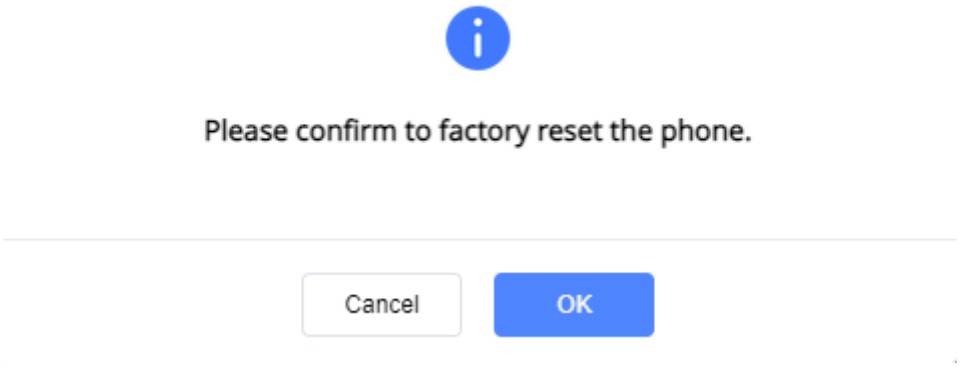
Restore to Factory Default via Web GUI

To reset the GHP63x/W 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**.



Factory Reset Confirmation

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

This section documents significant changes from previous versions for the admin guide of the GHP63x. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware 1.0.1.52

- No major changes

Firmware 1.0.1.50

- Added support for scheduled tasks. [SCHEDULED TASKS]
- Added support for Geolocation headers to follow RFC6442. [GEOLOCATION HEADER FORMAT]
- Added ability to configure whether or not the device will reboot when receiving "Event: CheckSync". [Reboot on check-sync event without "reboot="]

Firmware 1.0.1.45

- The security version of the phone can be viewed on the web GUI. [Security Version]

- Updated "Enable/Disable Weak Ciphers" default setting to reinforce the security of the device. [Enable/Disable Weak Cipher Suites]
- Updated "Enable Direct IP Call" default setting (enabled by default) to reinforce the security of the device. [Enable Direct IP Call]
- Increase the SSH key length to 2048 bits. [SSH Public Key]

Firmware 1.0.1.41

- No major changes.

Firmware 1.0.1.40

- Added support for deleting call logs after guest checkout when using the UCM. [Automatic Call History Clearing with UCM PMS Integration]

Firmware 1.0.1.28

- Added ability to disable missed calls and voicemail notifications. [Enable Missed Call Notification]

Firmware 1.0.1.26

- Added support to change the Date Display Format. [DATE DISPLAY FORMAT]
- Added support for disabling the center clock while the screen is active. [SHOW CLOCK]
- Added support for access control of settings accessible via LCD. [CONFIGURATION VIA KEYPAD MENU]

Firmware 1.0.1.24

- Increased "Off-hook Auto Dial Delay" max value from 10 to 30 seconds. [Off-hook Auto Dial Delay]

Firmware 1.0.1.23

- No major changes.

Firmware 1.0.1.13

- This is the initial firmware.