Grandstream Networks, Inc.

HT841/HT881

User Manual

HT841/HT881 – User Manual

Thank you for purchasing Grandstream's HT841/HT881.

The HT841/HT881 Analog FXO Gateway series is an easy-to-set-up IP communications solution that is suitable for small enterprises, as well as those with virtual and branch locations, who wish to benefit from their broadband network or integrate new IP technology with their existing phone system. This series of enterprise analog FXO gateway can convert SIP/RTP IP calls into conventional PSTN calls, and it is available in two models, the HT841 and HT881, with 4 and 8 FXO ports, respectively. Both models share the same installation process.

This User Manual aims to guide you in effectively operating and managing your HT841/HT881 Analog FXO Gateway, empowering you to utilize its numerous enhanced features, including seamless and swift installation.

PRODUCT OVERVIEW

Feature Highlights

The following table contains the major features of the HT841/HT881:

 **HT841/HT881**	• 2 FXO profiles supporting 2 different SIP Servers. • **HT841:** 4 FXO RJ11 Ports for PSTN Connections. • **HT881:** 8 FXO RJ11 Ports for PSTN Connections. • PoE in Support for NET2 port. • 2x 10/100 Mbps dual RJ45 network ports: NET2/NET1. • Advanced security protection with SRTP. • Wide range of caller ID formats. • T.38 Fax for creating Fax-over-IP • Strong AES encryption with security certificate per unit • Failover SIP server automatically switches to secondary server if main server loses connection. • Designed and tested for full interoperability with leading IP-PBXs, soft-switches and SIP-based environments. • Use with Grandstream's UCM series of IP PBXs for Zero Configuration provisioning • Automated provisioning options include TR-069 and XML config. • Lifeline support (FXS port will be hard-relayed to FXO port) in case of power outage.

HT841/HT881 Feature Highlights

HT841/HT881 Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings for the HT841/HT881.

- **HT841/HT881**

Interfaces	
Telephone Interfaces	One (1) RJ11 FXS port. **HT841:** Four (4) RJ11 FXO PSTN line port with lifeline support. **HT881:** Eight (8) RJ11 FXO PSTN line port with lifeline support.
Network Interface	Two (2) 10/100 Mbps ports (RJ45) with integrated NAT router

LED Indicators	POWER, FXO, FXS, NET1, NET2.
Factory Reset Button	Yes
Voice, Fax, Modem	
Telephony Features	Caller ID display or block, call waiting, flash, blind or attended transfer, forward, hold, do not disturb, 3-way conference
Voice Codecs	G.711 with Annex I (PLC) and Annex II (VAD/CNG), G.723.1, G.729A/B, G.726, iLBC, OPUS, dynamic jitter buffer, advanced line echo cancellation
Fax over IP	T.38 compliant Group 3 Fax Relay up to 14.4kpbs and auto-switch to G.711 for Fax Pass-through
Short/Long Haul Ring Load	3 REN: Up to 1km on 24 AWG
Caller ID	Bellcore Type 1 & 2, ETSI, BT, NTT, and DTMF-based CID
Disconnect Methods	Busy Tone, Polarity Reversal/Wink, Loop Current
Signaling	
Network Protocols	TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, FTP/FTPS, ARP/RARP, ICMP, DNS, DDNS, DHCP, NTP, TFTP, SSH, Telnet, STUN, SIP (RFC3261), SIP over TCP/TLS, SRTP, TR-069
QoS	Layer 2 (802.1Q VLAN, SIP/RTP 802.1p) and Layer 3 (ToS, Diffserv, MPLS).
DTMF Methods	In-audio, RFC2833 and/or SIP INFO
Provisioning and Control	HTTP, HTTPS, SSH, FTP, FTPS, Telnet, SSH, TFTP, TR-069, secure and automated provisioning using AES encryption, syslog
Security	
Media	SRTP
Control	TLS/SIPS/HTTPS
Management	Syslog support, SSH, Telnet remote management using web browser.
Physical	
Universal Power Supply	**POE Input:** 48 V / 0.5 A **DC Input:** 12V/1A
Environmental	Operational: 32° – 104°F or 0° – 40°C Storage: 14° – 140°F or -10° – 60°C Humidity: 10 – 90% Non-condensing
Dimensions and Weight	• **HT841/HT881** **Dimensions:** 190mm x 100mm x 28mm (L x W x D) **Weight:** 0.46KG

Compliance	
Compliance	FCC/CE/RCM/IC/UKCA

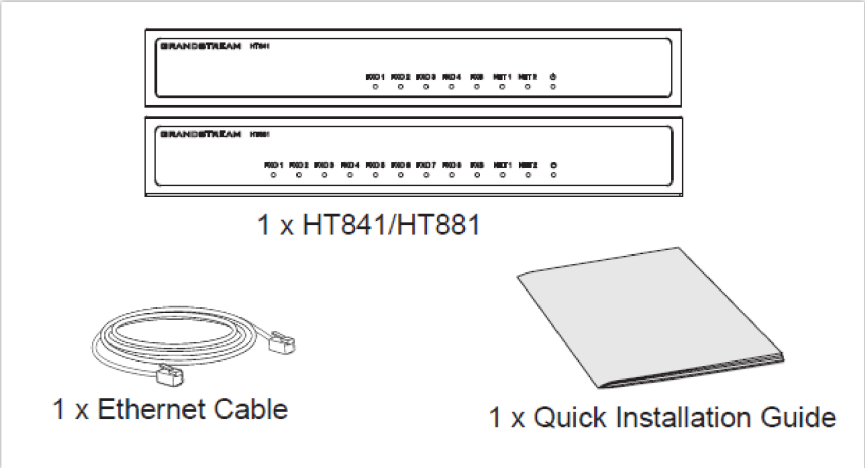
HT841/HT881 Technical Specifications

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the HT841/HT881.

Equipment Packaging

The HT841/HT881 FXO Gateway package contains:

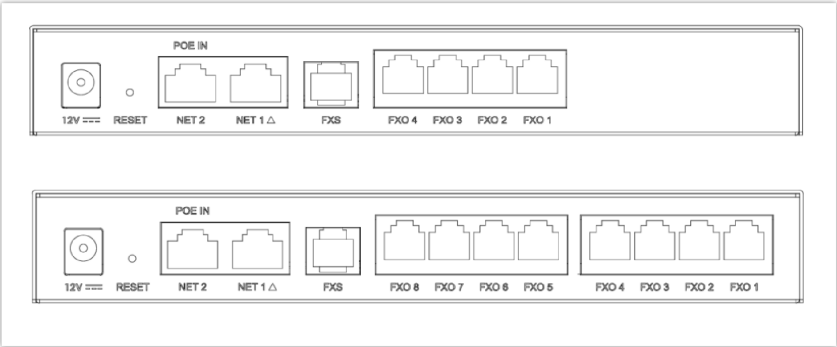


HT841/HT881 Package Content

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

HT841/HT881 Ports Description

The following figure describes the different ports on the back panel of the HT841/HT881.



HT841/HT881 Ports Description

Port	Description
DC 12V	Power socket. Used to power HT841/HT881 (12V - 0.5A)
NET 1/NET 2	Network NET 1 / NET 2 port. ● Used to power and connect your HT841/HT881 to local network when using as router.

	● Used to connect HT841/HT881 to your router or gateway using an Ethernet RJ45 cable.List Item 2
POE IN	PoE supported port.
FXS	FXS port to connect analog phone / fax machine to HT841/HT881 using RJ11 telephone cable.
FXO 1...4 **FXO 1....8**	FXO ports to be connected to physical PSTN line from a traditional PSTN PBX or PSTN Central Office. HT841 supports 4 FXO ports and HT881 supports 8 FXO Ports.
Reset	Factory reset button. Press for 7 seconds to reset to factory default settings. Quick press will only reboot the unit.

HT841/HT881 Supported ports

Note

- HT841/HT881 supports switching the working mode of NET1 and NET2 on the Web User interface.
- The default Device Mode for the HT841/881 is bridge. NET1 and NET2 ports function almost identically in bridge mode.

Connecting HT841/HT881

The HT841/HT881 is designed for easy configuration and easy installation. To connect your HT841/HT881, please follow the steps below:

Note

The default Device Mode for the HT841/881 is bridge. NET1 and NET2 ports function almost identically in bridge mode.

Connecting HT841/HT881 using WAN

When connecting HT841/HT881 using the NET1 port, it will act as a simple DHCP Client.

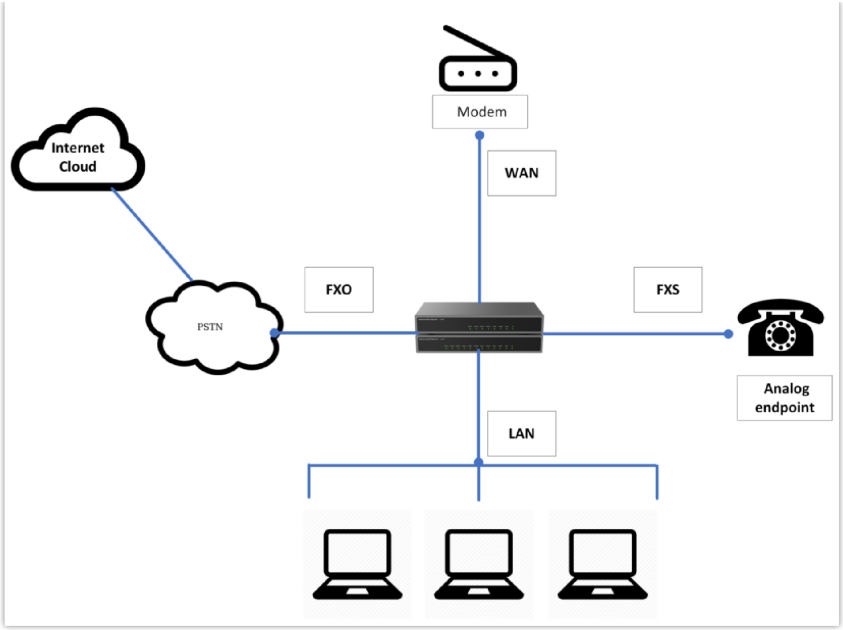
1. Insert a standard RJ11 telephone cable into the FXS port and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect the NET 1/ NET 2 port of the HT841/HT881 to a router, switch, or modem using an Ethernet cable.
3. Insert the power adapter into the HT841/HT881 and connect it to a wall outlet and make sure to respect the technical specifications of the power adapter used.
4. Power, NET1/NET2, FXO, and FXS LED will be solidly lit when the HT841/HT881 is ready for use.

Connecting HT841/HT881 using LAN

When connecting the HT841/HT881 using the NET2 port, it will act as a router and DHCP serving addresses, the devices connected with HT841/HT881 LAN will pull DHCP addresses from your HT841/HT881.

1. Insert a standard RJ11 telephone cable into the FXS port and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect a computer or switch to the NET1/NET2 port of the HT841/HT881 using an Ethernet Cable.
3. Insert the power adapter into the HT841/HT881 and connect it to a wall outlet and make sure to respect the technical specifications of the power adapter used. If the PoE switch is used in step 2, this step could be skipped.
4. Power, NET1/NET2 and FXS, and FXO LED will be solidly lit when the HT841/HT881 is ready for use.

Please make sure to enable NAT Router under Web GUI → Basic Settings → NAT/DHCP Server Information & Configuration → Device Mode.



Connecting the HT841/HT881

HT841/HT881 LEDs Pattern

There are five (5) LED types that help you manage the status of your HT841/HT881.

HT841/HT881 LED Patterns

LED Lights	Status
Power LED	The Power LED lights up when the HT841/HT881 is powered on and it flashes when the HT841/HT88 is booting up. **Note:** When powering up the unit with the PSU, the LED light will glow green, whereas it will be orange when using PoE.
NET1 LED	The NET 1 LED lights up when the HT841/HT881 is connected to your network through the NET1 port.
NET2 LED	The NET 2 LED lights up when the HT841/HT881 is connected to your network through the NET2 port.
FXS LED	The FXS LED indicates the status of the FXS port phone on the back panel. **OFF** – Unregistered **ON (Solid Green)** – Registered and Available **Blinking every 500 ms** – Off-Hook / Busy **Slow blinking** – FXS LED indicates voicemail
FXO LED	The FXO LEDs indicate the status of the FXO ports-phone on the back panel. **OFF** – Unregistered **ON (Solid Green)** – Registered and Available

	Blinking every 500 ms – Off-Hook / Busy **Slow blinking** – FXO LEDs indicate voicemail

HT841 HT881 LED Patterns

All LEDs display green when ON. The **Ready** light will only be ON when the network interface is ready and the Web User Interface is accessible.

During a ***firmware upgrade*** or ***configuration download*** the following LED pattern will be observed: Power, Ready, and NET1 LEDs will be ON. The FXO port LED will keep flashing during download and then stay OFF while the new files are written. The entire process may take between 20 to 30 minutes. The firmware upgrade is complete when you can login into the web configuration pages.

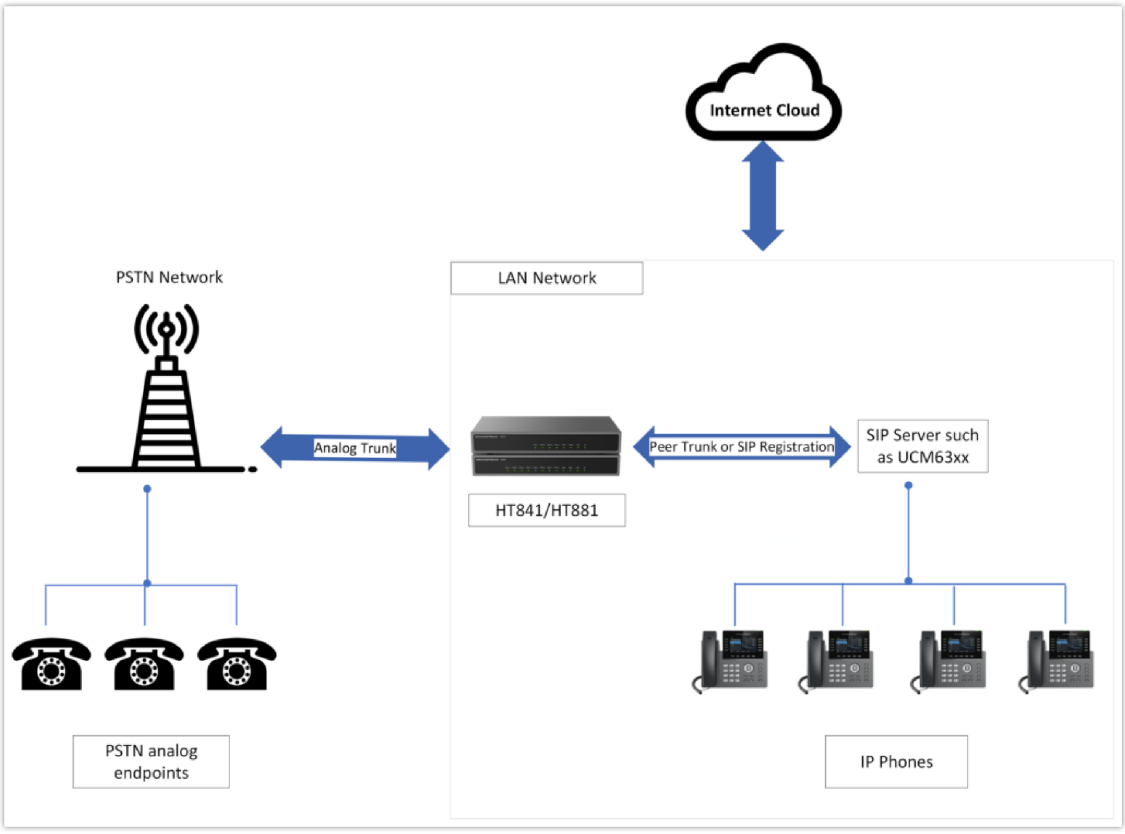
Application Description

IP PBX / SIP Server with HT841/HT881

A SIP proxy server such as UCM6xxx can be deployed with the HT841/HT881 series. In this environment, the SIP server handles SIP registration and call control, and the HT841/HT881 processes media conversion between IP and PSTN calls.

There are 2 ways to configure HT841/HT881 when using with a SIP Server:

1. **With SIP accounts configured on the Channels page.** In this case, the HT841/HT881 act like an endpoint requesting registration from the SIP Server. Under the Channels webpage, you will need to fill in information like SIP User ID, Password, etc. Now, when you try to make calls from IP, the call will be routed to the SIP Server which will forward it to one of the SIP accounts on the HT841/HT881, which will then forward it to the PSTN line.
2. **Without SIP accounts.** In this case, you simply have to configure the SIP Server to perform forwarding of the SIP INVITE message with the FXO destination number to the gateway's IP Address. The HT841/HT881 will receive the digits and immediately forward them on the FXO lines to the destination PSTN. Most of the configuration on the Gateway for this case will remain the default, except Stage Method needs to be set to 1, and SIP Server IP Address/DNS name has to be filled.

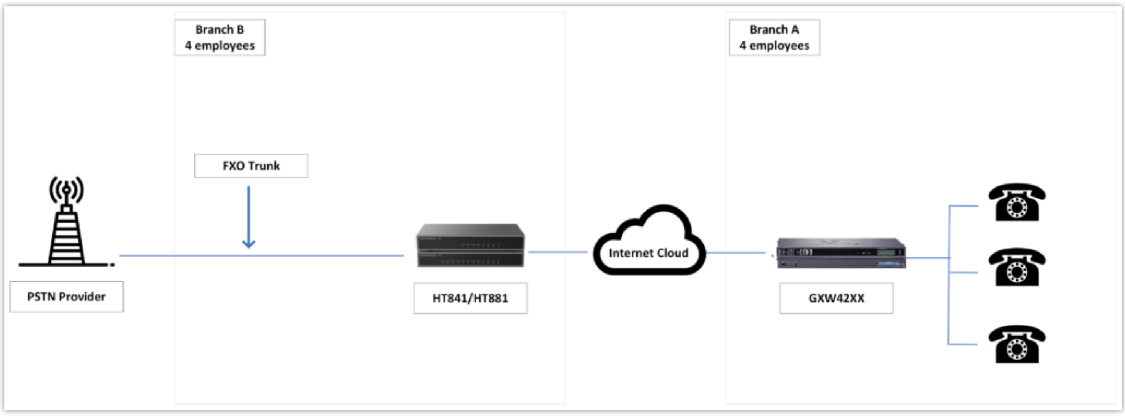


Functional Diagram of IP-PBX & HT841/HT881

For incoming calls from the PSTN analog endpoints to the HT841/HT881, the device will auto-forward each call to a configured IP extension. The SIP Server can then route the call based on its own configuration or IVR system.

FXS Gateway with HT841/HT881 [No SIP Server required]

Alternatively, the HT841/HT881 can be used without a SIP Server. You can use it in conjunction with an FXS Gateway (Ex. GXW42xx) and still be able to originate and terminate calls from IP to PSTN and vice versa. All you need to make sure is that the 2 gateways are able to locate each other (they should be on the same LAN or on Public IP addresses).



GXW42xx & HT8x1 Scenario/Toll-Free Calling between Locations

In this diagram, configure the SIP Server field to be the IP Address of the other gateway (i.e. configure the IP address of the FXS gateway to be SIP Server of HT841/HT881 and vice versa). Please be sure you set SIP Registration to No.

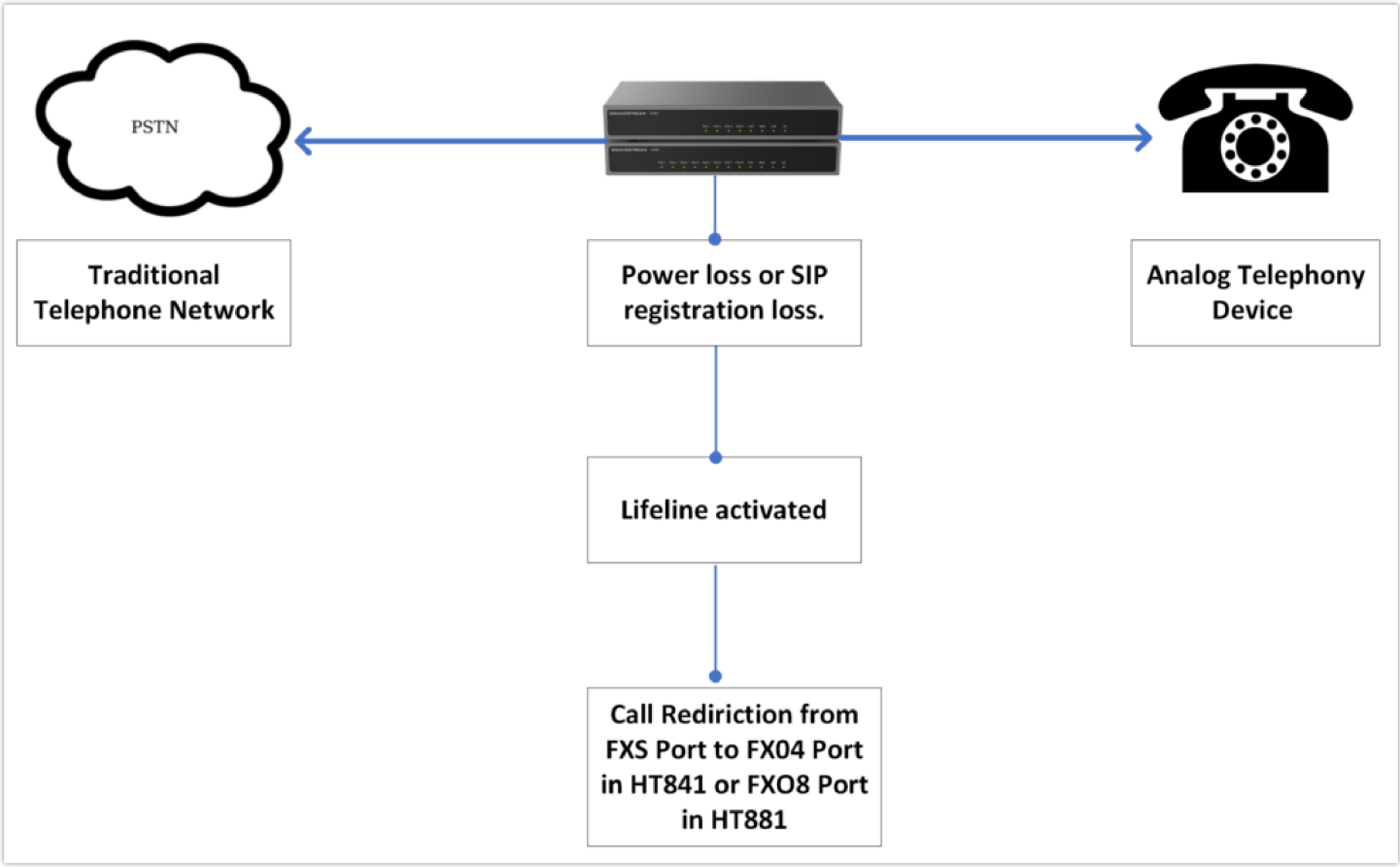
Expected Call Flow: Analog Phone (GXW42xx) picks up and dials destination PSTN number. The call gets routed to the HT841/HT881 which dials out the digit string onto the FXO Lines, thus reaching the destination PSTN endpoint. In reverse, incoming calls from PSTN endpoints will be routed automatically to the FXS Gateway through HT841/HT881.

GXW42xx Gateway	**HT841/HT881 Gateway**
Profile 1 SIP Server – Set it to the IP Address of HT841/HT881 SIP Registration – No Outgoing Call without Registration – Yes NAT traversal – No	**Advanced Settings** STUN Server – Blank Use Random Port – No
Advanced Settings STUN Server – Blank	**FXO lines** Wait for Dial Tone – Y or N (whichever works for your PSTN Service Provider) Stage Method – 1 Unconditional Call Forward to VOIP: ch1-8:444; @ch1-8:p1; ch1-8:5060++; **Channels** 1-8 5060 Profile 1 Local SIP Listen port (For VOIP to PSTN calls) – 5060++ **Profile 1** SIP Server – Set it to IP Address of GXW42xx SIP Registration – No NAT traversal – No

FXS and FXO Gateway Configuration Example

FXS/FXO Lifeline Implementation

The “Life Line” feature is a telecommunications feature that ensures users can still place or receive a Public Switched Telephone Network (PSTN) call in emergency situations or when there is a disruption in the internet service (SIP registration loss). The feature operates by connecting the PSTN line to an analog phone that is connected to the FXS port.



FXO/FXS Lifeline Support

*Refer to the following lifeline port info table:

Model	Lifeline Port Mapping		
HT841	FXS	⟷	FXO4
HT881	FXS	⟷	FXO8

The three modes of operation are as follows:

- **Auto Mode (Default):** In Auto mode, the Life Line feature will automatically activate when there is a power loss or when the device loses its registration with the SIP server (which means the VoIP service is unavailable). When this happens, the PSTN line will be seamlessly connected to the analog phone connected to the FXS port. This allows users to make and receive traditional phone calls through the PSTN network, providing a backup communication method during emergencies or internet outages.
- **Always Connected Mode:** In Always Connected mode, the Life Line feature is permanently active, meaning the PSTN line is always connected to the phone connected to the FXS port. In this configuration, VoIP calls will not be allowed. This mode ensures that the device prioritizes the traditional PSTN line for all communications and does not rely on VoIP services.
- **Always Disconnected Mode:** In Always Disconnected mode, the Life Line feature is disabled, and the device will only allow users to make and receive VoIP calls on the FXS port. PSTN calls via the FXS port will not be possible in this configuration. This mode is suitable for situations where the user wants to use VoIP exclusively and does not require the fallback option of PSTN connectivity.

FXS Telephony Implementation

When the FXS port on an FXO gateway is connected to an analog phone, the following basic telephony operations can typically be performed:

Placing a Phone Call

To make the outgoing calls using your HT841/HT881

1. Pick up the handset of the connected phone.
2. Dial the number directly and wait for 4 seconds (Default "No Key Entry Timeout"); or
3. Dial the number directly and press # (Use # as dial key" must be configured in web configuration).

Examples:

1. Dial an extension directly on the same proxy, (e.g. 1008), and then press the # or wait for 4 seconds.
2. Dial an outside number (e.g. (626) 666-7890), first enter the prefix number (usually 1+ or international code) followed by the phone number. Press # or wait for 4 seconds. Check with your VoIP service provider for further details on prefix numbers.

Direct IP Calls

Direct IP calling allows two parties, that is, an FXS Port with an analog phone and another VoIP Device, to talk to each other in an ad hoc fashion without a SIP proxy.

Elements necessary to completing a Direct IP Call:

- Both HT841/HT881 and other VoIP Devices, have public IP addresses, or
- Both HT841/HT881 and other VoIP Devices are on the same LAN using private IP addresses, or
- Both HT841/HT881 and other VoIP Devices can be connected through a router using public or private IP addresses (with necessary port forwarding or DMZ).

The HT841/HT881 supports two ways to make Direct IP Calling:

Using IVR

1. Pick up the analog phone then access the voice menu prompt by dialing "***"
2. Dial "47" to access the direct IP call menu
3. Enter the IP address after the dial tone and voice prompt "Direct IP Calling"

Using Star Code

1. Pick up the analog phone then dial "*47"
2. Enter the target IP address.

No dial tone will be played between steps 1 and 2 and destination ports can be specified using "*" (encoding for ":") followed by the port number.

Examples of Direct IP Calls:

a) If the target IP address is 192.168.0.160, the dialing convention **is *47 or Voice Prompt with option 47, then 192*168*0*160**, followed by pressing the "#" key if it is configured as a send key or wait 4 seconds. In this case, the default destination port 5060 is used if no port is specified

b) If the target IP address/port is 192.168.1.20:5062, then the dialing convention would be: ***47 or Voice Prompt with option 47, then 192*168*0*160*5062** followed by pressing the "#" key if it is configured as a send key or wait for 4 seconds.

Note: When completing a direct IP call, the "**Use Random SIP/RTP Port**" should be set to "NO".

CALL FEATURES

The HT841/HT881 supports all the traditional and advanced telephony features, the following table summarizes each key with its corresponding Call Feature.

Key	Call Features
*02	Forcing a Codec (per call) *027110 (PCMU), *027111 (PCMA), *02723 (G723), *02729 (G729), *027201 (iLBC).
*03	Disable LEC (per call) Dial "*03" +" number". No dial tone is played in the middle.
*16	Enable SRTP
*17	Disable SRTP
*30	Block Caller ID (for all subsequent calls)
*31	Send Caller ID (for all subsequent calls)
*47	Direct IP Calling. Dial "*47" + "IP address". No dial tone is played in the middle.
*50	Disable Call Waiting (for all subsequent calls)
*51	Enable Call Waiting (for all subsequent calls)
*67	Block Caller ID (per call). Dial "*67" +" number". No dial tone is played in the middle.
*82	Send Caller ID (per call). Dial "*82" +" number". No dial tone is played in the middle.
*69	Call Return Service: Dial *69 and the phone will dial the last incoming phone number received.
*70	Disable Call Waiting (per call). Dial "*70" +" number". No dial tone is played in the middle.
*71	Enable Call Waiting (per call). Dial "*71" +" number". No dial tone is played in the middle
*72	Unconditional Call Forward: Dial "*72" and then the forwarding number followed by "#". Wait for dial tone and hang up. (dial tone indicates successful forward)
*73	Cancel Unconditional Call Forward. To cancel "Unconditional Call Forward", dial "*73", wait for dial tone, then hang up.
*74	Enable Paging Call: Dial "*74" and then the destination phone number you want to page.
*78	Enable Do Not Disturb (DND): When enabled all incoming calls are rejected.
*79	Disable Do Not Disturb (DND): When disabled, incoming calls are accepted.
*87	Blind Transfer
*90	Busy Call Forward: Dial "*90" and then the forwarding number followed by "#". Wait for dial tone then hang up.
*91	Cancel Busy Call Forward. To cancel "Busy Call Forward", dial "*91", wait for dial tone, then hang up.
*92	Delayed Call Forward. Dial "*92" and then the forwarding number followed by "#". Wait for dial tone then hang up.
*93	Cancel Delayed Call Forward. To cancel Delayed Call Forward, dial "*93", wait for dial tone, then hang up

Flash/Hook	Toggles between active call and incoming call (call waiting tone). If not in conversation, flash/hook will switch to a new channel for a new call.
#	Pressing pound sign will serve as Re-Dial key.

HT841/HT881 Call Features

CONFIGURATION GUIDE

The HT841/HT881 can be configured in one of two ways:

- The IVR voice prompt menu.
- The embedded Web GUI on the HT841/HT881 using PC's web browser.

Obtain HT841/HT881 IP Address

HT841/HT881 is by default configured to obtain the IP address from the DHCP server where the unit is located. To know which IP address is assigned to your HT841/HT881, you should access the "Interactive Voice Response Menu" of your adapter via the connected phone and check its IP address mode.

Please refer to the steps below to access the interactive voice response menu:

1. Use a telephone connected to the FXS port of your HT841/HT881.
2. Press *** (press the star key three times) to access the IVR menu and wait until you hear "Enter the menu option ".
3. Press 02 and the current IP address will be announced.

Understanding HT841/HT881 IVR Menu

The HT841/HT881 has a built-in voice prompt menu for simple device configuration which lists actions, commands, menu choices, and descriptions. Connect an analog phone to FXS port. Pick up the handset and dial "***" to use the IVR menu.

Menu	Voice Prompt	Options
Main Menu	"Enter a Menu Option"	Press "*" for the next menu option Press "#" to return to the main menu Enter 01-05, 07,10, 12-17,47 or 99 menu options
01	"DHCP Mode", "Static IP Mode" "PPPoE Mode"	Press "9" to toggle the selection If using "Static IP Mode", configure the IP address information using menus 02 to 05. If using "Dynamic IP Mode", all IP address information comes from the DHCP server automatically after reboot. If using "PPPoE Mode", configure PPPoE Username and Password from web GUI to get IP from your ISP.
02	"IP Address " + IP address	The current WAN IP address is announced. If using "Static IP Mode", enter 12-digit new IP address. You need to reboot your HT841/HT881 for the new IP address to take Effect.
03	"Subnet " + IP address	Same as menu 02
04	"Gateway " + IP address	Same as menu 02
05	"DNS Server " + IP address	Same as menu 02
07	Preferred Vocoder	Press "9" to move to the next selection in the list:

		PCM U / PCM A iLBC G-726 G-723 G-729 OPUS
10	"MAC Address"	Announces the MAC address of the unit. **Note:** The device has two MAC addresses. One for the NET1 port and one for the NET2 port. The device MAC address announced is the address of NET2 port.
12	WAN Port Web Access	Press "9" to toggle between Auto / Enabled / Disabled. Default is Auto.
13	Firmware Server IP Address	Announces current Firmware Server IP address. Enter 12-digit new IP address.
14	Configuration Server IP Address	Announces current Config Server Path IP address. Enter 12-digit new IP address.
15	Upgrade Protocol	Upgrade protocol for firmware and configuration update. Press "9" to toggle between TFTP / HTTP / FTP / FTPS or HTTPS. Default is HTTPS.
16	Firmware Version	Announces Firmware version information.
17	Firmware Upgrade	Firmware upgrade mode. Press "9" to toggle among the following three options: ● Always check ● Check when pre/suffix changes ● Never upgrade
47	"Direct IP Calling"	Enter the target IP address to make a direct IP call, after dial tone. (See "Make a Direct IP Call".)
86	Voice Mail	Access to your voice mails messages.
99	"RESET"	Press "9" to reboot the device. Enter MAC address to restore factory default setting: RESTORE FACTORY DEFAULT SETTINGS
	"Invalid Entry"	Automatically returns to main menu
	"Device not registered"	This prompt will be played immediately after off hook If the device is not registered and the option "Outgoing Call without Registration" is in NO

HT841/HT881 IVR Menu

Four success tips when using the voice prompt

- "*" shifts down to the next menu option and "**#**" returns to the main menu
- "9" functions as the ENTER key in many cases to confirm or toggle an option.
- All entered digit sequences have known lengths – 2 digits for the menu option and 12 digits for the IP address. For IP address, add 0 before the digits if the digits are less than 3 (i.e. – 192.168.0.26 should be keyed in like 192168000026. No decimal is needed).
- Key entry cannot be deleted but the phone may prompt an error once it is detected.

Please make sure to reboot the device after changing network settings (IP Address, Gateway, Subnet…) to apply the new configuration.

Accessing the Web UI

- **Via NET1 port**

1. You may check your HT841/HT881 IP address using the IVR on the connected phone.

Please see Obtain the HT841/HT881 IP address via the connected analogue phone

2. Open the web browser on your computer.
3. Enter the HT841/HT881's IP address in the address bar of the browser.
4. Enter the administrator's password to access the Web Configuration Menu.

> The computer must be connected to the same sub-network as the HT841/HT881. This can be easily done by connecting the computer to the same hub or switch as the HT841/HT881.

- **Via NET2 port**

1. Power your HT841/HT881 using PSU with the right specifications.
2. Connect your computer or switch directly to your HT841/HT881 LAN port.
3. Open the web browser on your computer.
4. Enter the default LAN IP address (192.168.2.1) in the address bar of the browser.
5. Enter the administrator's password to access the Web Configuration Menu.
6. Make sure to reboot your device after changing your settings to apply the new configuration.

> Please make sure that your computer has a valid IP address on the range 192.168.2.x so you can access the web GUI of your HT841/HT881.

Web Configuration Pages Definitions

This section describes the options in the HT841/HT881 Web UI.

Status Page Definitions

System Info

Product Model	Displays the Product model: HT841 or HT881
Serial Number	Displays the device's serial number
Hardware Version	Displays the hardware version
Part Number	Displays the part number
Software Version	• **Program:** Displays the current software version running on the device • **Bootloader:** Displays the bootloader version • **Core:** Displays the Core version • **Base:** Displays the Base version • **CPE:** Displays the Customer Premises Equipment version
Software Status	Displays whether the software is running correctly on the device

Mem	Displays the memory usage
System Up Time	Displays the duration of the system up time
CPU Load	Displays the processor load
Provision	Displays the last status of provisioning
System Info	Downloads the system info

Network Status

MAC Address	Displays the device's MAC address
IPv4 Address	Displays the assigned IPv4 address
IPv6 Address	Displays the assigned IPv6 address
VPN IPv4 Address	Displays the connected VPN IPv4 address, if available.
VPN IPv6 Address	Displays the connected VPN IPv4 address, if available.
Network Cable Status	Displays the status of the NET1 and NET2 ports, it is shown as UP if connected, and DOWN if disconnected
PPPoE Link Up	Indicates active connectivity between the gateway and the network provider through PPPoE
NAT	Displays the type of NAT used
Certificate Type	Displays the certificate type

Port Status

Port Status	
Port	Displays the type of analog port : FXS, FXO1, FXO2....
Hook	Shows the status of the port, On Hook, Off Hook, Not connected...
User ID	Displays the SIP user ID registred on the port
Registration	Displays wether the port is registered or not
Sip Destination Port	Displays the SIP Destination port used by the analog interface.
Port Options	
Port	Displays the FXS port
DND	Displays whether the connected analog phone is on DND mode or not

Forward	Indicates the forwarding number
Busy Forward	Indicates the busy forwarding number
Delayed Forward	Indicates the delayed forwarding number
CID	Indicates the Caller ID
Call Waiting	Indicates if Call waiting is enabled
SRTP	Indicates if Secured RTP is enabled

System Settings Page Definitions

Basic Settings

Disable Voice Prompt	The voice prompt is disabled if set to Yes. Default value is "No"
Disable Direct IP Call	The direct IP call is disabled if set to Yes. Default value is "No"
Blacklist For Incoming Calls	Blocks calls from specific numbers. Use "," to separate numbers
Lock Keypad Update	The configuration update via keypad is disabled if set to Yes Default value is "No"
Play Busy Tone When Account is unregistered	If set to Yes, busy tone will be played when user goes offhook from an unregistered account. Default value is "No"
Prefix to Specify FXO Port	This option is used with hunting group. Dial pattern: prefix + port + (dialing) will request the port per call, dialing is necessary in 1 stage dial scenario. Maximum 10 digits, with no default value
Life Line Mode	Specifies a backup communications route that becomes the active route when the primary route fails, ensuring continued connectivity and call reliability, the available options are: ● **Auto:** In case of power loss or loss of SIP registration, the PSTN line will be seamlessly connected to analog phone connected to FXS port. ● **Always Disconnected:** PSTN line will be always connected to the phone connected to FXS port. VoIP calls will not be allowed in this configuration. ● **Always Connected:** User can only make/receive VoIP calls. PSTN calls will not be possible. Default setting is Auto. Default value is "Auto"
DHCP Option 17 Enterprise Number	Fill in the DHCP Option 17 enterprise number, the default is 3561
Disable SIP NOTIFY Authentication	If set to Yes, NOTIFY requests will be accepted without authentication

Time and Language

Time Zone	

NTP Server	This parameter sets the IP address of the NTP server. The device will obtain the date and time from the server
Allow DHCP Option 42 to override NTP server	If DHCP Option 42 is enabled, the NTP server can be changed. Enabled by default
Time Zone	Selects the time zone where the phone is located and control the date/time display
Self-Defined Time Zone	Allows users to define their own time zone when time zone is set to "Using self-defined Time Zone" The syntax is: std offset dst [offset], start [/time], end [/time] Default is set to: MTZ+6MDT+5,M3.2.0,M11.1.0 MTZ+6MDT+5 This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east. M4.1.0,M11.1.0 The 1st number indicates Month: 1,2,3.., 12 (for Jan, Feb, .., Dec) The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…) The 3rd number indicates weekday: 0,1,2,..,6 (for Sun, Mon, Tues, … ,Sat) Therefore, this example is the DST which starts from the Second Sunday of March to the 1st Sunday of November.
Allow DHCP server to set Time Zone	Allows the local server's DHCP option 2 to override the phone's time zone setting
Language	
IVR Language	Selects IVR voice prompt language type, the supported languages are: English, Chinese, Russian, Spanish

Ringtone

System Ring Cadence	Cadence on+off value range (0, 16000) milliseconds
Prompt Tone Access Code	The key pattern to get Prompt Tone. Maximum 20 digits. No default value provided
PSTN Disconnect Tone	The arrived Busy Tone is used as the disconnect signal. **Syntax:** fxoch x-y:f1=freq@vol,f2=freq@vol, c=on1/off1[-on2/off2[-on3/off3]];... **Allowed Range:** freq = 10 to 4000Hz; vol = -40 to -12dBm; **Default:** Busy **Tone**:fxo1-8:f1=480@-32,f2=620@-32,c=500/500;
CPT Settings: ● Dial Tone ● Ringback Tone ● Busy Tone ● Reorder Tone ● Confirmation Tone ● Call Waiting Tone ● Wait for Dial-Tone ● Conference Party Hangup Tone ● Special Proceed Indication Tone ● Special Condition Tone	Using these settings, users can configure tone frequencies and cadence according to their preference. By default, they are set to North American frequencies. Configure these settings with known values to avoid uncomfortable high pitch sounds. ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous tone, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Example configuration for N.A. **Dial tone:** fxsch1:f1=350@-17,f2=440@-17,c=0/0;fxoch1-4:f1=350@-17,f2=440@-17,c=0/0; **Syntax:** fxsch1:f1=val[,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]]; fxoch x-y:f1=val[,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]] (Frequencies are in (10, 4000) Hz and cadence on and off are in (0, 64000) ms)

Security Settings

Web/SSH Access	
Web Access Mode	Sets web page access protocol, the options are: HTTP, HTTPS, Disabled
HTTP Web Port	Defines the HTTP Web Port, defaut is 80
HTTPS Web Port	Defines the HTTPS Web Port, defaut is 443
Web Session Timeout	Defines the web session timeout, default value is 10 Minutes, the valid range is 1-60 minutes
Web Access Attempt Limit	Defines the Web Access Attempt Limit before locking the web access, default is 5, valid range is 1-10
Web Lockout Duration	Defines for how long the web access will be locked, default value is 15 Minutes, valid range is 0-60 Minutes
Disable User Level Web Access	Disables or enables user-level web access. Default value is "Yes" : the user level web access is disabled.
Disable Viewer Level Web Access	Disables or enables viewer-level web access. Default value is "Yes" : the viewer level web access is disabled.
Disable SSH	If set to "No", the phone will allow SSH access, Set to "No" by default
SSH Port	Defines the SSH port, default is 22. Cannot be the same as Telnet Port.
Disable Telnet	Enables/disables Telnet access. The default is "Yes"
Telnet Port	Defines the telnet port, the default is 23. Cannot be the same as SSH Port.
Security Controls for SSH/Telent Access	Specifies security measures and controls that apply to the SSH/Telnet protocol to ensure secure and authorized access to the device, the following options are supported ● **Only Allow SSH private IP users to set system Pvalue:** This option permits only users with SSH access from private IP addresses to modify specific system-level configuration parameters (system Pvalues). ● **Allow all SSH users to set system Pvalue:** With this setting, all users having SSH access can modify specific system-level configuration parameters (system Pvalues). ● **Allow all SSH users to set any Pvalue:** This allows all users with SSH access to modify any configuration parameter (P-value). ● **Allow any user to set any Pvalue:** Any user, regardless of their privileges, can modify any configuration parameter (Pvalue) through SSH or Telnet access. ● **Prohibit setting Pvalue:** This option blocks all users from modifying any configuration parameter (Pvalue) via SSH or Telnet access. The Default Value is "**Allow any user to set any PValue**"
WAN Side Web/SSH Access	Enables/Disables the Web and SSH access through the WAN port. The available options are the following: ● **No:** No access to the web or SSH from any IP address on the WAN side. ● **Yes:** Access for the Web GUI and SSH is enabled on the WAN side. ● **Auto:** Only private IP could access the web or SSH on the WAN side. Default setting is Yes.
White List for WAN Side	If WAN Side Web/SSH Access is set to Yes or Auto. Users can configure the white List for WAN Side to be used for remote management. Multiple IPs are supported and need to be separated by space.

	Example:192.168.5.222 192.168.5.223 192.168.7.0/24 Note: If both blacklist and whitelist are not empty, the blacklist is processed first, followed by the whitelist.
Black List for WAN Side	If WAN Side Web/SSH Access is set to Yes or Auto. Users can configure the black List for WAN Side to ban WAN side web access. Multiple IPs are supported and need to be separated by space. **Example:**192.168.5.222 192.168.5.223 192.168.7.0/24 **Note:** If both blacklist and whitelist are not empty, the blacklist is processed first, followed by the whitelist.
User Info Management	
Enable strict password rules	Enable strict password rules
Minimum password length	Defines the Minimum password length, Range: 4-30, default is 8
Required number of character classes	Sets the minimum number of character classes that a password should contain, composed of allowed combinations of different character classes;Range: 0-4, default is 3
Allowed Character classes	Defines the Allowed Character classes, which are: Lower case, Upper case, Numbers, Special characters
New Admin Password	Defines the new admin password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons
Confirm Admin Password	Confirms the entered admin password
New User Password	Defines the new user password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons
Confirm User Password	Confirms the entered user password
New Viewer Password	Defines the new viewer password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons
Confirm Viewer Password	Confirms the entered viewer password
Client Certificate	
Disable Weak TLS Cipher Suites	Allows users to disable weak ciphers DES/3DES and RC4, Symmetric Encryption SEED, Symmetric Authentication MD5, Protocol Version SSLv2/SSLv3 or Disable All of the Above Weak TLS Ciphers Suites. Default is No.
SIP TLS Certificate	Specifies SSL certificate used for SIP over TLS is in X.509 format. The HT8xx has built-in private key and SSL certificate. Maximum supported length is 8192.
SIP TLS Private Key	Specifies TLS private key used for SIP over TLS is in X.509 format. Maximum supported length is 4069.
SIP TLS Private Key Password	Specifies SSL Private key password used for SIP Transport in TLS/TCP.

Validate Server Certificates	This feature allows users to validate server certificates with our trusted list of TLS connections. The device needs to reboot after changing the setting. Default is enabled.
Minimum TLS Version	This feature allows customer to choose desired Minimum TLS Version. Choices are: Unlimited TLS 1.0 TLS 1.1 TLS 1.2 Default is Unlimited.
Maximum TLS Version	This feature allows customer to choose desired Maximum TLS Version. Choices are: Unlimited TLS 1.0 TLS 1.1 TLS 1.2 Default is Unlimited.
Custom Certificate	Allows users to update to the device their own certificate signed by a custom CA certificate to manage client authentication.
Trusted CA Certificates	
Load CA Certificates	This feature allows user to specify which certificate to trust when performing server authentication. **Build-in trusted:** (Default) Build-in trusted certificates **Custom trusted certificate:** Uploaded Certificates **All trusted Certificates:** Both built-in and uploaded Certificates
• **Trusted CA Certificates A** • **Trusted CA Certificates B** • **Trusted CA Certificates C** • **Trusted CA Certificates D**	These trusted CA certificates will be used for the authentication server TLS certificate

TR069

Enable TR-069	Sets the phone adapter system to enable the “CPE WAN Management Protocol” (TR-069). The default setting is Yes.
ACS URL	Specifies URL of TR-069 Auto Configuration Servers (e.g., http://acs.mycompany.com), or IP address. Default setting is: “https://acs.gdms.cloud”
ACS Username	Enter username to authenticate to ACS.
ACS Password	Enter password to authenticate to ACS.
Periodic Inform Enable	Sends periodic inform packets to ACS. Default is Yes.
Periodic Inform Interval	Sets frequency that the inform packets will be sent out to ACS. Default is 86400 seconds.
Connection Request Username	Enters username for ACS to connect to the HT8x1.
Connection Request Password	Enters password for ACS to connect to the HT8x1.

Connection Request Port	Configures the TR-069 connection request port. The value range is 0 to 65535.Default is 7547
CPE SSL Certificate	Configures the Cert File for the phone adapter to connect to the ACS via SSL.
CPE SSL Private Key	Specifies the Cert Key for the phone adapter to connect to the ACS via SSL.

RADIUS Settings

Enable RADIUS Web Access Control	Selects whether to enable RADIUS web access control. Default is no
Action upon Radius Auth Server Error	Select the RADIUS authentication server error handling method,the user can choose between: Reject Access, or Authentificate locally, the default is "local verification"
RADIUS Auth Protocol	Configures RADIUS authentication protocol
RADIUS Auth Server Address	Configures RADIUS authentication server address
RADIUS Auth Server Port	Configure RADIUS authentication server port
RADIUS Shared Secret	Configures the shared secret key
RADIUS VSA Vendor ID	Configure the RADIUS VSA provider ID to match the RADIUS server's configuration. The default value for Grandstream Networks Inc is 42397
RADIUS VSA Access Level Attribute	Configure the RADIUS VSA access level attributes to match the configuration of the RADIUS server. Incorrect settings will cause Radius authentication to fail.

E911/HELD

E911	
Enable E911	Enable Enhanced 911 call. Default is disabled
E911 Emergency Numbers	A user can configure multiple emergency numbers separated with the delimiter symbol ";".
Geolocation-Routing Header	If "Yes", E.911 INVITE message includes the "Geolocation-Routing" header with the value "Yes"
Priority Header	If "Yes", E.911 INVITE message includes the "Priority" header with the value "emergency"
HELD	
HELD Protocol	Configure HELD transfer protocol. HTTP or HTTPS
HELD Synchronization Interval	The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when the interval is 0.
HELD Location Types	Configure "locationType" element in the location request. "geodetic", "civic" and "location URI"
HELD NAI	Configure "locationType" element in the location request. "geodetic", "civic" and "location URI"
HELD Identity 1-10	The HELD Identity refers to Hierarchical Mobile IPv6 (HMIPv6) Enhanced Location-based Discovery (HELD) protocol. This protocol is utilized to determine the location of a mobile device when making an emergency call,

	such as a 911 call, over an IP-based network. You can configure up to 10 HELD identities.
HELD Identity 1-10 Value	Defines the HELD Identity value.
Location Server	
Location Server	Configures the location server (LIS) address
Location Server Username	Configures Location Server (LIS) username
Location Server Password	Configures Location Server (LIS) password
Secondary Location Server	Configures secondary location server (LIS) address
Secondary Location Server Username	Configures secondary location server (LIS) username
Secondary Location Server Password	Configures secondary location server (LIS) password

Network Settings Page Definitions

Ethernet Settings

General Settings	
Internet Protocol	Selects one of the following IP protocol modes: ● **IPv4 Only:** Enforce IPv4 protocol only. ● **IPv6 Only:** Enforce IPv6 protocol only. ● **Both, Prefer IPv4:** Enable both IPv4 and IPv6 and prefer IPv4. ● **Both, prefer IPv6:** Enable both IPv4 and IPv6 and prefer IPv6. **Note:** Make sure to reboot the HT841/HT881 unit for the changes to take effect.
IPv4 address type	Allows users to configure the appropriate network settings on the HT841/HT881 to obtain IPv4 address. Users could select DHCP, Static IP or PPPoE. By default, it is set to DHCP.
DHCP hostname	Specifies the name of the client. The name may or may not be qualified with the local domain name. This field is optional but may be required by ISP.
DHCP domain name	allows user to configure DHCP domain name. This option specifies the domain name that the client should use when resolving hostnames via the Domain Name System. This field is optional.
DHCP vendor class ID	Exchanges vendor class ID by clients and servers to convey particular configuration or other identification information about a client. Default is HT8X1.
PPPoE account ID	Defines the PPPoE username. Necessary if ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection.
PPPoE password	Specifies the PPPoE account password.
PPPoE Service Name	Defines PPPoE service name. If your ISP uses a service name for the PPPoE connection, enter the service name here. This field is optional.

Preferred DNS server 1-4	Specifies preferred DNS server to use when DHCP or PPPoE are set. You can set up yo 4 Preferred DNS Servers.
IPv6 address type	Configures the IPv6 address of the phone: ● **DHCP:** all the field values for the static IP mode are not used (even though they are still saved in the flash memory.) The FXO Gateway acquires its IP address from the first DHCP server it discovers from the LAN it is connected. ● **Static IP mode:** configure IP address, 1st and 2nd DNS server, preferred DNS server. These fields are set to zero by default. ● **Full Static:** When enabling the option full static, users need to specify the Static IPv6 and the IPv6 Prefix length. ● **Prefix Static:** When enabling the option prefix static, users need to specify the IPv6 Prefix (64 bits).
Static address type	1. **Full Static:** When enabling the option full static, users need to specify the Static IPv6 and the IPv6 Prefix length. 2. **Prefix Static:** When enabling the option prefix static, users need to specify the IPv6 Prefix (64 bits).
Static IPv6 Address	When using fully static type IPv6, enter a static IPv6 address
IPv6 Prefix Length	Enter the static IPv6 address prefix length
DNS Server 1	Enter DNS server 1 address
DNS Server 2	Enter DNS server 2 addres
Preferred DNS Server	Enter preferred DNS server address
Advanced Settings	
Layer 2 QoS 802.1Q/VLAN Tag	Enables VLAN tagging for Quality of Service (QoS) at Layer 2. Valid range: 0-4094
Layer 2 QoS SIP 802.1p	Prioritizes SIP traffic at Layer 2 using the 802.1p standard for Quality of Service (QoS). The valid range 0-7
Layer 2 QoS RTP 802.1p	Prioritizes RTP (Real-time Transport Protocol) traffic at Layer 2 using the 802.1p standard for Quality of Service (QoS). The valid range 0-7
Use DNS to detect network connectivity	Use DNS to detect WAN side network problems. The default setting is "No"
Use ARP to detect network connectivity	Use ARP to check network connection. The default value is "yes"
STUN server	Provides URL for STUN (Session Traversal Utilities for NAT) server that assists in establishing connections between the HT8x1 across network address translation (NAT) by discovering public IP addresses and ports of devices behind a NAT firewall.
Keep-alive Interval	Sends periodically a blank UDP packet to SIP server to keep the “ping hole” on the NAT router open. Default is 20 seconds. Valid range is 10-160 seconds
Use STUN to detect network connectivity	Use STUN keep-alive to detect WAN side network problems
Black List for WAN Side Port	Ports on the blacklist will be disabled on the device

SNMP Settings

Enable SNMP	Enables the Simple Network Management Protocol. Default is "No"
SNMP Version	Choose between (Version 1, Version 2c, or Version 3).
SNMP Port	Listening Port of SNMP daemon (Default 161).
SNMP Trap IP Address	IP address of trap destination. Up to 3 trap destinations are supported. Users should enter the IP addresses separated with comma (,).
SNMP Trap Port	Port of Trap destination (Default 162)
SNMP Trap Version	Choose between (Version 1, Version 2c, or Version 3).
SNMP Trap Interval	Time interval between traps (Default is 5).
SNMPv1/v2c Community	Name of SNMPv1/v2c community.
SNMPv1/v2c Trap Community	Name of SNMPv1/v2c trap community.
SNMPv3 User Name	Username for SNMPv3.
SNMPv3 Security Level	**noAuthUser:** Users with security level noAuthnoPriv and context name as noAuth. **authUser:** Users with security level authNoPriv and context name as auth. **privUser:** Users with security level authPriv and context name as priv.
SNMPv3 Authentication Protocol	Select the Authentication Protocol: “None” or “MD5” or “SHA.”
SNMPv3 Privacy Protocol	Select the Privacy Protocol: “None” or “AES/AES128” or “DES”.
SNMPv3 Authentication Key	Enter the Authentication Key.
SNMPv3 Privacy Key	Enter the Privacy Key.
SNMPv3 Trap User Name	Username for SNMPv3 Trap.
SNMPv3 Trap Security Level	**noAuthUser:** Users with security level noAuthnoPriv and context name as noAuth. **authUser:** Users with security level authNoPriv and context name as auth. **privUser:** Users with security level authPriv and context name as priv.
SNMPv3 Trap Authentication Protocol	Select the Authentication Protocol: “None” or “MD5” or “SHA”.
SNMPv3 Trap Privacy Protocol	Select the Privacy Protocol: “None” or “AES/AES128” or “DES”.
SNMPv3 Trap Authentication Key	Enter the Trap Authentication Key.
SNMPv3 Trap Privacy Key	Enter the Trap Privacy Key.

DDNS Settings

Enable DDNS	Enable DDNS function. Disabled by default
DDNS Server	Select DDNS server used, options are: ● dyndns.org ● freedns.afraid.org ● zoneedit.com ● no-ip.com ● oray.net
DDNS Username	Sets the username of the DDNS server
DDNS Password	Sets the password of the DDNS server
DDNS Hostname	Sets the domain name of the DDNS server
DDNS Hash	Sets the hash value of the DDNS server

LAN Settings

General Settings	
Working Mode of Network Interface	Refers to the configuration of the network interfaces on a device. ● **NET1 is WAN and NET2 is LAN (Default):** NET1 is set as the Wide Area Network (WAN) interface, typically used to connect to the internet or external networks, while NET2 is set as the Local Area Network (LAN) interface, used for internal local connections ● **NET1 is LAN and NET2 is WAN:** the roles of the interfaces are reversed, where NET1 becomes the LAN interface, and NET2 becomes the WAN interface.
Device Mode	Controls whether the device is working in NAT Router, Bridge, or WAN Only mode. ● **NAT Router:** In this mode, the WAN port acts as a DHCP client. LAN port is used as DHCP Base IP; devices connected behind the LAN port will be assigned an IP from HT841/HT881 DHCP Server. ● **Bridge:** In this mode, the WAN port acts as a DHCP client and pass-through to the LAN port; devices connected behind the LAN port will get an IP from your network DHCP server (same as the WAN port). ● **WAN Only:** In this mode, only the WAN port is active. LAN port is not used.List Item 3 The default mode is Bridge mode. Save the setting and reboot prior to configuring the HT841/HT881.
Enable UPnP support	When set to Yes, the HT841/HT881 acts as a UPnP gateway for your UPnP-enabled applications. UPnP = Universal Plug and Play. The default is No.
Uplink bandwidth	Specifies the maximum uplink bandwidth permitted by the device. This function is disabled by default. The total bandwidth can be set as 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M, or 15 M. The primary function of this setting is to limit the uplink bandwidth for the device's internal system, signaling, and NATed traffic. **Example:** When 512k is configured, there will be at least 512kbps limited for internal system, signaling, and NATed traffic. **Note:** Voice or RTP stream will never be limited.
Downlink bandwidth	Specifies the maximum downlink bandwidth permitted by the device. This function is disabled by default. The total bandwidth can be set as 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M, or 15 M. The primary function of this setting is to limit the download bandwidth for the device's internal system, signaling, and NATed traffic.

	Example: if 128 is configured, there will be at least 128kbps limited for internal system, signaling, and NATed traffic. **Note:** Voice or RTP stream will never be limited.
DMZ IP	This function forwards all WAN IP traffic to a specific IP address if no matching port is used by HT841/HT881 or in the defined port forwarding.
NAT maximum ports	Defines the number of ports that can be managed while in NAT router mode. Range: 0 - 4096, default is 1024. Typically, one port per connection
NAT TCP timeout	NAT TCP idle timeout in seconds. The connection will be closed after preconfigured, timeout if not refreshed. Range: 0 - 3600
NAT UDP timeout	NAT UDP idle timeout in seconds. The connection will be closed after preconfigured, timeout if not refreshed. Range: 0 - 3600, default is 300
Reply to ICMP on WAN port	When set to Yes, the HT841/HT881 responds to the PING command from other computers but is also made vulnerable to DOS attacks. The default is No.
Cloned WAN MAC Addr	This allows the user to change/set a specific MAC address on the WAN interface. Note: Set in Hex format.
LAN Port VLAN Feature Under Bridge Mode	This feature allows users to configure a different VLAN tag and priority value for the second network port when HT841/881 is configured in bridge mode. The priority value range is 0-7, The VLAN tag range is 0-4094. The default VLAN Tag and Priority value are 0.
Enable LAN DHCP	When set to Yes, the device will function as a simple router and the LAN port will provide IP addresses to the internal network. Connect the WAN port to ADSL/Cable modem or any other equipment that provides access to the public Internet. The default setting is Yes.
LAN DHCP Base IP	Base IP Address for a LAN port. The default factory setting is **192.168.2.1**. **Note**: When the device detects WAN IP is conflicting with LAN IP, the LAN base IP address will be changed based on the network mask the effective subnet will be increased by 1. For example; 192.168.2.1 will be changed to 192.168.3.1 if the netmask is 255.255.255.0. Then the device will reboot
LAN DHCP Start IP	The default value is 100. The last segment of IP address is assigned to the HT841/HT881 in the LAN Network. Default configuration assigns IP address (to local network devices) starting from 192.168.2.100.
LAN DHCP End IP	Default value is 199. This parameter allows a user to limit the number of local network devices connected to the internal router.
LAN Subnet Mask	Sets the LAN subnet mask. Default value is 255.255.255.0
DHCP IP Lease Time	Default value is 120 hrs. (5 days). The length of time the IP address is assigned to the LAN clients. Value is set in units of hours.
Port Forwarding	Forwards a matching (TCP/UDP) port to a specific LAN IP address with a specific (TCP/UDP) port. Up to 8 rules are available.

Management Interface

Management Interface	
Enable Management Interface	Allows activation of a dedicated interface for remote management and configuration of the device.

	Disabled by Default.
Management Access	defines the allowed methods (protocols) and permissions for remote access and configuration of the device, two options can be selected ● **Management Interface Only:** allows remote access and configuration solely through the dedicated management interface ● **Both Service and Management Interfaces:** permits remote access and configuration through both the management interface and the service interface.
Enable SNMP Through Management Interface	Allows the activation of SNMP (Simple Network Management Protocol) access exclusively through the dedicated management interface for monitoring and managing the device remotely. Disabled by Default
Enable TR069 Through Management Interface	Allows the activation of TR-069 protocol access exclusively through the dedicated management interface for remote device management and provisioning. Disabled by Default
Enable Syslog Through Management Interface	Allows the activation of syslog communication exclusively through the dedicated management interface for remote logging and monitoring of device events. Disabled by Default.
Management Interface IPv4 Address	
802.1Q/VLAN Tag	Allows the tagging of network packets with VLAN information to segment and prioritize network traffic. The Valid Range is 0-4094, Default value is 0
802.1p priority value	Assigns a priority value to network packets for Quality of Service (QoS) and traffic prioritization purposes. The Valid Range is 0-7, Default value is 0
IPv4 address type	Configures the address type of the management network port, the options are: ● Dynamically configured by DHCP ● Statically configured as
IP Address	Configure the IPv4 address of the management network port
Subnet Mask	Defines the subnet mask
Default Router	Defines default gateway
DNS Server 1	Defines DNS server 1 address
DNS Server 2	Defines DNS server 2 address

OpenVPN Settings

Enable OpenVPN	Allow user to enable OpenVPN®. Default is No.
OpenVPN Server Address	Specify the IP address or FQDN for the OpenVPN® Server.
OpenVPN Port	Specify the listening port of the OpenVPN® server. Default is 1194
OpenVPN Interface type	Specify the Interface type of OpenVPN® whether TAP or TUN. Default is TUN.
OpenVPN Transport	Specify the Transport Type of OpenVPN® whether UDP or TCP. The default is UDP.

Enable OpenVPN LZO Compression	Enable OpenVPN® LZO Compression. Default is Yes.
OpenVPN Encryption	Select the OpenVPN® Encryption. Default is BF-CBC 128 bit (default key).
OpenVPN Diges	Select the OpenVPN® Digest. Default is SHA1.
OpenVPN Username	Configure the OpenVPN® username.
OpenVPN Password	Configure the OpenVPN® password
OpenVPN CA	Specifies the OpenVPN® CA. Maximum Character Number is 8192.
OpenVPN Certificate	Specifies the OpenVPN® Certificate. Maximum Character Number is 8192.
OpenVPN Client Key	Specifies the Client Key. Maximum Character Number is 8192.
OpenVPN Client Key Password	Configures the OpenVPN® Client Key Password. Maximum Length is 64.

802.1x Settings

802.1x Mode	Allow users to enable/disable 802.1X Mode. Disabled by default
802.1x Identity	Enter 802.1X identity information
802.1x Password	Enter 802.1X MD5 password
802.1x CA Certificate	Paste down the 802.1X certificate .pem file
802.1x Client Certificate	Paste down the Client.pem certificate file containing certificate and key

Maintenance Settings Page Definitions

Upgrade

Firmware	
Upgrade via Manually Upload	Uploads the .bin firmware file
Upgrade Via	Selects firmware upgrade/provisioning method: TFTP, HTTP, HTTPS, FTP or FTPS. Default is HTTPS.
Firmware Server Path	Sets IP address or FQDN of firmware server. The URL of the server that hosts the firmware release. Note: You can specify the protocol used in the Firmware Server Path. (example: https://192.168.5.120), this will bypass the "Upgrade Via" method.
HTTP/HTTPS/FTP/FTPS User Name	Enters username to authenticate with HTTP/HTTPS FTP/FTPS server.
HTTP/HTTPS/FTP/FTPS Password	Enters password to authenticate with HTTP/HTTPS FTP/FTPS server.
Firmware File Prefix	Checks if firmware file is with matching prefix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.

Firmware File Postfix	Checks if firmware file is with matching postfix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server.
Config File	
Upload Configuration	Uploads the configuration file in .txt or .xml formats
Restore From Backup Configuration	Restore From Backup Configuration
Download Device Configuration	Downloads Device Configuration in .txt format
Download Device XML Configuration	Downloads Device Configuration in .xml format
Export Backup Configuration	Export Backup Configuration in .xml format
Config Upgrade via	Selects Config file upload method: TFTP, HTTP, HTTPS, FTP or FTPS. Default is HTTPS.
Config Server Path	Sets IP address or FQDN of configuration server. The URL of the server that hosts the configuration file to provision HT8xx. **Note:** You can specify the protocol used in the Config Server Path. (example: https://192.168.5.120), this will bypass the "Upgrade Via" method.
HTTP/HTTPS/FTP/FTPS User Name	Enters username to authenticate with HTTP/HTTPS FTP/FTPS server.
HTTP/HTTPS/FTP/FTPS Password	Enters password to authenticate with HTTP/HTTPS FTP/FTPS server.
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file using OpenSSL.
Config File Prefix	Checks if configuration files are with matching prefix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
Config File Postfix	Checks if configuration files are with matching postfix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server.
Provision	
Allow DHCP Option 66 or 160 to override server	Obtains configuration and upgrade server's information using options 66 from DHCP server. Note: If DHCP Option 66 is enabled, the HT8xx will attempt downloading the firmware file from the server URL provided by DHCP, even though Config Server Path is left blank. The server URL provided by DHCP can include authentication credentials using following format: "username:password@Provisioning_Server_IP".
3CX Auto Provision	Sends multicast "SUBSCRIBE" message for provisioning at booting stage, used for PnP (Plug-and-Play) configuration. Default is Yes.
Enable using tags in URL	Allows users to configure variables on the configuration server path to differentiate the directories on the server.
Always send HTTP Basic Authentication Information	Default is No. If set to Yes, The device will send configured user name and password within HTTP request before server sends authentication challenge.
Additional DHCP option	Additional DHCP options will be used as a firmware upgrade server in place of the configured or DHCP options 43 and 66 settings. This option will only take effect if "Enable DHCP options 43 and 66 server settings" is enabled

Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options: **No:** The HT8x1 will only do an upgrade once at boot up. **Check every X minutes:** User needs to specify a period in minutes. **Check every day:** User needs to specify the start hour and the end hour of the day (0-23). **Check every week:** User needs to specify "Day of the week (0-6)". (Day of week is starting from Sunday). Default is No.
Randomized Automatic Upgrade	Randomized Automatic Upgrade within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s).
Firmware upgrade and profile detection	Configure the detection method of firmware upgrade and configuration file requests
Advanced Settings	
Verify host when using HTTPS	Enables / disables the host verification when using HTTPS.
Authenticate Conf File	Authenticates configuration before being accepted. This protects the configuration from unauthorized modifications. Default is No.
Configuration File Types Allowed	Allows users to configure provision configuration file type in xml file only or all file types.
Download and Process All Available Config Files	This feature allows users to download and process all available config files. By default, the device will provision the first available config in the order of cfgMAC > cfgMAC.xml > cfgMODEL.xml > and cfg.xml (corresponding to device-specific, model-specific, and global configs). If this option is enabled, the device will inverse the downloading process to cfg.xml > cfgMODEL.xml > cfgMAC.bin > cfgMAC.xml and add cfgMAC_override.xml. The following files will override the files that have already been loaded and processed. The default value is "No"

System Diagnosis

Syslog	
Syslog Server	URL or IP address of the syslog server.
Syslog Level	Select the HT8xx to report the log level. Default is NONE. The level is one of EXTRA DEBUG, DEBUG, INFO, WARNING or ERROR. Syslog messages are sent based on the following events: 1. product model/version on boot up (INFO level) 2. NAT related info (INFO level) 3. sent or received SIP message (DEBUG level) 4. SIP message summary (INFO level) 5. inbound and outbound calls (INFO level) 6. registration status change (INFO level) 7. negotiated codec (INFO level) 8. Ethernet link up (INFO level) 9. SLIC chip exception (WARNING and ERROR levels) 10. memory exception (ERROR level) extra syslog style (EXTRA DEBUG level)
Syslog Protocol	Allow encrypted SSL/TLS transmission to the syslog server if SSL/TLS is selected, the default value is UDP **Note:** The validity of the server CA certificate will be verified
Send SIP Log	Sets whether to include SIP logs in the system log Default value is "Yes"
Debug	

Ethernet Capture	Enables the capturing and analysis of Ethernet network traffic for troubleshooting and monitoring purposes.
With secret key information	Allows users to make packet capture including the secret key to decrypt the captured TLS packets. Default value is No.
Port Record	Allows the recording of port-level call information, such as call duration, caller ID, and call status, for monitoring and logging purposes.
PSTN Detection	Detection will keep the call up for about 1 minute. If you have selected Semi-auto Detect, please follow the prompt in the "status", the following parameters can be defined: ● Detect Mode ● Source Port (to be detected) ● Destination Port ● Destination Number ● Status ● Results
Core Dump	Provides generated core dump file if unit malfunctions. Clean will be displayed if no issues.
GR909	
Test To Run	Selects the type of test that wll be performed for the specified line, the following tests can be performed: ● Hazardous Potential Test ● Foreign Electromotive Forces Test ● Resistive Faults Test ● Receiver Offhook Test ● Ringer Equivalent Number Test
FXS Line	Defines the FXS line under test
Run Interval	Defines the run Interval in seconds, the default value is 120 seconds, the default range is 0-604800 seconds

File Management

CDR Records	Displays a list of the last 1000 call records, the ionformation included in the records are the following: ● UserID ● ToNumber ● FromNumber ● StartTime ● StartTalkTime ● EndTime ● Duration ● State ● Direction Clicking the "Download" button will download the last 1000 call records Clicking the "Delete" button will delete the last 1000 call records
SIP Messages	The SIP messages tab displays a list of SIP headers that are captured after each triggered call, the information displayed on the tab are similar to the information that can be captured using the wireshark tool, and filtering by SIP protocol. An example of captured trace for the SIP header can be as shown below: ● HT841 --- 2024-05-03 04:43:09.827 SENDING TO 192.168.5.168:5060 REGISTER sip:192.168.5.168 SIP/2.0 Via: SIP/2.0/UDP 192.168.5.66:5060;branch=z9hG4bK443123589;rport From: <sip:1000@192.168.5.168>;tag=1597031286 To: <sip:1000@192.168.5.168>

	Call-ID: 963579881-5060-1@BJC.BGI.F.GG CSeq: 2138 REGISTER Contact: <sip:1000@192.168.5.66:5060>;reg-id=1;+sip.instance="<urn:uuid:00000000-0000-1000-8000-C074ADEAA59E>" Max-Forwards: 70 User-Agent: Grandstream HT841 1.0.5.9 Supported: path Expires: 3600 Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE Content-Length: 0 Clicking the "Download" icon will download the whole log of the captured traces. Clicking "Delete" will delete all the captured traces. This tool can be useful for network administrators that wantto treoubleshoot the call flows without having to use an external tool, for analyzing the network

Device Manager

Reboot	
Automatic restart	This option triggeres an automatic reboot of the unit, the available options are: ● **No** ● **Reboot everday:** you can specify the reboot hour ● **Reboot everyweek:** you can specify the day of the week, and the hour of the day, for the reboot to take place ● **Reboot every month:** you can specify the day of the month, and the hour of the day, for the reboot to take place
Restore Factory	
Reset Type	Gives the administrator the option to restore the default configuration on the HT841/HT881. There are 3 types of factory reset: ● **ISP Data Reset:** All ISP (Internet Service Provider) configurations that may affect the IP address will be reset (including WAN static IP). ● **VoIP Data Reset:** All VoIP-related configurations (mainly everything located on FXS/FXO page). ● **Full Reset:** Both VoIP and ISP-related configuration at the same time. **Note:** After choosing the reset type, you will have to click the reset button for it to take effect.

Ports Settings Page Definitions

FXS Profile

General Settings	
Account Registration	
Profile Active	Activates / Deactivates the accounts. The FXS port configuration will not change if disabled, although the port will not be operational, in this state, there will be no dial tone when picking up the analog phone and making/receiving calls will not be possible.
Primary SIP Server	Configures SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). This is the primary SIP server used to send/receive SIP messages from/to HT841/HT881.
Failover SIP Server	Defines failover SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6

	fe80::20b:82ff:fe75:211d:). This server will be used if primary SIP server becomes unavailable.
Prefer Primary SIP Server	Selects to prefer primary SIP server. The account will register to primary Server if registration with Failover server expires. Default is No.
Outbound Proxy	Specifies IP address (Supports both IPv4 and IPv6 addresses) or domain name of outbound Proxy, or media gateway, or session border controller. (For example: proxy.myprovider.com, IPv4: 192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). It's Used by HT841/HT881 for firewall or NAT penetration in different network environments. If symmetric NAT is detected, STUN will not work and only outbound proxy can correct the problem
Backup Outbound Proxy	Configures the backup outbound proxy to be used when the "Outbound Proxy" registration fails. (For example: proxy.myprovider.com, or IP address, if any: IPv4: 192.168.5.170/ IPv6: fe80::20b:82ff:fe75:211d). By default, this field is left empty.
Prefer Primary Outbound Proxy	If the user configures this option to "Yes", when the registration expires, the device will re-register via primary outbound proxy. By default, this option is disabled.
From Domain	Allows users to add the actual domain name, it will override the from header.This is an optional configuration.
Allow DHCP Option 120 (override SIP server)	Configures the HT841/HT881 to collect SIP server address from DHCP option 120. Default is No.
Network Settings	
Layer 3 QoS SIP DSCP	the Diff-Serv value for SIP packets in decimal, the range is 0-63, default value is 26
Layer 3 QoS RTP DSCP	Diff-Serv valuefor RTP packets in decimal, the range is 0-63, default value is 46
DNS Mode	Selects DNS mode to use for the client to look up server. One mode can be chosen. **A Record (Default):** resolves IP Address of target according to domain name. **SRV:** DNS SRV resource records indicate how to find services for various protocols. **NAPTR/SRV:** Naming Authority Pointer according to RFC 2915. **Use Configured IP:** If the SIP server is configured as domain name, device will not send DNS queries, but will use "Primary IP" or "Backup IP" to send SIP message if at least one of them is not empty. It will try to use "Primary IP" first, after 3 tries without any response, it will switch to "Backup IP 1", then "Backup IP 2", and then it will switch back to "Primary IP" after 3 retries.
DNS SRV Failover Mode	Configure the preferred IP mode when DNS Mode is SRV or NAPTR/SRV. • Default SIP request will always be sent to the address with the top priority based on the SRV query result, even if this address is different from the registered IP address. • Saved one until DNS TTL SIP request will always be sent to the registered IP address until DNS TTL expires or registered IP address is unreachable. • Saved on until no response SIP request will always be sent to the registered IP address only until registered IP address is unreachable. • Failback follows failback expiration time: the primary server regains control only after the failback expiration time, allowing the secondary server to handle requests until then.
Failback Timer	When the primary SBC is up, device will send SIP requests to the primary SBC. If at any point device fails over to the secondary SBC, the SIP requests will stay on the failover SBC for the duration of the failback timer. When the timer expires, device will send SIP requests to the primary SBC, (in minutes. Default is 60 minutes, max 45 days).
Maximum Number of SIP Request Retries	This feature allows user to configure the number of SIP retries before failover occurs. (between 1 and 10, default is 2).
Register Before DNS SRV Failover	This feature is used to control whether the device need to initiate a new registration request (following existing DNS SRV fail-over mode) first and then direct the non-registration SIP request (INVITE) to the new successfully registered server or not.

Primary IP	The main IP address used for communication and control.
Backup IP1	The secondary IP address used as a backup for communication in case the Primary IP fails.
Backup IP2	The third IP address used as an additional backup for communication in case both the Primary IP and Backup IP1 fail.
NAT Traversal	Indicates type of NAT for each account. This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, Keep-alive, STUN, UPnP. Default setting is No.
Use NAT IP	Defines NAT IP address used in SIP/SDP messages. It should only be used if required by ITSP.
Proxy-Require	Determines a SIP Extension to notify the SIP server that the HT841/HT881 is behind a NAT/Firewall.
SIP Settings	
SIP Basic Settings	
SIP Registration	Controls whether the HT841/HT881 needs to send REGISTER messages to the proxy server. The default setting is Yes.
SIP Transport	Selects transport protocol for SIP packets; UDP or TCP or TLS. Please make sure your SIP Server or network environment supports SIP over the selected transport method. Default is UDP.
Unregister On Reboot	Controls whether to clear SIP user's information by sending un-register request to the proxy server. The un-registration is performed by sending a REGISTER message with "Expires=0" parameter to the SIP server. This will unregister the SIP account under the concerned FXS page.Unregister on reboot option can be set to "No", "All" or "Instance". 1. **Set to "No":** If the "Unregister on reboot" option is set to "No", it means that the SIP user's information will not be cleared when the device reboots. In other words, the SIP account will remain registered with the server even after the device is rebooted. 2. **Set to "All":** If the "Unregister on reboot" option is set to "All", it means that all SIP accounts associated with the device will be unregistered when the device reboots. This option clears the SIP user's information for all the FXS ports on the device. 3. **Set to "Instance":** If the "Unregister on reboot" option is set to "Instance", it means that only the SIP account associated with the concerned FXS port will be unregistered when the device reboots. This option clears the SIP user's information for only the specific FXS port that is affected by the reboot. Default value is set to "No"
Outgoing Call without Registration	Enables the ability to place outgoing calls even if the account is not registered (if allowed by ITSP); device will not be able to receive incoming calls. Default is No.
Register Expiration	Refreshes registration periodically with specified SIP proxy (in minutes). Maximum interval is 65535 minutes (about 45 days). Default is 60 minutes (or 1 hour).
Reregister before Expiration	Sends re-register request after specific time (in seconds) to renew registration before the previous registration expires.
SIP Registration Failure Retry Wait Time	Sends re-register request after specific time (in seconds) when registration process fails. Maximum interval is 3600 seconds (1 hour). Default is 20 seconds.
SIP Registration Failure Retry Wait Time upon 403 Forbidden	Sends re-register request after specific time (in seconds) when registration process fails with error 403 Forbidden. Maximum interval is 3600 seconds (1 hour). Default is 1200 seconds.

Port Voltage Off upon no SIP Registration or SIP Registration Failure	Cuts off voltage to the port if there is no SIP registration or if SIP registration fails, preventing unwanted calls. (in minutes. Between 0-60, default is 0. 0 means port voltage is never turned off)
Delay Time of Port Voltage Off Timer Since Boot	Sets the delay time after boot before the FXO port voltage turns off. It controls the timing for powering down FXO ports on the gateway. The value is in minutes. Between 0-60, default is 0
Enable SIP OPTIONS/NOTIFY Keep Alive	Enables SIP OPTIONS or SIP NOTIFY to track account registration status so the ATA will send periodic OPTIONS/NOTIFY message to server to track the connection status with the server. Default setting is No.
SIP OPTIONS/NOTIFY Keep Alive Interval	Configures the time interval when the ATA send OPTIONS or NOTIFY message to SIP server. The default setting is 30 seconds, which means the ATA will send an OPTIONS/NOTIFY message to the server every 30 seconds. The default range is 1-64800.
SIP OPTIONS/NOTIFY Keep Alive Max Lost	Defines the Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3.
Local SIP Port	Defines local port to use by the HT841/HT881 for listening and transmitting SIP packets. Default value is 5060
Local RTP Port	Defines the local RTP-RTCP port pair the HT841/HT881 will listen and transmit. It is the HT841/HT881 RTP port for channel 0. The default value for FXS port is 5004
Use Random SIP Port	Controls whether to use configured or random SIP ports. This is usually necessary when multiple HT841/HT881 are behind the same NAT. The default is No.
Use Random RTP Port	Controls whether to use configured or random RTP ports. This is usually necessary when multiple HT841/HT881 are behind the same NAT. The default is No.
RTP/RTCP Keep Alive On Hold	Enables or disables RTP/RTCP keep-alive packets during call hold to maintain connectivity and prevent session timeouts. Disabled by default.
Hold Target Before Refer	Allows user to hold or not hold the phone call before referring. The default setting is Yes.
Refer-To Use Target Contact	Includes target's "Contact" header information in "Refer-To" header when using attended transfer. Default is No.
Remove OBP from Route Header	Removes outbound proxy info in "Route" header when sending SIP packets. Default setting is No.
Support SIP Instance ID	Gives the users the possibility of making conference calls by pressing "Flash" key, when it's enabled by dialing *23 +second callee number. Default is No
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	Controls the port information in the Via header and Contact header. If set to "No", these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. Default is No.
Tel URI	Indicates E.164 number in "From" header by adding "User=Phone" parameter or using "Tel:" in SIP packets, if the HT841/HT881 has an assigned PSTN Number. Disabled: Use "SIP User ID" information in the Request-Line and "From" header. User=Phone: "User=Phone" parameter will be attached to the Request-Line and "From" header in the SIP

	request to indicate the E.164 number. If set to “Enable”. Enabled: “Tel:” will be used instead of “sip:” in the SIP request. Please consult your carrier before changing this parameter. The default is Disabled.
Use Privacy Header	Determines if the “Privacy header” will be presented in the SIP INVITE message and if it includes the caller info in this header. If set to Default, it will add Privacy header unless special feature is Telkom SA or CBCOM. Default is Default.
Use P-Preferred-Identity Header	Specifies if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to “default”, the P-Preferred-Identity Header will be omitted in SIP INVITE message when Telkom SA or CBCOM is active. If set to “Yes”, the P-Preferred- Identity Header will always be presented. If set to “No”, it will be omitted. Default setting is: Default.
Use P-Access-Network-Info Header	With this feature enabled, device will populate the WAN access node with IEE-802.11a, IEE-802.11b in P-Access-Network-Info SIP header.
Use P-Emergency-Info Header	This feature support of IEEE-48-addr and IEEE-EUI-64 in SIP header for emergency calls.
Use P-Asserted-Identity Header	When this feature is set to Yes, device will send P-Asserted-Identity Header on the SIP Invite. Default setting is No.
Caller ID Fetch Order	Selects the Caller ID display order which need to be respected by the ATA. The available options are: **Auto:** When set to “Auto”, the ATA 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:** When set to “Disabled”, all incoming calls are displayed with “Unavailable”. **From Header:** When set to “From Header”, the ATA will use the FROM header to display the caller ID.
SIP T1 Timeout	Defines T1 timeout value. It is an estimate of the round-trip time between the client and server transactions. For example, HT841/HT881 will attempt to send a request to a SIP server. The time it takes between sending out the request to the point of getting a response is the SIP T1 timer. If no response is received the timeout is increased to (2*T1) and then (4*T1). Request re-transmit retries would continue until a maximum amount of time is defined by T2. The default is 0.5 seconds.
SIP T2 Interval	Identifies maximum retransmission interval for non-INVITE requests and INVITE responses. Retransmitting and doubling of T1 continues until it reaches the T2 value. The default is 4 seconds.
SIP Timer D	Configures SIP Timer D defined in RFC3261. 0 – 64 seconds. Default is 0.
Do Not Escape '#' as %23 in SIP URI	Replaces # by %23 in some special situations. Default is No.
Disable Multiple m line in SDP	Sends only one m line in SDP, regardless of how many m fields are in the incoming SDP. Default is No.
Enable 100rel	Appends “100rel” attribute to the value of the required header of the initial signaling messages. Default is No.
Add Auth Header On Initial REGISTER	Adds “Authentication” header with blank “nonce” attribute in the initial SIP REGISTER request. Default is No.
Enable Call Waiting Alert-Info in 180 Ringing Response	Activates the Call Waiting feature by including Call Waiting Alert-Info in the 180 Ringing response sent to the caller during an incoming call. Default value is no.
Conference URI	Allows users to manually configure the conference URL. The default is null.
Allow SIP Factory Reset	Allows to reset the devices directly through SIP Notify. If “Allow SIP Factory Reset” is set to “YES” under FXO PORT, then the ATA receives the NOTIFY from the SIP server with Event: reset, the HT should perform a factory reset after the authentication.

	The authentication in this case can be either with: The admin password if no SIP account is configured on the HT. With the credentials of the SIP account if configured on the ATA.
SIP User-Agent	This feature allows users to configure SIP User Agent. If not configured, device will use the default User Agent header.
SIP User-Agent Postfix	Configures the SIP User-Agent Postfix
Add MAC in User-Agent	This feature allows users to configure "User-Agent" in the SIP header field, when this feature is set to"No", "User-Agent" does not carry a MAC, when this feature is set "Yes except REGISTER", "User-Agent" in REGISTERSIP header field does not carry MAC but other SIP packet header fields carries MAC, when this feature is set to "Yes to all SIP", "User-Agent" in the SIP packet header field will carries the MAC.
Use MAC Header	This feature allows users to configure MAC Header in the SIP packet header field, when this feature is set to "No" ,the MAC header field is not carried in the SIP packet header field, when this feature is set to "REGISTER Only", the register packet header field carries the MAC header field but the remaining SIP packets do not carry MAC header fields, when this feature is set to "Yes to all SIP", the MAC header field is carried in the SIP data packet header field.
Session Timer	
Enable Session Timer	Disable the session timer when this option is set to "No". By default, this option is enabled.
Session Expiration	Enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). When the session interval expires, if there is no refresh via an UPDATE or re-INVITE message, the session will be terminated. Session Expiration is the time (in seconds) at which the session is considered timed out, if no successful session refresh transaction occurs beforehand. Valid range is 90-64800 seconds. Default is 180 seconds.
Min-SE	Defines Minimum session expiration (in seconds). Default is 90 seconds.
Caller Request Timer	Uses session timer when making outbound calls if remote party supports it. Valid range is 90-64800 seconds. Default is No.
Callee Request Timer	Uses session timer when receiving inbound calls with session timer request. Default is No.
Force Timer	Uses session timer even if the remote party does not support this feature. Selecting "No" will enable session timer only when the remote party supports it. To turn off Session Timer, select "No" for Caller and Callee Request Timer, and Force Timer. Default is No
UAC Specify Refresher	Specifies which end will act as refresher for outgoing calls. Default is Omit. UAC: The device acts as the refresher. UAS: Callee or proxy server act as the refresher.
UAS Specify Refresher	Specifies which end will act as refresher for incoming calls. Default is Omit.: UAS: The device acts as the refresher. UAC: Callee or proxy server act as the refresher.
Force INVITE	Uses INVITE message to refresh the session timer. Default is No.
When To Restart Session After Re-INVITE received	Allows users to delay posting Media Change Event, it can be set to "Immediately" or to "After replying 200OK" The default value is "Immediately".
Security Settings	
Validate Incoming SIP Message	Checks the authenticity and integrity of incoming SIP messages for enhanced security.

Check SIP User ID for incoming INVITE	Checks the SIP User ID in the Request URI of the incoming INVITE; if it doesn't match the HT841/HT881 SIP User ID, the call will be rejected. Direct IP calling will also be disabled. The default is No.
Authenticate incoming INVITE	Challenges the incoming INVITE for authentication with SIP 401 Unauthorized message. Default is No.
Allow Incoming SIP Messages from SIP Proxy Only	Checks SIP address of the Request URI in the incoming SIP message; if it doesn't match the SIP server address of the account, the call will be rejected. Default is No.
Authenticate server certificate domain	Configures whether to validate the domain certificate when download the firmware/config file. If it is set to "Yes", the phone will download the firmware/config file only from the legitimate server. The default setting is "No".
Trusted domain name list	Supports setting specific domain names and wildcard domain names, wildcard domain names such as "*.grandstream.com", use "," to separate domain names
Authenticate server certificate chain	Verifies certificate when communication method is TCP/TLS
Codec Settings	
DTMF Settings	
Preferred DTMF method	Sorts DTMF methods (in-audio, via RTP (RFC2833) or via SIP INFO) by priority.
Inband DTMF Duration	Allows users to config the Inband DTMF Duration and inter-duration. The default Duration is 100 ms. Valid range: 40-2000 ms. The default Inter-duration is 50 ms. Valid range: 40-2000 ms.
DTMF Payload Type	Defines payload type for DTMF using RFC2833.
Inband DTMF Tx Gain	Adjusts the transmit gain for inband Dual-Tone Multi-Frequency (DTMF) tones during call signaling. The Valid range is -12-12 db, default is 0
DSP DTMF Detector Duration Threshold	Allows users to config the DSP DTMF Detector Duration Threshold. The default Duration is 30 ms. Valid range: 20-2000 ms. The default Inter-duration is 30 ms. Valid range: 20-2000 ms.
DSP DTMF Detector Min Level	determines the minimum level of DTMF tones that the DSP DTMF detector can reliably detect, range is -45-0 dBm, default is -25
DSP DTMF Detector Snr	Sets the signal-to-noise ratio threshold for the DSP DTMF detector, determining the sensitivity to distinguish DTMF tones from background noise in the audio signal. Range: 0-12, default is 1
DSP DTMF Detector Deviation	Specifies the allowed frequency deviation from standard DTMF tones that the DSP DTMF detector can accommodate. Range: 0-25, default is 25
DSP DTMF Detector Twist	Defines the maximum deviation from ideal tone frequencies allowed for reliable DTMF detection by the DSP. Range: 0-12dB, default is 5
Disable DTMF Negotiation	Uses DTMF order without negotiation. Default is No.
RFC2833 Events Count	This feature allows users to customize the count of RFC2833 events. Default is 8.

RFC2833 End Events Count	This feature allows users to customize the count of RFC2833 end events. Default is 3.
Preferred Vocoder	
Preferred Vocoder (in listed order)	Configures vocoders in a preference list (up to 8 preferred vocoders) that will be included with same order in SDP message. Vocoder types are G.711 A-/U-law, G.726-32, G.723, G.729, iLBC and OPUS
Voice Frames per TX	Transmits a specific number of voice frames per packet. Default is 2; increases to 10/20/32/64 for G711/G726/G723/other codecs respectively.
G723 Rate	Operates at specified encoding rate for G.723 vocoder. Available encoding rates are 6.3kbps or 5.3kbps. Default is 6.3kbps.
iLBC Frame Size	Specifies iLBC packet frame size (20ms or 30ms). Default is 20ms.
Disable OPUS Stereo in SDP	Disables OPUS stereo in SDP. Default is No.
iLBC Payload Type	Determines payload type for iLBC. Valid range is between 96 and 127. Default is 97.
OPUS Payload Type	Determines payload type for OPUS. Valid range is between 96 and 127. Default is 123.
Enable Audio RED with FEC	Enables the use of audio redundancy (RED) with forward error correction (FEC) to enhance audio quality and resilience against packet loss in real-time communication systems such as VoIP
Audio FEC Payload Type	Specifies the payload type used for transmitting audio forward error correction (FEC) packets in a VoIP system.
Audio RED Payload Type	Defines the payload type assigned to audio redundancy (RED) packets in a VoIP system,
VAD	Allows detecting the absence of audio and conserves bandwidth by preventing the transmission of “silent packets” over the network. Default is No.
Use First Matching Vocoder in 200OK SDP	Includes only the first matching vocoder in its 200OK response, otherwise it will include all matching vocoders in same order received in INVITE. Default is No.
Symmetric RTP	Changes the destination to send RTP packets to the source IP address and port of the inbound RTP packet last received by the device. Default is No.
Enable RTCP	Allows users to enable RTCP. The default setting is “Yes”.
Fax Mode	Specifies the fax mode: T.38 (Auto Detect) FoIP by default, or Pass-Through. If using Pass-through mode, select preference codec as PCMU or PCMA.
Re-INVITE After Fax Tone Detected	Permits the unit to send out the re-INVITE for T.38 or Fax Pass Through if a fax tone is detected. Default is Enabled
Jitter Buffer Type	Selects jitter buffer type (Fixed or Adaptive) based on network conditions.
Jitter Buffer Length	High (initial 200ms, min 40ms, max 600ms) **Note:** not all vocoders can meet the high requirement. Medium (initial 100ms, min 20ms, max 200ms). Low (initial 50ms, min 10ms, max 100ms).
SRTP Mode	Selects SRTP mode to use (“Disabled”, “Enabled but not forced”, or “Enabled and forced”). Default is Disabled It uses SDP Security Description to exchange key. Please refer to

	SDES: https://tools.ietf.org/html/rfc4568 **SRTP:** https://www.ietf.org/rfc/rfc3711.txt
SRTP Key Length	Allows users to select supported SRTP Key Length. the available values are :
Crypto Life Time	Adds crypto life time header to SRTP packets. Default is Yes.
Analog signal line configuration	
SLIC Setting	Depends on standard phone type (and location).
Caller ID Scheme	Selects the caller id scheme, for example: Bellcore/Telcordia, ETSI-FSK …
Polarity Reversal	Reverses the polarity upon call establishment and termination. Default is No.
Loop Current Disconnect	Allows the traditional PBX used with HT841/HT881 to apply this method for signaling call termination. The method initiates a short voltage drop on the line when the remote (VoIP) side disconnects an active call. The default is No.
Play busy/reorder tone before Loop Current Disconnect	Allow user to configure if it will play busy/reorder tone before loop current disconnect upon call fail. Default is No.
Loop Current Disconnect Duration	Configures the duration of voltage drop described in the topic above. HT841/HT881 support a duration range from 100 to 10000ms. The default value is 200.
Enable Pulse Dialing	Allow users to enable Pulse Dialing option under FXS Port. Default is No.
Pulse Dialing Standard	Allows users to use Swedish pulse dialing standard or New Zealand pulse dialing standard. Default is General Standard.
Enable Hook Flash	Enables the FLASH button to be used for terminating calls. Default is Yes.
Hook Flash Timing	Defines the time period when the cradle is pressed (Hook Flash) to simulate FLASH. To prevent unwanted activation of the Flash/Hold and automatic phone ring-back, adjust this time value. HT841/HT881 support a range from 40 to 2000 ms. Default values are 300 minimum and 1100 maximum.
On Hook Timing	Specifies the on-hook time for an on-hook event to be validated. HT841/HT881 support a range from 40 to 2000 ms. Default value is 400.
Gain	Adjusts the voice path volume. • Rx is a gain level for signals transmitted by FXS • Tx is a gain level for signals received by FXS. Default = 0dB for both parameters. Loudest volume: +6dB Lowest volume: -6dB. User can adjust volume of call using the Rx gain level parameter and the Tx gain level parameter located on the FXS port configuration page. If call volume is too low when using the FXS port (ie. the ATA is at user site), adjust volume using the Rx gain level parameter under the FXS port configuration page. If voice volume is too low at the other end, user may increase the far end volume using the Tx gain level parameter under the FXS port configuration PAGE.
Disable Line Echo Canceller (LEC)	Disables the LEC per call base. Recommended for Fax/Data calls. Default is No.
Enable High Ring Power	Configures a high ringing voltage output for the device.

OnHook DC Feed Current	This feature is used to adjust DC feed current.
Call Settings	
Offhook Auto-Dial Delay	Sets the delay time before automatic dialing begins after going off-hook on an FXO port. Range is 0-60 seconds, default is 0
No Key Entry Timeout	Initiates the call within this time interval if no additional key entry during dialing stage. Default is 4 seconds.
Early Dial	Sends an early INVITE each time a key is pressed when a user dials a number. Otherwise, only one INVITE is sent after full number is dialed (user presses Dial Key or after "no key entry timeout" expires). This option should be used only if there is a SIP proxy is configured and supporting "484 Incomplete Address" responses. Otherwise, the call will likely be rejected by the proxy (with a 404 Not Found error). Default is No. This feature is NOT designed to work with and should NOT be enabled for direct IP-to-IP calling.
Dial Plan Prefix	Adds specified prefix to dialed number.
Dial Plan	Dial Plan Rules: 1. Accept Digits: 1,2,3,4,5,6,7,8,9,0 , *, #, A,a,B,b,C,c,D,d 2. Grammar: x – any digit from 0-9; a. xx+ – at least 2 digits number; b. xx – exactly 2 digits number; c. ^ – exclude; d. . – wildcard, matches one or more characters e. [3-5] – any digit of 3, 4, or 5; f. [147] – any digit 1, 4, or 7; g. <2=011> – replace digit 2 with 011 when dialing h. <=1> – add a leading 1 to all numbers dialed, vice versa will remove a 1 from the number dialed i. | – or j. Flag T when adding a "T" at the end of the dial plan, the phone will wait for 3 seconds before dialing out. This gives users more flexibility on their dial plan setup. E.g. with dial plan 1XXT, phone will wait for 3 seconds to let user dial more than just 3 digits if needed. Originally the phone will dial out immediately after dialing the third digit. Example 1: {[369]11 | 1617xxxxxxx} – Allow 311, 611, 911, and any 10-digit numbers of leading digits 1617 Example 2: {^1900x+ | <=1617>xxxxxxx} – Block any number with leading digits 1900 and add prefix 1617 for any dialed 7-digit numbers Example 3: {1xxx[2-9]xxxxxx | <2=011>x+} – Allow any length of number with leading digit 2 and 10 digit-numbers of leading digit 1 and leading exchange number between 2 and 9; If leading digit is 2, replace leading digit 2 with 011 before dialing. 1. Default: Outgoing – { x+ | +x+ | *x+ | *xx*x+ } 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 dialing 7 numbers and 1617 area code will be added automatically 1[2-9]xx[2-9]xxxxxx – allows dialing to any US/Canada Number with 11 digits length 011[2-9]x. – allows international calls starting with 011 [3469]11 – allow dialing special and emergency numbers 311, 411, 611 and 911 Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider. In this case * should be predefined inside dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.
Use # as Dial Key	Treats "#" as the "Send" (or "Dial") key. If set to "No", this "#" key can be included as part of the dialed number. Default is Yes.
Disable # as Redial Key	Disables # to act as Redial key. If set to "Yes" and feature "Use # as Dial Key" set to Yes, the # key will act as dial key but not as redial key. Default is No.
RFC2543 Hold	Toggles between RFC2543 hold and RFC3261 hold. RFC2543 hold allows to disable the hold music sent to the other side, in this case IP address (0.0.0.0) it will be sent in SDP instead of the IP address of the unit .

	RFC3261 (a line) will play the hold music to the other side.
Disable Call-Waiting	Disables receiving a second incoming call when the line is engaged. Default is No.
Disable Call-Waiting Caller ID	Disables displaying caller ID when receiving a second incoming call. Default is No.
Disable Call-Waiting Tone	Disables playing call waiting tone during active call when receiving a second incoming call. The CWCID will still be displayed. Default is No.
Disable Connected Line ID	Disables displaying the number of the person answering the phone. Default is No.
Disable Receiver Offhook Tone	Enables / disables the warning to alert that the phone has been left off-hook for an extended period of time. Default is No.
Disable Reminder Ring for On-Hold Call	Enables playing the reminder ring. Default is No.
Disable Reminder Ring for DND	This feature allows user to disable reminder ring when FXS port is on DND mode. Default is Yes.
Disable Visual MWI	Disables use of visual message waiting indicator when there is an unread voicemail message. Default is No.
Visual MWI Type	Configures Visual WMI Type of signal sent to the analog phone to make it turn the lamp ON upon receiving a Voice mail. Check the phone's manual to find out what signal is supported, FSK (default) or Neon. **Note:** Some phones (depending on the model of the analog phone) when this feature is set to NEON it might auto ring (short beeps) when there is a voice mail available for that FXS port where it is connected.
MWI Tone	When set to Default, device will play Stutter Dial Tone when there is voicemail, if set to Special Proceed Indication Tone, device will play the configured special proceed indication tone upon user offhook when there is voicemail
Transfer on Conference Hangup	Determines whether a call is automatically transferred to a specified destination after a conference call ends. Disabled by Default
Send Hook Flash Event	Default is No. If set to yes, flash will be sent as DTMF event.
Flash Digit Control	When it set to YES it allows the user to perform some call setting when both channels are used while pressing: **"Flash + 1"** in order to hang up the current call and resume a call that was held. **"Flash + 2"** in order to hold the current call and resume a call that was held. **"Flash + 3"** in order to perform 3-way conference. **"Flash + 4"** in order to perform attended transfer.
Callee Flash to 3WC	When this feature is set to Yes, device would be able to set up the 3-way conference call even when device is the callee in the second call. Default is No.
Ring Timeout	Stops ringing when incoming call if not answered within a specific period of time. When set to 0 there will be no ringing timeout. Default is 60 seconds.
Delayed Call Forward Wait Time	Forwards incoming call if not answered within a specific period of time when delayed call forward is activated locally (using *92 code). Default value is 20 seconds.
SUBSCRIBE for MWI	Sends SUBSCRIBE periodically (depends on "Register Expiration" parameter) for message waiting indication. Default is No.

Send Anonymous	Sets “From”, “Privacy” and “P_Asserted_Identity” headers in outgoing INVITE message to “anonymous”, blocking caller ID. Default is No.
Anonymous Call Rejection	Rejects incoming calls with anonymous caller ID with “486 Busy here” message. Default is No.
Special Feature	Selects Soft switch vendors’ special requirements Examples of vendors: BroadSoft, CBCOM, RNK, Huawei, China Mobile, ZTE IMS, PhonePower, TELKOM SA, Vonage, Metaswitch, CenturyLink, MTS, Oi_BR, Telefonica, GIBTELECOM. The default is Standard.
Disable Unknown Caller ID	Disable analog phone’s caller ID when receiving a call with “Anonymous”, “unavailable” or “unknown” in FROM header and without “Display info”. **Note:** This relies also on analog phone’s design, some phones will still display “unknown” with this feature enabled. Default is No.
Replace Beginning '+' with 00 in Caller ID	When this feature is set to Yes, device will replace the “+” sign at the beginning of a number in the FROM header. Default is No.
Number of Beginning Digits to Strip from Caller ID	Removes a specified number of digits from the beginning of the Caller ID information received before displaying it to the called party. The range is between 0 and 10, default is 0
Outgoing Call Duration Limit	Defines the call duration limit for the outgoing calls. Default is 0 (No limit).
Incoming Call Duration Limit	Defines the call duration limit for the incoming calls. Range is 0-180 minutes, default is 0 (No Limit)
PSTN Access Code	Defines Key pattern to use PSTN line. Maximum 5 digits. Default is "*00"
Enable Call Features	When enabled, Do No Disturb, Call Forward and other call features can be used via the local feature codes on the phone. Otherwise, the ITSP feature codes will be used. Enable All will override all individual features enable setting. Default is Yes
Reset Call Features	Allows users to reset all call features configuration. Default is No
SRTP Feature	Allow users to customize the SRTP feature codes. Default is Yes
Enable SRTP per call	Enable SRTP: Default is 16
Disable SRTP per call	Disable SRTP: Default is 17
SRTP per call Feature	– Enable SRTP per call: Default is 18 – Disable SRTP per call: Default is 19
Enable SRTP per call	Set the function code to enable SRTP (the default value is 18), which is only valid for the current call
Disable SRTP per call	Set the function code to disable SRTP (the default value is 18), which is only valid for the current call
CID Feature	Allow users to customize the CID feature codes. Default is Yes
Enable CID	Enable CID: Default is 31
Disable CID	Disable CID: Default is 30
CID per call Feature	Whether to display the user ID, it is only valid for the current call

Enable CID per call	Enable CID per call: Default is 82
Disable CID per call	Disable CID per call: Default is 67
Direct IP Calling Feature	Allow users to customize the Direct IP feature code. Default is Yes
Direct IP Calling	Direct IP Calling: Default is 47
CW Feature	Allow users to customize the call waiting feature codes. Default is Yes
Enable CW	Enable CW: Default is 51
Disable CW	Disable CW: Default is 50
CW per call Feature	Enable or cancel the call waiting function, only the current call is valid
Enable CW per call	Enable CW per call: Default is 71
Disable CW per call	Disable CW per call: Default is 70
Call Return Feature	Allow users to customize the Call Return feature code. Default is Yes
Call Return	Call return: Default is 69
Unconditional Forward Feature	Allow users to customize the Unconditional Forward feature codes. Default is Yes
Enable Unconditional Forward	Set the function code to enable unconditional call forwarding (default value is 72)
Disable Unconditional Forward	Set the function code to cancel unconditional call forwarding (default value is 73)
Busy Forward Feature	Whether to enable the call forwarding function when busy
Enable Busy Forward	Set the function code to enable call forwarding when busy (default value is 90)
Disable Busy Forward	Set the function code to cancel call forwarding when busy (default value is 91)
Delayed Forward Feature	Whether to enable the function of transferring calls without answering
Enable Delayed Forward	Set the function code to enable call transfer without answering (default value is 92)
Disable Delayed Forward	Set the function code for canceling unanswered call transfer (default value is 93)
Paging Feature	Allow users to customize the Paging feature code. Default is Yes
Paging	Paging: Default is 74
DND Feature	Allow users to customize the CW feature codes. Default is Yes
Enable DND	Enable DND: Default is 78
Disable DND	Disable DND: Default is 79

Blind Transfer Feature	Allow users to customize the Blind Transfer feature code. Default is Yes
Enable Blind Transfer	Enable Blind Transfer: Default is 87
Disable LEC per call Feature	Whether to disable the LEC (Line Echo Cancellation) function of the current call (only the current call is prohibited)
Disable LEC per call	Set the function code to disable the LEC call function for the current call (default value is 03)
Play registration id Feature	Whether it is displayed as a registration ID
Enable playing registration id	Set to enable the function code to display the registration ID (default value is 98)
Disable Bellcore Style 3-Way Conference	Whether to set the function code for the three-party conference will only take effect after closing the Bellcore three-party conference
Star Code 3WC Feature	Allows users to initiate a three-way conference call by dialing a predefined star code
Star Code 3WC	Set the function code of the three-party conference (default value is 23)
Forced Codec Feature	Whether to enable the function of forcing the speech encoding type
Forced Codec	Sets the function code to enable forced voice coding type calls (default value is 02)
PCMU Codec Feature	Whether to force PCMU speech encoding
PCMU Codec	Sets the function code to enable forced PCMU voice encoding calls (default value is 7110)
PCMA Codec Feature	enables the PCMU codec for audio encoding and decoding in VoIP communications,
PCMA Codec	Set the function code to enable forced PCMA voice encoding (default value is 7111)
G723 Codec Feature	Whether to force G723 speech encoding
G723 Codec	Set the function code to enable forced G723 speech encoding (default value is 723)
G729 Codec Feature	Whether to force G729 speech encoding
G729 Codec	Set the function code to enable forced G729 speech encoding (default value is 729)
iLBC Codec Feature	Whether to force iLBC voice encoding
iLBC Codec	Set the function code to enable forced iLBC voice encoding (default value is 7201)
G722 Codec Feature	Whether to force G722 speech encoding
G722 Codec	Set the function code to enable forced G722 codec voice encoding (The default value is 722)
Ringtone	
Custom Ring Tone 1	Set the caller ID using custom ringtone 1
Custom Ring Tone 1 will be used when the caller is	If the caller number matches, a custom ringtone 1 will be used

Custom Ring Tone 2	Set the caller ID using custom ringtone 2
Custom Ring Tone 2 will be used when the caller is	If the caller number matches, a custom ringtone 2 will be used
Custom Ring Tone 3	Set the caller ID using custom ringtone 3
Custom Ring Tone 3 will be used when the caller is	If the caller number matches, a custom ringtone 3 will be used
Ring Tone 1-10	Define the Ringtone(s) frequencies, Syntax: c=on1/ off1[- on2/ off2[- on3/ off3]]; (melody on/off time must be a multiple of 1ms) Default value: c=2000/4000;
Call Waiting Tone 1-3	If the caller number matches, a custom call waiting tone will be used
Call Waiting Tone 1-3 used if incoming caller ID is	Set the incoming call number using custom call waiting tone
Call Waiting Tone 1-10	Defines the call waiting tone cadence **Syntax:** f1=val, f2=val[, c=on1/ off1[- on2/ off2[- on3/ off3]]]; (f is in Hz, on and off are calculated in 1ms. on is the ringing time , off is the silent time) Default value: f1=440@-13,c=300/10000;

FXO Profile 1 / FXO Profile 2

General Settings	
Account Registration	
Profile Active	Activates / Deactivates the accounts. The FXO port configuration will not change if disabled, although the port will not be operational, in this state, there will be no dial tone when picking up the analog phone and making/receiving calls will not be possible.
Primary SIP Server	Configures SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). This is the primary SIP server used to send/receive SIP messages from/to HT841/HT881.
Failover SIP Server	Defines failover SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6 fe80::20b:82ff:fe75:211d:). This server will be used if primary SIP server becomes unavailable.
Prefer Primary SIP Server	Selects to prefer primary SIP server. The account will register to primary Server if registration with Failover server expires. Default is No.
Outbound Proxy	Specifies IP address (Supports both IPv4 and IPv6 addresses) or domain name of outbound Proxy, or media gateway, or session border controller. (For example: proxy.myprovider.com, IPv4: 192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). It's Used by HT841/881 for firewall or NAT penetration in different network environments. If symmetric NAT is detected, STUN will not work and only outbound proxy can correct the problem
Backup Outbound Proxy	Configures the backup outbound proxy to be used when the "Outbound Proxy" registration fails. (For example: proxy.myprovider.com, or IP address, if any: IPv4: 192.168.5.170/ IPv6: fe80::20b:82ff:fe75:211d). By default, this field is left empty.
Prefer Primary Outbound Proxy	If the user configures this option to "Yes", when the registration expires, the device will re-register via primary

	outbound proxy. By default, this option is disabled.
From Domain	Allows users to add the actual domain name, it will override the from header.This is an optional configuration.
Network Settings	
Layer 3 QoS SIP DSCP	the Diff-Serv value for SIP packets in decimal, the range is 0-63, default value is 26
Layer 3 QoS RTP DSCP	Diff-Serv valuefor RTP packets in decimal, the range is 0-63, default value is 46
DNS Mode	Selects DNS mode to use for the client to look up server. One mode can be chosen. **A Record (Default):** resolves IP Address of target according to domain name. **SRV:** DNS SRV resource records indicate how to find services for various protocols. **NAPTR/SRV:** Naming Authority Pointer according to RFC 2915. **Use Configured IP:** If the SIP server is configured as domain name, device will not send DNS queries, but will use “Primary IP” or “Backup IP” to send SIP message if at least one of them is not empty. It will try to use “Primary IP” first, after 3 tries without any response, it will switch to “Backup IP 1”, then “Backup IP 2”, and then it will switch back to “Primary IP” after 3 retries.
DNS SRV Failover Mode	Configure the preferred IP mode when DNS Mode is SRV or NAPTR/SRV. • Default SIP request will always be sent to the address with the top priority based on the SRV query result, even if this address is different from the registered IP address. • Saved one until DNS TTL SIP request will always be sent to the registered IP address until DNS TTL expires or registered IP address is unreachable. • Saved on until no response SIP request will always be sent to the registered IP address only until registered IP address is unreachable. • Failback follows failback expiration time: the primary server regains control only after the failback expiration time, allowing the secondary server to handle requests until then.
Failback Timer	When the primary SBC is up, device will send SIP requests to the primary SBC. If at any point device fails over to the secondary SBC, the SIP requests will stay on the failover SBC for the duration of the failback timer. When the timer expires, device will send SIP requests to the primary SBC, (in minutes. Default is 60 minutes, max 45 days).
Maximum Number of SIP Request Retries	This feature allows user to configure the number of SIP retries before failover occurs. (between 1 and 10, default is 2).
Register Before DNS SRV Failover	This feature is used to control whether the device need to initiate a new registration request (following existing DNS SRV fail-over mode) first and then direct the non-registration SIP request (INVITE) to the new successfully registered server or not.
Primary IP	The main IP address used for communication and control.
Backup IP1	The secondary IP address used as a backup for communication in case the Primary IP fails.
Backup IP2	The third IP address used as an additional backup for communication in case both the Primary IP and Backup IP1 fail.
NAT Traversal	Indicates type of NAT for each account. This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, Keep-alive, STUN, UPnP. Default setting is No.
Use NAT IP	Defines NAT IP address used in SIP/SDP messages. It should only be used if required by ITSP.
Proxy-Require	Determines a SIP Extension to notify the SIP server that the HT841/HT881 is behind a NAT/Firewall.
SIP Settings	

SIP Basic Settings	
SIP Registration	Controls whether the HT841/HT881 needs to send REGISTER messages to the proxy server. The default setting is Yes.
SIP Transport	Selects transport protocol for SIP packets; UDP or TCP or TLS. Please make sure your SIP Server or network environment supports SIP over the selected transport method. Default is UDP.
Unregister On Reboot	Controls whether to clear SIP user's information by sending un-register request to the proxy server. The un-registration is performed by sending a REGISTER message with "Expires=0" parameter to the SIP server. This will unregister the SIP account under the concerned FXS page.Unregister on reboot option can be set to "No", "All" or "Instance". 1. **Set to "No":** If the "Unregister on reboot" option is set to "No", it means that the SIP user's information will not be cleared when the device reboots. In other words, the SIP account will remain registered with the server even after the device is rebooted. 2. **Set to "All":** If the "Unregister on reboot" option is set to "All", it means that all SIP accounts associated with the device will be unregistered when the device reboots. This option clears the SIP user's information for all the FXS ports on the device. 3. **Set to "Instance":** If the "Unregister on reboot" option is set to "Instance", it means that only the SIP account associated with the concerned FXS port will be unregistered when the device reboots. This option clears the SIP user's information for only the specific FXS port that is affected by the reboot. Default value is set to "No"
Outgoing Call without Registration	Enables the ability to place outgoing calls even if the account is not registered (if allowed by ITSP); device will not be able to receive incoming calls. Default is No.
Register Expiration	Refreshes registration periodically with specified SIP proxy (in minutes). Maximum interval is 65535 minutes (about 45 days). Default is 60 minutes (or 1 hour).
Reregister before Expiration	Sends re-register request after specific time (in seconds) to renew registration before the previous registration expires.
SIP Registration Failure Retry Wait Time	Sends re-register request after specific time (in seconds) when registration process fails. Maximum interval is 3600 seconds (1 hour). Default is 20 seconds.
SIP Registration Failure Retry Wait Time upon 403 Forbidden	Sends re-register request after specific time (in seconds) when registration process fails with error 403 Forbidden. Maximum interval is 3600 seconds (1 hour). Default is 1200 seconds.
Enable SIP OPTIONS/NOTIFY Keep Alive	Enables SIP OPTIONS or SIP NOTIFY to track account registration status so the ATA will send periodic OPTIONS/NOTIFY message to server to track the connection status with the server. Default setting is No.
SIP OPTIONS/NOTIFY Keep Alive Interval	Configures the time interval when the ATA send OPTIONS or NOTIFY message to SIP server. The default setting is 30 seconds, which means the ATA will send an OPTIONS/NOTIFY message to the server every 30 seconds. The default range is 1-64800.
SIP OPTIONS/NOTIFY Keep Alive Max Lost	Defines the Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3.
Local SIP Port	Defines local port to use by the HT841/HT881 for listening and transmitting SIP packets. Default value is 6060 **Note:** The formula of defining the FXO SIP ports is the following: SIP port = Profile's base SIP port + Port Id * 2, while the Port Id is defined as follows: FXS = 0, FXO1-8 = 1 – 8 for HT881 and FXO1-4 = 1 – 4 for HT841, in this case, if we set FXO profile 1 local SIP port to 6060, then FXO1 will use port 6062, FXO2 will use 6064, FXO3 will use 6066 and so on…
Local RTP Port	Defines the local RTP-RTCP port pair the HT841/HT881 will listen and transmit. It is the HT841/HT881 RTP port for channel 0.

	The default value for FXS port is 6004
Use Random SIP Port	Controls whether to use configured or random SIP ports. This is usually necessary when multiple HT841/HT881 are behind the same NAT. The default is No.
Use Random RTP Port	Controls whether to use configured or random RTP ports. This is usually necessary when multiple HT841/HT881 are behind the same NAT. The default is No.
RTP/RTCP Keep Alive On Hold	Enables or disables RTP/RTCP keep-alive packets during call hold to maintain connectivity and prevent session timeouts. Disabled by default.
Remove OBP from Route Header	Removes outbound proxy info in “Route” header when sending SIP packets. Default setting is No.
Support SIP Instance ID	Gives the users the possibility of making conference calls by pressing “Flash” key, when it’s enabled by dialing *23 +second callee number. Default is No
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	Controls the port information in the Via header and Contact header. If set to “No”, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. Default is No.
Tel URI	Indicates E.164 number in “From” header by adding “User=Phone” parameter or using “Tel:” in SIP packets, if the HT841/HT881 has an assigned PSTN Number. Disabled: Use “SIP User ID” information in the Request-Line and “From” header. User=Phone: “User=Phone” parameter will be attached to the Request-Line and “From” header in the SIP request to indicate the E.164 number. If set to “Enable”. Enabled: “Tel:” will be used instead of “sip:” in the SIP request. Please consult your carrier before changing this parameter. The default is Disabled.
Use Privacy Header	Determines if the “Privacy header” will be presented in the SIP INVITE message and if it includes the caller info in this header. If set to Default, it will add Privacy header unless special feature is Telkom SA or CBCOM. Default is Default.
Use P-Preferred-Identity Header	Specifies if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to “default”, the P-Preferred-Identity Header will be omitted in SIP INVITE message when Telkom SA or CBCOM is active. If set to “Yes”, the P-Preferred- Identity Header will always be presented. If set to “No”, it will be omitted. Default setting is: Default.
Use P-Access-Network-Info Header	With this feature enabled, device will populate the WAN access node with IEE-802.11a, IEE-802.11b in P-Access-Network-Info SIP header.
Use P-Emergency-Info Header	This feature support of IEEE-48-addr and IEEE-EUI-64 in SIP header for emergency calls.
Use P-Asserted-Identity Header	When this feature is set to Yes, device will send P-Asserted-Identity Header on the SIP Invite. Default setting is No.
SIP T1 Timeout	Defines T1 timeout value. It is an estimate of the round-trip time between the client and server transactions. For example, HT841/HT881 will attempt to send a request to a SIP server. The time it takes between sending out the request to the point of getting a response is the SIP T1 timer. If no response is received the timeout is increased to (2*T1) and then (4*T1). Request re-transmit retries would continue until a maximum amount of time is defined by T2. The default is 0.5 seconds.
SIP T2 Interval	Identifies maximum retransmission interval for non-INVITE requests and INVITE responses. Retransmitting

	and doubling of T1 continues until it reaches the T2 value. The default is 4 seconds.
SIP Timer D	Configures SIP Timer D defined in RFC3261. 0 – 64 seconds. Default is 0.
Do Not Escape '#' as %23 in SIP URI	Replaces # by %23 in some special situations. Default is No.
Disable Multiple m line in SDP	Sends only one m line in SDP, regardless of how many m fields are in the incoming SDP. Default is No.
Enable 100rel	Appends “100rel” attribute to the value of the required header of the initial signaling messages. Default is No.
Add Auth Header On Initial REGISTER	Adds “Authentication” header with blank “nonce” attribute in the initial SIP REGISTER request. Default is No.
Conference URI	Allows users to manually configure the conference URL. The default is null.
Allow SIP Factory Reset	Allows to reset the devices directly through SIP Notify. If “Allow SIP Factory Reset” is set to “YES” under FXO PORT, then the ATA receives the NOTIFY from the SIP server with Event: reset, the HT should perform a factory reset after the authentication. The authentication in this case can be either with: The admin password if no SIP account is configured on the HT. With the credentials of the SIP account if configured on the device.
SIP User-Agent	This feature allows users to configure SIP User Agent. If not configured, device will use the default User Agent header.
SIP User-Agent Postfix	Configures the SIP User-Agent Postfix
Add MAC in User-Agent	This feature allows users to configure "User-Agent" in the SIP header field, when this feature is set to“No”, "User-Agent" does not carry a MAC, when this feature is set “Yes except REGISTER”, "User-Agent" in REGISTERSIP header field does not carry MAC but other SIP packet header fields carries MAC, when this feature is set to “Yes to all SIP”, "User-Agent" in the SIP packet header field will carries the MAC.
Use MAC Header	This feature allows users to configure MAC Header in the SIP packet header field, when this feature is set to “No” ,the MAC header field is not carried in the SIP packet header field, when this feature is set to “REGISTER Only”, the register packet header field carries the MAC header field but the remaining SIP packets do not carry MAC header fields, when this feature is set to “Yes to all SIP”, the MAC header field is carried in the SIP data packet header field.
Session Timer	
Enable Session Timer	Disable the session timer when this option is set to “No”. By default, this option is enabled.
Session Expiration	Enables SIP sessions to be periodically “refreshed” via a SIP request (UPDATE, or re-INVITE). When the session interval expires, if there is no refresh via an UPDATE or re-INVITE message, the session will be terminated. Session Expiration is the time (in seconds) at which the session is considered timed out, if no successful session refresh transaction occurs beforehand. Valid range is 90-64800 seconds. Default is 180 seconds.
Min-SE	Defines Minimum session expiration (in seconds). Default is 90 seconds.
Caller Request Timer	Uses session timer when making outbound calls if remote party supports it. Valid range is 90-64800 seconds. Default is No.
Callee Request Timer	Uses session timer when receiving inbound calls with session timer request. Default is No.

Force Timer	Uses session timer even if the remote party does not support this feature. Selecting "No" will enable session timer only when the remote party supports it. To turn off Session Timer, select "No" for Caller and Callee Request Timer, and Force Timer. Default is No
UAC Specify Refresher	Specifies which end will act as refresher for outgoing calls. Default is Omit. **UAC:** The device acts as the refresher. **UAS:** Callee or proxy server act as the refresher.
UAS Specify Refresher	Specifies which end will act as refresher for incoming calls. Default is Omit.: **UAS:** The device acts as the refresher. **UAC:** Callee or proxy server act as the refresher.
Force INVITE	Uses INVITE message to refresh the session timer. Default is No.
When To Restart Session After Re-INVITE received	Allows users to delay posting Media Change Event, it can be set to "Immediately" or to "After replying 200OK" The default value is "Immediately".
INVITE Ring-No-Answer Timeout (sec)	Sets the duration in seconds before considering an INVITE request unanswered Range is 5-300 seconds. Default 40 seconds
Security Settings	
Validate Incoming SIP Message	Checks the authenticity and integrity of incoming SIP messages for enhanced security.
Check SIP User ID for incoming INVITE	Checks the SIP User ID in the Request URI of the incoming INVITE; if it doesn't match the HT841/HT881 SIP User ID, the call will be rejected. Direct IP calling will also be disabled. The default is No.
Authenticate incoming INVITE	Challenges the incoming INVITE for authentication with SIP 401 Unauthorized message. Default is No.
Allow Incoming SIP Messages from SIP Proxy Only	Checks SIP address of the Request URI in the incoming SIP message; if it doesn't match the SIP server address of the account, the call will be rejected. Default is No.
Authenticate server certificate domain	Configures whether to validate the domain certificate when download the firmware/config file. If it is set to "Yes", the phone will download the firmware/config file only from the legitimate server. The default setting is "No".
Trusted domain name list	Supports setting specific domain names and wildcard domain names, wildcard domain names such as "*.grandstream.com", use "," to separate domain names
Authenticate server certificate chain	Verifies certificate when communication method is TCP/TLS
Codec Settings	
DTMF Settings	
Preferred DTMF method	Sorts DTMF methods (in-audio, via RTP (RFC2833) or via SIP INFO) by priority.
Inband DTMF Duration	Allows users to config the Inband DTMF Duration and inter-duration. The default Duration is 100 ms. Valid range: 40-2000 ms. The default Inter-duration is 50 ms. Valid range: 40-2000 ms.
DTMF Payload Type	Defines payload type for DTMF using RFC2833.

Inband DTMF Tx Gain	Adjusts the transmit gain for inband Dual-Tone Multi-Frequency (DTMF) tones during call signaling. The Valid range is -12-12 db, default is 0
DSP DTMF Detector Duration Threshold	Allows users to config the DSP DTMF Detector Duration Threshold. The default Duration is 30 ms. Valid range: 20-2000 ms. The default Inter-duration is 30 ms. Valid range: 20-2000 ms.
DSP DTMF Detector Min Level	Determines the minimum level of DTMF tones that the DSP DTMF detector can reliably detect, range is -45-0 dBm, default is -25
DSP DTMF Detector Snr	Sets the signal-to-noise ratio threshold for the DSP DTMF detector, determining the sensitivity to distinguish DTMF tones from background noise in the audio signal. Range: 0-12, default is 1
DSP DTMF Detector Deviation	Specifies the allowed frequency deviation from standard DTMF tones that the DSP DTMF detector can accommodate. Range: 0-25, default is 25
DSP DTMF Detector Twist	Defines the maximum deviation from ideal tone frequencies allowed for reliable DTMF detection by the DSP. Range: 0-12dB, default is 5
Disable DTMF Negotiation	Uses DTMF order without negotiation. Default is No.
RFC2833 Events Count	This feature allows users to customize the count of RFC2833 events. Default is 8.
RFC2833 End Events Count	This feature allows users to customize the count of RFC2833 end events. Default is 3.
Preferred Vocoder	
Preferred Vocoder(in listed order)	Configures vocoders in a preference list (up to 8 preferred vocoders) that will be included with same order in SDP message. Vocoder types are G.711 A-/U-law, G.726-32, G.723, G.729, iLBC and OPUS
Voice Frames per TX	Transmits a specific number of voice frames per packet. Default is 2; increases to 10/20/32/64 for G711/G726/G723/other codecs respectively.
G723 Rate	Operates at specified encoding rate for G.723 vocoder. Available encoding rates are 6.3kbps or 5.3kbps. Default is 6.3kbps.
iLBC Frame Size	Specifies iLBC packet frame size (20ms or 30ms). Default is 20ms.
Disable OPUS Stereo in SDP	Disables OPUS stereo in SDP. Default is No.
iLBC Payload Type	Determines payload type for iLBC. Valid range is between 96 and 127. Default is 97.
OPUS Payload Type	Determines payload type for OPUS. Valid range is between 96 and 127. Default is 123.
Enable Audio RED with FEC	Enables the use of audio redundancy (RED) with forward error correction (FEC) to enhance audio quality and resilience against packet loss in real-time communication systems such as VoIP
Audio FEC Payload Type	Specifies the payload type used for transmitting audio forward error correction (FEC) packets in a VoIP system.
Audio RED Payload Type	Defines the payload type assigned to audio redundancy (RED) packets in a VoIP system.
VAD	Allows detecting the absence of audio and conserves bandwidth by preventing the transmission of “silent packets” over the network.

	Default is No.
Use First Matching Vocoder in 200OK SDP	Includes only the first matching vocoder in its 200OK response, otherwise it will include all matching vocoders in same order received in INVITE. Default is No.
Symmetric RTP	Changes the destination to send RTP packets to the source IP address and port of the inbound RTP packet last received by the device. Default is No.
Enable RTCP	Allows users to enable RTCP. The default setting is “Yes”.
Fax Mode	Specifies the fax mode: T.38 (Auto Detect) FoIP by default, or Pass-Through. If using Pass-through mode, select preference codec as PCMU or PCMA.
Re-INVITE After Fax Tone Detected	Permits the unit to send out the re-INVITE for T.38 or Fax Pass Through if a fax tone is detected. Default is Enabled
Jitter Buffer Type	Selects jitter buffer type (Fixed or Adaptive) based on network conditions.
Jitter Buffer Length	High (initial 200ms, min 40ms, max 600ms) **Note:** not all vocoders can meet the high requirement. Medium (initial 100ms, min 20ms, max 200ms). Low (initial 50ms, min 10ms, max 100ms).
SRTP Mode	Selects SRTP mode to use (“Disabled”, “Enabled but not forced”, or “Enabled and forced”). Default is Disabled It uses SDP Security Description to exchange key. Please refer to SDES: https://tools.ietf.org/html/rfc4568 SRTP: https://www.ietf.org/rfc/rfc3711.txt
SRTP Key Length	Allows users to select supported SRTP Key Length.
Crypto Life Time	Adds crypto life time header to SRTP packets. Default is Yes.
Analog signal line configuration	
Caller ID Scheme	Selects the caller id scheme, for example: Bellcore/Telcordia, ETSI-FSK …
Pulse Dialing Standard	Allows users to use Swedish pulse dialing standard or New Zealand pulse dialing standard. Default is General Standard.
Hook Flash Timing	Defines the time period when the cradle is pressed (Hook Flash) to simulate FLASH. To prevent unwanted activation of the Flash/Hold and automatic phone ring-back, adjust this time value. HT841/HT881 support a range from 40 to 2000 ms. Default values are 300 minimum and 1100 maximum.
Gain	Adjusts the voice path volume. • Rx is a gain level for signals transmitted by FXS • Tx is a gain level for signals received by FXS. Default = 0dB for both parameters. Loudest volume: +6dB Lowest volume: -6dB. User can adjust volume of call using the Rx gain level parameter and the Tx gain level parameter located on the FXS port configuration page. If call volume is too low when using the FXS port (ie. the ATA is at user site), adjust volume using the Rx gain level parameter under the FXS port configuration page. If voice volume is too low at the other end, user may increase the far end volume using the Tx gain level parameter under the FXS port configuration PAGE.

Disable Line Echo Canceller (LEC)	Disables the LEC per call base. Recommended for Fax/Data calls. Default is No.
Ring Frequency	Customizes ring frequency. Valid options: 20Hz – 25Hz. Default is 20Hz.
FSK Caller ID Minimum RX Level (dB)	Sets the minimum signal level required to detect and receive FSK Caller ID information accurately. The valid range is -96 - 0dB. Default -40dB
FSK Caller ID Seizure Bits	Represents the number of bits used to detect the start of a Caller ID transmission. The valid range is 0 - 800 bits. Default 70
FSK Caller ID Mark Bits	Represents the number of bits used to identify the caller's mark frequency during Caller ID transmission. The Valid range is 1 - 800 bits. Default 40
Caller ID Transport Type	Refers to the method used to transmit Caller ID information, which can be: ● **Relay via SIP Form:** Caller ID information is transmitted using the "From" field in the SIP header. ● **Relay via P-SIP Asserted identity:** Caller ID information is transmitted using the "P-Asserted-Identity" header in the SIP message. ● **Relay via P-SIP Preferred identity:** Caller ID information is transmitted using the "P-Preferred-Identity" header in the SIP message. ● **Send Anonymous:** Caller ID information is transmitted using the "P-Asserted-Identity" header in the SIP message. ● **Disable:** Caller ID information is transmitted using the "P-Asserted-Identity" header in the SIP message. Set to **Relay via SIP Form** by Default.
Send Hook Flash To PSTN	Refers to the capability of sending a signal to the Public Switched Telephone Network (PSTN) to simulate a hook flash during a call, typically used to access certain telephony features or services.
Hook Flash Duration (ms)	Refers to the time duration, measured in milliseconds, for which the hook flash signal is transmitted to the Public Switched Telephone Network (PSTN) during a call, typically used to trigger specific telephony features or services.
Call Settings	
Auto Send DTMF Upon Call Start	Enables the option to automatically sends DTMF tones when a call starts.
Early Dial	Sends an early INVITE each time a key is pressed when a user dials a number. Otherwise, only one INVITE is sent after full number is dialed (user presses Dial Key or after “no key entry timeout” expires). This option should be used only if there is a SIP proxy is configured and supporting “484 Incomplete Address” responses. Otherwise, the call will likely be rejected by the proxy (with a 404 Not Found error). Default is No. This feature is NOT designed to work with and should NOT be enabled for direct IP-to-IP calling.
Dial Plan Prefix	Adds specified prefix to dialed number.
Dial Plan	Dial Plan Rules: 1. Accept Digits: 1,2,3,4,5,6,7,8,9,0 , *, #, A,a,B,b,C,c,D,d 2. Grammar: x – any digit from 0-9; a. xx+ – at least 2 digits number; b. xx – exactly 2 digits number; c. ^ – exclude; d. . – wildcard, matches one or more characters e. [3-5] – any digit of 3, 4, or 5; f. [147] – any digit 1, 4, or 7; g. <2=011> – replace digit 2 with 011 when dialing h. <=1> – add a leading 1 to all numbers dialed, vice versa will remove a 1 from the number dialed i. | – or j. Flag T when adding a “T” at the end of the dial plan, the phone will wait for 3 seconds before dialing out. This gives users more flexibility on their dial plan setup. E.g. with dial plan 1XXT, phone will wait for 3 seconds to let

	user dial more than just 3 digits if needed. Originally the phone will dial out immediately after dialing the third digit. Example 1: {[369]11 | 1617xxxxxxx} – Allow 311, 611, 911, and any 10-digit numbers of leading digits 1617 Example 2: {^1900x+ | <=1617>xxxxxxx} – Block any number with leading digits 1900 and add prefix 1617 for any dialed 7-digit numbers Example 3: {1xxx[2-9]xxxxxx | <2=011>x+} – Allow any length of number with leading digit 2 and 10 digit-numbers of leading digit 1 and leading exchange number between 2 and 9; If leading digit is 2, replace leading digit 2 with 011 before dialing. 1. Default: Outgoing – { x+ | +x+ | *x+ | *xx*x+ } 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 dialing 7 numbers and 1617 area code will be added automatically 1[2-9]xx[2-9]xxxxxx – allows dialing to any US/Canada Number with 11 digits length 011[2-9]x. – allows international calls starting with 011 [3469]11 – allow dialing special and emergency numbers 311, 411, 611 and 911 Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider. In this case * should be predefined inside dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.
Use # as Dial Key	Treats "#" as the "Send" (or "Dial") key. If set to "No", this "#" key can be included as part of the dialed number. Default is Yes.
Disable # as Redial Key	Disables # to act as Redial key. If set to "Yes" and feature "Use # as Dial Key" set to Yes, the # key will act as dial key but not as redial key. Default is No.
Disable Reminder Ring for DND	This feature allows user to disable reminder ring when FXS port is on DND mode. Default is Yes.
MWI Tone	When set to Default, device will play Stutter Dial Tone when there is voicemail, if set to Special Proceed Indication Tone, device will play the configured special proceed indication tone upon user offhook when there is voicemail
Flash Digit Control	When it set to YES it allows the user to perform some call setting when both channels are used while pressing: **"Flash + 1"** in order to hang up the current call and resume a call that was held. **"Flash + 2"** in order to hold the current call and resume a call that was held. **"Flash + 3"** in order to perform 3-way conference. **"Flash + 4"** in order to perform attended transfer. **Note:** Please refer to the user guide for detailed steps to perform above operations.More additional Digit events were added on the new firmware 1.0.43.10.
Callee Flash to 3WC	When this feature is set to Yes, device would be able to set up the 3-way conference call even when device is the callee in the second call. Default is No.
Hunting Group Type	Specifies the group ringing type, the avilable options are: Linear or Circular
Anonymous Call Rejection	Rejects incoming calls with anonymous caller ID with "486 Busy here" message. Default is No.
Special Feature	Selects Soft switch vendors' special requirements Examples of vendors: BroadSoft, CBCOM, RNK, Huawei, China Mobile, ZTE IMS, PhonePower, TELKOM SA, Vonage, Metaswitch, CenturyLink, MTS, Oi_BR, Telefonica, GIBTELECOM. The default is Standard.
Disable Unknown Caller ID	Disable analog phone's caller ID when receiving a call with "Anonymous", "unavailable" or "unknown" in FROM header and without "Display info". **Note:** This relies also on analog phone's design, some phones will still display "unknown" with this feature enabled. Default is No.
Replace Beginning '+' with 00 in Caller ID	When this feature is set to Yes, device will replace the "+" sign at the beginning of a number in the FROM header. Default is No.

Outgoing Call Duration Limit	Defines the call duration limit for the outgoing calls. Default is 0 (No limit).
Incoming Call Duration Limit	Defines the call duration limit for the incoming calls. Default is 0 (No limit).
FXO Termination	
Enable Current Disconnect	This value should be used in case the PSTN provider uses line power drop to indicate call completion to the end point. In this case the HT841/HT881 will search for a power drop.
Current Disconnect Threshold (ms)	This is a preconfigured value of duration for a line power drop used by specific service providers. For example, for a configured value of 500ms the device will ignore any random voltage drops on the line if duration of such drop is less than 500ms and the call will NOT be considered as terminated. This is useful to prevent unnecessary call drops in some low quality PSTN lines. Default is 100 ms. Range from 50 to 800 ms.
Enable PSTN Disconnect Tone Detection	If set to Yes, arrived Busy Tone is used as the disconnect signal. Default is "No"
Enable Polarity Reversal	This should be set to Yes only if the FXO lines are subscribed to PR service from PSTN Service provider. It is merely a PR detect feature. Default is No. **Note:** If there is no PR service from provider on the FXO line, and this setting is configured to Yes, calls will not be successful.
Polarity On Answer Delay	Determines the delay in milliseconds before polarity reversal signaling is initiated upon answering an FXO call. Range 200-30000 milliseconds. Default value 1000 milliseconds
AC Termination Model	You can select the AC termination by Country or by Impedance. Default is Country-based.
Country-based	Selects the impedance used by the PSTN service provider 15 Countries are selectable in this version of the F/W. **USA** **AUSTRIA** **AUSTRALIA/NEW ZEALAND** **BELGIUM** **CHINA** **FINLAND** **FRANCE** **GERMANY** **GREECE** **ITALY** **JAPAN** **NORWAY** **SPAIN** **SWEDEN** **UK** Default is USA
Impedance-based	Select the Impedance used by the PSTN service provider. **600R – 600 ohms** **600C – 600 ohms + 2.16uF** **900R – 900 ohms** **900C – 900 ohms + 2.16uF** **COMPLEX1 – 220 ohms + (820 ohms || 115nF)** **COMPLEX2 – 270 ohms + (750 ohms || 150nF)** **COMPLEX3 – 370 ohms + (620 ohms || 310nF)** **COMPLEX4 – 600R, 270 ohms + (750 ohms || 150nF)** **COMPLEX5 – 320 ohms + (1050 ohms || 230nF)** **COMPLEX6 – 350 ohms + (1000 ohms || 210nF)** **COMPLEX7 – 200 ohms + (680 ohms || 100nF)** **COMPLEX8 – 370 ohms + (820 ohms || 110nF)** **COMPLEX9 – 275 ohms + (780 ohms || 115nF)**

	COMPLEX10 – 120 ohms + (820 ohms || 110nF) Default is 600R – 600 ohms
Number of Rings	The FXO port will ring the number of times configured in this field before sending the call to the VoIP side. The supported range is 1-50. Default is 4.
PSTN Ring Thru FXS	If set to yes, all incoming PSTN calls will ring the FXS port after the Ring Thru Delay timer is reached.
PSTN Ring Thru Delay (sec)	If the PSTN Ring Thru Delay is set to Yes, all incoming PSTN calls through FXO will ring the phone connected to the FXO port, after this delay or after caller id is detected (whichever comes first).
PSTN Ring Timeout (sec)	Range is 2-10 seconds. Default is 6 seconds. Option is used to detect PSTN hang up when FXO port is not answered.
PSTN Idle Wait Timeout between Outgoing Calls	Used to customize timeout value between PSTN outgoing calls. Range is 0-10 seconds. Default is 4 seconds.
PIN for VoIP-to-PSTN Calls	Requires users to enter a Personal Identification Number (PIN) before making calls from VoIP to the traditional Public Switched Telephone Network (PSTN) to enhance security and prevent unauthorized usage.
PIN for PSTN-to-VoIP Calls	Requires users to enter a Personal Identification Number (PIN) before initiating calls from the traditional Public Switched Telephone Network (PSTN) to the VoIP network, ensuring secure access and preventing unauthorized usage.
Enable Early Media for VoIP-to-PSTN Calls	Only for calls without 2 stage dialing but with polarity reversal enabled. Default No
Chaneel Dialing	
DTMF Digit Length (ms)	Digit length and Dial Pause are port digit dialing configurations; FXO needs to dial out digits for VoIP to PSTN 1 stage calls, and unconditional call forward to PSTN, and route to PSTN. Digit Length is the play time for each digit. Note: In order to receive the caller ID information, the delay should be set to a value larger than the delay required to complete the PSTN caller ID delivery.
DTMF Dial Pause (ms)	Dial pause is the time between 2 digits for the same scenario as explained above.
First Digit Timeout (sec)	Used for PSTN to VoIP calls. PSTN users need to enter the FIRST digit within the first digit timeout period. Otherwise the call will be dropped. Range 1-20 seconds. Default 10 seconds
Inter-Digit Timeout (sec)	Sets the time in seconds before the gateway considers a sequence of dialed digits complete. 1-15 seconds. Default 4 seconds
Wait for Dial-Tone	Determines whether the FXO gateway waits for a dial tone before initiating dialing. Disabled by default.
Stage Method (1/2)	This configuration is applicable for VoIP to PSTN calls and indicates one or two stage dialing methods.
Min Delay Before Dial PSTN Number	The time to wait before HT841/HT881 initiates the call via PSTN line. Default 500ms, range is from 50 to 65000ms.

FXS Port

FXS Port	Displays the specifc port number. **Note:** The HT8x1 supports only one FXS port

SIP User ID	Defines user account information provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Authenticate ID	Determines account authenticate ID provided by VoIP service provider (ITSP). Can be identical to or different from “SIP user ID”.
Authenticate Password	Specifies account password provided by VoIP service provider (ITSP) to register to SIP servers.
Name	Chooses a name to be associated to user.
Profile ID	Defines the profile ID for each port.
Enable Port	Enables / Disables the port
Offhook Auto-Dial	Configures a User ID or extension number that is automatically dialed when off-hook. Only the user part of a SIP address needs is entered here. The HT841/HT881 will automatically append the “@” and the host portion of the corresponding SIP address.

FXO Ports

FXO PORTS	Displays the specifc port number. **Note:** HT841 supports 4 FXO ports, HT881 supports 8 FXO ports.
SIP User ID	Defines user account information provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
Authenticate ID	Determines account authenticate ID provided by VoIP service provider (ITSP). Can be identical to or different from “SIP user ID”.
Authenticate Password	Specifies account password provided by VoIP service provider (ITSP) to register to SIP servers.
Name	Chooses a name to be associated to user.
Profile ID	Defines the profile ID for each port, FXO Profile 1 or 2.
Hunting Group	This option allows incoming calls to be distributed across multiple FXO ports based on availability, ensuring efficient call handling and avoiding busy signals. The available options are: ● Disabled ● Active: If the port is busy, this will go through all the other FXO ports other than the one used, in a serial manner. ● 1 | 2 | 3 | 4 : refering to the port number where the call will be routed if the current port is busy
Request URI Routing ID	This option helps to route incoming calls to specific destinations based on the information contained in the request Uniform Resource Identifier (URI),
Enable Port	Enables/Disables the port
Unconditional Call Forward to PSTN	Enables all incoming calls from the VoIP network to be automatically forwarded to the traditional Public Switched Telephone Network (PSTN) without any conditions or restrictions. You can Configure Unconditional Call Forward to PSTN on four or eight FXO ports depending on the device model.
Unconditional Call Forward to VOIP	allows all incoming calls from the traditional Public Switched Telephone Network (PSTN) to be automatically forwarded to a VoIP network without any conditions or restrictions. You can configure Unconditional Call Forward to VoIP on four or eight FXO ports depending on the device

	model. Please configure the following parameters for each port: • **CID:** Shows the caller ID of the destination where the call will be forwarded. • **Sip Server:** Displays the SIP Server • **Sip Destination Port:** Displays the destination port

IMPORTANT WEB CONFIGURATIONS

The HT841/HT881 embedded Web server responds to HTTP/HTTPS GET/POST requests. Embedded HTML pages allow a user to configure the HT841/HT881 through a web browser such as Google Chrome, Mozilla Firefox and Microsoft's IE.

- **Microsoft Internet Explorer:** version 10 or higher.
- **Google Chrome**: version 58.0.3 or higher.
- **Mozilla Firefox**: version 53.0.2 or higher.
- **Safari**: version 5.1.4 or higher.
- **Opera**: version 44.0.2 or higher.

Web UI Access Level Management

There are three default passwords for the login page:

User Level	Password	Web Pages Allowed
Administrator Level	admin password is found on a sticker on the back of the unit	All pages.
End User Level	123	Only Status and Basic Settings
Viewer Level	viewer	Only checking. Not allowed to modify content.

HT841/HT881 Access Level Types

> **Note**
>
> The password is case sensitive with maximum length of 30 characters. When changing any settings, always submit them by pressing **Update or Apply** button on the bottom of the page. After submitting the changes in all the Web GUI pages, if a reboot is required, the web page will prompt the user to reboot by offering a reboot button on the web page.

Saving the Configuration Changes

After users make changes to the configuration, pressing **Update** button will save but not apply the changes until **Apply** button is clicked. Users can instead directly press **Apply** button. When a reboot is required to apply changes, the web page will prompt the user to reboot by offering a reboot button on the web page.

Changing Admin Level Password

1. Access your HT841/HT881 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: The password found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and enter the new admin password. (Must contain 4-30 characters, Purposely not displayed for security protection.)

5. Confirm the new admin password.
6. Press **Apply** at the bottom of the page to save your new settings.

HT841/HT881 Admin Password change

Note

After first time log in attempt, the user will be forced to change his initial admin password.

Changing User Level Password

1. Access your HT841/HT881 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: The password found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and **e**nter the new end-user password. (Must contain 4-30 characters, Purposely not displayed for security protection.)
5. Confirm the new end-user password.
6. Press **Apply** at the bottom of the page to save your new settings.

HT841/HT881 User Password change

Note

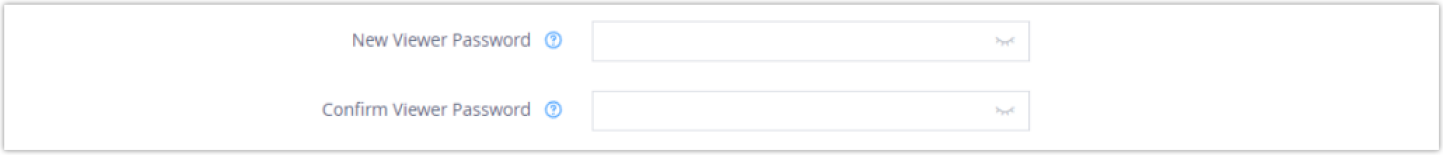
After first time log in attempt, the user will be forced to change his initial user level password defined by the administrator.

Note

For the viewer level access to work, make sure to set “Disable User Level Web Access” to “No”, under System Settings => Security Settings => Web/SSH Access

Changing Viewer Password

1. Access your HT841/HT881 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: The password found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and **e**nter the new viewer password. (Must contain 4-30 characters. Purposely not displayed for security protection.)
5. Confirm the new viewer password.
6. Press **Save and Apply** at the bottom of the page to save your new settings.



Note

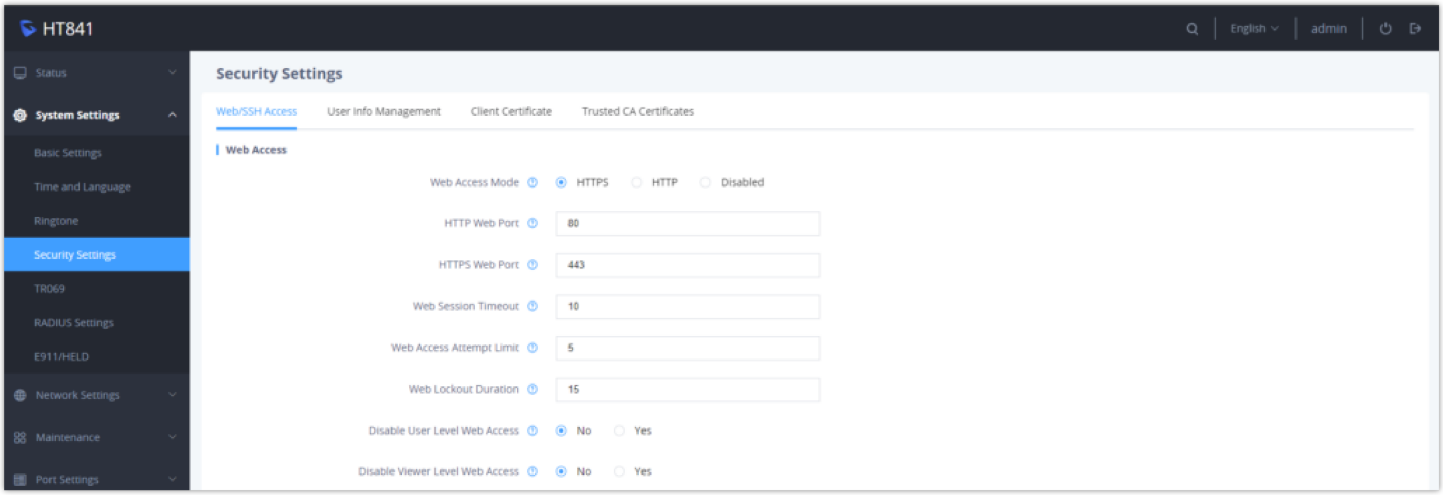
After first time log in attempt, the user will be forced to change his initial viewer password that was defined by the administrator.

Note

For the viewer level access to work, make sure to set “Disable Viewer Level Web Access” to “No”, under System Settings => Security Settings => Web/SSH Access

Changing HTTP/HTTPS Web Port

1. Access your HT841/HT881 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: The password found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **Basic Settings → HTTP(S) Web Port**.
5. Make sure that the **Web Access Mode** is set to **HTTP(S)**.
6. Change the current port to your new HTTP(S) port. Ports accepted are in range [1-65535].
7. Press **Apply** at the bottom of the page to save your new settings



Configuring HT841/HT881 Through Voice Prompts

As mentioned previously, The HT841/HT881 has a built-in voice prompt menu for simple device configuration. Please refer to “Understanding HT841/HT881 Interactive Voice Prompt Response Menu” for more information about IVR and how to access its menu.

- **DHCP MODE**

Select voice menu option 01 to allow the HT841/HT881 to use DHCP.

- **STATIC IP MODE**

Select voice menu option 01 to allow the HT841/HT881 to enable the STATIC IP mode, then use option 02, 03, 04, 05 to set up IP address, Subnet Mask, Gateway and DNS server respectively.

- **PPPOE MODE**

Select voice menu option 01 to allow the HT841/HT881 to enable the PPPoE mode. PPPoE Username and Password should be configured from web GUI.

- **FIRMWARE SERVER IP ADDRESS**

Select voice menu option 13 to configure the IP address of the firmware server.

- **CONFIGURATION SERVER IP ADDRESS**

Select voice menu option 14 to configure the IP address of the configuration server.

- **UPGRADE PROTOCOL**

Select the menu option 15 to choose firmware and configuration upgrade protocol between TFTP, FTP, FTPS, HTTP and HTTPS. Default is HTTPS.

- **FIRMWARE UPGRADE MODE**

Select voice menu option 17 to choose firmware upgrade mode among the following three options:

"Always check, check when pre/suffix changes, and never upgrade".

- **WAN PORT WEB ACCESS**

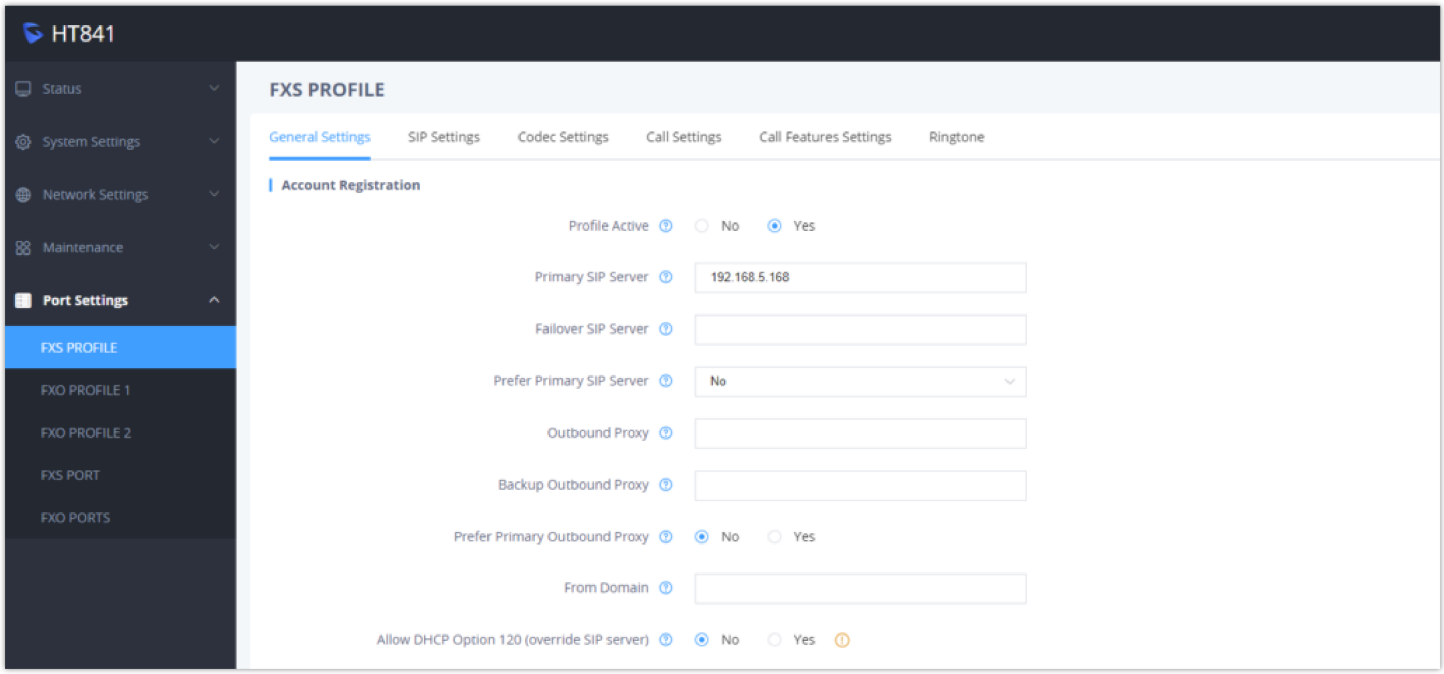
Select voice menu option 12 to enable/disable web access from WAN port. Press 9 in this menu to toggle between enable / disable.

Register a SIP Account

The HT841 supports 1 SIP account for FXS port, and 4 accounts for FXO ports, While the HT881 supports 1 SIP account for FXS port, and 8 accounts for FXO ports.

Please refer to the following steps in order to register your accounts via web user interface.

- Access your HT841/HT881 web UI by entering its IP address in your favorite browser.
- Enter your admin password (default: found on the sticker on the back of the unit).
- Press **Login** to access your settings.
- Go to **FXS Profile** (same steps for **FXO Profile 1&2**) web pages and set the following:
  1. **Account Active** to **Yes.**
  2. **Primary SIP Server** field with your SIP server IP address or FQDN.
  3. **Failover SIP Server** with your Failover SIP Server IP address or FQDN. Leave empty if not available.
  4. **Prefer Primary SIP Server** to **No** or **Yes** depending on your configuration. Set to **No** if no Failover SIP Server is defined. If "**Yes"**, account will register to Primary SIP Server when failover registration expires.
  5. **Outbound Proxy:** Set your Outbound Proxy IP Address or FQDN. Leave empty if not available.

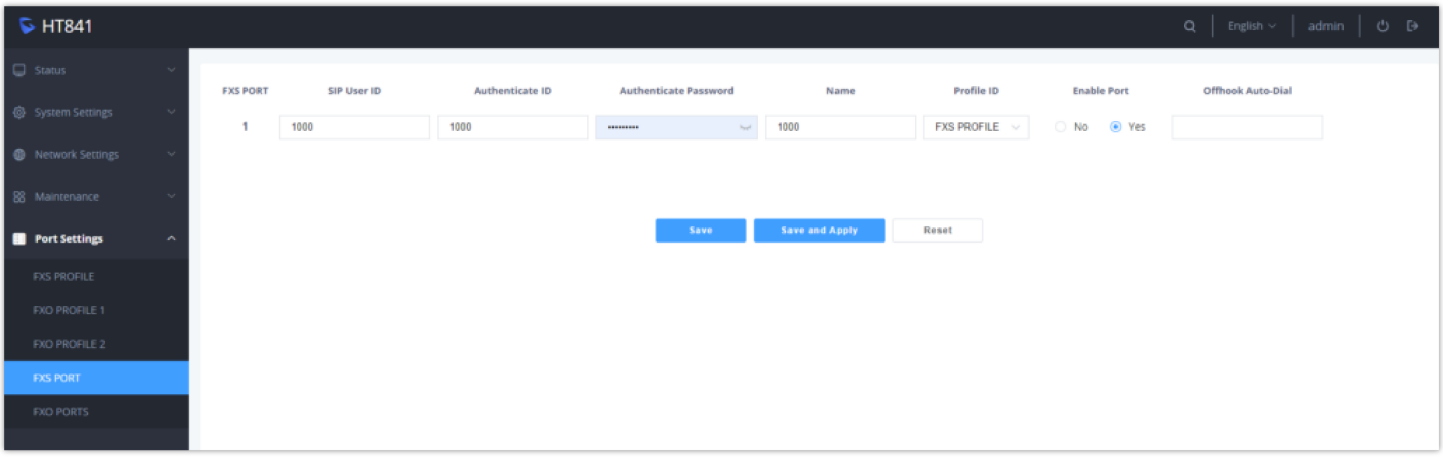


Configure SIP Server

- Go to **FXS Port** web page and set the following

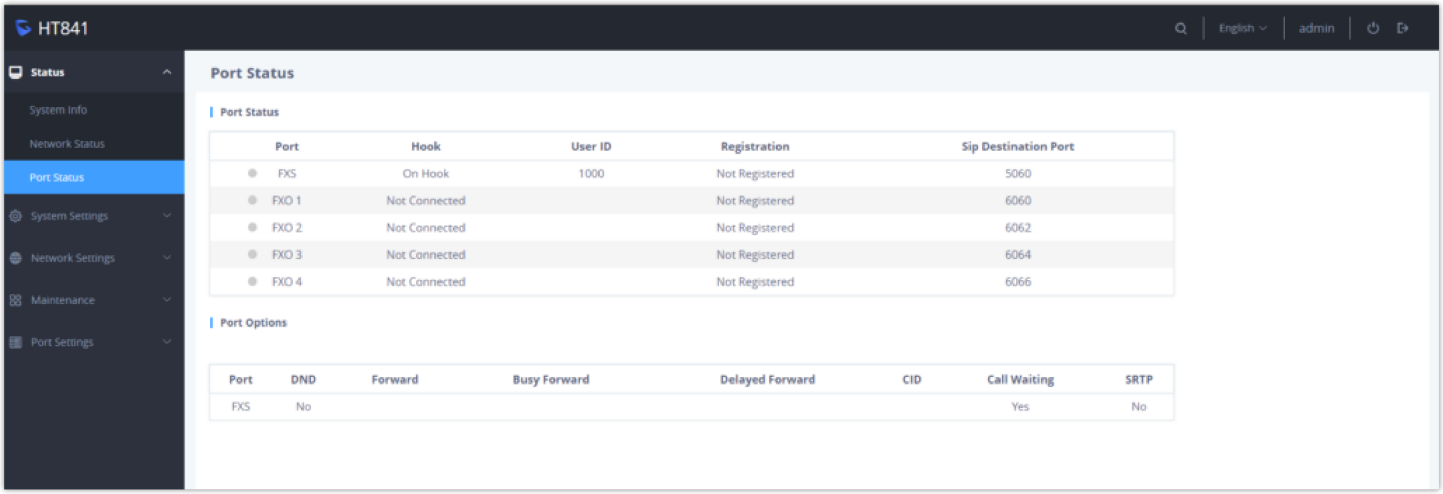
1. **SIP User ID**: Under **Ports** Web Page , Enter the SIP User ID User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
2. **Authenticate ID**: SIP service subscriber's Authenticate ID used for authentication. Can be identical to or different from SIP User ID.
3. **Authenticate Password**: SIP service subscriber's account password to register to SIP server of ITSP. For security reasons, the password will field will be shown as empty.
4. **Name**: Any name to identify this specific user.

- Press **Apply** at the bottom of the page to save your configuration.



Register SIP Account

After applying your configuration, your account will register to your SIP Server, you can verify if it has been correctly registered with your SIP server from your HT841/HT881 web interface under **Status → Port Status → Registration** (If it displays **Registered**, it means that your account is fully registered, otherwise it will display **Not Registered** so in this case you must double check the settings or contact your provider).



Account Registered

Rebooting HT841/HT881 from Remote

Press the "Reboot" button at the bottom of the configuration menu to reboot the FXO Gateway remotely. The web browser will then display a message window to confirm that reboot is underway. Wait 30 seconds to log in again.

UPGRADING AND PROVISIONING

The HT841/HT881 can be upgraded via FTP/FTPS/TFTP/HTTP/HTTPS by configuring the URL/IP Address for the FTP/FTPS/TFTP/HTTP/HTTPS server and selecting a download method. Configure a valid URL for TFTP or FTP/FTPS or HTTP/HTTPS (default is HTTPS); the server name can be FQDN or IP address.

Examples of valid URLs:

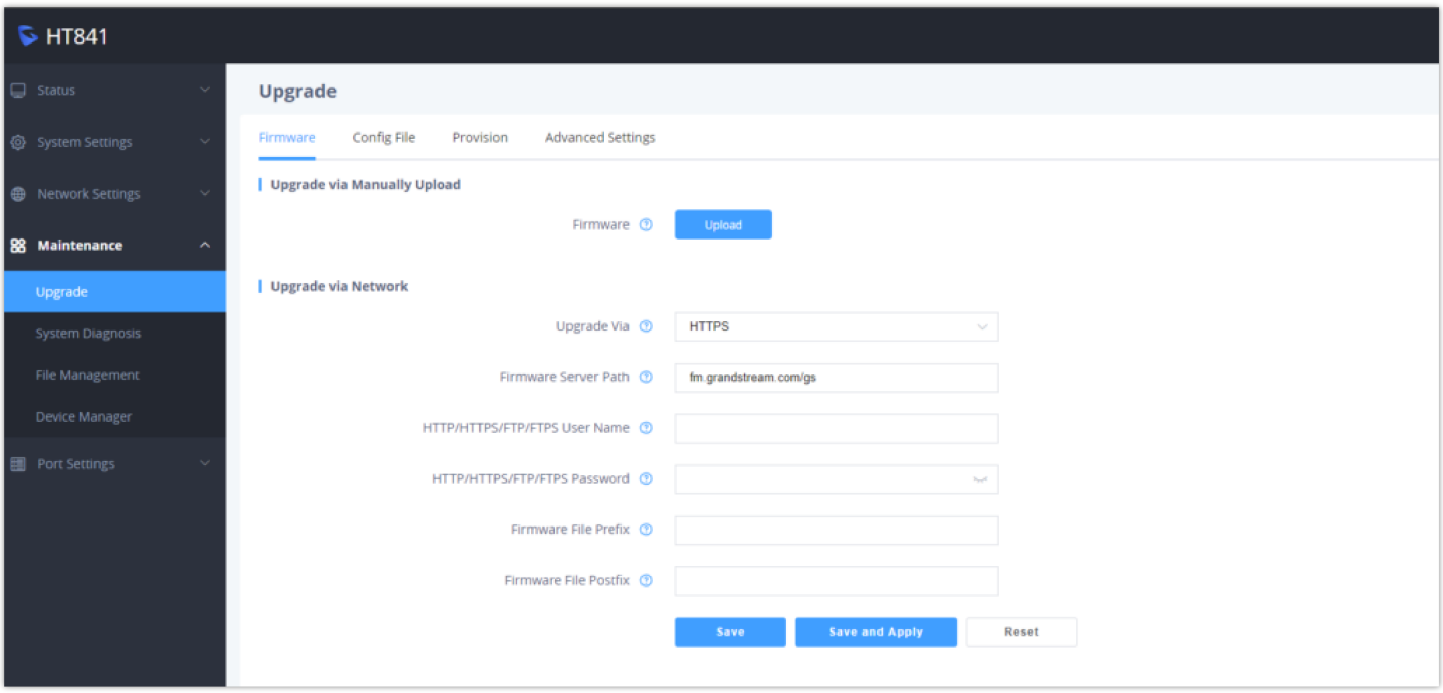
firmware.grandstream.com

fw.ipvideotalk.com/gs

Firmware Upgrade procedure

Please follow below steps in order to upgrade the firmware version of your HT841/HT881:

1. Access your HT881/HT841 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: Found on a sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **Maintenance → Upgrade → Firmware** page, and enter the IP address or the FQDN for the upgrade server in "**Firmware Server Path**" field and choose to upgrade via **TFTP , FTP/FTPS or HTTP/HTTPS**.
5. Make sure to check "**Always Check for New Firmware**".
6. Update the change by clicking the " **Apply**" button at the bottom of the page. Then "**Reboot**" or power cycle the HT841/HT881 to update the new firmware.



Firmware Upgrade Page

Upgrading via Local Directory

1. Download the firmware file from Grandstream web site
2. Unzip it and copy the file in to a folder in your PC
3. From the HT841/HT881 web interface (Advanced Settings page) you can browse your hard drive and select the folder you previously saved the file.
4. Click "Upload" and wait few minutes until the new program is loaded.

> Always check the status page to see that the program version has changed.

Upgrading via Local TFTP/HTTP Servers

For users that would like to use remote upgrading without a local TFTP/HTTP server, Grandstream offers a NAT-friendly HTTP server. This enables users to download the latest software upgrades for their devices via this server. Please refer to the webpage: https://www.grandstream.com/support/firmware

Alternatively, users can download a free TFTP or HTTP server and conduct a local firmware upgrade. A free window 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. Save and Apply the changes and reboot the HT841/HT881.

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

Firmware and Configuration File Prefix and Postfix

Firmware Prefix and Postfix allows device to download the firmware name with the matching Prefix and Postfix. This makes it the possible to store all of firmware with different version in one single directory. Similarly, Config File Prefix and Postfix allows device to download the configuration file with the matching Prefix and Postfix. Thus, multiple configuration files for the same device can be stored in one directory.

In addition, when the field "Check New Firmware only when F/W pre/suffix changes" is set to "Yes", the device will only issue firmware upgrade request if there are changes in the firmware Prefix or Postfix.

Managing Firmware and Configuration File Download

When "Automatic Upgrade" is set "**Yes, every**" the auto check will be done in the minute specified in this field. If set to "**daily at hour (0-23)"**, Service Provider can use P193 (Auto Check Interval) to have the devices do a daily check at the hour set in this field with either Firmware Server or onfig Server. If set to "**weekly on day (0-6)"** the auto check will be done on the day specified in this field. This allows the device periodically check there are any new changes need to be taken on a scheduled time. By defining different intervals in P193 for different devices, Server Provider can spread the Firmware or Configuration File download in minutes to reduce the Firmware or Provisioning Server load at any given time

Configuration File Download

Grandstream SIP Devices can be configured via the Web Interface as well as via a Configuration File (binary or XML) through TFTP or FTP/FTPS or HTTP/HTTPS. The **Config Server Path** is the TFTP or FTP/FTPS or HTTP/HTTPS server path for the configuration file. It needs to be set to a valid URL, either in FQDN or IP address format. The **Config Server Path** can be the same or different from the **Firmware Server Path**.

A configuration parameter is associated with each particular field in the web configuration page. A parameter consists of a Capital letter P and 2 to 3 (Could be extended to 4 in the future) digit numeric numbers. i.e., P2 is associated with the "New Password" in the Web GUI->Maintenance->Web/SSH Access page->Admin Password. For a detailed parameter list, please refer to the corresponding firmware release configuration template.

When the HT841/HT881 boots up or reboots, it will send a request to download the xml file named "cfgxxxxxxxxxxxx.xml" followed by the binary file named "cfgxxxxxxxxxxxx", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If the download of "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file. The configuration file name should be in lower case letters.

For more details on XML provisioning, please refer to: https://documentation.grandstream.com/knowledge-base/sip-device-provisioning-guide/

RESTORE FACTORY DEFAULT SETTINGS

> Restoring the Factory Default Settings will delete all configuration information on the phone. Please backup or print all the settings before you restore to the factory default settings. Grandstream is not responsible for restoring lost parameters and cannot connect your device to your VoIP service provider.

There are three (3) methods for resetting your unit:

Using the Reset Button

To reset default factory settings using the reset button please follow the steps above:

1. Unplug the Ethernet cable.
2. Locate the reset hole on the back panel of your HT841/HT881.
3. Insert a pin in this hole, and press for about 7 seconds.
4. Take out the pin. All unit settings are restored to factory settings

Using the IVR Command

Reset default factory settings using the IVR prompt:

1. Dial "***" for voice prompt.
2. Enter "99" and wait for "reset" voice prompt.
3. Enter the encoded MAC address (Look below on how to encode MAC address).
4. Wait 15 seconds and device will automatically reboot and restore factory settings.

Encode the MAC Address

1. Locate the MAC address of the device. It is the 12-digit HEX number on the bottom of the unit.
2. Key in the MAC address. Use the following mapping:

Key	Mapping
0-9	0-9
A	22 (press the "2" key twice, "A" will show on the LCD)
B	222
C	2222
D	33 (press the "3" key twice, "D" will show on the LCD)
E	333
F	3333

MAC Address Key Mapping

For example: if the MAC address is 000b8200e395, it should be keyed in as "0002228200333395"

Reset from Web Interface (Reset Type)

1. Access your HT841/HT881 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: Found on a sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **Basic Settings → Reset Type**
5. Press **Reset** button (after selecting the reset type).
    - **Full Reset:** This will make a full reset

- **ISP Data:** This will reset only the basic settings, like IP mode, PPPoE and Web port
- **VOIP Data:** This will reset only the data related with a service provider like SIP server, sip user ID, provisioning and others.

- Factory Reset will be disabled if the "Lock keypad update" is set to "Yes".
- If the HT841/HT881 was previously locked by your local service provider, pressing the RESET button will only restart the unit. The device will not return to factory default settings.

CHANGE LOG

This section documents significant changes from previous versions of the user guide for HT841/HT881. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.5.10

- Set the "Disable User Level Web Access" (P28158) to "Yes" by default. [Disable User Level Web Access]
- Set the "Disable Viewer Level Web Access" (P28159) to "Yes" by default. [Disable Viewer Level Web Access]
- Force user to change the password upon first login using the default password to the Admin/User/Viewer Account. [Changing Admin Level Password] [Changing User Level Password] [Changing Viewer Password]

Firmware Version 1.0.5.9

- Added support for New Web UI Style. [Web Configuration Pages Definitions]
- Added support for "Enable Early Media for VoIP-to-PSTN Calls". [Enable Early Media for VoIP-to-PSTN Calls]
- Added support for tone configuration by port. [Ringtone]
- Added support for "Request URI Routing ID" on FXO port. [Request URI Routing ID]
- Added support for "SIP Destination Port" on the "Port Status" page. [SIP Destination Port]
- Added the status check whether local sip ports are the same between different profiles. [Port Status]
- Updated the FXO's Hook Flash Timing from "300 – 1500" to "100 – 1500". [Hook Flash Timing]
- Added support for "Auto Send DTMF Upon Call Start". [Auto Send DTMF Upon Call Start]
- Updated the "DSP DTMF Detector SNR" value range from "0 – 2" to "0 – 12". [DSP DTMF Detector SNR]
- Added RTP/RTCP Keep Alive on Hold. [RTP/RTCP Keep Alive on Hold]
- Added support for p-value (P28834/28835/28836) corresponding to Initial Line Polarity.

Firmware Version 1.0.3.4

- Added support "Polarity On Answer Delay". [Polarity On Answer Delay]
- Updated config file download request starts from cfgMAC.xml [Configuration File Download]
- Added new value "4 – Auto" in NAT Traversal. [NAT Traversal]
- Added support "AVS DTMF Detector Parameter" in both FXS and FXO profiles. [DSP DTMF Detector Min Level] [DSP DTMF Detector SNR] [DSP DTMF Detector Deviation] [DSP DTMF Detector Twist]
- Added support "Radius auth protocol".[Radius auth protocol]
- Removed "Ring Timeout" from FXO page.

Firmware Version 1.0.1.2

- This is the Initial Release.

Need Support?

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

CONTACT SUPPORT