Grandstream Networks, Inc.

HT801/HT802

Analog Telephone Adaptors

Administration Guide

COPYRIGHT

The latest electronic version of this user manual is available for download here:

https://www.grandstream.com/support

CAUTION

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

WARNING

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

GNU GPL INFORMATION

HT801/HT802 firmware contains third-party software licensed under the GNU General Public License (GPL). Grandstream uses software under the specific terms of the GPL. Please see the GNU General Public License (GPL) for the exact terms and conditions of the license.

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

Table of Content

Table of Tables

Table of Figures

DOCUMENT PURPOSE

This document describes the basic concept and tasks necessary to use and configure your HT801/HT802. In addition, it covers the topic of connecting and configuring the HT801/HT802, making basic operations and the call features. Please visit https://www.grandstream.com/support to download the latest "HT801/HT802 User Guide".

This guide covers following topics:

- Product overview
- Getting started
- Configuration guide
- Upgrade and provisioning
- Restore factory default settings

CHANGE LOG

This section documents significant changes from previous versions of administration guide for HT801/HT802. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware version 1.0.35.4

- Added support to allow HT8xx provision admin password without special characters. [UPGRADING AND PROVISIONING]
- Added support for Israel time zone with DST. [Time Zone]

Firmware version 1.0.33.4

- Added feature Special Proceed Indication Tone. [Special Proceed Indication Tone].
- Added feature MWI Tone. [MWI Tone].

Firmware version 1.0.31.1

- Added support to always send HTTP basic authentication information. [Always Send HTTP Basic Authentication Information]
- Added support to enable call waiting alert-info in 180 ringing response. [Enable Call Waiting alert-info In 180 Ringing Response]

Firmware version 1.0.29.8

- Added support to authenticate based on OpenVPN Username and OpenVPN Password [OpenVPN USERNAME and PASSWORD]
- Added feature “OnHook DC Feed Current” [OnHook DC FEED CURRENT]

Firmware version 1.0.27.2

- No Major Changes

Firmware version 1.0.25.5

- Added support for “OpenVPN”. [OpenVPN]
- Added support of “Maximum Number of SIP Request Retries”. [Maximum Number of SIP Request Retries]
- Added support for “Failback Timer”. [Failback Timer]

Firmware version 1.0.23.5

- Added support for “DNS SRV Failover Mode”. [DNS SRV Failover Mode]

- Added support of “Register Before DNS SRV Failover”. [Register Before DNS SRV Failover]
- Added support for “Offhook Auto-Dial DTMF”. [Off Hook Auto-Dial DTMF]
- Added Special Feature IZZI to support N-Way conference hosted on Nokia IMS. [Special Feature]

Firmware version 1.0.21.4

- Added support for IPv6 address without square brackets. [Primary SIP Server] [Failover SIP Server] [Outbound Proxy] [Backup Outbound Proxy]
- Added support for DHCP Domain Name configuration. [DHCP domain name]
- Added support of “Use Configured IP” for “DNS Mode”. [Use Configured IP]
- Added support for “Play Busy Tone When Account is unregistered”. [Play Busy Tone When Account is unregistered]

Firmware version 1.0.19.11

- Added “Disable" option for Web access mode. [Web Access Mode]
- Moved “Trusted CA certificates” from Profile1/Profie2 to Advanced Settings and renamed as Trusted CA Certificates A and Trusted CA Certificates B. [Trusted CA certificates A] [Trusted CA certificates B]
- Added Feature “Disable User Level Web Access” and “Disable Viewer Level Web Access”. [Disable User Level Web Access][Disable Viewer Level Web Access]
- Added Feature “Use P-Asserted-Identity Header”. [Use P-Asserted-Identity Header]
- Added Feature” Load CA Certificates”. [Load CA Certificates]
- Added Feature “Connection Request Port”. [Connection Request Port]
- Added OI_BR to special feature. [Special Feature]
- Added support to set Ring Timeout to 0 for unlimited ring timeout. [Ring Timeout]
- Added New Zealand Standard for Pulse Dialing Standard. [Pulse Dialing Standard]
- Added support for Russian Language. [Language]
- Increased “SIP TLS Certificate” and “SIP TLS Private Key” supported maximum length from 2048 to 4096.[SIP TLS Certificate][SIP TLS Private Key]

Firmware Version 1.0.17.5

- Added support for Minimum TLS Version. [Minimum TLS Version]
- Added support for Maximum TLS Version. [Maximum TLS Version]
- Added support for Traditional Chinese language.[Language]

Firmware Version 1.0.15.4

- Added more choices to feature “Disable Weak TLS Ciphers”. [Disable Weak TLS Cipher Suites]
- Added feature “Syslog Protocol”. [Syslog Protocol]
- Added support for “Distinctive Call Waiting Tone”. [Distinctive Call Waiting Tone]
- Added support for “Call Waiting Tones”. [Call Waiting Tones]
- Added support for DHCP option 67. [Configuration File Download]

- Added support for GDMS platform. [ACS URL]

Firmware Version 1.0.13.7

- Added ability to support provisioning server path containing the server authentication credentials for the DHCP option 66. [Allow DHCP Option 66 to Override Server]
- Added support to send SNMP trap to 3 different servers. [SNMP Trap IP Address]
- Added feature “Call Features Settings”. [Call Features Settings]
- Added feature “Use SIP User Agent”. [SIP User-Agent]
- Updated “Use SIP User Agent Header” to “SIP User Agent Postfix”. [SIP User Agent Postfix].
- Added feature “Disable Reminder Ring for DND”. [Disable Reminder Ring for DND]
- Added feature “CDR File Option”. [CDR File Option]
- Added feature “SIP File Option”. [SIP File Option]
- Added feature “Disable Weak TLS Cipher Suites”. [Disable Weak TLS Cipher Suites]
- Added feature “Pulse Dialing Standard”. [Pulse Dialing Standard]
- Added feature “Callee Flash to 3WC”. [Callee Flash to 3WC]
- Added feature “RFC2833 Count”. [RFC2833 Events Count] [RFC2833 End Events Count]
- Added feature “Replace Beginning ‘+’ with 00 in Caller ID”. [Replace Beginning '+' with 00 in Caller ID]
- Added feature “Disable Unknown Caller ID”. [Disable Unknown Caller ID]
- Added feature “Disable # as Redial Key”. [Disable # as Redial Key]
- Added feature “Reset Call Features”. [Reset Call Features]
- Added support to view, download, and delete the call history through device Web UI. [CDR File]
- Added support to store SIP file locally. [SIP File]

Firmware Version 1.0.11.6

- Added support to display CPU load on the device web STATUS page. [CPU Load]
- Added support for SIP keep-alive to use SIP NOTIFY. [Enable SIP OPTIONS/NOTIFY Keep Alive]
- Added feature “Network Cable Status” on Web UI status page. [Network Cable Status]
- Added support for Management Interface. [Enable Management Interface]
- Added feature “SSH Idle Timeout”. [SSH Idle Timeout]
- Added feature “Telnet Idle Timeout”. [Telnet Idle Timeout]
- Added feature “Use ARP to detect network connectivity”. [Use ARP to detect network connectivity]
- Added feature “Call Record”. [CDR File]

Firmware Version 1.0.10.6

- Added feature “Inband DTMF Duration”. [Inband DTMF Duration]
- Added feature “RFC2543 Hold”. [RFC2543 Hold]
- Added feature “Visual MWI Type”. [Visual MWI Type]
- Added feature “Ring Frequency”. [Ring Frequency]
- Added feature “Allow SIP Factory Reset”. [Allow SIP Factory Reset] [Reset using SIP NOTIFY]

- Added support for G722 Codec. [HT801/HT802 Technical Specifications]
- Added support for allow user to choose preference codec from PCMU and PCMA for FAX pass-through codec. [Fax Mode]

Firmware Version 1.0.9.3

- Added feature “Custom Certificate”. [Custom Certificate]
- Added feature “Use P-Access-Network-Info Header”. [Use P-Access-Network-Info Header]
- Added feature “Use P-Emergency-Info Header”. [Use P-Emergency-Info Header]
- Added feature “Conference Party Hang up Tone” when “Special Feature” is set to MTS. [Call Progress Tones]
- Add support for HTTPS based on TLS v1.2

Firmware Version 1.0.8.7

- Added [CenturyLink, MTS] to Special Feature.
- Added support for upgrade device via [FTP/FTPS] server. [UPGRADING AND PROVISIONING]
- Added support to have the call waiting tone through SIP INFO.
- Added feature “Validate Server Certificates”. [Validate Server Certificates]
- Added support for [DDNS]
- Added feature Blacklist for Incoming Calls. [Blacklist for Incoming Calls]
- Added support for [Telnet]
- Added feature [Play busy/reorder tone before Loop Current Disconnect]

Firmware Version 1.0.5.11

- Changed default "Upgrade Via" from HTTP to HTTPS. [Upgrade via] [UPGRADE PROTOCOL]
- Added the ability to schedule [Automatic Reboot]
- Added support for [SNMP]
- Added support for 3 level access through RADIUS authorization (Admin, User and [viewer])
- Added option to customize number of failed [Web Access Attempt Limit] to access web GUI
- Added option to customize idle time to logout the web access with [Web Session Timeout]
- Added option to disable WAN side ports [Blacklist for WAN Side Port]
- Added feature “Caller ID Fetch Order” option under FXS port settings. [Caller ID Fetch Order]
- Added feature “Enable High Ring Power” option under FXS port settings. [Enable High Ring Power]
- Added feature “Internet Protocol” to choose from “IPv4 Only”, “IPv6 Only”, “Both, prefer IPv4”, “Both, prefer IPv6”. [Internet Protocol]
- Added feature “IPv6 Address” to configure IPv6 Address. [IPv6 Address]

Firmware Version 1.0.3.7

- Added option “Use Actual Ephemeral Port in Contact with TCP/TLS” to force device to use actual ephemeral port. [Use Actual Ephemeral Port in Contact with TCP/TLS]

- Added option “SIP URI Scheme When Using TLS” to choose between ‘SIP’ and ‘SIPS’. [SIP URI Scheme When Using TLS]
- Added Option “Backup Outbound Proxy” to use backup Outbound Proxy if Outbound Proxy registration expires. [Backup Outbound Proxy]
- Added option “Prefer Primary Outbound Proxy” to enable registration through primary outbound proxy if registration expires. [Prefer Primary Outbound Proxy]
- Added option “Enable RTCP” to enable RTCP function through Web UI. [Enable RTCP]
- Added option “Hold Target Before Refer” to enable device to hold before being referred. [Hold Target Before Refer]
- Added Option “Enable Session Timer” to disable session timer. [Enable Session Timer]
- Added feature “Conference URI” to support Conference URI. [Conference URI]
- Added feature “Whitelist for WAN Side” for remote management. [Whitelist for WAN Side]
- Added feature “Blacklist for WAN Side” for remote management. [Blacklist for WAN Side]
- Added option “Web Access Mode” to choose between “HTTPS” and “HTTP” to access device Web UI.
- Added feature “HTTPS Web Port” to set HTTPS web port instead of using default HTTPS port. [HTTPS Web Port]
- Added feature “SSH Port” to self-configure SSH port. [SSH Port]
- Added SNMP related features.

Firmware Version 1.0.3.2

- This is the initial version for HT801.
- Added option “DNS SRV use Registered IP” [DNS SRV use Registered IP].
- Changed default NTP server from us.pool.ntp.org to pool.ntp.org.

Firmware Version 1.0.2.5

- Changed OPUS Payload Type default value to 123 to match other GS products. [OPUS Payload Type].

Firmware Version 1.0.2.3

- Added a re-enter box to confirm change user and admin password on web GUI to avoid typo or mistakes [Confirm Admin Password][Confirm End User Password].
- Add new iLBC libraries to improve iLBC audio quality.

Firmware Version 1.0.1.9

- This is the initial version.

WELCOME

The HT801/HT802 analog telephone adaptors provide transparent connectivity for analog phones and faxes to the world of internet voice. Connecting to any analog phone, fax, or PBX, the HT801/HT802 are an effective and flexible solution for accessing internet-based telephone services and corporate intranet systems across established LAN and internet connections. The Grandstream handy tones HT801/HT802 are new additions to the popular handy tone ATA product family. This manual will help you learn how to operate and manage your HT801/HT802 analog telephone adaptor and make the best use of its many upgraded features including simple and quick installation, 3-way conferencing, direct IP-IP Calling, and new provisioning support among other features. The HT801/HT802 are very easy to manage and configure and are specifically designed to be an easy to use and affordable VoIP solution for both the residential user and the teleworker.

PRODUCT OVERVIEW

The HT801 is a one-port analog telephone adapter (ATA) while the HT802 is a 2-port analog telephone adapter (ATA) that allows users to create a high-quality and manageable IP telephony solution for residential and office environments. Its ultra-compact size, voice quality, advanced VoIP functionality, security protection and auto provisioning options enable users to take advantage of VoIP on analog phones and enables service providers to offer high quality IP service. The HT801/HT802 are an ideal ATA for individual use and for large scale commercial IP voice deployments.

Feature Highlights

The following table contains major features of HT801 and HT802:

Table 1: HT801/HT802 Features at a Glance

HT801  **HT802** 	• 1 SIP profile through 1 FXS port on HT801, 2 SIP profiles through 2 FXS ports on HT802 and single 10/100Mbps port on both models. • 3-way voice conferencing. • Wide range of caller ID formats. • Advanced telephony features, including call transfer, call forward, call-waiting, do not disturb, message waiting indication, multi-language prompts, flexible dial plan and more. • T.38 Fax for creating Fax-over-IP and GR-909 Line Testing Functionalities. • TLS and SRTP security encryption technology to protect calls and accounts. • Automated provisioning options include TR-069 and XML config files. • Failover SIP server automatically switches to secondary server if main server loses connection. • Use with Grandstream's UCM series of IP PBXs for Zero Configuration provisioning.

HT801/HT802 Technical Specifications

Following tables resumes all the technical specifications including the protocols/standards supported, voice codecs, telephony features, languages, and upgrade/provisioning settings for the HT801 and the HT802.

Table 2: HT801/HT802 Technical Specifications

Interfaces		
	HT801	**HT802**
Telephone Interfaces	One (1) RJ11 FXS port	Two (2) RJ11 FXS ports.
Network Interface	One (1) 10/100Mbps auto-sensing Ethernet port (RJ45).	
LED Indicators	POWER, INTERNET, PHONE	POWER, INTERNET, PHONE1, PHONE2.
Factory Reset Button	Yes.	
Voice, Fax, Modem		
	HT801	**HT802**
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, G.722, 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	5 REN: Up to 1km on 24 AWG.	2 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		
	HT801	**HT802**
Network Protocols	TCP/IP/UDP, RTP/RTCP, FTP/FTPS, HTTP/HTTPS, ARP/RARP, ICMP, DNS, DDNS, DHCP, NTP, TFTP, SSH, Telnet, STUN, SIP (RFC3261), SIP over TCP/TLS, SRTP, TR-069.	
QoS	Layer 3 (ToS, DiffServ, MPLS).	
DTMF Methods	In-audio, RFC2833 and/or SIP INFO.	
Provisioning and Control	HTTP, HTTPS, FTP, FTPS, SSH, Telnet, TFTP, TR-069, secure and automated provisioning using AES encryption, syslog.	

Security		
	HT801	**HT802**
Media	SRTP.	
Control	TLS/SIPS/HTTPS/SSH/Telnet.	
Management	Syslog support, SSH, Telnet remote management using web browser.	
Physical		
	HT801	**HT802**
Universal Power Supply	Input: 100-240VAC, 50-60Hz. Output: 5.0VDC/1.0A.	
Environmental	Operational: 32º – 104ºF or 0º – 40ºC. Storage: 14º – 140ºF or -10º – 60ºC. Humidity: 10 – 90% Non-condensing.	
Dimensions and Weight	• 100mm x 100mm x 29.5mm • 102g	• 100mm x 100mm x 29.5mm • 114g (without package).
Compliance		
	HT801	**HT802**
Compliance	FCC Part15B EN55032, EN55024, EN61000-3-2, EN61000-3-3, EN60950-1, AS/NZS CISPR22, AS/NZS60950.1, S003	FCC 15B, AS/NZS CISPR22, AS/NZS60950, EN55022, EN55024, EN60950, EN61000-3-2, EN61000-3-3, UL (Power supply).

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and information for obtaining the best performance with the HT801/HT802.

Equipment Packaging

The HT801 ATA package contains:

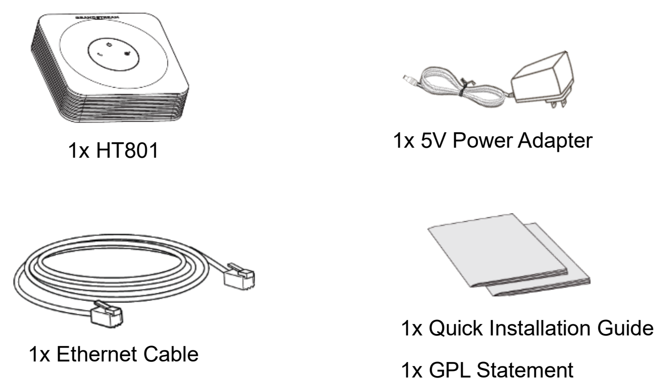

Figure 1: HT801 Package Contents

The HT802 ATA package contains:

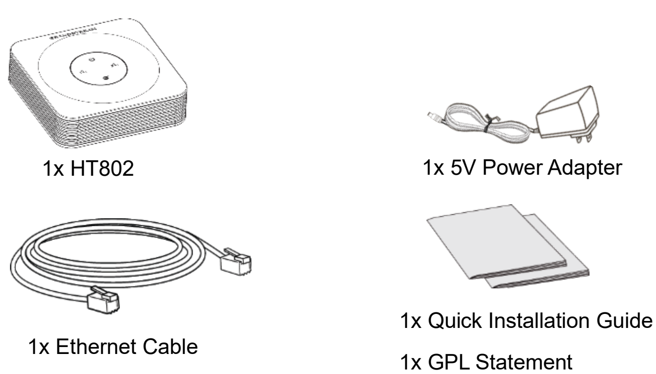

Figure 2: HT802 Package Contents

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

HT801/HT802 Ports Description

The following figure describes the different ports on the back panel of the HT801.

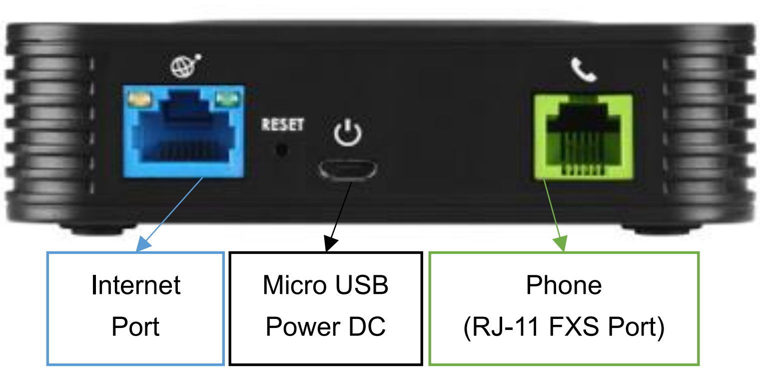

Figure 3: HT801 Back Panel

The following figure describes the different ports on the back panel of the HT802.

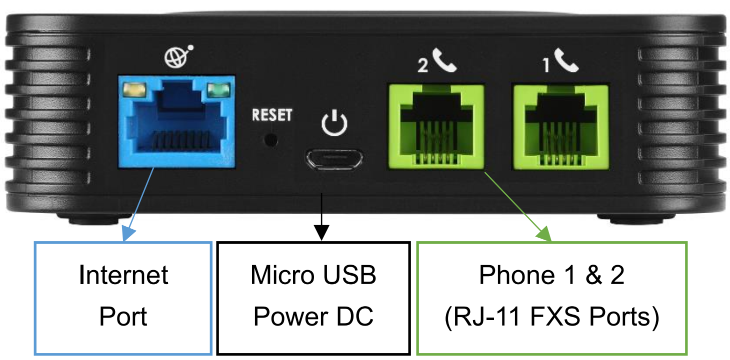

Figure 4: HT802 Back Panel

Table 3: Definition of the HT801/HT802 Connectors

Phone for HT801 Phone 1 & 2 for HT802	Connects the analog phones / fax machines to the phone adapter using an RJ-11 telephone cable.
Internet port	Connects the phone adapter to your router or gateway using an Ethernet RJ45 network cable.
Micro-USB Power	Connects the phone adapter to PSU (5V – 1A).
Reset	Factory reset button. Press for 7 seconds to reset factory default settings.

Connecting HT801/HT802

The HT801 and HT802 are designed for easy configuration and easy installation, to connect your HT801 or HT802, please follow the steps above:

1. Insert a standard RJ11 telephone cable into the phone port and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Insert the Ethernet cable into the internet or LAN port of the HT801/ht802 and connect the other end of the Ethernet cable to an uplink port (a router or a modem, etc.)
3. Insert the power adapter into the HT801/HT802 and connect it to a wall outlet.

Power, Ethernet, and Phone LEDs will be solidly lit when the HT801/HT802 is ready for use.

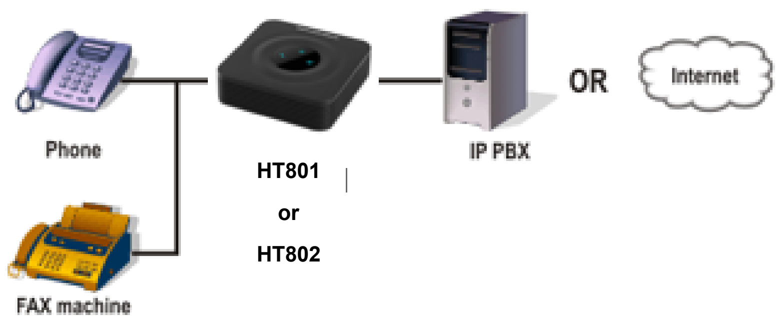

Figure 5: Connecting the HT801/HT802

HT801/HT802 LEDs Pattern

There are 3 LED buttons on HT801 and 4 LED buttons on HT802 that help you manage the status of your Handy Tone.

Figure 6: HT801/HT802 LEDs Pattern

Table 4: HT801/HT802 LEDs Pattern Description

LED Lights	Status
Power LED	The Power LED lights up when the HT801/HT802 is powered on, and it flashes when the HT802 is booting up
Internet LED	The Ethernet LED lights up when the HT801/HT802 is connected to your network through the Ethernet port, and it flashes when there is data being sent or received.
Phone LED for HT801 **Phone LED 1&2 for HT802**	The phone LED 1 & 2 indicate status of the respective FXS port-phone on the back panel • **OFF** - Unregistered • **ON (Solid Blue)** - Registered and Available • **Blinking every second** - Off-Hook / Busy • **Slow blinking** - FXS LEDs indicates voicemail

CONFIGURATION GUIDE

The HT801/HT802 can be configured via one of two ways:

- The IVR voice prompt menu.
- The Web GUI embedded on the HT801/HT802 using PC's web browser.

Obtain HT801/HT802 IP Address via Connected Analogue Phone

HT801/HT802 is by default configured to obtain the IP address from DHCP server where the unit is located. To know which IP address is assigned to your HT801/HT802, you should access to 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 phone ports of your HT801/HT802.
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 HT801/HT802 Interactive Voice Prompt Response Menu

The HT801/HT802has a built-in voice prompt menu for simple device configuration which lists actions, commands, menu choices, and descriptions. The IVR menu works with any phone connected to the HT801/HT802. Pick up the handset and dial "***" to use the IVR menu.

Table 5: Voice Prompt 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, 13-17,47 or 99 menu options
01	"DHCP Mode", "Static IP 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.
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 the HT801/HT802 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 • G722
10	"MAC Address"	Announces the Mac address of the unit.
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** / **HTTPS** / **FTP** / **FTPS**. 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 (See **Restore Factory Default Setting** section)
701-702	Phone calls between different ports of the same HT802	HT802 supports inter-port calling from voice menu. 70X (X is the port number)
	"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

Five 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 menu option and 12 digits for 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 key in like 192168000026. No decimal is needed).
- Key entry cannot be deleted but the phone may prompt error once it is detected.

Configuration via Web Browser

The HT801/HT802 embedded Web server responds to HTTP GET/POST requests. Embedded HTML pages allow a user to configure the HT801/HT802 through a web browser such as Google Chrome, Mozilla Firefox, and Microsoft's IE.

Accessing the Web UI

1. Connect the computer to the same network as your HT801/HT802.
2. Make sure the HT801/HT802 is booted up.
3. You may check your HT801/HT802 IP address using the IVR on the connected phone.
   Please see Obtain HT801/HT802 IP Address via Connected Analogue Phone
4. Open Web browser on your computer.
5. Enter the HT801/HT802's IP address in the address bar of the browser.
6. Enter the administrator's password to access the Web Configuration Menu (default password is admin).

Notes:

- The computer must be connected to the same sub-network as the HT801/HT802. This can be easily done by connecting the computer to the same hub or switch as the HT801/HT802.
- Recommended Web browsers:
  - **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 two default passwords for the login page:

Table 6: Web access level management

User Level	Username	Password	Web Pages Allowed
End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	admin	All pages
Viewer Level	viewer	viewer	View all pages. Changes not allowed.

The password is case sensitive with maximum length of 25 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, reboot HT801/HT802 to have the changes take effect if necessary; most of the options under the **Advanced Settings** and **FXS Port (x)** pages require reboot.

Saving the Configuration Changes

After users makes 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. We recommend rebooting or powering cycle the phone after applying all the changes.

Changing Admin Level Password

1. Access your HT801/HT802 web UI by entering its IP address in your favorite browser (screenshots below are from HT802 but the same applies to HT801).
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings and navigate to **Advanced Settings→Admin Password.**
4. Enter the new admin password.
5. Confirm the new admin password.
6. Press **Apply** at the bottom of the page to save your new settings.

   Note: Provision admin password without special characters is supported.

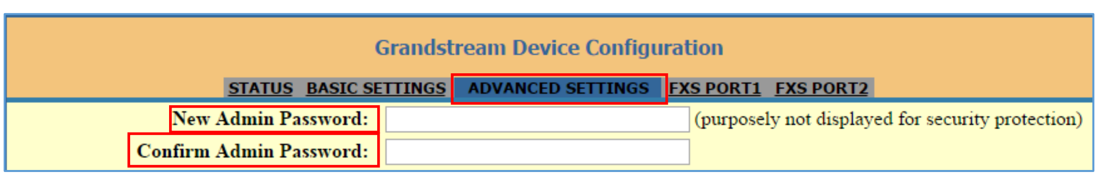

Figure 7: Admin Level Password

Changing User Level Password

1. Access your HT801/HT802 web UI by entering its IP address in your favorite browser.

2. Enter your admin password (default: admin).
3. Press **Login** to access your settings and navigate to **Basic Settings→End User Password.**
4. Enter the new end-user password.
5. Confirm the new end-user password.
6. Press **Apply** at the bottom of the page to save your new settings.

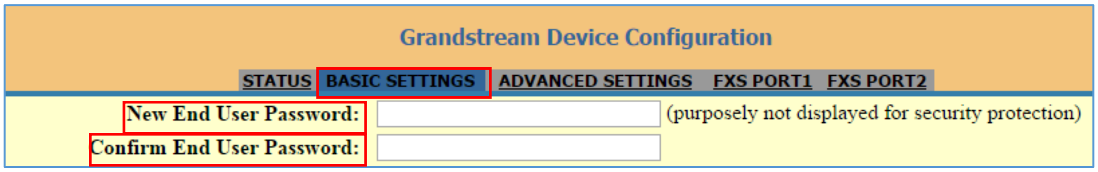

Figure 8: User Level Password

Changing Viewer Password

1. Access your HT801/HT802 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **Basic Settings → New Viewer Password** and **e**nter the new viewer password.
5. Confirm the new viewer password.
6. Press **Apply** at the bottom of the page to save your new settings.

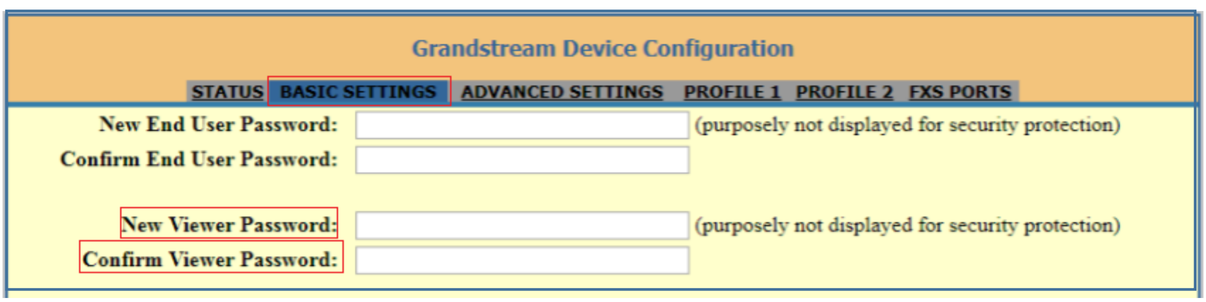

Figure 9: Viewer Level Password

Changing HTTP Web Port

1. Access your HT801/HT802 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings and navigate to **Basic Settings→Web Port.**
4. Change the current port to your desired/new HTTP port. Ports accepted are in range [1-65535].
5. Press **Apply** at the bottom of the page to save your new settings.

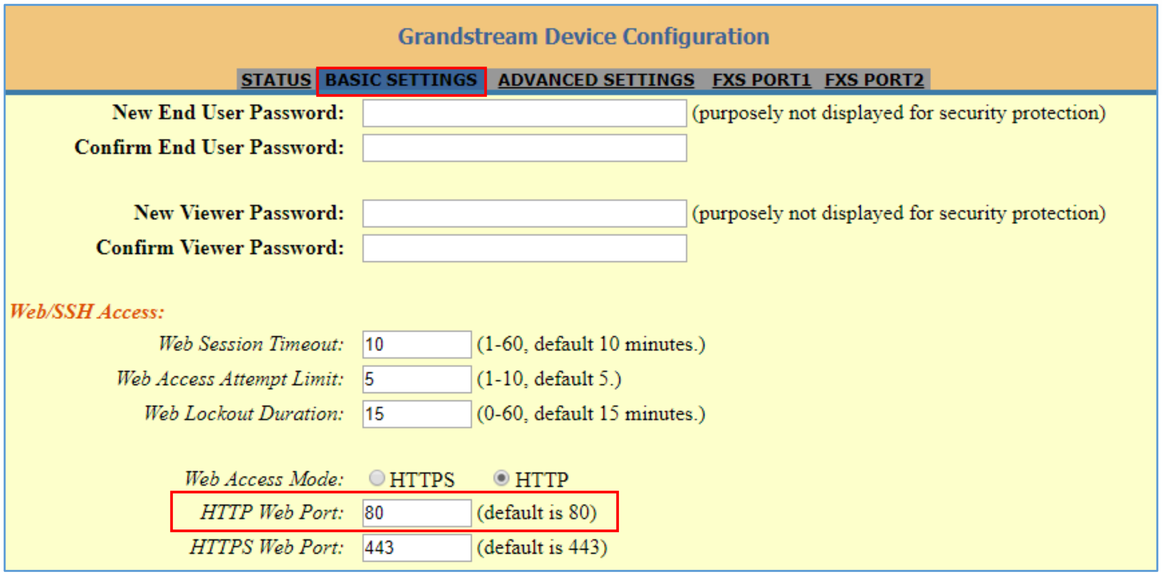

Figure 10: Web HTTP Port

Web Configuration Pages Definitions

This section describes the options in the HT801/HT802 Web UI. As mentioned, you can log in as an administrator or an end user.

- **Status:** Displays the system info, network status, account status, and line options.
- **Basic Settings:** Configures the end user level password, IP address modes, web access, time zone settings and language.
- **Advanced Settings:** Configures networks, upgrading and provisioning, TR-069, security settings, date and time, syslog, audio settings, call settings and call progress tones.
- **FXS Port (1,2):** Configures SIP settings, SIP registration, accounts settings, NAT settings, call features, ring tones.

Advanced Settings Page Definitions

Table 7: Advanced Settings

Advanced Settings	
New Admin Password	Defines the administrator level password to access the Advanced Web Configuration page. This field is case sensitive. Only the administrator can configure the "Advanced Settings" page. Password field is purposely left blank for security reasons after clicking update and saved. Max. length is 39 characters and minimum are 8, the password should contain at least 1 upper case and 1 lower case and 1 special character.

Confirm Admin Password	Confirms the new admin password.
Disable User Level Web Access	Disable or enable User Level Web Access. Default is **No**.
Disable Viewer Level Web Access	Disable or enable Viewer Level Web Access Default is **No**.
Layer 2 QoS	Sets values for 802.1Q/VLAN Tag. Default is **0**. Valid range is 0-4094. SIP 802.1p. Default is **0**. Valid range is 0-7. RTP 802.1p. Default is **0**. Valid range is 0-7.
Blacklist for WAN Side Port	It could be either port range or single port separated by a “,” Example: “5000-6000, 7000 “.
STUN Server is	Configures IP address or domain name of STUN server. Only non-symmetric NAT routers work with STUN.
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.
Use STUN to detect network connectivity	Uses STUN keep-alive to detect WAN side network problems. If keep-alive request does not yield any response for configured number of times (minimum 3), the device will restart the TCP/IP stack. If the STUN server does not respond when the device boots up, the feature is disabled. Default setting is **No**.
Use DNS to detect network connectivity	Uses DNS to detect WAN side network problems. Default setting is “**No**”.
Use ARP to detect network connectivity	Uses ARP to check the network connectivity. Default is “**Yes**”.
Verify host when using HTTPS	Enables / disables the host verification when using HTTPS.
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. Default is **fm.grandstream.com/gs**.
Config Server Path	Sets IP address or FQDN of configuration server. The URL of the server that hosts the configuration file to provision HT801/HT802. Default is **fm.grandstream.com/gs**.
XML Config File Password	Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file using OpenSSL.
HTTP/HTTPS FTP/FTPS Username	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 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.
Allow DHCP Option 66 to Override Server	Obtains configuration and upgrade server's information using options 66 from DHCP server. **Note:** If DHCP Option 66 is enabled, the HT801/HT802 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**.
Automatic Upgrade	Specifies when the firmware upgrade process will be initiated; there are 4 options: • **No**: The HT801/HT802 will only do upgrade once at boot up. • **Check every X minute**: 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).
Always Check for New Firmware at Boot up	Configures the HT801/HT802 to always search for the new firmware at boot up. During the boot stage, the HT801/HT802 will contact the firmware upgrade server to search for a new firmware, when available it will start the upgrade process, otherwise it will boot normally.
Check New Firmware only when F/W pre/suffix changes	Configure the HT801/HT802 to search for the new firmware when the firmware prefix / suffix changes. When this option is selected, the HT801/HT802 will check for updates only when the pre/suffix has been changed.
Always Skip the Firmware Check	Configures the HT801/HT802 to skip the firmware check, when this option is selected the HT801/HT802 will always skip searching for a new firmware.
Disable SIP NOTIFY Authentication	Disables the SIP NOTIFY Authentication on the phone adapter. If set to "Yes", the phone adapter will not challenge NOTIFY with 401. The default setting is "**No**"
Authenticate Conf File	Authenticates configuration before being accepted. This protects the configuration from unauthorized modifications. Default is **No**.
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. DDNS

Trusted CA certificates A	Uses the certificate for Authentication if “Check Domain Certificates” is set to “Yes” under “Account”--> “SIP Settings”.
Trusted CA certificates B	Uses the certificate for Authentication if “Check Domain Certificates” is set to “Yes” under “Account”--> “SIP Settings”.
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
SIP TLS Certificate	Specifies SSL certificate used for SIP over TLS is in X.509 format. The HT801/HT802 has built-in private key and SSL certificate. Maximum supported length is 4069.
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.
Custom Certificate (Private Key + Certificate)	Allows users to update to the device their own certificate signed by custom CA certificate to manage client authentication.
Enable TR-069	Sets the phone adapter system to enable the “CPE WAN Management Protocol” (TR-069). 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	Enters username to authenticate to ACS.
ACS Password	Enters 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 HT801/HT802.
Connection Request Password	Enters password for ACS to connect to the HT801/HT802.
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.
Enable SNMP	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 Username	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 Username	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.
Enable RADIUS Web Access Control	Default is **No**.
Action upon RADIUS Auth Server Error	Choose action upon RADIUS server error. Default is Authenticate Locally (Default Authenticate Locally)
RADIUS Auth Server Address	Address of RADIUS Auth server.
RADIUS Auth Server Port	Port of RADIUS Auth server.
RADIUS Shared Secret	Set RADIUS shared secret.
RADIUS VSA Vendor ID	Configure RADIUS VSA Vendor ID to match RADIUS server's configuration. Default is 42397 for Grandstream Networks Inc.
RADIUS VSA Access Level Attribute	Configure RADIUS VSA Access Level Attribute to match RADIUS server's configuration. Incorrect setting would cause Radius authenticate fail.

Enable DDNS	Allow users to use DDNS.
DDNS Server	Selects DDNS Server: dyndns, freedns.afraid.org, zoneedit.com, no-ip.com, oray.net. Default is dyndns.
DDNS Username	64 characters as Max String Length.
DDNS Password	64 characters as Max String Length.
DDNS Hostname	64 characters as Max String Length.
DDNS Hash	64 characters as Max String Length.
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. 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 Digest	Select the OpenVPN Digest. Default is SHA1.
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.
OpenVPN username	Configure the OpenVPN username.

OpenVPN password	Configure the OpenVPN password
System Ring Cadence	Configuration option is set ring cadence on FXS port for all incoming calls. *Syntax:* **c=on1/off1-on2/off2-on3/off3;** (3 cadences maximum) Default is set to **c=2000/4000;** (US standards)
Call Progress Tones: • **Dial Tone** • **Ringback Tone** • **Busy Tone** • **Reorder Tone** • **Confirmation Tone** • **Call Waiting Tone** • **Prompt Tone** • **Conference Party Hangup Tone *** • **Special Proceed Indication 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. <u>Example configuration for N.A.</u> Dial tone: f1=350@-13, f2=440@-13, c=0/0; *Syntax:* **f1=freq@vol, f2=freq@vol, c=on1/off1-on2/off2-on3/off3; [...]** (Note: freq: 0 - 4000Hz; vol: -30 - 0dBm) * "Conference Party Hang-up Tone" will apply only if the "Special Feature" is set to "MTS". Special Proceed Indication Tone: This feature allows user to configure the tone played when user goes offhook and there is voicemail on the subscribed mailbox. Need to set 'MWI Tone' to 'Special Proceed Indication Tone' to use this feature.
Prompt Tone Access Code	Key pattern to get Prompt Tone. Maximum 20 digits.
Lock Keypad Update	Configuration update via keypad (analog phone connected to FXS port keypad using IVR menu) is disabled if set to Yes.
Disable Voice Prompt	Voice prompt is disabled if set to Yes.
Disable Direct IP Call	Direct IP call is disabled if set to Yes.
Play Busy Tone When Account is unregistered	When this feature is set to Yes, device will play busy tone when the FXS port account is not registered, and the attached analog phone is offhook.

Blacklist for Incoming Calls	Allow users to block incoming calls from specific list of numbers. Maximum allow 10 SIP numbers and each number should be separated by a comma (‘,’) in web UI. Other allowed characters are 0-9, comma (“,”), asterisk (‘*’), pound sign (‘#’) and plus sign (‘+’).
NTP Server	Defines the URL or IP address of the NTP server. The ATA may obtain the date and time from the server. The default setting is “pool.ntp.org.”
Allow DHCP Option 42 to override NTP server	Defines whether DHCP Option 42 should override NTP server or not. When enabled, DHCP Option 42 will override the NTP server if it is set up on the LAN. The default setting is **Yes**.
DHCP Option 17 Enterprise Number	Configure the DHCP option 17 number. Default is **3561**
CDR File Option	By default, the device will split the allowed memory for CDR file into 2 parts. Device will create the first CDR file which is half of the allowed size, when it is full, device will create the second file. • When “CDR File Option” is set to Default “**Keep**”, device will keep the call records when both files are full, no more new record will be stored. • When this feature is set to “**Override”**, device will clear the first CDR file and start storing again. The CDR file output will be available at Status page: [CDR File]
SIP File Option	By default, the device will split the allowed memory for SIP file into 2 parts. Device will create the first SIP file which is half of the allowed size, when it is full, device will create the second file. • When “SIP File Option” is set to Default “**Keep**”, device will keep the call records when both files are full, no more new record will be stored. • When this feature is set to “**Override**”, device will clear the first SIP file and start storing again. The SIP file output will be available at Status page: [SIP File] **Note:** “**Send SIP Log**” must be enabled to be able to capture the trace.

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.**
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**.
Syslog Protocol	If set to SSL/TLS, the syslog messages will be sent through secured TLS Protocol to syslog server. Default setting is UDP. **Note:** The CA certificate is required to connect with the TLS server A reboot is required to take effect.
Syslog Server	URL or IP address of syslog server. **Note:** A reboot is required to take effect.
Syslog Level	Select the HT801/HT802 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) 11. extra syslog style (EXTRA DEBUG level) **Note:** A reboot is required to take effect.
Send SIP Log	Configures whether the SIP log will be included in the syslog messages. The default setting is **No**.
Always Send HTTP Basic Authentication Information	If set to Yes, the device will send configured username and password within HTTP request without server sending authentication challenge.
Automatic Reboot	Default is **No**. When “Yes, reboot every day at hour” or “Yes, reboot every week at day” or “Yes, reboot every month at day” is checked, user can specify “Hour of the day (0-23)” or “Day of the week (0-6)” or “Day of the month (0-30)”. Default time is Monday 1AM.
Download Device Configuration	Press **Download** button to download device configuration file to local computer. The filename is “config.txt”. The file is plain text and not including password fields.
Download Device XML Configuration	Press **Download** to download device configuration file to local computer. The filename is “config.xml”. The file will not include password fields.
Upload Firmware	Press **Upload from local directory** button to load the firmware file to the device from your computer. The firmware filename should be “ht80xfw.bin” (ht802fw.bin for HT802 for instance).
Upload Configuration	Press **Upload from local directory** button to load configuration file to the device from your computer. The configuration file should be an XML file (for instance: “config.xml”). Note: The field <mac> is not mandatory in the document but if available only device with specified MAC address will accept the configuration file.
Export Backup Configuration	Press **Download** button to export device backup configuration to computer. The output is “cfg<mac>_enc.xml” (where <mac> is the MAC address of the

	device). The file is encrypted and can be used on same device only.
Restore From Backup Configuration	Press **Upload** button to restore device configuration from previously exported backup configuration.

Status Page Definitions

Table 8: Status Page Definitions

Account Status	
MAC Address	Shows device ID in hexadecimal format. This is needed by network administrators for troubleshooting. The MAC address will be used for provisioning and can be found on the label on original box and on the label located on the bottom panel of the device.
IPv4 Address	Displays assigned IPv4 address.
IPv6 Address	Displays assigned IPv6 address.
VPN IPv4 Address	Displays assigned OpenVPN IPv4 address.
VPN IPv6 Address	Displays assigned OpenVPN IPv6 address.
Product Model	Displays product model info. Default is **HT801/HT802**.
Hardware Version	Displays the hardware revision information and the part number.
Software version	• **Program:** Specifies Program version. This is the main firmware release number, which is always used for identifying the software system of the HT801/HT802. • **Bootloader:** Specifies Boot version. • **Core:** Specifies Core version. • **Base:** Specifies Base version. • **CPE:** Specifies CPE version. CPE version is displayed only when HT801/HT802 is connected to an ACS using TR-069 protocol.
Software Status	Indicates actual software status.
System Up Time	Indicates actual system time and uptime since last reboot.
CPU Load	Indicates CPU load (%)
Network Cable Status	Indicates physical network cable status: **Status** (Up/Down), **Speed** (Mbps), **Operational Mode** (Full/Half Duplex)

PPPoE Link Up	Indicates PPPoE connection status.
NAT	Indicates type of NAT when it is configured.
Port Status	Displays relevant information regarding the FXS ports, their registration, current status and their appropriate User ID.
Port Options	Displays DND and call forward information on FXS ports.
CDR File	**Download**, **Preview**. Or **Delete** call history records from the web GUI. Only the last 1000 records will be available.
SIP File	**Download**, **Preview** or, **Delete** locally stored SIP trace. **Note:** "**Send SIP Log**" must be enabled to be able to capture the trace.
Provision	Displays provisioning status.
Core Dump	Provides generated core dump file if unit malfunctions. **Clean** will be displayed if no issues.
GR909	Click on "Test Page" to be redirected to lines tests page (Hazardous Potential, Foreign Electromotive Forces, Resistive Faults, Receiver Off hook and Ringer Equivalent Number)

Basic Settings Page Definitions

Table 9: Basic Settings Page

Basic Settings	
New End User Password	Configures user level password. Case sensitive and max. Length of 25 characters.
Confirm End User Password	Re-enter the end user password to confirm change user password on web GUI to avoid typo or mistakes.
New Viewer Password	Configures viewer level password. Case sensitive and max. Length of 25 characters.
Confirm Viewer Password	Re-enter the viewer password to confirm change viewer password on web GUI to avoid typo or mistakes.
Web Session Timeout	Configure timer to logout web session during idle. Default is 10 min. Range is 2-60 min.

Web Access Attempt Limit	Configure attempt limit before lockout. Default is 5. Range is 1-10.
Lockout time interval	If login attempt failed 5 times, login would be locked out for the time length. (Default 15 mins. Range 1-15 min).
Web Access Mode	Allows users to choose the Web Access Mode between “HTTPS”, “HTTP” and “Disabled”. If “Disabled” is selected, web UI access will be disabled. By default, “HTTP” is selected.
HTTP Web Port	Customizes HTTP port used to access the HT801/HT802 web UI. Default is **80**.
HTTPS Web Port	Customizes HTTPS port used to access the HT801/HT802 web UI. Default is **443**.
Disable SSH	Enables/disables the SSH access. Default is **No** (enabled).
SSH Port	Allows users to self-configure SSH Port number. By default, the port number is **22**.
SSH Idle Timeout	Configures SSH session timeout. [0 – 86400] seconds; Default is **0**.
Disable Telnet	Enables/disables the Telnet access. Default is **Yes** (disabled).
Telnet Port	Allows users to self-configure Telnet Port number. By default, the port number is **23**.
Telnet Idle Timeout	Configure Telnet session timeout. [0 – 86400] seconds; Default is **0**.
Whitelist for WAN Side	Users can configure the whitelist 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.
Blacklist for WAN Side	Users can configure the blacklist 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.
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 phone for the changes to take effect.
IPv4 Address	Allows users to configure the appropriate network settings on the HT80x to obtain IPv4 address. Users could select "DHCP", "Static IP" or "PPPoE". By default, it is set to "DHCP".
Dynamically assigned via DHCP	All the field values for the static IP mode are not used (even though they are still saved in the flash memory.) The HT801/802 acquires its IP address from the first DHCP server it discovers from the LAN it is connected. • **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:** Specifies the domain name that client should use when resolving hostname via the Domain Name System. • **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 **HT8XX**.
Use PPPoE	Set the PPPoE account settings. If selected, ATA attempt to establish a PPPoE session if any of the PPPoE fields is set. • **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. Default is blank.
Preferred DNS server	Specifies preferred DNS server to use when DHCP or PPPoE are set.
Statically configured as IP address	Configure IP address, subnet Mask, default router IP address, 1st preferred DNS server, 2nd preferred DNS server. These fields are set to zero by default.
IPv6 Address	Allows users to configure the appropriate network settings on the HT80x to obtain IPv6 address. Users could select "DHCP", "Static IP”. By default, it is set to "DHCP". • **DHCP mode:** all the field values for the static IP mode are not used (even though they are still saved in the flash memory.) The HT801/HT802 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).
Enable Management Interface	Allows administrator to setup a Virtual Network Interface on top of the physical interface for device management. Default is **No.**
Management Access	Chooses whether to access using “**Management Interface Only**” (Default) Or “**Both Service and Management Interfaces**”
Management Interface IPv4 Address	Configures Voice VLAN Type : • Default is **dynamically assigned via DHCP** Or, • **statically configured as**: o IP Address : Default is **192.168.100.100** o Subnet Mask : Default is **255.255.255.0** o Default Router : Default is **192.168.100.1** o DNS Server 1 : Default is **0.0.0.0**

	◦ DNS Server 2 : Default is **0.0.0.0** • **802.1Q/VLAN Tag** vlan tagging : [0 – 4094]; Default is **0** • **802.1p priority value** : priority : [0 – 7]; Default is **0**
Time Zone	Selects time zone to define date/time on the device.
Self-Defined Time Zone	Allows users to define their own time zone.
Allow DHCP server to set Time Zone	Obtains time zone setting (offset) from a DHCP server using DHCP Option 2; it will override selected time zone. If set to "No", the analogue adapter will use selected time zone even if provided by DHCP server. The Default setting is **Yes**.
Language	Configures the languages of the voice prompt and web interface, except Spanish that it is only in IVR. Available languages: English, Chinese, Traditional Chinese, Russian, Spanish IVR.
Reset Type	Gives the administrator the option to restore default configuration on the HT801/HT802. There are 3 types of factory reset: • **ISP Data Reset:** All VoIP related configuration (mainly everything located on FXS page). • **VOIP Data Reset:** All ISP (Internet Service Provider) configuration which may affect the IP address. • **Full Reset:** Both VoIP and ISP related configuration at the same time. **Note:** After you choose the reset type, you must click the reset button to take effect.

FXS Ports Pages Definitions

Table 10: FXS Ports

FXS Port (1,2)	
Accounts 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: 2001:1260:1:277::3). This is the primary SIP server used to send/receive SIP messages from/to HT8xx.
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: 2001:1260:1:277::3)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, or IP address, if any: IPv4: 192.168.5.170/ IPv6: 2001:1260:1:277::3). Used by HT801/HT802 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: 2001:1260:1:277::3). By default, this field is left empty.
Prefer Primary Outbound Proxy	If the user configures this option to “**Yes**”, when registration expires, the device will re-register via primary outbound proxy. By default, this option is disabled.
Allow DHCP Option 120 (override SIP Server)	Configures the HT802 to collect SIP server address from DHCP option 120. Default is **No**.
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**.
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. The default setting is "**No**".
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**.
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.
DNS Mode	Selects DNS mode to use for the client to look up server. One mode can be chosen. Default is **A Record**. • **A Record:** 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 SIP server is configured as domain name, device will not send DNS query, but will use "Primary IP" or "Backup IP" to send SIP message if at least one of them are 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 re-tries.
DNS SRV use Registered IP	When this option is set to "Yes", when the HT is registered on second SRV and makes an outbound call, it will try the second SRV (registered IP) first. By default, this option is disabled, and the DNS SRV will use first SRV

	instead of the registered IP.
DNS SRV Failover Mode	Configure the preferred IP mode for DNS SRV or NAPTR/SRV. If "default" is selected, first IP from query result will be applied; If "Saved one until DNS TTL" is selected, previous IP will be applied before reaches DNS timeout; If "Saved one until no response" is selected, previous IP will be applied even after DNS time out until it is unreachable. • **Default:** If the option is set with "default", it will again try to send register messages to one IP at a time, and the process repeats. • **Saved one until DNS TTL**: If the option is set to "Saved one until DNS TTL", it will send register messages to the previously registered IP first. If no response, it will try to send one at a time for each IP. This behavior lasts if DNS TTL (time-to-live) is up. • **Saved one until no responses:** If the option is set with "Saved one until no responses", it will send register messages to the previously registered IP first, but this behavior will persist until the registered server does not respond.
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).
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 nonregistration SIP request (INVITE) to the new successfully registered server or not.
TEL URI	Indicates E.164 number in "From" header by adding "User=Phone" parameter or using "Tel:" in SIP packets, if the HT801/HT802 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. Default is

	Disabled.
SIP Registration	Controls whether the HT801/HT802 needs to send REGISTER messages to the proxy server. Default setting is **Yes**.
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. Default is **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.
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
Enable SIP OPTIONS/NOTIFY Keep Alive	Enables SIP OPTIONS or SIP NOTIFY to track account registration status so the phone adapter will send periodic OPTIONS/NOTIFY messages 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 phone adapter sends OPTIONS or NOTIFY messages to the SIP server. The default setting is 30 seconds, which means the phone adapter 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 or SIP NOTIFY Keep Alive before re-registration. Between 3-10, default is **3**.
Layer 3 QoS	Defines Diff-Serv values for SIP and RTP. SIP DSCP (Diff-Serv value in decimal, 0-63, default **26**) RTP DSCP (Diff-Serv value in decimal, 0-63, default **46**)
Local SIP Port	Defines local port to use by the HT801/HT802 for listening and transmitting SIP packets. Default value for FXS 1 is 5060 and 5062 for FXS 2.
Local RTP Port	Defines the local RTP-RTCP port pair the HT801/HT802 will listen and transmit. It is the HT801/HT802 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 HT801/HT802 are behind the same NAT. Default is **No**.
Use Random RTP Port	Controls whether to use configured or random RTP ports. This is usually necessary when multiple HT801/HT802 are behind the same NAT. Default is **No**.
Enable RTCP	Allows users to enable RTCP. Default setting is **Yes**.
Hold Target Before Refer	Allows user to hold the phone call before referring it. If set to No, the call will not be hold before referred. Default is **Yes**.
Refer-To Use Target Contact	Includes target's "Contact" header information in "Refer-To" header when using attended transfer. Default is **No**.
Transfer on Conference Hang-up	If set to "Yes", when the phone hangs up as the conference initiator, the conference call will be transferred to the other parties so that other parties will remain in the conference call. Default setting is **No**.
Remove OBP from Route Header	Removes outbound proxy info in "Route" header when sending SIP packets. Default is **No**.
Support SIP Instance ID	Includes "SIP Instance ID" attribute to "Contact" header in REGISTER request as defined in IETF SIP outbound draft. Default is **No**.
Validate Incoming SIP Message	Validates incoming messages. Default is **No**.

Check SIP User ID for Incoming INVITE	Checks SIP User ID in the Request URI of incoming INVITE; if it does not match the HT801/HT802 SIP User ID, the call will be rejected. Direct IP calling will also be disabled. Default is **No**.
Authenticate Incoming INVITE	Challenges the incoming INVITE for authentication with SIP 401 Unauthorized message. 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. Default setting is "**No**".
Authenticate server certificate chain	Configures whether to validate the server 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. Default setting is "**No**".
Allow Incoming SIP Messages from SIP Proxy Only	Checks SIP address of the Request URI in the incoming SIP message; if it does not match the SIP server address of the account, the call will be rejected. Default is **No**.
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 **CBCO** 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	With this feature set to Yes, device will send' P-Asserted-Identity Header' on the SIP Invite. Default is **No**

SIP REGISTER Contact Header Uses	Specifies which address (LAN or WAN address) the device will detect to use it in SIP Register Contact Header. When set to **LAN**, Contact header will include local IP from ATA in REGISTER messages, while if set to **WAN**, host/port/contact will be updated from SIP 401/403/404/407 Via header "received"/"rport" parameters in REGISTER messages. Default is **LAN Address**.
Caller ID Fetch Order	Selects the Caller ID display order which need to be respected by the HT801/HT802. The available options are: ● **Auto**: When set to "Auto", the HT801/HT802 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 HT801/HT802 will use the FROM header to display the caller ID.
Allow SIP Factory Reset	Allows to reset the devices directly through SIP Notify. If "Allow SIP Factory Reset" is set to "YES" under FXS 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.
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 4)
SIP T1 Timeout	Defines T1 timeout value. It is an estimate of the round-trip time between the client and server transactions. For example, the HT801/HT802 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 defined by T2. 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 T2 value. Default is **4** seconds.
SIP Timer D	Configure the SIP Timer D defined in RFC3261. 0 - 64 seconds. Default is **0**.
DTMF Payload Type	Defines payload type for DTMF using RFC2833. Default is **101**.
Preferred DTMF method (in order)	Sorts DTMF methods (in-audio, via RTP (RFC2833) or via SIP INFO) by priority.
Inband DTMF Duration	Allows to adjust the inband DTMF duration sent from ATA to IPPBX. Default is **100** ms. Valid range: 40-2000 ms. Inter-duration: 50 ms. Valid range: 40-2000 ms.
Disable DTMF Negotiation	Uses above DTMF order without negotiation. Default is **No**.
Generate Continuous RFC2833 Events	When enabled, the RFC2833 events are generated until key is released. Default is **No**.
Send Hook Flash Event	If set to yes, flash will be sent as DTMF event. Default is **No.**
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.
Enable Call Waiting alert-info In 180 Ringing Response	When set to Yes, Alert-Info header will be added in 180 Ringing for Call Waiting case
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**.

Off Hook 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 to be entered. The HT80x will automatically append the "@" and the host portion of the corresponding SIP address.
Off Hook Auto Dial Delay	Specifies the auto-dial delay in seconds after off hook. Valid range is 0-60 seconds. Default is 0.
Off Hook Auto-Dial DTMF	When 'Off Hook Auto-Dial' is configured, this feature allows user to configure DTMF digits to send after 'OffHook auto-dial' call gets connected.
Proxy-Require	Determines a SIP Extension to notify the SIP server that the HT801/HT802 is behind a NAT/Firewall.
Use NAT IP	Defines NAT IP address used in SIP/SDP messages. It should only be used if required by ITSP.
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
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 RFC 3261 (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 Off Hook 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 **No**
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 (depends 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.
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**.
Ring Timeout	Stops ringing when incoming call if not answered within a specific period of time. Valid range is 0-300 seconds, 0 means no 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.
No Key Entry Timeout	Initiates the call within this time interval if no additional key entry during dialing stage. Valid range is 1-15 seconds. 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 responses (Incomplete Address). 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.

<table>
<tr><td>Use # as Dial Key</td><td>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.</td></tr>
<tr><td>Disable # as Redial Key</td><td>With this feature and feature ‘Use # as Dial Key’ set to Yes, the # key will act as dial key but not as redial key. Default No.</td></tr>
<tr><td>Dial Plan</td><td>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.
3. Default: Outgoing - { x+ | \+x+ | *x+ | *xx*x+ }
<u>Example of a simple dial plan used in a Home/Office in the US</u>:
{ ^1900x. | <=1617>[2-9]xxxxxx | 1[2-9]xx[2-9]xxxxxx | 011[2-9]x. |</td></tr>
</table>

	[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. As an example **{ *x+ }** will allow to dial * followed by any length of numbers.
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 Example of vendors: BroadSoft, CBCOM, RNK, Huawei, China Mobile, ZTE IMS, PhonePower, TELKOM SA, Vonage, Metaswitch, CenturyLink, MTS, TELEFONICA SPAIN, IZZ, Oi_BR, ROSTELECOM. Default is **Standard**.
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). Valid range is 90-64800 seconds. Default is **90** seconds.

Caller Request Timer	Uses session timer when making outbound calls if remote party supports it. 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. Default is **No**. To turn off Session Timer, select "No" for Caller and Callee Request Timer, and Force Timer.
UAC Specify Refresher	Specifies which end will act as refresher for outgoing calls. • **UAC**: The handy tone acts as the refresher. • **UAS**: Callee or proxy server act as the refresher. Default is **Omit**.
UAS Specify Refresher	Specifies which end will act as refresher for incoming calls: • **UAS**: The handy tone acts as the refresher. • **UAC**: Callee or proxy server act as the refresher. Default is **Omit**.
Force INVITE	Uses INVITE message to refresh the session timer. 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.
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**.
Preferred Vocoder	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, G722, 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. If set to Yes, HT8XX will remove /2 from offer. 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**.
VAD	Allows detecting the absence of audio and conserves bandwidth by preventing the transmission of "silent packets" over the network. 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**.
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-IINVITE after Fax Tone Detection Mode	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. Default is **Adaptive**.
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
Crypto Life Time	Adds crypto life time header to SRTP packets. Default is **Yes**.

SLIC Setting	Depends on standard phone type (and location).
Caller ID Scheme	Selects the caller ID scheme. For example: Bellcore/Telcordia, ETSI-FSK …
DTMF Caller ID	Defines the start and stop tones (Default, A, B, C, D or #) to delimit CID.
Disable Unknown Caller ID	This feature allows users to disable the analog phone's caller ID when the device receive a call with Anonymous, unavailable or unknown as FROM USER and without Display-INFO. Default **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 with "00". Default is **No**.
Polarity Reversal	Reverses the polarity upon call establishment and termination. Default is **No**.
Loop Current Disconnect	Allows the traditional PBX used with HT801/HT802 to apply this method for signaling call termination. Method initiates short voltage drop on the line when remote (VoIP) side disconnects an active call. Default is **No**.
Play busy/reorder tone before Loop Current Disconnect	Allows 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 topic above. HT80X supports a duration range from 100 to 10000 ms. 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 and New Zealand 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. HT801/HT802 supports 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. HT801/HT802 supports 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 (i.e., 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 will per call base. Recommended for FAX/Data calls. Default is **No**.
Disable Network Echo Suppressor	Disables the NEC will per call base. Recommended for FAX/Data calls. Default is **No**.
Outgoing Call Duration Limit	Defines the call duration limit for the outgoing calls. Valid range is 0-180 minutes. Default is **0 (No limit)**.
Ring Frequency	Customizes ring frequency. Valid options: 20Hz – 25Hz. Default is **20**Hz.
Enable High Ring Power	Configures a high ringing voltage output for the HT801/802.
OnHook DC Feed Current	Adjust DC feed current.
RFC2833 Events Count	This feature allows users to customize the count of RFC2833 events. Valid range is 2 – 10. Default is **8**.
RFC2833 End Events Count	This feature allows users to customize the count of RFC2833 end events. Valid range is 2 – 10. Default is **3**.
Distinctive Ring Tone	Customizes the Ring Tone 1 to 10 with associate caller ID: when selected, if caller ID is configured, then the device will ONLY use this ring tone when the incoming call is from the Caller ID. System Ring Tone is used for all other calls. When selected but no Caller ID is configured, the selected ring tone will be used for all incoming calls using the FXS port. Distinctive ring tones can be configured not only for matching a whole number, but also for matching prefixes. In this case symbol “x+” will be used. **For example**: If configured as 617x+, Ring Tone 1 will be used in case of call arrived from the area code 617. Any other incoming call will ring using cadence defined in parameter System Ring Cadence located under Advanced Settings Configuration page. **Note:** If server supports Alert-Info header and standard ring tone set (Bellcore) or distinctive ring tone 1-10 is specified, then the ring tone in the

	Alert-Info header from server will be used. Bellcore rings and tones are independent from custom ring tones. The custom ring tones can also be specified by alert-info header, for example *Alert-Info: ;info=ring5*
Ring tones	Configures the ring tone cadence preferences. User has 10 choices. *(Syntax: c=on1/off1-on2/off2-on3/off3;)* Note: The configuration, completed in Distinctive Ring Tones block in the same page, applies to ring tones cadences configured here. Default is **c=2000/4000;**
Distinctive Call Waiting Tone	Customizes the Call Waiting Tone 1 to 10 with associate caller ID: when selected, if caller ID is configured, then the device will ONLY use this call waiting tone when the incoming call waiting is from the Caller ID. When selected but no Caller ID is configured, the selected call waiting tone will be used for all incoming waiting calls using the FXS port. Distinctive Call Waiting Tones can be configured not only for matching a whole number, but also for matching prefixes. In this case symbol "x+" will be used. **For example**: If configured as 617x+, Call Waiting Tone 1 will be used in case of waiting call arrived from the area code 617. Any other incoming call waiting will be using cadence defined in parameter Call Waiting Tone located under Advanced Settings Configuration page.
Call Waiting Tones	This feature allows user to customize call waiting tone. User has 10 choices. *Syntax: f1=val[,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]];* (Frequencies are in (300, 3400) Hz and cadence on and off are in (0, 64000) ms) Note: The configuration, completed in Distinctive Call Waiting Tones block in the same page, applies to call waiting cadences configured here. Default is **f1=440@-13,c=300/10000;**
Call Features Settings	
Enable Call Features	When enabled, Do Not 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: Default is **16**

	- Disable SRTP: Default is **17**
SRTP per call Feature	- Enable SRTP per call: Default is **18** - Disable SRTP per call: Default is **19**
CID Feature	Allow users to customize the CID feature codes. Default is **Yes** - Enable CID: Default is **31** - Disable CID: Default is **30**
CID per call Feature	- Enable CID per call: Default is **82** - 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: Default is **47**
CW Feature	Allow users to customize the CW feature codes. Default is **Yes** - Enable CW: Default is **51** - Disable CW: Default is **50**
CW per call Feature	- Enable CW per call: Default is **71** - Disable CW per call: Default is **70**
Call Return Feature	Allow users to customize the Call Return feature code. Default is **Yes** - Call return: Default is **69**
Unconditional Forward Feature	Allow users to customize the Unconditional Forward feature codes. Default is **Yes** - Enable Unconditional Forward: Default is **72** - Disable Unconditional Forward: Default is **73**
Busy Forward Feature	Allow users to customize the Busy Forward feature codes. Default is **Yes** - Enable Busy Forward: Default is **90** - Disable Busy Forward: Default is **91**
Delayed Forward Feature	Allow users to customize the Delayed Forward feature codes. Default is **Yes** - Enable Delayed Forward: Default is **92** - Disable Delayed Forward: Default is **93**
Paging Feature	Allow users to customize the Paging feature code. Default is **Yes** - Paging: Default is **74**
DND Feature	Allow users to customize the CW feature codes. Default is **Yes** - Enable DND: Default is **78** - Disable DND: Default is **79**

Blind Transfer Feature	Allow users to customize the Blind Transfer feature code. Default is Yes - Enable Blind Transfer: Default is **87**
Disable LEC per call Feature	Default is **Yes** - Disable LEC per call: Default is **03**
Disable Bellcore Style 3-Way Conference	Gives the users the possibility of making conference calls by pressing "Flash" key, when it is enabled by dialing *23 +second callee number. Default is **No**
Star Code 3WC Feature	Default is **Yes** - Star Code 3WC: Default is **23**
Forced Codec Feature	Allow users to customize the Forced Codec feature code. Default is **Yes** **-** Forced Codec: Default is **02**
PCMU Codec Feature	Default is **Yes** - PCMU Codec: Default is **7110**
PCMA Codec Feature	Default is **Yes** - PCMA Codec: Default is **7111**
G723 Codec Feature	Default is **Yes** - G723 Codec: Default is **723**
G729 Codec Feature	Default is **Yes** - G729 Codec: Default is **729**
iLBC Codec Feature	Default is **Yes** - iLBC Codec: Default is **7201**
G722 Codec Feature	Default is **Yes** - G722 Codec: Default is **722**

NAT Settings

If you plan to keep the handy tone within a private network behind a firewall, we recommend using STUN Server. The following three settings are useful in the STUN Server scenario:

1. STUN Server (under advanced settings webpage) enter a STUN server IP (or FQDN) that you may have or look up a free public STUN server on the internet and enter it on this field. If using public IP, keep this field blank.
2. Use random SIP/RTP ports (under advanced settings webpage), this setting depends on your network settings. Generally, if you have multiple IP devices under the same network, it should be set to Yes. If using a public IP address, set this parameter to No.

3. NAT traversal (under FXS web page): Set to “Yes” when gateway is behind firewall on a private network.

DTMF Methods

The HT801/HT802 support the following DTMF mode:

- DTMF in-audio
- DTMF via RTP (RFC2833)
- DTMF via SIP INFO

Set priority of DTMF methods according to your preference. This setting should be based on your server DTMF setting.

Preferred Vocoder (Codec)

The HT801/HT802 support following voice codecs. On FXS ports pages, choose the order of your favorite codecs:

- PCMU/A (or G711µ/a)
- G729 A/B
- G723.1
- G726
- iLBC
- OPUS
- G722

Configuring HT801/HT802 Through Voice Prompts

As mentioned previously, The HT801/HT802 has a built-in voice prompt menu for simple device configuration.

Please refer to “Understanding HT801/HT802 Interactive Voice Prompt Response Menu” for more information about IVR and how to access its menu.

- **DHCP MODE**

  Select voice menu option 01 to enable HT801/HT802to use DHCP.

- **STATIC IP MODE**

  Select voice menu option 01 to enable HT801/HT802 to use STATIC IP mode, then use option 02, 03, 04, 05 to set up IP address, Subnet Mask, Gateway and DNS server respectively.

- **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, HTTP, HTTPS, FTP and FTPS. Default is HTTPS.

- **FIRMWARE UPGRADE MODE**

  Select voice menu option 17 to choose firmware upgrade mode among the following three options: 1) Always check, 2) check when pre/suffix changes, and 3) never upgrade.

Register a SIP Account

The HT801/HT802 supports 2 FXS ports which can be configured with 2 SIP accounts. Please refer to the following steps in order to register your accounts via web user interface:

1. Access your HT801/HT802 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **FXS Port (1** or **2)** pages.
5. In **FXS Port** tab, set the following:
   a. **Account Active** to **Yes.**
   b. **Primary SIP Server** field with your SIP server IP address or FQDN.
   c. **Failover SIP Server** with your Failover SIP Server IP address or FQDN. Leave empty if not available.
   d. **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.
   e. **Outbound Proxy:** Set your Outbound Proxy IP Address or FQDN. Leave empty if not available.
   f. **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.
   g. **Authenticate ID**: SIP service subscriber's Authenticate ID used for authentication. Can be identical to or different from SIP User ID.
   h. **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.
   i. **Name**: Any name to identify this specific user.

For more information, related to above options please refer to FXS Port Settings.

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

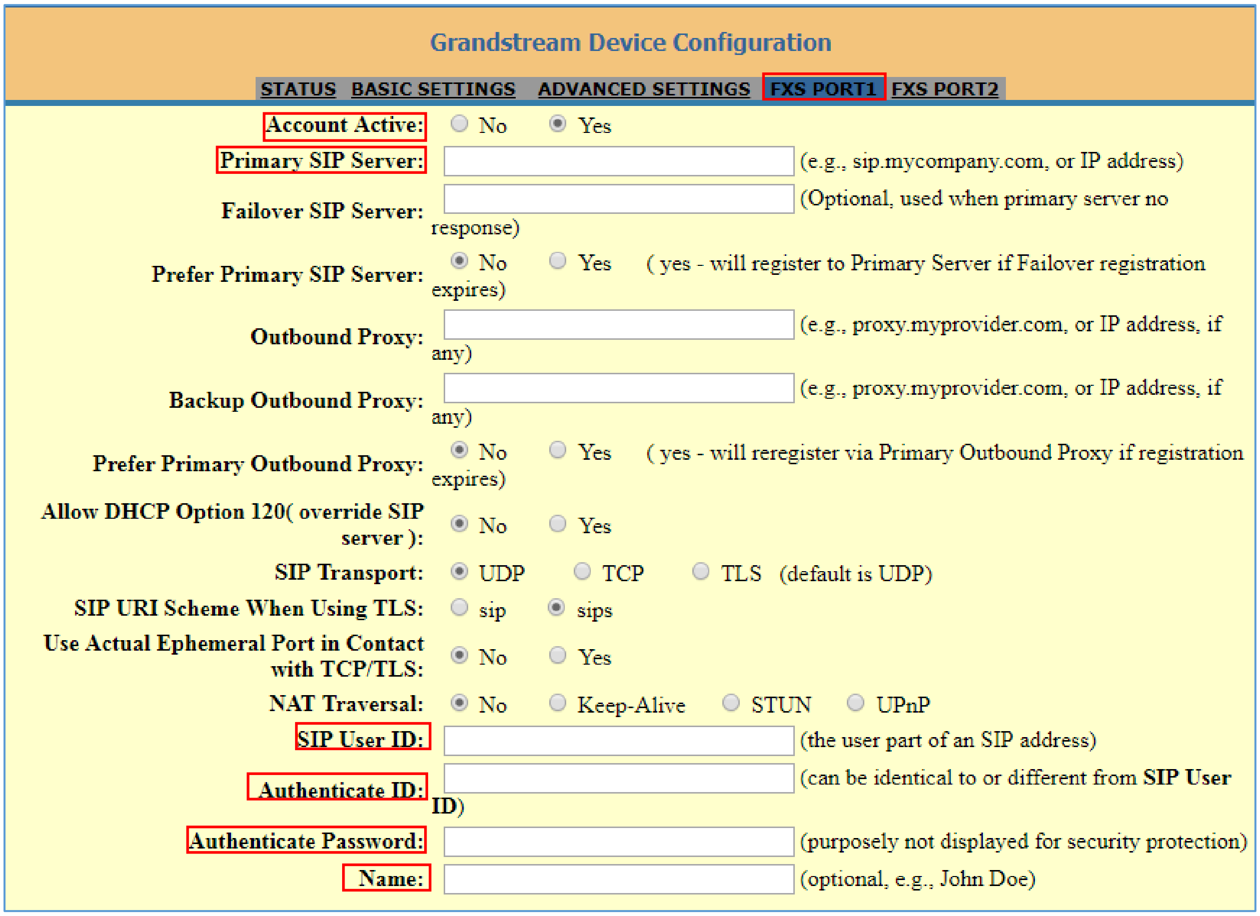

Figure 11: SIP Accounts Settings

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 or from your HT801/HT802 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).

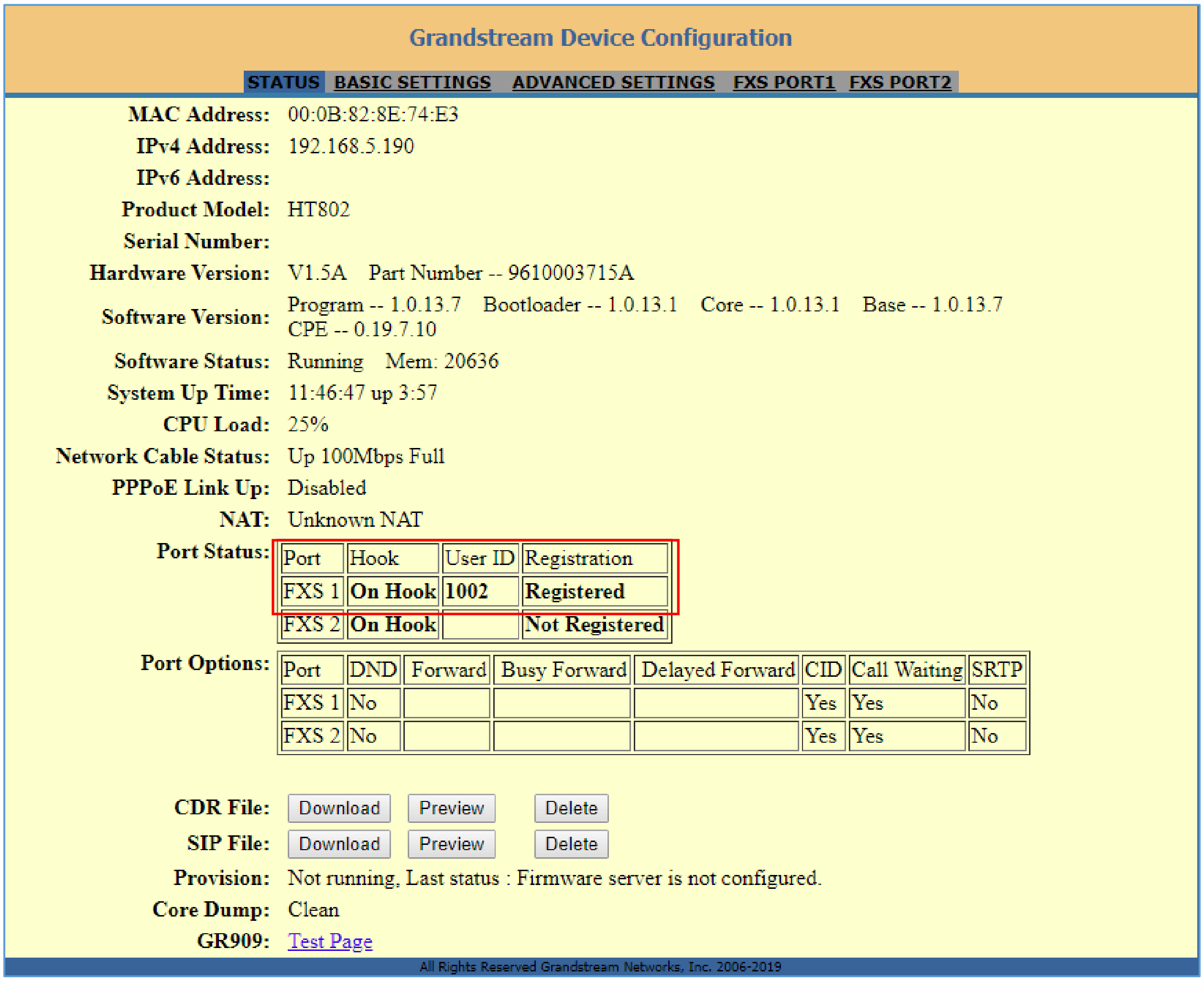

Figure 12: Account Status

Note: When all the FXS ports are registered (for HT802), the simultaneous ring will have one second delay between each ring on each phone.

Call Features

The HT801/HT802 support all the traditional and advanced telephony features.

Table 11: HT801/HT802 Call Features

Key	Call features
*02	**Forcing a Codec** (per call) *027110 (PCMU), *027111 (PCMA), *02723 (G723), *02729 (G729), *027201 (iLBC). *02722 (G722).
*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.

Rebooting HT801/HT802 from Remote

Press the “Reboot” button at the bottom of the configuration menu to reboot the ATA 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 HT801/HT802 can be upgraded via TFTP/HTTP/HTTPS/FTP/FTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS/FTP/FTPS server and selecting a download method. Configure a valid URL for TFTP or FTP/FTPS or HTTP/HTTPS (default is HTTPS); the server's 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 to upgrade the firmware version of your HT801/HT802:

1. Access your HT801/HT802 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **Advanced Settings→Firmware Upgrade and Provisioning** 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 HT802 to update the new firmware.

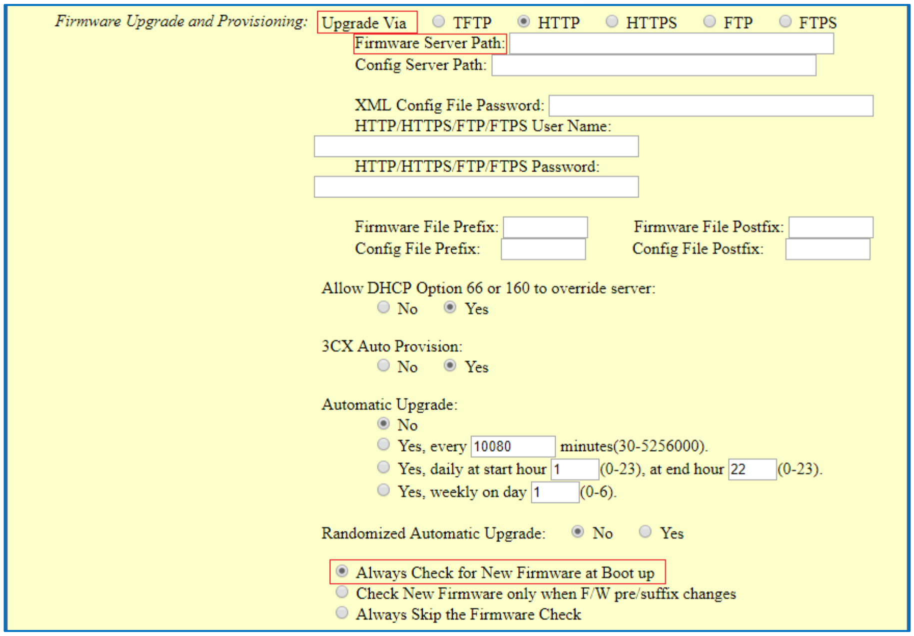

Figure 13: Firmware Upgrade Page

Upgrading via Local Directory

1. Download the firmware file from Grandstream web site;
2. Unzip it and copy the file into a folder in your PC;
3. From the HT801/HT802 web interface (Advanced Settings page) you can browse your hard drive and select the folder you previously saved the file (HT802fw.bin);
4. Click “Upload Firmware” and wait few minutes until the new program is loaded.

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

Upgrading via Local TFTP/HTTP/HTTPS/FTP/FTPS Servers

For users that would like to use remote upgrading without a local TFTP/HTTP/HTTPS/FTP/FTPS 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, for example, 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 HT801/HT802.

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 the 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 Config 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 to check if 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, FTP/FTPS or HTTP/HTTPS. The **Config Server Path** is the TFTP, 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 HT801/HT802 boots up or reboots, it will send a request to download a file named "cfgxxxxxxxxxxxx" followed by a configuration XML file named "cfgxxxxxxxxxxxx.xml", 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 and then download cfg<Model>.xml. The configuration file name should be in lower case letters.

HT801/HT802 supports DHCP option 67 allowing to provide custom name for the provisioning file. If DHCP option 67 is used, the following file download sequence will be applied:
Step 1: cfg<MAC>
Step 2: <option 67 bootfile> → cfg<MAC>.xml → cfg.xml → cfg<Model>.xml

Notes:

1. Only XML or binary config file formats are accepted.
2. The MAC header in XML config file should be the device MAC or needs to be removed completely.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- HT802 XML Provisioning Configuration -->
<gs_provision version="1">
   <mac>000B82B04B4E</mac>
 - <config version="2">
       <P855>0</P855>
       <P28107>0</P28107>
       <P730>0</P730>
       <P694>97</P694>
```

Figure 14: XML Config File - MAC Header

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

RESTORE FACTORY DEFAULT SETTINGS

⚠ **Warning:**

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

There are 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 HT801/HT802.
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:

Table 12: MAC Address Key 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

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

Reset from Web Interface (Reset Type)

1. Access your HT801/HT802 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
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.

Note:

- Factory Reset will be disabled if the "Lock keypad update" is set to "Yes".
- If the HT801/HT802 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.

Reset using SIP NOTIFY

1. Access your HT801/HT802 UI by entering its IP address in your favorite browser.
2. Go to **FXS Port.**
3. Set "Allow SIP Factory Reset" to "Yes".
4. Once a SIP NOTIFY with "event: reset" is received, the phone will perform factory reset.

Note: Received SIP NOTIFY will be first challenged for authentication purpose before taking factory reset action. The authentication can be done either using admin credentials (if no SIP account is configured) or using SIP account credentials.

EXPERIENCING HT801/HT802

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

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

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

Thank you again for purchasing Grandstream analogue telephone adapter, it will be sure to bring convenience to both your business and personal life.