Grandstream Networks, Inc.

HT818 - Administration Guide

The HT818 analog telephone adapter provide transparent connectivity for analog phones and faxes to the world of internet voice. Connecting to any analog phone, fax or PBX, the HT818 is an effective and flexible solution for accessing internet-based telephone services and corporate intranet systems across established LAN and internet connections. This Grandstream Handy Tones are a new addition to the popular Handy Tone ATA product family. This manual will help you to learn how to operate and manage your HT818 analog telephone adaptor and make the best use of their many upgraded features including simple and quick installation, 3- way conferencing, direct IP-IP Calling, and new provisioning support among other features. The HT818 is very easy to manage and configure, and it is specifically designed to be an easy to use and affordable VoIP solution for both the residential user and the teleworker.

PRODUCT OVERVIEW

The HT818 is an 8 ports analog telephone adapter (ATA) that allow users to create a high-quality and manageable IP telephony solution for residential and office environments. Their 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 HT818 is an ideal ATA for individual use and for large scale commercial IP voice deployments since it permits small and medium businesses to create integrated IP and PSTN telephony systems that efficiently manage communication costs. HT818's inclusion of an integrated NAT router and dual 10/100/1000Mbps Ethernet WAN and LAN ports enables a shared broadband connection between multiple Ethernet devices as well as the extension of VoIP services to analog phones.

Feature Highlights

The following table contains the major features of the HT818:

 **HT818**	● Support dual 10/100/1000Mbps Ethernet port, 2 SIP profiles through 8 FXS ports ● Support 3-way voice conferencing. ● Support wide range of caller ID formats. ● Support advanced telephony features, including call transfer, call forward, call-waiting, do not disturb, message waiting indication, multi-language prompts, flexible dial plan and more. ● Support T.38 Fax for creating Fax-over-IP. ● 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. ● Strong AES encryption with security certificate per unit. ● GR-909 Line Testing Functionalities. ● Exceptional voice quality with wide-band HD codec.

HT818 Features at a Glance

HT818 Technical Specifications

The following table resumes all the technical specifications including the protocols/standards supported, voice codecs, telephony features, languages and upgrade/provisioning settings for the HT818.

Interfaces	
Telephone Interfaces	Eight (8) RJ11 FXS ports
Network	Two (2) 10/100/1000 Mbps Ethernet port (RJ45).

Interface	
LED Indicators	POWER, LAN, WAN, PHONE1, PHONE2, PHONE3, PHONE4, PHONE 5, PHONE 6, PHONE 7 and PHONE 8.
Factory Reset Button	Yes.
Voice, Fax, Modem	
Telephony Features	Caller ID display or block, call waiting, flash, blind or attended transfer, forward, hold, do not disturb, 3-way conference.
Voice Codecs	G.711 with Annex I (PLC) and Annex II (VAD/CNG), G.722, G.723.1, G.729A/B, G.726-32, 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	2 REN, up to 1km on 24AWG line
Caller ID	Bellcore Type 1 & 2, ETSI, BT, NTT, and DTMF-based CID.
Dial Methods	DTMF, Pulse
Disconnect Methods	Busy Tone, Polarity Reversal/Wink, Loop Current.
Signaling	
Network Protocols	TCP/IP/UDP, RTP/RTCP (RFC1889, 1890), HTTP/HTTPS, ARP/RARP, ICMP, DNS, DHCP, NTP, TFTP, SSH, Telnet, STUN (RFC3489, 5389), SIP (RFC3261), SIP over TCP/TLS, SRTP, SNMP, TR-069, IMS/3GPP, IPoE
QoS	Layer 2 (802.1Q VLAN, SIP/RTP 802.1p) and Layer 3 (ToS, Diffserv, MPLS), Traffic Shaping
DTMF Methods	In-audio, RFC2833 and/or SIP INFO.
Provisioning and Control	HTTP, HTTPS, FTP, FTPS, SSH, TFTP, TR-069, secure and automated provisioning using TR069, syslog.
Security	
Media	SRTP.
Control	TLS/SIPS/HTTPS.
Management	Syslog support, SSH, remote management using web browser.
Physical	
Universal Power Supply	Input: 100-240VAC, 50-60Hz Output: 12V/1.5A.
Environmental	Operational: 32o – 104oF or 0º – 40ºC. Storage: 14o – 140oF or -10º – 60ºC.

	Humidity: 10 – 90% Non-condensing.
Dimensions and Weight	Dimension : 36 x 120 x 180 mm (H x W x D) Weight: 356g
Compliance	
Compliance	FCC/CE/RCM.

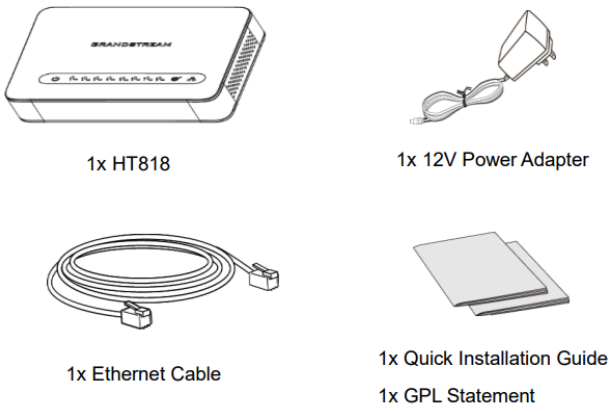
HT818 Technical Specifications

GETTING STARTED

This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the HT818.

Equipment Packaging

The HT818 ATA package contains

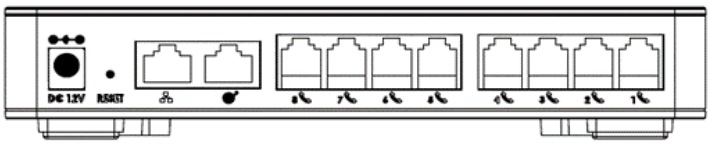


HT818 Package Contents

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

HT818 Ports Description

The following figure describes the different ports on the back panel of the HT818.



HT818 Back Panel

Phone 1- 8 (HT818)	Connects the analog phones / fax machines to the phone adapter using an RJ-11 telephone cable.
WAN	Connects the phone adapter to your router, switch or modem using an Ethernet RJ45 network cable.
LAN	Connects the phone adapter to your PC or switch using an Ethernet RJ45 network cable.

DC Power	Connects the phone adapter to PSU (12V – 1.5A).
Reset	Factory reset button. Press for 7 seconds to reset factory default settings.

Definition of the HT818 Connectors

Connecting HT818

The HT818 is designed for easy configuration and easy installation, to connect your HT818, please follow the steps below:

Scenario 1: Connecting the HT818 using WAN Port

When connecting HT818 using the WAN port, it will act as simple DHCP Client.

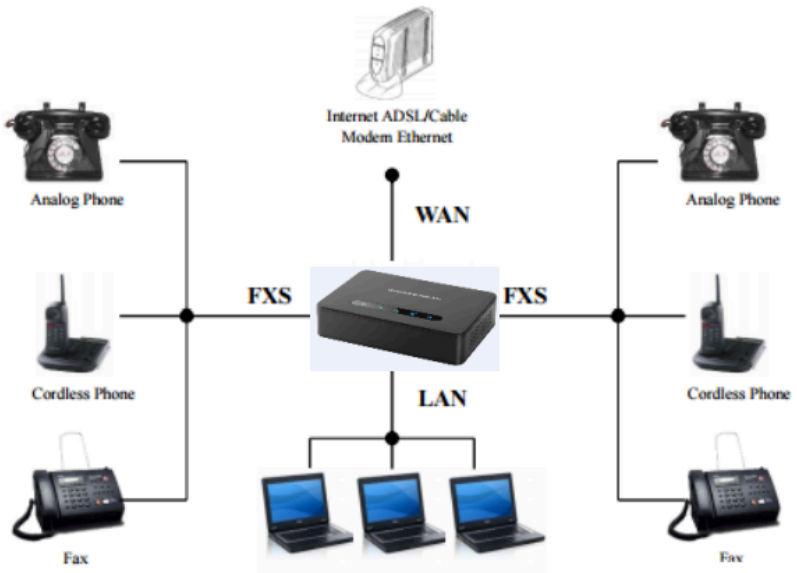
1. Insert a standard RJ11 telephone cable into the phone ports and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect the WAN port of the HT818 to a router, switch or modem using an Ethernet cable.
3. Insert the power adapter into the HT818 and connect it to a wall outlet and make sure to respect the technical specifications of the power adapter used.
4. Power, WAN and Phone LEDs will be solidly lit when the HT818 is ready for use.

Scenario 2: Connecting the HT818 using LAN Port

When connecting the HT818 using the LAN port, it will act as a router and DHCP serving addresses, the devices connected with HT818 LAN will pull DHCP addresses from your HT818.

1. Insert a standard RJ11 telephone cable into the phone ports and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect a computer or switch to the LAN port of the HT818 using an Ethernet Cable.
3. Insert the power adapter into the HT818 and connect it to a wall outlet and make sure to respect the technical specifications of the power adapter used.
4. Power, LAN and Phone LEDs will be solidly lit when the HT818 is ready for use.

> Please make sure to enable NAT Router under Web GUI → Basic Settings →Device Mode.



HT818 LEDs Pattern

There are four (4) LED types that help you manage the status of your HT818.

HT818 LEDs Pattern

LED Lights	Status
Power LED	The Power LED lights up when The HT818 is powered on and it flashes when the HT818 is booting up
WAN LED	The WAN LED lights up when The HT818 is connected to your network through the WAN port.
LAN LED	The LAN LED lights up when The HT818 is connected to your network through the LAN port.
Phone LED 1- 8	The phone LEDs indicate status of the respective FXS port-phone on the back panel ● OFF – Unregistered ● ON (Solid Blue) – Registered and Available List Item 2 ● Blinking every 500 ms – Off-Hook / Busy ● Slow blinking – FXS LEDs indicates voicemail

HT818 LEDs Pattern Description

CONFIGURATION GUIDE

The HT818 can be configured via one of two ways:

- The IVR voice prompt menu.
- The Web GUI embedded on the HT818 using PC's web browser.

Obtain HT818 IP Address via Connected Analogue Phone

HT818 is by default configured to obtain the IP address from DHCP server where the unit is located. In order to know which IP address is assigned to your HT818, 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 (FXS) of your HT818.
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 HT818 Interactive Voice Prompt Response Menu

The HT818 has 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 HT818. Pick up the handset and dial "***" to use the IVR menu.

Menu	Voice Prompt	Options
Main Menu	"Enter a Menu Option"	Press "*" for the next menu option Press "#" to return to the main menu Enter 01-05, 07,10, 12-17,47 or 99 menu options
01	"DHCP Mode", "Static IP Mode" "PPPoE Mode"	Press "9" to toggle the selection If using "Static IP Mode", configure the IP address information using menus 02 to 05. If using "Dynamic IP Mode", all IP address information comes from the DHCP server automatically after reboot. If using "PPPoE Mode", configure PPPoE Username and Password from web GUI to get IP from your ISP.
02	"IP Address " + IP address	The current WAN IP address is announced If using "Static IP Mode", enter 12-digit new IP address. You need to reboot your HT818 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. Note: The device has two MAC addresses. One for the WAN port and one for the LAN port. The device MAC address announced is the address of LAN port.
12	WAN Port Web Access	Press "9" to toggle between enable / disable. Default is disabled.
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/HTTP /FTP/FTPS
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.
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)
	“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

Voice Prompt Menu

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.
- Dial *98 to announce the extension number of the port.

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

Configuration via Web Browser

The HT818 embedded Web server responds to HTTP GET/POST requests. Embedded HTML pages allow a user to configure the HT818 through a web browser such as Google Chrome, Mozilla Firefox and Microsoft’s IE.

- **Microsoft Internet Explorer:** version 10 or higher.
- **Google Chrome**: version 58.0.3 or higher.

- **Mozilla Firefox**: version 53.0.2 or higher.
- **Safari**: version 5.1.4 or higher.
- **Opera**: version 44.0.2 or higher.

Accessing the Web UI

- **Via WAN port**

For the initial setup, the Web access is by default enabled when the device is using private IP and disabled when using public IP, and you cannot access the Web UI of your HT818 until it's enabled, the following steps will show you how to enable it via IVR.

1. Power your HT818 using PSU with the right specifications.
2. Connect your analog phone to phone ports (FXS) of your HT818.
3. Press *** (press the star key three times) to access the IVR menu and wait until you hear "Enter the menu option ".
4. Press 12, the IVR menu will announce that the web access is disabled, press 9 to enable it.
5. Reboot your HT818 to apply the new settings.

Please refer to steps below if your HT818 is connected via WAN port:

1. You may check your HT818 IP address using the IVR on the connected phone.

Please see Obtain the HT818 IP address via the connected analogue phone

2. Open the web browser on your computer.
3. Enter the HT818's IP address in the address bar of the browser.
4. Enter the administrator's password to access the Web Configuration Menu.

> The computer must be connected to the same sub-network as the HT818. This can be easily done by connecting the computer to the same hub or switch as the HT818.

- **Via LAN port**

Please refer to steps below if your HT818 is connected via LAN port:

1. Power your HT818 using PSU with the right specifications.
2. Connect your computer or switch directly to your HT818 LAN port.
3. Open the web browser on your computer.
4. Enter the default LAN IP address (192.168.2.1) in the address bar of the browser.
5. Enter the administrator's password to access the Web Configuration Menu.
6. Make sure to reboot your device after changing your settings to apply the new configuration.

> Please make sure that your computer has a valid IP address on the range 192.168.2.x so you can access the web GUI of your HT818.

Web UI Access Level Management

There are two default passwords for the login page:

User Level	User	Password	Web Pages Allowed

End User Level	user	123	Only Status and Basic Settings
Administrator Level	admin	admin	Browse all pages
Viewer Level	viewer	viewer	View all pages. No changes allowed.

Note

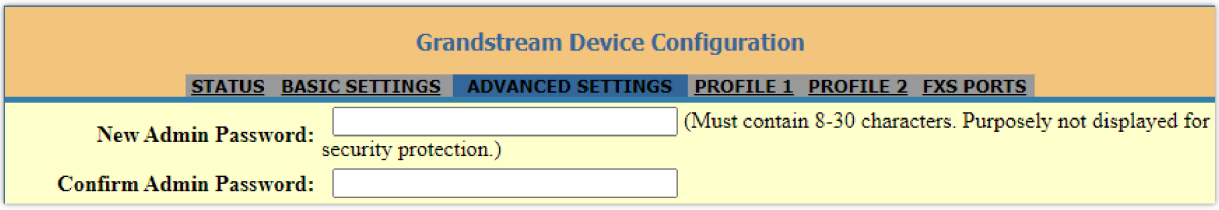
- The password is case-sensitive and must contain 8-30 characters,When changing any settings, always submit them by pressing Update or Apply button at the bottom of the page. After submitting the changes in all the Web GUI pages, if a reboot is required, the web page will prompt the user to reboot by offering a reboot button on the web page.
- The user and viewer level access is disabled by default, to enable it,go under **Advanced Settings.**
- After initial login using the default admin password, the user will be prompted to change the password immediately.

Saving the Configuration Changes

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

Changing Admin Level Password

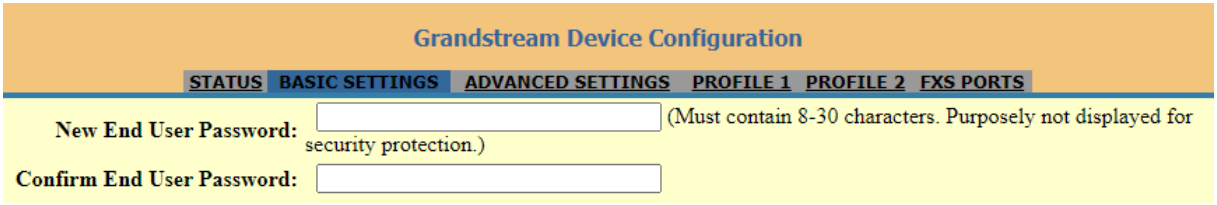
1. Access your HT812/HT814 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **Advanced Settings → New Admin Password** and enter the new admin password.
5. Confirm the new admin password.
6. Press **Apply** at the bottom of the page to save your new settings.



Admin Level Password

Changing User Level Password

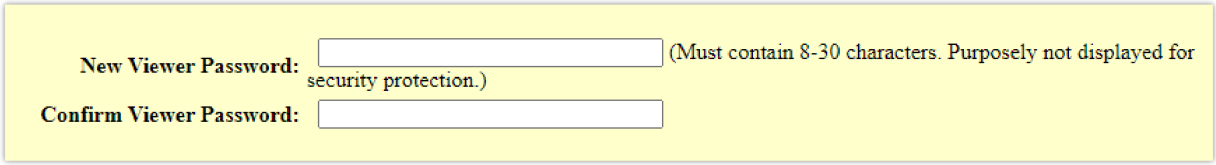
1. Access your HT812/HT814 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **Basic Settings → New End User Password** and **e**nter the new end-user password.
5. Confirm the new end-user password.
6. Press **Apply** at the bottom of the page to save your new settings.



User Level Password

Changing Viewer Password

1. Access your HT812/HT814 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.



Viewer Level Password

Web Configuration Pages Definitions

This section describes the options in the HT818 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.
- **Profile (1, 2):** Configures the SIP Server, SIP Registration, NAT settings, call features, ring tones.
- **FXS Ports:** Configures SIP accounts settings, Off hook Auto-dial.

Status Page Definitions

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. **Note:** The device has two MAC addresses, one for the WAN port and one for the LAN port. The MAC address located on the bottom panel of the device is the MAC address of LAN port. The MAC address of WAN port is MAC address of LAN port +1. Example: MAC Address: WAN – "00:0B:82:25:AF:32", LAN – "00:0B:82:25:AF:31".
WAN IPv4 Address	Displays assigned IPv4 address.
WAN IPv6 Address	Displays assigned IPv6 address.
Product Model	Displays product model info. Default is HT818.
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 HT818. **Bootloader:** Specifies Boot version. **Core:** Specifies Core version. **Base:** Specifies Base version. **CPE:** Specifies CPE version. CPE version is displayed only when HT818 is connected to an ACS using TR-069 protocol.
Software Status	Indicates the current software status of the HT (Running or Stopped).
System Up Time	Indicates actual system time and uptime since last reboot.
CPU Load	Indicates CPU load (%)
Network Cable Status	Indicates status of the cable (Up/Down) and speed information of the connection (Full/Half). Up/Down means cable connected/disconnected. Full/Half means full duplex/half duplex.
PPPoE Link Up	Indicates PPPoE connection status.
NAT	Indicates type of NAT when it's configured.
Port Status	Displays relevant information regarding the FXS ports about their registration, current status and their appropriate User ID.
Port Options	Displays relevant information regarding the FXS ports about their DND and call forward features.
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.

Status Page Definitions

Basic Settings Page Definitions

Basic Settings	
New End User Password	Configures user-level password. Case sensitive and max. Length of 20 characters. **Note:** The new Password must contain 8-30 characters, at least one number, one uppercase, and a lowercase letter. Purposely not displayed for security reasons.
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 20 characters. **Note:** The new Password must contain 8-30 characters, at least one number, one uppercase, and a lowercase letter. Purposely not displayed for security reasons.
Confirm Viewer Password	Re-enter the viewer password to confirm change viewer password on web GUI to avoid typo

	or mistakes.
Web/SSH Access	
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.
Web Lockout Duration	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.
Security Controls for SSH/Telnet Access	Allows the user to choose the security control for SSH or Telnet Access, the options can be : 1. Only allow SSH private IP users to set system Pvalue. 2. Allow all SSH users to set system Pvalue. 3. Allow all SSH users to set any Pvalue. 4. Allow any user to set any Pvalue. 5. Prohibit setting Pvalue. By default , it is set to "Allow any user to set any Pvalue".
WAN Side Web/SSH Access	Enables / Disables the Web and SSH access through the WAN port. The available options are the following: ● **No**: No access to the web or SSH from any IP address on the WAN side. ● **Yes**: Access for the Web GUI and SSH is enabled on the WAN side. ● **Auto**: Only private IP could access the web or SSH on the WAN side. Default setting is **Auto**.
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 mod**e: 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”
Enable SNMP Through Management Interface	This feature allows users to route SNMP packets through management interface. Default setting is No.

Enable TR-069 Through Management Interface	This feature allows users to route TR-069 packets through the management interface. Default setting is No.
Enable Syslog Through Management Interface	This feature allows users to route Syslog packets through the management interface. Default setting is No.
Enable RADIUS Through Management Interface	This feature allows users to configure the management interface by RADIUS. Default setting is No.
Management Interface IPv4 Address	Configures Voice VLAN Type : ● Default is **dynamically assigned via DHCP** Or, ● **statically configured** as: ○ IP Address : Default is **192.168.100.100** ○ Subnet Mask : Default is **255.255.255.0** ○ Default Router : Default is **192.168.100.1** ○ 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.
NAT/DHCP Server Information & Configuration	
Device Mode	Controls whether the device works in NAT router mode, Bridge mode, or WAN-only mode. ● **NAT Router Mode:** ATA acts as a router, assigns private IPs, and performs address translation for connected devices. ● **Bridge Mode:** ATA operates as a transparent bridge, converting analog voice to digital packets without IP routing. ● **WAN Only Mode:** ATA acts as a network client, relying on an external router for IP routing and address translation. By default it is set to NAT Router Mode.
NAT maximum ports	Defines the number of ports that can be managed while in NAT router mode. Range: 0 – 4096, default is 1024. Typically, one port per connection.
NAT TCP timeout	NAT TCP idle timeout in seconds. Connection will be closed after preconfigured, timeout if not refreshed. Range: 0 – 3600
NAT UDP timeout	NAT TCP idle timeout in seconds. Connection will be closed after preconfigured, timeout if

	not refreshed. Range: 0 – 3600, default is 300
Uplink bandwidth	Specifies the maximum uplink bandwidth permitted by the device. This function is disabled by default. The total bandwidth can be set as: 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M or 15M. The primary function of this setting is to limit the uplink bandwidth for the device internal system, signaling and NATed traffic. Example: When 512k is configured, there will be at least 512kbps limited for internal system, signaling and NATed traffic. Voice or RTP stream will never be limited.
Downlink bandwidth	Specifies the maximum downlink bandwidth permitted by the device. This function is disabled by default. The total bandwidth can be set as: 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M or 15M. The primary function of this setting is to limit the download bandwidth for the device internal system, signaling and NATed traffic. Example: if 128 is configured, there will be at least 128kbps limited for internal system, signaling and NATed traffic. Voice or RTP stream will never be limited.
Enable UPnP support	When set to "Yes", the HT812/HT814 acts as an UPnP gateway for your UPnP enabled applications. **UPnP = "Universal Plug and Play"**
Reply to ICMP on WAN port	Default is No. When set to "Yes", the HT812/HT814 responds to the PING command from other computers, but is also made vulnerable to DOS attacks.
Cloned WAN MAC Addr	This allows the user to change/set a specific MAC address on the WAN interface. *Note:* Set in Hex format
LAN Port VLAN Feature Under Bridge Mode	Allows users to configure the customized VLAN tag and priority value under switch mode. VLAN Tag range is 0-4094, the Priority Vlaue range is 0-7. The Default for both is 0
Enable LAN DHCP	When set to "Yes", device will function as a simple router and LAN port will provide IP addresses to internal network. Connect the WAN port to ADSL/Cable modem or any other equipment that provides access to public Internet
LAN DHCP Base IP	Base IP Address for a LAN port. Default factory setting is 192.168.2.1. Note: When the device detects WAN IP is conflicting with LAN IP, the LAN base IP address will be changed based on the network mask — the effective subnet will be increased by 1. For example; 192.168.2.1 will be changed to 192.168.3.1 if net mask is 255.255.255.0. Then the device will reboot
LAN DHCP Start IP	Default value is 100. The last segment of IP address assigned to the HT812/HT814 in the LAN Network. Default configuration assigns IP address (to local network devices) starting from 192.168.2.100.
LAN DHCP End IP	Default value is 199. This parameter allows a user to limit the number of local network devices connected to the internal router. Default configuration assigns IP address (to devices connected to the LAN port) in a range from 192.168.2.100 up to 192.168.2.199.
LAN Subnet Mask	Sets the LAN subnet mask. Default value is 255.255.255.0
DHCP IP Lease Time	Default value is 120 hrs (5 days). The length of time the IP address is assigned to the LAN clients. Value is set in units of hours.
DMZ IP	This function forwards all WAN IP traffic to a specific IP address if no matching port is used by HT812/HT814 or in the defined port forwarding.

Port Forwarding	Forwards a matching (TCP/UDP) port to a specific LAN IP address with a specific (TCP/UDP) port. Up to 8 rules are available.
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 ISP (Internet Service Provider) configuration which may affect the IP address will be reseted (including WAN static IP). ● **VOIP Data Rese**t: All VoIP related configuration (mainly everything located on FXS page). ● **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.

Basic Settings Page

Advanced Settings Page Definitions

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. The password field is purposely left blank for security reasons after clicking update and saved. **Note:** The new Password must contain 8-30 characters. Purposely not displayed for security reasons
Confirm Admin Password	Confirms the new admin password.
Disable User Level Web Access	Disables User Level Web Access. This option is enabled by default.
Disable Viewer Level Web Access	Disables Viewer Level Web Access. This option is enabled by default.
Enable strict password rules	This feature allows users to enable or disable the strict password rules, set the minimum password length, set the required number of character classes, and select the allowed character classes. Enabled by Default.
Minimum password length	Sets the Minimum Password Length. Valid Range is 4-30, Default is 8
Required number of character classes	Sets the required number of character classes. Valid Range is 0-4, Default is 3.
Allowed Character classes	Defines the number of Allowed Charcter classes, this includes Lower case , Upper case, Numbers and Special characters, Default is 7.
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.
Provision and upgrade to new Gen-2 certificate	Configures whether or not to upgrade to a new Gen-2 certificate, It is set to no upgrade by Default.
Firmware Server Path	Sets IP address or FQDN of firmware server. The URL of the server that hosts the firmware release. **Note:** You can specify the protocol used in the Firmware Server Path. (example: https://192.168.5.120), this will bypass the "Upgrade Via" method. 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 HT8xx. Users can also add the variable **$PN** and **$MAC** in Config Server Path. **$PN** refers to the **Product Model**, and **$MAC** is equivalent to the **MAC address**. **- Example 1:** 192.168.5.74/$PN **$PN** will be replaced with the ATA's model (HT818) **- Example 2:** 192.168.5.74/$MAC **$MAC** will be replaced with the ATA's MAC address (e.g. 000b82a688a4) **Note:** You can specify the protocol used in the Config Server Path. (example: **https:**//192.168.5.120), this will bypass the "Upgrade Via" method. 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.
Enable using tags in URL	Allows users to configure variables on the configuration server path to differentiate the directories on the server.
Always send HTTP Basic Authentication Information	Default is No. If set to Yes, The device will send configured user name and password within HTTP request before server sends authentication challenge.
Allow DHCP Option 66 or 160 to Override Server	Obtains configuration and upgrade server's information using options 66 from DHCP server. Note: If DHCP Option 66 is enabled, the HT8xx will attempt downloading the firmware file from the server URL provided by DHCP, even though Config Server Path is left blank. The server URL provided by DHCP can include authentication credentials using following format: "username:password@Provisioning_Server_IP".
Additional Override DHCP Option	Allows users to enable the Additional Override DHCP Option in Option 150. The default value is "None".
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 HT8xx will only do an upgrade once at boot up. **Check every X minutes:** User needs to specify a period in minutes. **Check every day:** User needs to specify the start hour and the end hour of the day (0-23). **Check every week:** User needs to specify "Day of the week (0-6)". (Day of week is starting from Sunday). Default is No.
Randomized Automatic Upgrade	Randomized Automatic Upgrade within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s).
Always Check for New Firmware at Boot up	Configures the HT8xx to always search for the new firmware at boot up. During the boot stage, the HT8xx 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 HT8xx to search for the new firmware when the firmware prefix / suffix changes. When this option is selected, the HT8xx will check for updates only when the pre/suffix has been changed.
Always Skip the Firmware Check	Configures the HT8xxto skip the firmware check, when this option is selected the HT8xx will always skip searching for a new firmware.
Configuration File Types Allowed	Allows users to configure provision configuration file type in xml file only or all file types.
Download and Process All Available Config Files	This feature allows users to download and process all available config files. By default, the device will provision the first available config in the order of cfgMAC > cfgMAC.xml > cfgMODEL.xml > and cfg.xml (corresponding to device-specific, model-specific, and global configs). If this option is enabled, the device will inverse the downloading process to cfg.xml > cfgMODEL.xml > cfgMAC.bin > cfgMAC.xml and add cfgMAC_override.xml. The following files will override the files that have already been loaded and processed. The default value is "No"

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.
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
Root CA Version	Configures the Root CA version. can be set to either Current root or new root. Default Value is New Root.
SIP TLS Certificate	Specifies SSL certificate used for SIP over TLS is in X.509 format. The HT8xx has built-in private key and SSL certificate. Maximum supported length is 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 a custom CA certificate to manage client authentication.
Gen-2 EC private key	Configures the Gen-2 Elliptic Curve Private Key. based on RFC 5915. The Max value length is 8192 characters.
Enable TR-069	Sets the phone adapter system to enable the “CPE WAN Management Protocol” (TR-069). Default setting is Yes. **Note**: TR-069 supports XMPP (Extensible Messaging and Presence Protocol) based connection requests.
TR-069 firewall rules	Configures the TR-069 firewall rules , Value port range is 1-65535
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 HT8xx.
Connection Request Password	Enters password for ACS to connect to the HT8xx.
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	Enables/disables SNMP to allow users to retreive information about the device including local network information. Default setting 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	Allows you to enhance the security of your web-based resources by integrating RADIUS authentication and authorization. The default is No.
Action upon RADIUS Auth Server Error	Choose action upon RADIUS server error. Default is Authenticate Locally (Default Authenticate Locally)
RADIUS Auth Protocol	Configure RADIUS authentication protocol, the available options are: **PAP (Password Authentication Protocol):** PAP sends the username and password in plaintext, making it less secure than other methods. **CHAP (Challenge Handshake Authentication Protocol):** CHAP uses a challenge-response mechanism for authentication, enhancing security. **MsCHAPv1 (Microsoft Challenge Handshake Authentication Protocol version 1):** An older Microsoft-specific CHAP variant. **MsCHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2):** A more secure and improved Microsoft-specific CHAP variant with mutual authentication support. Default value is "PAP".
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. The default is UDP.
Enable OpenVPN® LZO Compression	Enable OpenVPN® LZO Compression. Default is Yes.
OpenVPN® Encryption	Select the OpenVPN® Encryption. Default is BF-CBC 128 bit (default key).
OpenVPN® 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
OpenVPN Additional Options	Configures the OpenVPN® additional options feature
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 Special Condition Tone	Using these settings, users can configure tone frequencies and cadence according to their preference. By default, they are set to North American frequencies. Configure these settings with known values to avoid uncomfortable high pitch sounds. ON is the period of ringing ("On time" in 'ms') while OFF is the period of silence. In order to set a continuous tone, OFF should be zero. Otherwise, it will ring ON ms and a pause of OFF ms and then repeat the pattern. Example configuration for N.A. Dial tone: 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. When a prefix number is configured under this feature, and a number with the same prefix is dialed, the whole dialed number will be sent. 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 “Overwrite”, device will clear the first CDR file and start storing again. When the feature is disabled the device will not record any calls. 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 “Overwrite”, 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 HT8xx to report the log level. Default is NONE. The level is one of EXTRA DEBUG, DEBUG, INFO, WARNING or ERROR. Syslog messages are sent based on the following events: 1. product model/version on boot up (INFO level) 2. NAT related info (INFO level) 3. sent or received SIP message (DEBUG level) 4. SIP message summary (INFO level) 5. inbound and outbound calls (INFO level) 6. registration status change (INFO level) 7. negotiated codec (INFO level) 8. Ethernet link up (INFO level) 9. SLIC chip exception (WARNING and ERROR levels) 10. memory exception (ERROR level) extra syslog style (EXTRA DEBUG level) 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.
With Secret Key Information	Allows users to make packet capture including the secret key to decrypt the captured TLS packets. Default value is No.
Information Capture	Allows the device to make a packet capture, by clicking the capture button, when that is set, the user can define the following: 1. **With Secret Key information:** Allows users to make packet capture including the secret key to decrypt the captured TLS packets., set to "No" By Default 2. **Status:** Set to "Idle" when the packet capture is not started and to "Running" when packet capture is enabled. 3. **Capture file:** stores the registered Captured file and make it ready for download.
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 the Download button to download the device configuration file to the local computer. The filename is “config.txt”. The file is plain text and not including password fields. **Note:** Device configuration can be exported through SSH by accessing the configuration menu (typing config on PuTTY) and typing the command "export". The P-values on the configuration are sorted in ascending order.
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. **Note:** Config File Download request starts from the file " cfgMAC.xml".
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), "ht81xfw.bin” for HT812/HT814 or "ht818fw.bin” for HT818.

Upload Configuration	Press the Upload from the local directory button to load the configuration file to the device from your computer. The configuration file can be an XML or a TXT file (for instance: “config.xml”, “config.txt”). **Note:** The field <mac> is not mandatory in the document, but only devices with a specified MAC address will accept the configuration file if available.
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.
E911/HELD Protocol:	
Enable E911	Enable Enhanced 911 call. Default is disabled
HELD Protocol	Configure HELD transfer protocol. HTTP or HTTPS
HELD Synchronization Interval	The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when the interval is 0.
Location Server	Configure the primary Location Information Server (LIS) address
Location Server Username	Configure the user name of the primary Location Information Server (LIS)
Location Server Password	Configure the password of the primary Location Information Server (LIS)
Secondary Location Server	Configure the seconary Location Information Server (LIS) address
Secondary Location Server Username	Configure the user name of the secondary Location Information Server (LIS)
Secondary Location Server Password	Configure the password of the secondary Location Information Server (LIS)
HELD Location Types	Configure "locationType" element in the location request. "geodetic", "civic" and "location URI"
HELD NAI	Configure "locationType" element in the location request. "geodetic", "civic" and "location URI"
HELD Identity 1-10	HELD Identity
HELD Identity 1-10 Value	HELD Identity value
E911 Emergency Numbers	A user can configure multiple emergency numbers separated with the delimiter symbol ";".
Geolocation-Routing Header	If "Yes", E.911 INVITE message includes the "Geolocation-Routing" header with the value "Yes"
Priority Header	If "Yes", E.911 INVITE message includes the "Priority" header with the value "emergency"

Advanced Settings Page

Profiles Pages Definitions

Profiles (1,2)	
Profile Active	Activates / Deactivates the accounts. The FXS port configuration will not change if disabled, although the port will not be operational, in this state, there will be no dial tone when picking up the analog phone and making/receiving calls will not be possible.
Primary SIP Server	Configures SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). This is the primary SIP server used to send/receive SIP messages from/to HT81x.
Failover SIP Server	Defines failover SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6 fe80::20b:82ff:fe75:211d:). This server will be used if primary SIP server becomes unavailable.
Prefer Primary SIP Server	Selects to prefer primary SIP server. The account will register to the primary Server if registration with the Failover server expires. ● **Will register to Primary Server if Failover registration expires:** If failover server registration ends, the client reverts to the main server. ● **Will register to Primary Server if Primary Server responds, need to enable SIP OPTIONS/NOTIFY Keep-Alive:** Client registers with the main server if it's responsive, requiring keep-alive methods. ● **No:** The client doesn't prioritize the main SIP server**.** The default is No.
Outbound Proxy	Specifies IP address (Supports both IPv4 and IPv6 addresses) or domain name of outbound Proxy, or media gateway, or session border controller. (For example: proxy.myprovider.com, IPv4: 192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). It's Used by HT818 for firewall or NAT penetration in different network environments. If symmetric NAT is detected, STUN will not work and only outbound proxy can correct the problem
Backup Outbound Proxy	Configures the backup outbound proxy to be used when the "Outbound Proxy" registration fails. (For example: proxy.myprovider.com, or IP address, if any: IPv4: 192.168.5.170/ IPv6: fe80::20b:82ff:fe75:211d). By default, this field is left empty.
Prefer Primary Outbound Proxy	If the user configures this option to "Yes", when the registration expires, the device will re-register via primary outbound proxy. By default, this option is disabled.
From Domain	allows users to add the actual domain name, it will override the from header.This is an optional configuration.
Allow DHCP Option 120 (override SIP Server)	Configures the HT81x 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. Default 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, VPN, and Auto.

	● **No:** Disables NAT traversal, potentially causing connection issues for the ATA if it's behind a NAT router. ● **Keep-alive:** Periodically sends signals to maintain the NAT mapping for the ATA, preventing disconnection. ● **STUN:** Utilizes the STUN protocol to discover and adapt to NAT settings for seamless VoIP communication. ● **UPnP:** Allows the ATA to dynamically configure NAT port mappings, streamlining VoIP traffic. ● **VPN:** Requires the ATA to establish a secure VPN connection for VoIP, bypassing NAT restrictions. ● **Auto:** Automatically selects the most suitable NAT traversal method based on network conditions, ensuring reliable ATA connectivity. Default setting is No.
DNS Mode	Selects DNS mode to use for the client to look up server. One mode can be chosen. **A Record (Default):** resolves IP Address of target according to domain name. **SRV:** DNS SRV resource records indicate how to find services for various protocols. **NAPTR/SRV:** Naming Authority Pointer according to RFC 2915. **Use Configured IP:** If the SIP server is configured as domain name, device will not send DNS queries, but will use “Primary IP” or “Backup IP” to send SIP message if at least one of them is not empty. It will try to use “Primary IP” first, after 3 tries without any response, it will switch to “Backup IP 1”, then “Backup IP 2”, and then it will switch back to “Primary IP” after 3 retries.
DNS SRV use Registered IP	When the HT81x is registered using the second SRV record, making 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 when DNS Mode is SRV or NAPTR/SRV. • Default SIP request will always be sent to the address with the top priority based on the SRV query result, even if this address is different from the registered IP address. • Saved one until DNS TTL SIP request will always be sent to the registered IP address until DNS TTL expires or registered IP address is unreachable • Saved on until no response SIP request will always be sent to the registered IP address only until registered IP address is unreachable.
Failback 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 non-registration 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 HT81x 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.
Use Request Routing ID in SIP INVITE Header	If set to Yes, device will use the configured [Request URI Routing ID] in the SIP INVITE. This option is usually used under a SIP trunk account’s configuration. Default is No.
SIP Registration	Controls whether the HT81x 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.Unregister on reboot option can be set to "No", "All" or "Instance". 1. **Set to "No":** If the "Unregister on reboot" option is set to "No", it means that the SIP user's information will not be cleared when the device reboots. In other words, the SIP account will remain registered with the server even after the device is rebooted. 2. **Set to "All":** If the "Unregister on reboot" option is set to "All", it means that all SIP accounts associated with the device will be unregistered when the device reboots. This option clears the SIP user's information for all the FXS ports on the device. 3. **Set to "Instance":** If the "Unregister on reboot" option is set to "Instance", it means that only the SIP account associated with the concerned FXS port will be unregistered when the device reboots. This option clears the SIP user's information for only the specific FXS port that is affected by the reboot. Default value is set to "No"
Outgoing Call Without Registration	Enables the ability to place outgoing calls even if the account is not registered (if allowed by ITSP); device will not be able to receive incoming calls. Default is No.
Register Expiration	Refreshes registration periodically with specified SIP proxy (in minutes). Maximum interval is 65535 minutes (about 45 days). Default is 60 minutes (or 1 hour).
Reregister Before Expiration	Sends re-register request after specific time (in seconds) to renew registration before the previous registration expires.
SIP Registration Failure Retry Wait Time	Sends re-register request after specific time (in seconds) when registration process fails. Maximum interval is 3600 seconds (1 hour). Default is 20 seconds.
SIP Registration Failure Retry Wait Time upon 403 Forbidden	Sends re-register request after specific time (in seconds) when registration process fails with error 403 Forbidden. Maximum interval is 3600 seconds (1 hour). Default is 1200 seconds.
Port Voltage Off upon no SIP Registration or SIP Registration Failure	Allows users to configure the timer of Port Voltage Off. For Port Voltage Off upon no SIP, the Valid Range is 0 to 60 with the Default value being 0 (0 means the port voltage is never turned off)
Delay Time of Port Voltage Off Timer Since Boot	Allows users to set a delay time of FXS line voltage when there is no SIP registration. The valid Range is 0 to 60, and the Default value is 0.
Enable SIP OPTIONS/NOTIFY Keep Alive	Enables SIP OPTIONS or SIP NOTIFY to track account registration status so the ATA will send periodic OPTIONS/NOTIFY message to server to track the connection status with the server. Default setting is No.
SIP OPTIONS/NOTIFY Keep Alive Interval	Configures the time interval when the ATA send OPTIONS or NOTIFY message to SIP server. The default setting is 30 seconds, which means the ATA will send an OPTIONS/NOTIFY message to the server every 30 seconds. The default range is 1-64800.
SIP OPTIONS Keep Alive Max Lost	Defines the Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3.
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 HT81x 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 HT81x will listen and transmit. It is the HT81x 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 HT81x 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 HT81x are behind the same NAT. Default is No.
Random RTP Port Range	This feature allows users to specify the minimum and maximum RTP port ranges that can be used with the HT device. The Valid range is between 1024-65535
Enable RTCP	Allows users to enable RTCP. The default setting is “Yes”.
RTP/RTCP Keep Alive On Hold	When set to "Yes", RTP/RTCP packets are sent during call hold. Default settings is "No".
Hold Target Before Refer	Allows user to hold or not hold the phone call before referring. The default setting is Yes.
Refer-To Use Target Contact	Includes target’s “Contact” header information in “Refer-To” header when using attended transfer. Default is No.
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.
Ringing Transfer	Allows users to trigger the transfer once the user hangs up the call, Default setting is "No".
Disable Bellcore Style 3-Way Conference	Gives the users the possibility of making conference calls by pressing “Flash” key, when it’s enabled by dialing *23 +second callee number. Default is No
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.
Support Outbound	This feature allows users to set RFC5626 outbound. Enabled “Support SIP Instance ID” and “Support outbound” which could support RFC 5626 Disabled by Default.
Support GRUU	This feature allows users to set RFC5627 GRUU. Enabled “Support SIP Instance ID” and “Support GRUU” which could support RFC 5627 Disabled by Default.
Validate Incoming SIP Messages	Validates incoming SIP messages. Default is No.
Check SIP User ID for Incoming INVITE	Checks SIP User ID in the Request URI of incoming INVITE; if it doesn’t match the HT81x 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. The 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. The 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 doesn’t 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 CBCOM is active. If set to “Yes”, the P-Preferred- Identity Header will always be presented. If set to “No”, it will be omitted. Default setting is: Default.
Use P-Access-Network-Info Header	With this feature enabled, device will populate the WAN access node with IEE-802.11a, IEE-802.11b in P-Access-Network-Info SIP header.
Use P-Emergency-Info Header	This feature support of IEEE-48-addr and IEEE-EUI-64 in SIP header for emergency calls.
Use P-Asserted-Identity Header	When this feature is set to Yes, device will send P-Asserted-Identity Header on the SIP Invite. Default setting is No.
Use P-Early-Media Header	Allows users to set up the P-Early-Media Header. Once activated via "Ringback Tone at No Early Media," the phone will emit a ringback tone if early media RTP packets face obstruction from the intermediary server. Furthermore, the phone will acquire a "P-Early-Media" header within the 180/183 response, indicating "inactive," "recvonly," or "gated" values to signify the absence of incoming RTP packets. Disabled by Default.
SIP REGISTER Contact Header Uses	Specifies which address (LAN or WAN address) the device will detect to use it in SIP Register Contact Header. Default is LAN Address.
Caller ID Fetch Order	Selects the Caller ID display order which need to be respected by the ATA. The available options are: **Auto:** When set to “Auto”, the ATA will look for the caller ID in the order of P-Asserted Identity Header, Remote-Party-ID Header and From Header in the incoming SIP INVITE. **Disabled:** When set to “Disabled”, all incoming calls are displayed with “Unavailable”. **From Header:** When set to “From Header”, the ATA will use the FROM header to display the caller ID.
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 2).
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 HT81x 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	Configures SIP Timer D defined in RFC3261. 0 – 64 seconds. Default is 0.
DTMF Payload Type	Defines payload type for DTMF using RFC2833.
Preferred DTMF method (in order)	Sorts DTMF methods (in-audio, via RTP (RFC2833) or via SIP INFO) by priority.
Force DTMF to be sent via SIP INFO simultaneously	This option forces the DTMF signals to be sent using the SIP INFO method for better compatibility with VoIP systems. Disabled by Default.
Inband DTMF Duration	allows users to config the Inband DTMF Duration and inter-duration. The default Duration is 100 ms. Valid range: 40-2000 ms. The default Inter-duration is 50 ms. Valid range: 40-2000 ms.
Inband DTMF Tx Gain	Allows users to configure the Inband DTMF Tx Gain. The Valid rand is -12 to 12 db. The Default value is 0db.
DSP DTMF Detector Duration Threshold	Allows users to config the DSP DTMF Detector Duration Threshold The default Duration is 30 ms. Valid range: 20-2000 ms. The default Inter-duration is 30 ms. Valid range: 20-2000 ms.
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	Default is No. If set to yes, flash will be sent as DTMF event.
Flash Digit Control	When it set to YES it allows the user to perform some call setting when both channels are used while pressing: "**Flash + 1**" in order to hang up the current call and resume a call that was held. "**Flash + 2**" in order to hold the current call and resume a call that was held. "**Flash + 3**" in order to perform 3-way conference. "**Flash + 4**" in order to perform attended transfer. Note: Please refer to the user guide for detailed steps to perform above operations.More additional Digit events were added on the new firmware 1.0.43.10.
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 Delay	Specifies the auto-dial delay after off hook.

Proxy-Require	Determines a SIP Extension to notify the SIP server that the HT81x 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
Add MAC in User-Agent	This feature allows users to configure "User-Agent" in the SIP header field, when this feature is set to“No”, "User-Agent" does not carry a MAC, when this feature is set “Yes except REGISTER”, "User-Agent" in REGISTERSIP header field does not carry MAC but other SIP packet header fields carries MAC, when this feature is set to “Yes to all SIP”, "User-Agent" in the SIP packet header field will carries the MAC.
Use MAC Header	This feature allows users to configure MAC Header in the SIP packet header field, when this feature is set to “No” ,the MAC header field is not carried in the SIP packet header field, when this feature is set to “REGISTER Only”, the register packet header field carries the MAC header field but the remaining SIP packets do not carry MAC header fields, when this feature is set to “Yes to all SIP”, the MAC header field is carried in the SIP data packet header field.
RFC2543 Hold	Toggles between RFC2543 hold and RFC3261 hold. RFC2543 hold allows to disable the hold music sent to the other side, in this case IP address (0.0.0.0) it will be sent in SDP instead of the IP address of the unit . RFC3261 (a line) will play the hold music to the other side.
Disable Call Waiting	Disables receiving a second incoming call when the line is engaged. Default is No.
Disable Call Waiting Caller ID	Disables displaying caller ID when receiving a second incoming call. Default is No.
Disable Call Waiting Tone	Disables playing call waiting tone during active call when receiving a second incoming call. The CWCID will still be displayed. Default is No.
Disable Connected Line ID	Disables displaying the number of the person answering the phone. Default is No.
Disable Receiver 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 Yes.
Disable Visual MWI	Disables use of visual message waiting indicator when there is an unread voicemail message. Default is No.
Visual MWI Type	Configures Visual WMI Type of signal sent to the analog phone to make it turn the lamp ON upon receiving a Voice mail. Check the phone’s manual to find out what signal is supported, FSK (default) or Neon. **Note:** Some phones (depending on the model of the analog phone) when this feature is set to NEON it might auto ring (short beeps) when there is a voice mail available for that FXS port where it is connected.

MWI Tone	When set to Default, device will play Stutter Dial Tone when there is voicemail, if set to Special Proceed Indication Tone, device will play the configured special proceed indication tone upon user offhook when there is voicemail
Ringback Tone at No Early Media	Allows users to customize the "Ringback Tone at No Early Media" setting. Upon activation with "Use P-Early-Media Header," the phone will emit a ringback tone if early media RTP packets encounter obstruction from the intermediate server. The phone also obtains a "P-Early-Media" header in the 180/183 response, indicating values like "inactive," "recvonly," or "gated," signifying the absence of incoming RTP packets. Disabled by Default.
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. When set to 0 there will be no ringing timeout. Default is 60 seconds.
Hunting Group Ring Timeout	If call is not answered within this designated time period, the call will be forwarded to the next member of a Hunt Group. Default value is 20 seconds.
Hunting Group Type	Specifies Hunting Group Type, either "Linear" or "Circular". Linear style will sort the call to the lowest numbered available line, this is also called "serial hunting". Circular style will distribute the calls "round-robin". If a call is assigned to line 1, the next call goes to 2 and the next to 3. The succession throughout each of the lines continues even if one of the previous lines becomes available. When the end of the hunt group is reached, the hunting starts over at the first line. Lines are skipped if they are still busy on a previous call. Default is Circular.
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. Default is 4 seconds.
Early Dial	Sends an early INVITE each time a key is pressed when a user dials a number. Otherwise, only one INVITE is sent after full number is dialed (user presses Dial Key or after "no key entry timeout" expires). This option should be used only if there is a SIP proxy is configured and supporting "484 Incomplete Address" responses. Otherwise, the call will likely be rejected by the proxy (with a 404 Not Found error). Default is No. This feature is NOT designed to work with and should NOT be enabled for direct IP-to-IP calling.
Dial Plan Prefix	Adds specified prefix to dialed number.
Use # as Dial Key	Treats "#" as the "Send" (or "Dial") key. If set to "No", this "#" key can be included as part of the dialed number. Default is Yes.
Disable # as Redial Key	Disables # to act as Redial key. If set to "Yes" and feature "Use # as Dial Key" set to Yes, the # key will act as dial key but not as redial key. Default is No.
Dial Plan	Dial Plan Rules: 1. Accept Digits: **1,2,3,4,5,6,7,8,9,0 , *, #, A,a,B,b,C,c,D,d**

	2. Grammar: **x** – any digit from 0-9; a. **xx+** – at least 2 digits number; b. **xx** – exactly 2 digits number; c. ^ – exclude; d. **.** – wildcard, matches one or more characters e. **[3-5]** – any digit of 3, 4, or 5; f. **[147]** – any digit 1, 4, or 7; g. **<2=011>** – replace digit 2 with 011 when dialing h. **<=1>** – add a leading 1 to all numbers dialed, vice versa will remove a 1 from the number dialed i. | – or j. Flag **T** when adding a "T" at the end of the dial plan, the phone will wait for 3 seconds before dialing out. This gives users more flexibility on their dial plan setup. E.g. with dial plan 1XXT, phone will wait for 3 seconds to let user dial more than just 3 digits if needed. Originally the phone will dial out immediately after dialing the third digit. Example 1: {[369]11 | 1617xxxxxxx} – Allow 311, 611, 911, and any 10-digit numbers of leading digits 1617 Example 2: {^1900x+ | <=1617>xxxxxxx} – Block any number with leading digits 1900 and add prefix 1617 for any dialed 7-digit numbers Example 3: {1xxx[2-9]xxxxxx | <2=011>x+} – Allow any length of number with leading digit 2 and 10 digit-numbers of leading digit 1 and leading exchange number between 2 and 9; If leading digit is 2, replace leading digit 2 with 011 before dialing. 1. Default: Outgoing – { x+ | +x+ | *x+ | *xx*x+ } Example of a simple dial plan used in a Home/Office in the US: { ^1900x. | <=1617>[2-9]xxxxxx | 1[2-9]xx[2-9]xxxxxx | 011[2-9]x. | [3469]11 } Explanation of example rule (reading from left to right): ^1900x. – prevents dialing any number started with 1900 <=1617>[2-9]xxxxxx – allows dialing to local area code (617) numbers by dialing 7 numbers and 1617 area code will be added automatically 1[2-9]xx[2-9]xxxxxx – allows dialing to any US/Canada Number with 11 digits length 011[2-9]x. – allows international calls starting with 011 [3469]11 – allow dialing special and emergency numbers 311, 411, 611 and 911 Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider. In this case * should be predefined inside dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers.
SUBSCRIBE for MWI	Sends SUBSCRIBE periodically (depends on "Register Expiration" parameter) for message waiting indication. Default is No.
Subscribe Retry Wait Time upon 403 Forbidden	This feature allows users to adjust the subscribe retry waiting time while it is rejected with 403 forbidden. Default is 0. Valid range: 0-10080 in minutes. Note: Not supported on HT818
Send Anonymous	Sets "From", "Privacy" and "P_Asserted_Identity" headers in outgoing INVITE message to "anonymous", blocking caller ID. Default is No.
Anonymous Call Rejection	Rejects incoming calls with anonymous caller ID with "486 Busy here" message. Default is No.
Special Feature	Selects Soft switch vendors' special requirements Examples of vendors: BroadSoft, CBCOM, RNK, Huawei, China Mobile, ZTE IMS, PhonePower, TELKOM SA, Vonage, Metaswitch, CenturyLink, MTS, Oi_BR, Telefonica, GIBTELECOM. The default is Standard.
Enable Session Timer	Disable the session timer when this option is set to "No". By default, this option is enabled.
Session Expiration	Enables SIP sessions to be periodically "refreshed" via a SIP request (UPDATE, or re-INVITE). When the session interval expires, if there is no refresh via an UPDATE or re-

	INVITE message, the session will be terminated. Session Expiration is the time (in seconds) at which the session is considered timed out, if no successful session refresh transaction occurs beforehand. Valid range is 90-64800 seconds. Default is 180 seconds.
Min-SE	Defines Minimum session expiration (in seconds). Default is 90 seconds.
Caller Request Timer	Uses session timer when making outbound calls if remote party supports it. Valid range is 90-64800 seconds. Default is No.
Callee Request Timer	Uses session timer when receiving inbound calls with session timer request. Default is No.
Force Timer	Uses session timer even if the remote party does not support this feature. Selecting "No" will enable session timer only when the remote party supports it. To turn off Session Timer, select "No" for Caller and Callee Request Timer, and Force Timer. Default is No.
UAC Specify Refresher	Specifies which end will act as refresher for outgoing calls. Default is Omit. **UAC:** The HandyTone acts as the refresher. **UAS:** Callee or proxy server act as the refresher.
UAS Specify Refresher	Specifies which end will act as refresher for incoming calls. Default is Omit.: **UAS:** The HandyTone acts as the refresher. **UAC:** Callee or proxy server act as the refresher.
Force INVITE	Uses INVITE message to refresh the session timer. Default is No.
When To Restart Session After Re-INVITE received	Allows users to delay posting Media Change Event, it can be set to "Immediately" or to "After replying 200OK" The default value is "Immediately".
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, iLBC and OPUS
Voice Frames per TX	Transmits a specific number of voice frames per packet. Default is 2; increases to 10/20/32/64 for G711/G726/G723/other codecs respectively.
G723 Rate	Operates at specified encoding rate for G.723 vocoder. Available encoding rates are 6.3kbps or 5.3kbps. Default is 6.3kbps.
iLBC Frame Size	Specifies iLBC packet frame size (20ms or 30ms). Default is 20ms.

Disable OPUS Stereo in SDP	Disables OPUS stereo in SDP. Default is No.
iLBC Payload Type	Determines payload type for iLBC. Valid range is between 96 and 127. Default is 97.
OPUS Payload Type	Determines payload type for OPUS. Valid range is between 96 and 127. Default is 123.
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-Invite after Fax Tone Detected	Permits the unit to send out the re-INVITE for T.38 or Fax Pass Through if a fax tone is detected. Default is Enabled
Jitter Buffer Type	Selects jitter buffer type (Fixed or Adaptive) based on network conditions.
Jitter Buffer Length	**High** (initial 200ms, min 40ms, max 600ms) Note: not all vocoders can meet the high requirement. **Medium** (initial 100ms, min 20ms, max 200ms). **Low** (initial 50ms, min 10ms, max 100ms).
SRTP Mode	Selects SRTP mode to use ("Disabled", "Enabled but not forced", or "Enabled and forced"). Default is Disabled It uses SDP Security Description to exchange key. Please refer to **SDES**: https://tools.ietf.org/html/rfc4568 **SRTP:** https://www.ietf.org/rfc/rfc3711.txt
SRTP Key Length	Allows users to select supported SRTP Key Length. the available values are : 1. AES 128&256 bit 2. AES 128 bit 3. AES 256 bit Set to AES 128&256 bit By Default.
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	Disable analog phone's caller ID when receiving a call with "Anonymous", "unavailable" or "unknown" in FROM header and without "Display info". Note: This relies also on analog phone's design, some phones will still display "unknown" with this feature enabled. Default is No.
Replace Beginning '+' in Caller ID with	Allows users to replace the + sign with a defined string instead of the predefined 00.

Number of Beginning Digits to Strip from Caller ID	Allows users to remove specified digits from incoming caller IDs, ensuring displayed numbers are concise and recognizable on connected analog phones. This helps eliminate unnecessary information and enhance caller identification.
Polarity Reversal	Reverses the polarity upon call establishment and termination. Default is No.
Loop Current Disconnect	Allows the traditional PBX used with HT81x 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	Allow user to configure if it will play busy/reorder tone before loop current disconnect upon call fail. Default is No.
Loop Current Disconnect Duration	Configures the duration of voltage drop described in topic above. HT81x support a duration range from 100 to 10000ms. Default value is 200.
Enable Pulse Dialing	Allow users to enable Pulse Dialing option under FXS Port. Default is No.
Pulse Dialing Standard	Allows users to use Swedish pulse dialing standard or New Zealand pulse dialing standard. Default is General Standard.
Enable Hook Flash	Enables the FLASH button to be used for terminating calls. Default is Yes.
Hook Flash Timing	Defines the time period when the cradle is pressed (Hook Flash) to simulate FLASH. To prevent unwanted activation of the Flash/Hold and automatic phone ring-back, adjust this time value. HT81x support a range from 40 to 2000 ms. Default values are 300 minimum and 1100 maximum.
On Hook Timing	Specifies the on-hook time for an on-hook event to be validated. HT81x support a range from 40 to 2000 ms. Default value is 400.
Gain	Adjusts the voice path volume. • Rx is a gain level for signals transmitted by FXS • Tx is a gain level for signals received by FXS. Default = 0dB for both parameters. Loudest volume: +6dB Lowest volume: -6dB. User can adjust volume of call using the Rx gain level parameter and the Tx gain level parameter located on the FXS port configuration page. If call volume is too low when using the FXS port (ie. the ATA is at user site), adjust volume using the Rx gain level parameter under the FXS port configuration page. If voice volume is too low at the other end, user may increase the far end volume using the Tx gain level parameter under the FXS port configuration PAGE.
Disable Line Echo Canceller	Disables the LEC per call base. Recommended for Fax/Data calls. Default is No.
Disable Network Echo Suppressor	Disables the NEC per call base. Recommended for Fax/Data calls. Default is No.
Outgoing Call Duration Limit	Defines the call duration limit for the outgoing calls. Default is 0 (No limit).
Incoming Call Duration Limit	allows users to configure the Incoming Call Duration Limit. Valid Range is 0 - 180 (0 is no limit) Default value is 0.

Ring Frequency	Customizes ring frequency. Valid options: 20Hz – 25Hz. Default is 20Hz.
Enable High Ring Power	Configures a high ringing voltage output for the ATA.
OnHOOK DC Feed Current	This feature is used to adjust DC feed current.
RFC2833 Events Count	This feature allows users to customize the count of RFC2833 events. The Valid Value Range is between 2 and 10 , if it is set to 0 , it means continuous RFC2833 events are activated Default is 8.
RFC2833 End Events Count	This feature allows users to customize the count of RFC2833 end events. Default is 3.
RFC2833 Convert Mode	Allows users set the way DTMF tones (tones from phone keypresses) are transmitted in VoIP calls using the RFC2833 Convert Mode. The available options include a default mode, a mode for analog telephone adapters, and modes involving digital signal processors. These options determine how DTMF tones are encoded, sent, and processed during calls. 1. **ATA Mode:** Involves configuring how DTMF tones from analog phones are transmitted over a digital network. It's used when connecting traditional analog phones to VoIP systems, converting analog signals to digital for transmission. 2. **DSP Normal Mode: C**onfigures how DTMF tones are processed by a digital signal processor during VoIP calls. It follows a standard procedure for handling and converting these tones within the digital environment. 3. **DSP Permanent Mode:** DSP permanent mode is a configuration where the digital signal processor is continuously ready to handle DTMF tones in VoIP calls. This means it's always active, eliminating the need for switching between different modes for DTMF processing. The default value is "DSP Normal Mode"
Distinctive Ring Tone	Customizes the Ring Tone 1 to 3 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 the 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: <127.0.0.1>; info=ring5***
Ring tones	Configures the ring tone cadence preferences. User has 10 choices. The configuration, completed in Distinctive Ring Tones block in the same page, applies to ring tones cadences configured here.
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 No Disturb, Call Forward and other call features can be used via the local feature codes on the phone. Otherwise, the ITSP feature codes will be used. Enable All will override all individual features enable setting. Default is Yes
Reset Call Features	Allows users to reset all call features configuration. Default is No
SRTP Feature	Allow users to customize the SRTP feature codes. Default is Yes – Enable SRTP: 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	Default is No
Star Code 3WC Feature	Default is Yes – Star Code 3WC: Default is 23
Play registration id Feature	Allows users to hear their device's account or registration number. – Enable playing registration id : Default is 98
Set Offhook Auto-Dial Feature	Allows users to configure Enable/Disable the Set Off hook auto dial Feature Code. – Enable Set Offhook Auto-Dial : Default is 77
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

Profiles Settings Page

FXS Ports Page Definitions

Port	Display the port number
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”.

Password	Specifies account password provided by VoIP service provider (ITSP) to register to SIP servers.
Name	Chooses a name to be associated to user.
Profile ID	Defines the profile ID for each port.
Hunting Group	Configures hunting group feature on the specific port. For example: Port 1, 2, and 3 are members of the same Hunting Group. Port 1 is registered with a SIP account. Ports 2, and 3 are not registered. Ports 2 and 3 will be able to place outbound calls using the SIP account of port 1. Select appropriate value for Hunting Group feature. The original SIP account should be set to Active while the group members should be set to the port number of the Active Port. Example configuration of a Hunting group: FXS Port #1: SIP UserID and Authenticate ID entered, Hunting group set to "Active" FXS Port #2: SIP UserID and Authenticate ID left blank, Hunting Group set to "1" FXS Port #3: SIP UserID and Authenticate ID left blank, Hunting Group set to "1" FXS Port #4: SIP UserID and Authenticate ID entered, Hunting group set to "None" Hunting Group 1 contains ports 1, 2, 3. FXS port 4 is registered but it is not added to the Hunting Group 1. **Note:** HT818 will use CID name from FXS port initiating the outgoing call if the "Name" field is entered for that specific port.
Request URI Routing ID	If configured, device will route the incoming call to designated port by request URI user ID in SIP INVITE.
Enable Port	Enables / Disables the port
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 is entered here. The HT818 will automatically append the "@" and the host portion of the corresponding SIP address.

FXS Ports Settings Page

Static DNS Settings

A Record Settings	
Name	The domain name to which the record refers. Maximum supported length is 512 characters.
TTL	(Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again. Valid range is from 300 to 65535. Default value is "300"
Address	The IP address associated with the domain.
SRV Settings	

Name	The domain name of the wanted service. Maximum supported length is 512 characters.
TTL	(Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again. Valid range is from 300 to 65535. Default value is "300"
Priority	Enables to prioritize target hosts that support the given service. Lowest number will get the highest priority. Target hosts with the same priority will be tried in an order defined by the weight field. Valid range is from 0 to 65535. Default value is "0"
Weight	Specifies the weight for entries with the same priority. Larger weight will get higher priority. Valid range is from 0 to 65535. Default value is "0"
Port	The port on the target host of the specified service. The valid range is 0-65535. Default value is "0"
Target	The domain name of the target host.
NAPTR Settings	
Name	The domain name to which this resource record refers. Maximum length is 512 characters.
TTL	(Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again. Valid range is from 300 to 65535. Default value is "300"
Order	Specifies the order in which the NAPTR record need to be processed, low numbers are processed before high numbers. Valid range is from 0 to 65535.
Preference	Refers to the order in which NAPTR records with the same “Order” values need to be processed. records are processed from lower preference numbers to higher preference numbers. Valid range is from 0 to 65535.
Flags	Indicate what happens next after this lookup, at this time 4 flags are defined. ● The “**S**” flag indicates that the next lookup should be an SRV lookup. ● The “**A**” flag indicates that the next step is a DNS A, AAAA, A6 record lookup. ● The “**U**” flag means that the next step is not a DNS lookup but that the output of the Regexp field is an URI that adheres to the ‘absoluteURI’. ● The “**P**” flag indicates that the remainder of the lookup are defined by the application that uses the NAPTR.
Service	Specifies the services available in this domain. The replacement field is used to get to this service. It can also specify the protocol used to communicate with the server that offers this service. In SIP, three services are defined along with their resolution services (resolution services are defined after the “+” sign): ● “**SIPS+D2T**”: Secure SIP, TLS over TCP. ● “**SIP+D2T**”: SIP over TCP. ● “**SIPS+D2S**”: Secure SIP, TLS over SCTP. ● “**SIP+D2S**”: SIP over SCTP.

	● "**SIP+D2U**":SIP over UDP. Maximum length is 512 characters and default value is "SIP+D2U"
Regexp	Contains a substitution expression that is applied to the original string held by the client in order to construct the next domain name to lookup.
Replacement	Depending on the value of the Flag field, this parameter contains the next FQDN to query for NAPTR, SRV, or address records.

Static DNS Settings Page

Important Settings

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 the FXS web page), set this to Yes when gateway is behind firewall on a private network.

DTMF Methods

The HT818 supports 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 HT818 support following voice codecs. On Profile pages, choose the order of your favorite codecs:

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

Configuring HT818 through Voice Prompts

As mentioned previously, The HT818 has a built-in voice prompt menu for simple device configuration. Please refer to "Understanding HT818 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 HT818 to use DHCP.

- **STATIC IP MODE**

Select voice menu option 01 to enable HT818 to use STATIC IP mode, then use option 02, 03, 04, 05 to set up IP address, Subnet Mask, Gateway and DNS server respectively.

- **PPPOE MODE**

Select voice menu option 01 to allow the HT818 to enable the PPPoE mode. PPPoE Username and Password should be configured from web GUI.

- **FIRMWARE SERVER IP ADDRESS**

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

- **CONFIGURATION SERVER IP ADDRESS**

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

- **UPGRADE PROTOCOL**

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

- **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.

- **WAN PORT WEB ACCESS**

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

Configuration through a Central Server

The HT818 can be automatically configured from a central provisioning system. When HT818 boots up, it will send TFTP, HTTP/HTTPS or FTP/FTPS requests to download configuration files, “cfg000b82xxxxxx” and “cfg00082xxxxxx.xml”, where “000b82xxxxxx” is the LAN MAC address of the HT818. If the download of “cfgxxxxxxxxxxxx.xml” is not successful, the provision program will issue request a generic configuration file “cfg.xml”. Configuration file name should be in lower case letters. The configuration data can be downloaded via TFTP, HTTP/HTTPS or FTP/FTPS from the central server. A service provider or an enterprise with large deployment of HT818 can easily manage the configuration and service provisioning of individual devices remotely from a central server.

Grandstream provides a central provisioning system GAPS (Grandstream Automated Provisioning System) to support automated configuration of Grandstream devices. GAPS uses HTTPS and other communication protocols to communicate with each individual Grandstream device for firmware upgrade, remote reboot, etc. Grandstream provides GAPS service to VoIP service providers. Use GAPS for either simple redirection or with certain special provisioning settings. At boot-up, Grandstream devices by default point to Grandstream provisioning server GAPS, based on the unique MAC address of each device, GAPS provision the devices with redirection settings so that they will be redirected to customer’s TFTP, HTTP/HTTPS or FTP/FTPS server for further provisioning. Grandstream also provides configuration tools (Windows and Linux/Unix version) to facilitate the task of generating device configuration files.

The Grandstream configuration tools are free to end users. The configuration tools and configuration templates are available for download from https://www.grandstream.com/support/tools

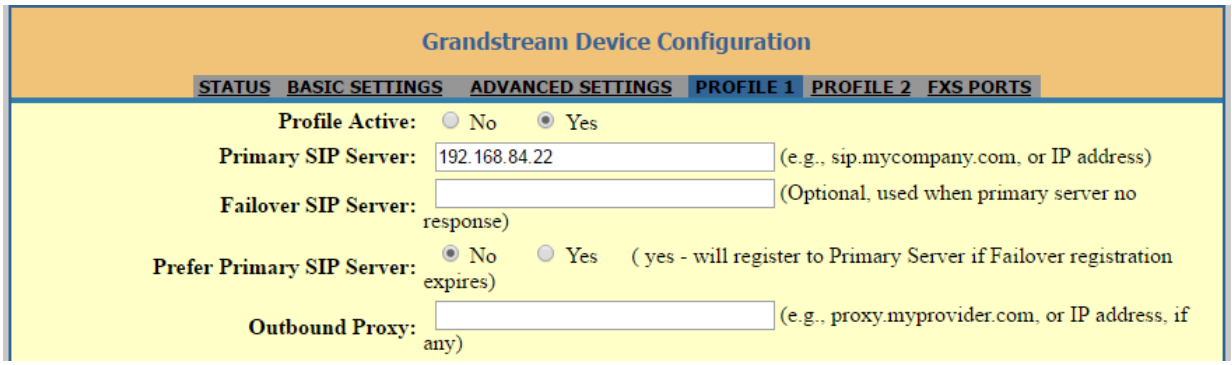
Register a SIP Account

The HT818 support 2 profiles which can be configured with 2 SIP accounts. Please refer to the following steps to register your accounts via web user interface

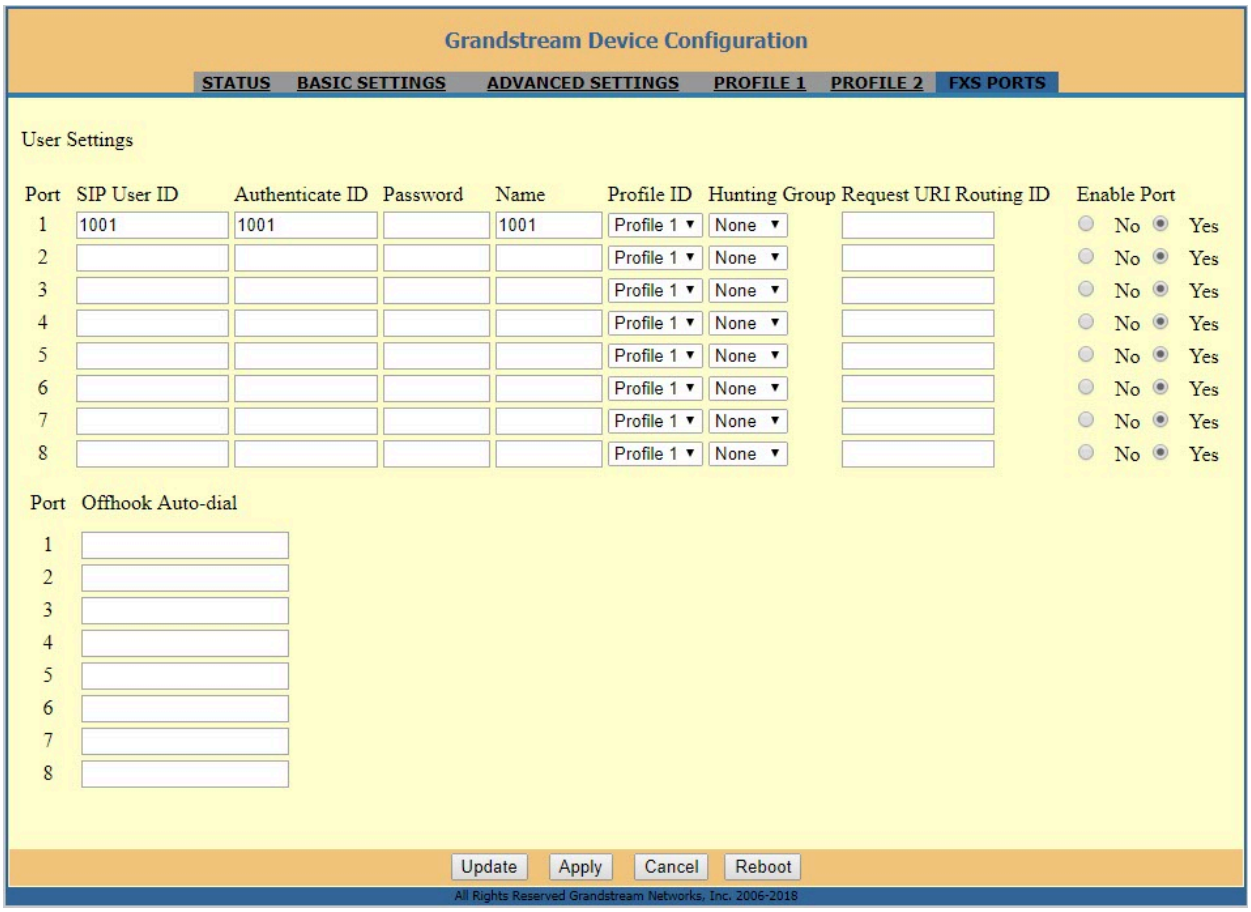
1. Access your HT818 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: admin).
3. Press **Login** to access your settings.
4. Go to **Profile (1** or **2)** pages.
5. In **Profile** tab, set the following:
    1. **Account Active** to **Yes.**
    2. **Primary SIP Server** field with your SIP server IP address or FQDN.
    3. **Failover SIP Server** with your Failover SIP Server IP address or FQDN. Leave empty if not available.
    4. **Prefer Primary SIP Server** to **No** or **Yes** depending on your configuration. Set to **No** if no Failover SIP Server is defined. If "**Yes"**, account will register to Primary SIP Server when failover registration expires.
    5. **Outbound Proxy:** Set your Outbound Proxy IP Address or FQDN. Leave empty if not available.
6. After configuring the SIP server and activating the profiles, you should access to **FXS Ports** page to register your accounts. In **FXS Ports** tab, set the following:
    1. **SIP User ID**: User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
    2. **Authenticate ID**: SIP service subscriber's Authenticate ID used for authentication. Can be identical to or different from SIP User ID.
    3. **Authenticate Password**: SIP service subscriber's account password to register to SIP server of ITSP. For security reasons, the password will field will be shown as empty.
    4. **Name**: Any name to identify this specific user.
    5. Set **Enable Port** to **Yes.**

For more information, related to above options please refer to Profile(s) settings and FXS Ports Settings

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

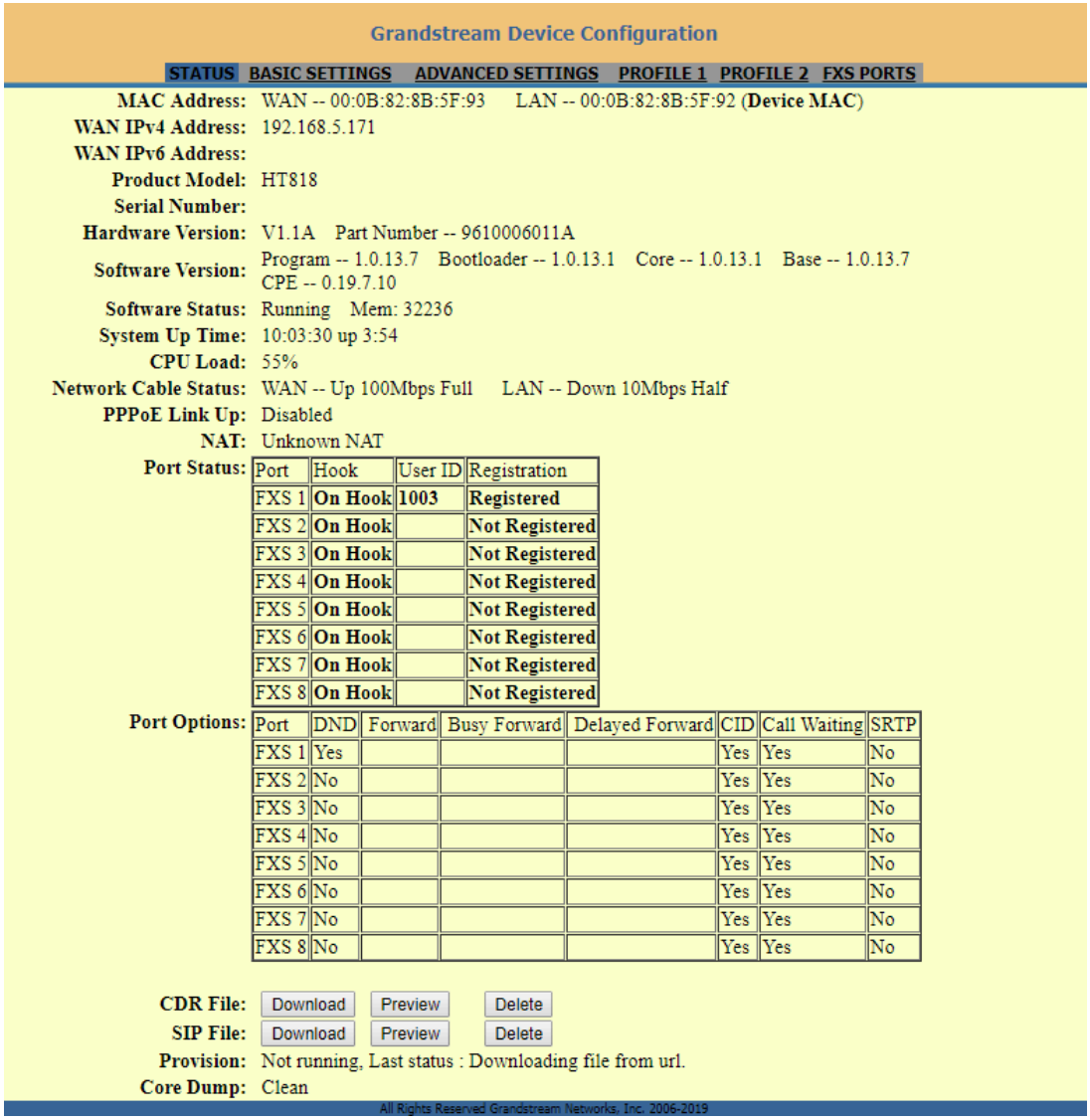


SIP Profiles Settings



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 from your HT818 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).



Accounts Status

When all the FXS ports are registered, the simultaneous ring will have one second delay between each ring on each phone.

Call Features

The HT818 support all the traditional and advanced telephony 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.

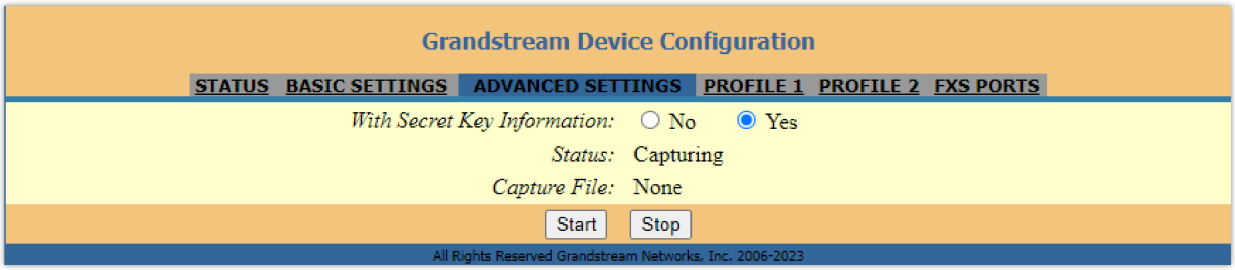
HT818 Call Features

Information Capture

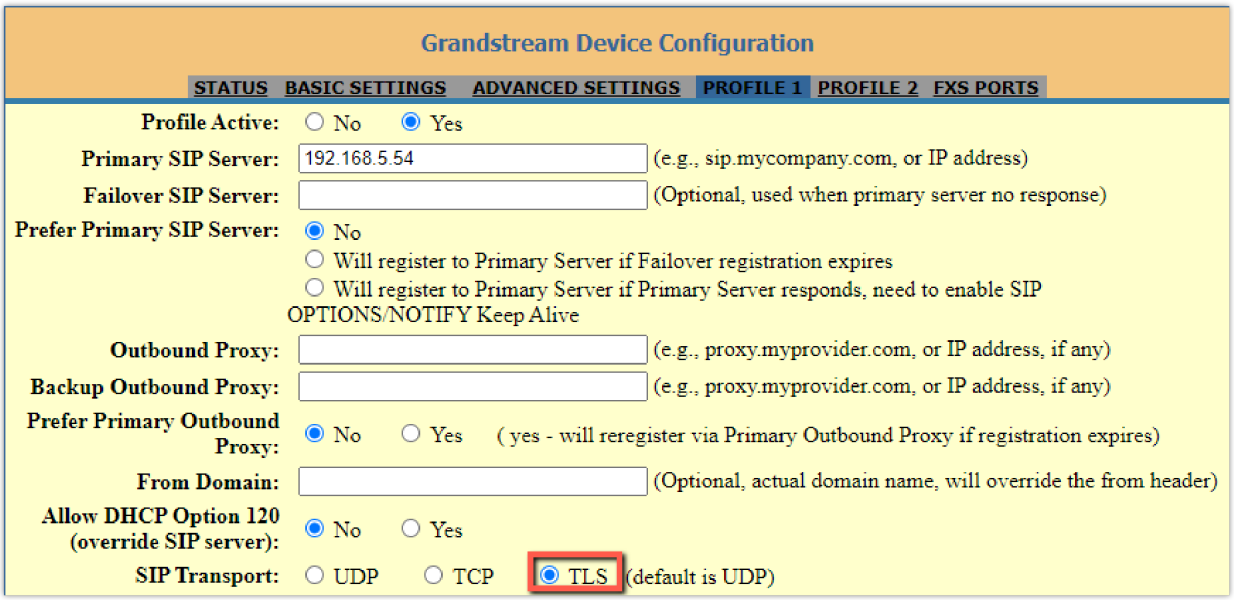
Information Capture involves intercepting a secret key information file during the TLS handshake between the HT8xx and a SIP server for the purpose of extracting the secret key information file during the TLS handshake, the file downloaded is a .txt file including the client secret key.

The process includes initiating capture, re-registering the HT8xx with TLS to a SIP server, waiting for a SIP Register request, and then stopping the capture. The goal is to extract the secret key information file, to do that please follow the below steps described below:

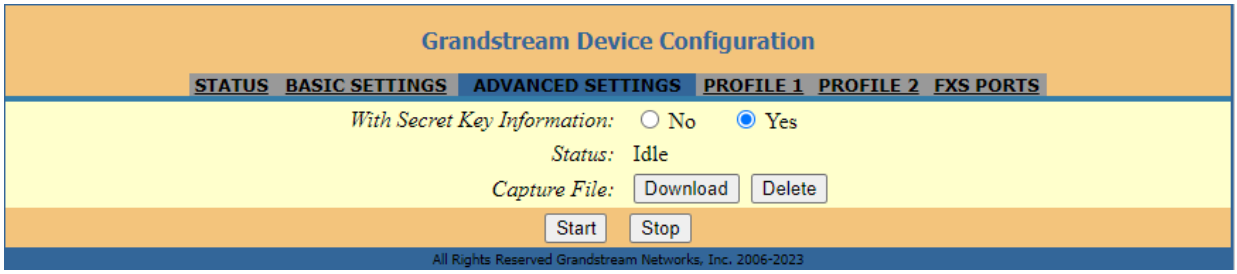
- Start capturing the communication between the HT8xx and the server. to do that go to **Advanced settings => Information capture**, make sure **"With Secret Key information"** is set to Yes



- Re-register the HT8xx account or port to the SIP server using the TLS protocol.

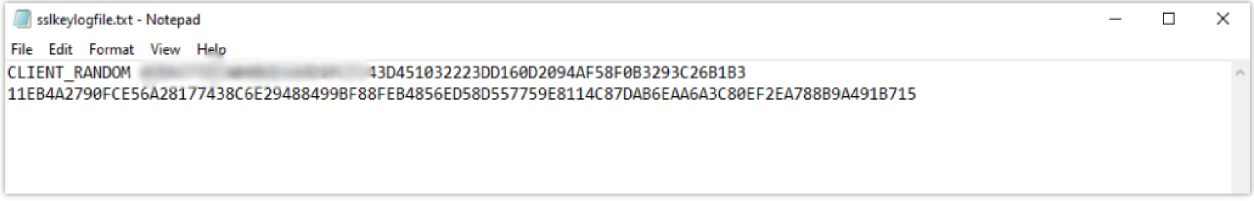


- Allow the system to wait until the ATA sends a SIP Register request to the server.
- Once the SIP Register request is sent, stop capturing the communication.



- You have the possibility to now download the secret key.

- After completing the above steps, the expectation is that the captured data will include the secret key information file in a .txt file under the name **"sslkeylogfile"**



The extracted key gives you the possibility to decrypt the secured communication between the HT8xx and the SIP server.

Important

Please use Information capture only when authorized since extracting secret key information without proper authorization is considered unethical.

Rebooting HT818 from Remote

Press “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 HT818 can be upgraded via TFTP/HTTP/HTTPS/FTP/FTPS by configuring the URL/IP Address for the TFTP/HTTP/HTTPS/FTP/FTPS server and selecting a download method. Configure a valid URL for TFTP, HTTP/HTTPS or FTP/FTPS; the server name can be FQDN or IP address.

Examples of valid URLs:

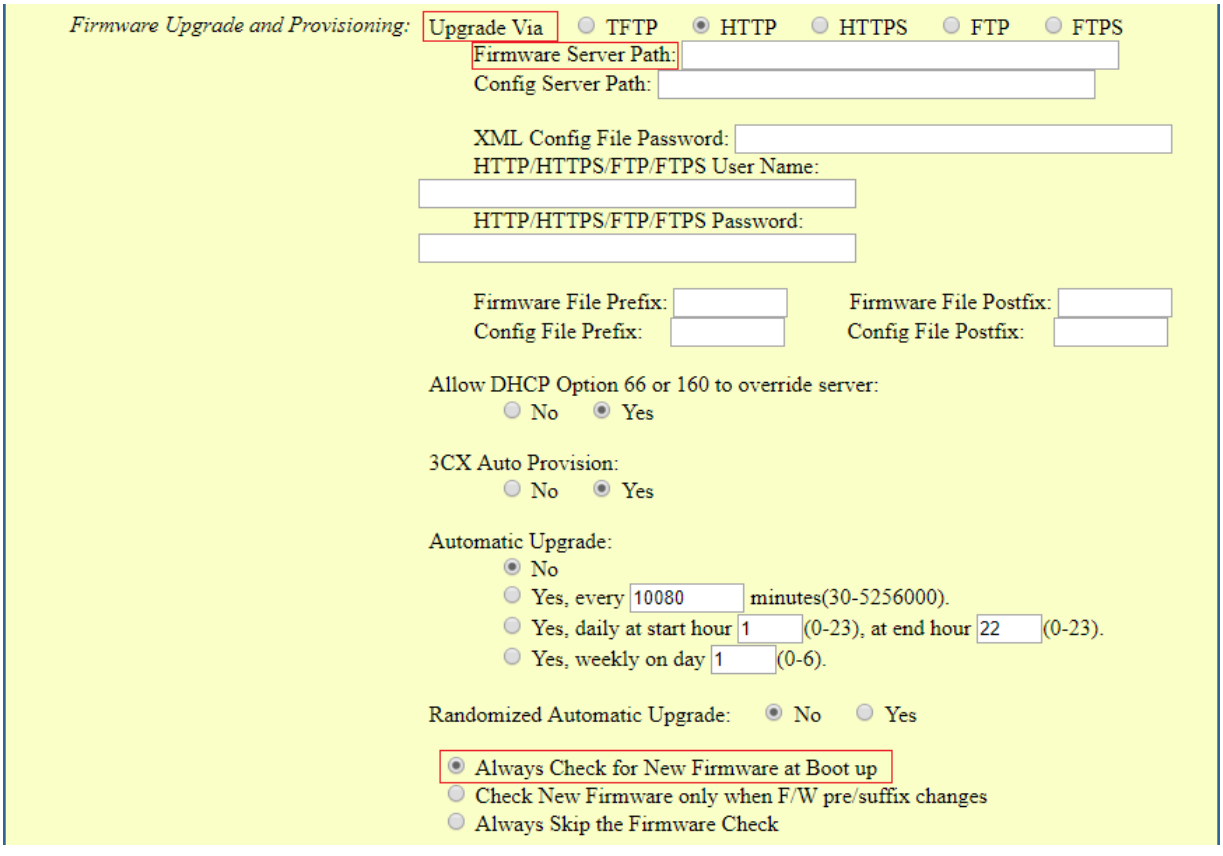
firmware.grandstream.com

fw.ipvideotalk.com/gs

Firmware Upgrade procedure

Please follow below steps in order to upgrade the firmware version of your HT818:

1. Access your HT818 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, HTTP/HTTPS or FTP/FTPS**.
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 HT818 to update the new firmware.



Upgrading via Local Directory

1. Download the firmware file from Grandstream web site
2. Unzip it and copy the file in to a folder in your PC
3. From the HT818 web interface (Advanced Settings page) you can browse your hard drive and select the folder you previously saved the file (HT8xfw.bin)
4. Click "Upload Firmware" and wait few minutes until the new program is loaded.

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

> the filename in URL for the firmware upgrade has been disabled on the latest firmware upgrade 1.0.43.10

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 HT818.

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 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, HTTP/HTTPS or FTP/FTPS. The **Config Server Path** is the TFTP, HTTP/HTTPS or FTP/FTPS server path for the configuration file. It needs to be set to a valid URL, either in FQDN or IP address format. The **Config Server Path** can be the same or different from the **Firmware Server Path**.

A configuration parameter is associated with each 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 HT818 boots up or reboots, it will send a request to download the xml file named "cfgxxxxxxxxxxxx.xml" followed by the binary file named "cfgxxxxxxxxxxxx", where "xxxxxxxxxxxx" is the MAC address of the phone, i.e., "cfg000b820102ab" and "cfg000b820102ab.xml". If the download of "cfgxxxxxxxxxxxx.xml" file is not successful, the provision program will download a generic cfg.xml file and then download cfg<Model>.xml. The configuration file name should be in lower case letters.

HT818 supports DHCP option 67allowing 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. The Only acceptable Config file formats to be used when provisioning are XML or binary.

2. Make sure the MAC header on the Config file is the provisioned device's MAC address or you can remove the header completely.

For more details on XML provisioning, please refer to:

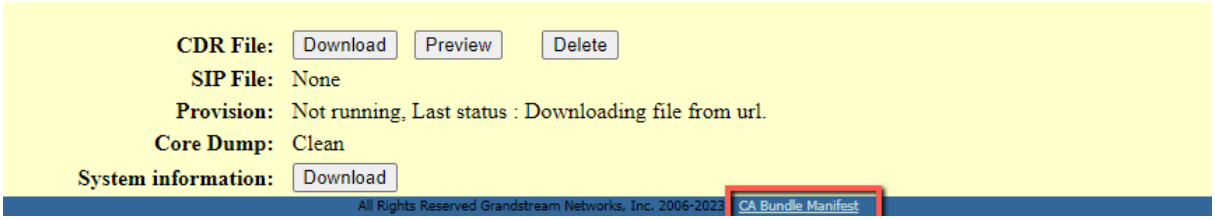
https://documentation.grandstream.com/knowledge-base/sip-device-provisioning-guide/

- The filename in URL for config provision has been disabled on the latest firmware upgrade 1.0.43.10
- The following parameters were added in firmware 1.0.55.5 and are only present on the config file (not on the Web UI) : [P28834/28835] **Initial line polarity** (0 – Forward, 1 – Reverse. The default is 1) and [P82307] **Syslog Setting and Internal Logs Protection** (0- No, 1- Yes. The default is 0).

CA Bundle Manifest

CA (Certification Authority) Bundle Manifest is a collection of trusted security certificates used to verify the authenticity of websites or services. It helps ensure secure and encrypted connections by confirming the identity of the remote server, protecting against unauthorized access and data interception.

you can access the **CA Bundle Manifest** by clicking on the bottom corner of the web page as displayed in the screenshot below:



This will redirect you to a web page displaying a list of certification names and details, with their corresponding expiration dates:

CA Bundle Manifest

Certificate Name	Expiration
GlobalSign Root CA	Jan 28 12:00:00 2028 GMT
Entrust.net Certification Authority (2048)	Jul 24 14:15:12 2029 GMT
Baltimore CyberTrust Root	May 12 23:59:00 2025 GMT
Entrust Root Certification Authority	Nov 27 20:53:42 2026 GMT
AAA Certificate Services	Dec 31 23:59:59 2028 GMT
QuoVadis Root CA 2	Nov 24 18:23:33 2031 GMT
QuoVadis Root CA 3	Nov 24 19:06:44 2031 GMT
Security Communication RootCA1	Sep 30 04:20:49 2023 GMT
XRamp Global Certification Authority	Jan 1 05:37:19 2035 GMT
Go Daddy Class 2 Certification Authority	Jun 29 17:06:20 2034 GMT
Starfield Class 2 Certification Authority	Jun 29 17:39:16 2034 GMT
DigiCert Assured ID Root CA	Nov 10 00:00:00 2031 GMT
DigiCert Global Root CA	Nov 10 00:00:00 2031 GMT
DigiCert High Assurance EV Root CA	Nov 10 00:00:00 2031 GMT
SwissSign Gold CA - G2	Oct 25 08:30:35 2036 GMT
SwissSign Silver CA - G2	Oct 25 08:32:46 2036 GMT
SecureTrust CA	Dec 31 19:40:55 2029 GMT
Secure Global CA	Dec 31 19:52:06 2029 GMT
COMODO Certification Authority	Dec 31 23:59:59 2029 GMT
Network Solutions Certificate Authority	Dec 31 23:59:59 2029 GMT
COMODO ECC Certification Authority	Jan 18 23:59:59 2038 GMT
Certigna	Jun 29 15:13:05 2027 GMT
ePKI Root Certification Authority	Dec 20 02:31:27 2034 GMT
certSIGN ROOT CA	Jul 4 17:20:04 2031 GMT
NetLock Arany (Class Gold) Főtanúsítvány	Dec 6 15:08:21 2028 GMT
Hongkong Post Root CA 1	May 15 04:52:29 2023 GMT
SecureSign RootCA11	Apr 8 04:56:47 2029 GMT
Microsec e-Szigno Root CA 2009/emailAddress=info@e-szigno.hu	Dec 30 11:30:18 2029 GMT
GlobalSign	Mar 18 10:00:00 2029 GMT
Autoridad de Certificacion Firmaprofesional CIF A62634068	Dec 31 08:38:15 2030 GMT
Izenpe.com	Dec 13 08:27:25 2037 GMT
Go Daddy Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT
Starfield Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT
Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT
AffirmTrust Commercial	Dec 31 14:06:06 2030 GMT
AffirmTrust Networking	Dec 31 14:08:24 2030 GMT

RESTORE FACTORY DEFAULT SETTINGS

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

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

Using the Reset Button

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

1. Unplug the Ethernet cable.
2. Locate the reset hole on the back panel of your HT818.
3. Insert a pin in this hole and press for about 7 seconds.
4. Take out the pin. All unit settings are restored to factory settings

Using the IVR Command

Reset default factory settings using the IVR prompt:

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

Encode the MAC Address

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

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

MAC Address Key Mapping

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

Reset from Web Interface (Reset Type)

1. Access your HT818 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 Reset:** This will reset only the data related with a service provider like SIP server, sip user ID, provisioning and others.

- Factory Reset will be disabled if the "Lock keypad update" is set to "Yes".
- If the HT818 were 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 HT818 UI by entering its IP address in your favorite browser.
2. Go to **Profile #** page.
3. Set "Allow SIP Factory Reset" to "Yes". (Default is No)
4. Once a SIP NOTIFY with "event: reset" is received, the ATA will perform factory reset.

> 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.

CHANGE LOG

This section documents significant changes from previous versions of the admin guide for HT818. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.55.5

- Added support to configure Static DNS settings. [Static DNS Settings]
- Added support of variable $PN and $MAC in Config Server Path. [Config Server Path]
- Added support to upload TXT format config file. [Upload Configuration]
- Added support for Ringing Transfer. [Ringing Transfer]
- Added support for RTP/RTCP Keep Alive. [RTP/RTCP Keep Alive On Hold]
- Added support for OpenVPN Additional Options. [OpenVPN Additional Options]
- Added support for the ability to pull the local network information via SNMP. [Enable SNMP]
- Added P-values not present on the WebUI [Initial Line Polarity][Syslog Setting and Internal Logs Protection]
- Added sorting of parameters in the configuration file exported through SSH. [Download Device Configuration]
- Added support for XMPP connection on TR-069. [Enable TR-069]
- Updated the "Prompt Dial Tone Code" feature to support the prefix number. [Prompt Tone Access Code]

Firmware Version 1.0.53.3

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

Firmware Version 1.0.53.2

- No Major Changes

Firmware Version 1.0.51.1

- Added new value "4 – Auto" in NAT Traversal. [NAT Traversal]
- Added support Enable/Disable the Set Off hook auto dial Feature Code. [Set Offhook Auto-Dial Feature]
- Added support Set Off hook auto dial Feature Code. [Enable Set Offhook Auto-Dial]

- Added support Force DTMF to be sent via SIP INFO simultaneously. [Force DTMF to be sent via SIP INFO simultaneously]
- Added support Radius auth protocol. [Radius Auth Protocol]
- Updated config file download request starts from cfgMAC.xml [Download Device XML Configuration]
- Removed complex admin password requirements. [Admin Password]
- Added support to CA bundle manifest on WebUI. [CA Bundle Manifest]

Firmware Version 1.0.49.2

- Added ability to send RADIUS traffic for web access through Management Interface. [Enable RADUIS Through Management Interface]
- Added new customized admin password rules. [Customized Admin Password Rules]
- Added ability to disable FXS voltage on no SIP registration.[Delay Time of Port Voltage Off Timer Since Boot]
- Added RFC2833 Convert Mode. [RFC2833 Convert Mode]
- Added support to customize Early media response. [Use P-Early-Media Header]
- Added the ability to force local ringback tone. [Ringback Tone at No Early Media]
- Added support for RFC 5626. [Support outbound]
- Added support for RFC 5627. [Support GRUU]
- Added ability to replace + sign on the incoming call with a predefined string. [Replace Beginning '+' in Caller ID with:]
- Added ability to remove specified digits from incoming caller IDs, [Number of Beginning Digits to Strip from Caller ID]
- Added support Random RTP Port Range. [Random RTP Port Range]
- Added ability to export config file via SSH. [Download Device Configuration]
- Added new option in "Prefer Primary SIP Server". [Will register to Primary Server if Primary Server responds, need to enable SIP OPTIONS/NOTIFY Keep Alive]

Firmware Version 1.0.45.2

- Added override config file option "cfgMAC_override.xml". [cfgMAC_override.xml]
- Added option "Download and Process All Available Config File. [Download and Process All Available Config Files]
- Added option "When To Restart Session After Re-INVITE received" [When To Restart Session After Re-INVITE received]
- Updated the option in "Unregister On Reboot" to 0 – No, 1 – All, 2 – Instance. [Unregister On Reboot]

Firmware Version 1.0.43.10

- Added Charter CA to the approved certificate list. [Load CA Certificates]
- Added support for TR-069 on the management interface. [Enable TR-069 Through Management Interface]
- Added ability to send Syslog traffic through Management Interface.[Enable Syslog Through Management Interface]
- Added support for variable on Provisioning link. [Enable Using tags in URL]
- Updated the default option of "Disable Reminder Ring for DND" to "Yes". [Disable Reminder Ring for DND]
- Add SSL Key Log File. [With Secret Key Information]
- Add Information Capture. [Information Capture]
- Allow configuring devices through SSH from different networks. [Security Controls for SSH/Telnet Access]
- Removed Telnet Idle Timeout Configuration Option.[Telnet Idle Timeout]
- Added additional Flash Digit events.[Flash Digit Control]
- Optimized the layout of the software version on the status page to make it look better.
- Add support of DHCP Option 150. [Additional Override DHCP Option]
- Merge DHCP Option 160 with DHCP Option 66. [Allow DHCP Option 66 or 160 to Override Server]
- Add a new special feature option "GIBTELECOM". [Special Feature]
- Add support for the "From Domain" option. [From Domain]
- GUI enhancement to display correctly port status.

- Added support for SRTP Key Length. [SRTP Key Length]
- Increased Admin/User/Viewer Password length to 30 characters. [User/Viewer Password] [Admin Password]
- Added support for Inband DTMF Duration. [Inband DTMF Duration]
- Added support for DSP DTMF Detector Duration Threshold. [DSP DTMF Detector Duration Threshold]
- Added new attribute values on WebUI :
  - TR-069 firewall rules (Value Range:1-65535, no default). [TR-069 firewall rules]
  - Root CA Version (0 – Current Root; 1 – New Root, default is 1) [Root CA Version]
  - Provision and upgrade to new Gen-2 certificate. (1- upgrade; 0 – no upgrade, default is 0). [Gen-2 certificate.]
  - Contents (text string) of Gen-2 certificate to upgrade. (String. Max length 8192, no default). [Gen-2 certificate]
  - Contents (text string) of Gen-2 EC private key to upgrade. (String. Max length 8192, no default) [Gen-2 EC private key]
  - Disable filename in URL for config provision. [Configuration File Download]
  - Disable filename in URL for firmware upgrade. [Firmware Upgrade procedure]

Firmware Version 1.0.41.2

- Updated Time Zone option "GMT+01:00 (Paris, Vienna, Warsaw)" to "GMT+01:00 (Paris, Vienna, Warsaw, Brussels)". [Basic Settings Page Definitions]
- Added star code [*98] to play registration ID.

Firmware Version 1.0.39.4

- Added feature to send SNMP traffic through Management Interface. [Basic Settings Page Definitions]
- Added feature support e911 compliance and HELD protocol. [Advanced Settings Page Definitions]
- Updated the default value of "Maximum Number of SIP Request Retries" from 4 to 2. [Profiles Page Settings]
- Updated CDR File Option | SIP File Option (P8534/8535) value from "1 – Override" to "Overwrite". [Advanced Settings Page Definitions]
- Added Local IVR option that announces extension number of the port. [Understanding HT818 Interactive Voice Prompt Response Menu]

Firmware Version 1.0.37.1

- Added feature Configuration File Types Allowed. [Advanced Settings Page Definitions].
- Added feature MAC in User-Agent [Profile Page Definitions]
- Added feature Use MAC Header [Profile Page Definitions]

Firmware Version 1.0.35.4

- Added support to allow HT8xx provision admin password without special characters.
- Added support for Israel time zone with DST.

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 OpenVPN 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 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 support for Telnet. [Disable Telnet]
- Added “Disable” option for “Web Access Mode” feature. [Web Access Mode]
- Moved “Trusted CA certificates” from Profile1/Profie2 to Advanced Settings and renamed as Trusted CA Certificates A, B, C, D. [Advanced Settings]
- Added options to Disable User/Viewer Levels Web Access. [Disable User Level Web Acces][Disable Viewer Level Web Access]
- Added support for “Use P-Asserted-Identity Header”. [Use P-Asserted-Identity Header]
- Added Feature “Load CA Certificates”. [Load CA Certificates]
- Added support to configure TR-069 connection request port. [Connection Request Port]
- Added support to set Ring Timeout to 0 for unlimited ring timeout. [Ring Timeout]
- Added OI_BR to special feature. [Special Feature]
- Added New Zealand Standard for Pulse Dialing Standard. [Pulse Dialing Standard]
- 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 TLS version configuration. [TLS Version]
- Updated “São Paulo” time zone to UTC-3. [Time Zone]

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 to allow CID name fields for ports that are part of the active hunting group to take effect. [Hunting Group]
- Added support for GDMS. [ACS URL]
- Added Russian language to Web UI and IVR. [Language]

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 or 160 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 “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 1.0.11.7

- Added support for SIP keep-alive to use SIP NOTIFY. [SIP OPTIONS/NOTIFY Keep Alive]
- Added support to display CPU load on the device web STATUS page. [CPU load]
- Added feature “RFC2543 Hold”. [RFC2543 Hold]
- Added feature “Call Record”. [Call Record]
- Added feature “Use ARP to detect network connectivity”. [Use ARP to detect network connectivity]

Firmware Version 1.0.10.6

- Added feature “Visual MWI Type”. [Visual MWI Type]
- Added feature “Disable Unknown Caller ID”. [Disable Unknown Caller ID]
- Added feature “Disable # as Redial Key”. [Disable # as Redial Key]
- Added feature “Ring Frequency”. [Ring Frequency]
- Added feature “Allow SIP Factory Reset”. [Allow SIP Factory Reset]
- Added feature “Management Interface”. [Enable Management Interface] [Management Access] [Management Interface IPv4 Address]
- Added Web menu in Spanish. [Language]
- Added support to display WAN/LAN port cable status on the Web UI. [Network Cable Status]

Firmware Version 1.0.9.3

- Added support for G722 (wide-band) codec. [HT818 Technical Specifications]
- Added support for FTP/FTPS for provision and firmware upgrade. [UPGRADING AND PROVISIONING]

- Added feature “Conference Party Hang-up Tone” when “Special Feature” is set to MTS. [Call Progress Tones]

Firmware Version 1.0.8.7

- 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 support for “Blacklist for Incoming Calls”. [Blacklist for Incoming Calls]
- Added feature “Play busy/reorder tone before Loop Current Disconnect”. [Play busy/reorder tone before Loop Current Disconnect]
- Removed “Ring Frequency” from web UI

Firmware Version 1.0.5.18

- No major changes

Firmware Version 1.0.0.5

- This is the initial version for HT818