# HT81x V2 - Administration Guide

# PRODUCT OVERVIEW

The HT81x V2 analog telephone adapters (ATA) 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 allow service providers to offer high-quality IP service. The HT81x V2 are ideal ATAs for individual use and large-scale commercial IP voice deployments since it will enable small and medium businesses to create integrated IP and PSTN telephony systems that efficiently manage communication costs. HT81x V2'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 and the extension of VoIP services to analog phones.

## Feature Highlights

The following table contains the major features of the HT81x V2:

| | |
|---|---|
|  <br>**HT812 V2**<br>  <br>**HT814 V2**<br>  <br>**HT818 V2** | • Support 2 SIP profiles through 2 FXS ports for HT812 V2, 4 FXS port for HT814 V2 and 8 FXS port for HT818 V2.<br>• Support dual 10/100/1000Mbps Ethernet port.<br>• Support 3-way voice conferencing.<br>• Support wide range of caller ID formats.<br>• 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.<br>• Support T.38 Fax for creating Fax-over-IP.<br>• TLS and SRTP security encryption technology to protect calls and accounts.<br>• Automated provisioning options include TR-069 and XML Config files.<br>• Failover SIP server automatically switches to secondary server if main server loses connection.<br>• Use with Grandstream's UCM series of IP PBXs for Zero Configuration provisioning.<br>• Strong AES encryption with security certificate per unit.<br>• GR-909 Line Testing Functionalities.<br>• Exceptional voice quality with wide-band HD codec. |

*HT81x V2 Features at a Glance*

## HT81x V2 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 HT81x V2.

| **Interfaces** | |
|---|---|
| **Telephone Interfaces** | Two (2) RJ11 FXS ports for HT812 V2.<br>Four (4) RJ11 FXS sports for HT814 V2.<br>Eight (8) RJ11 FXS ports for HT818 V2. |
| **Network Interface** | Two (2) 10/100/1000 Mbps Ethernet port (RJ45). |

| | |
|---|---|
| **LED Indicators** | POWER, LAN, WAN, PHONE1, PHONE2 for HT812 V2.<br>POWER, LAN, WAN, PHONE1, PHONE2, PHONE3, PHONE4 for HT814 V2.<br>POWER, NET1, NET2, PHONE1, PHONE2, PHONE3, PHONE4, PHONE 5, PHONE 6, PHONE 7 and PHONE 8 for HT818 V2. |
| **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** | For HT812 V2: 3 REN, up to 1km on 24AWG line.<br>For HT814 V2 and HT818 V2: 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,<br>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<br>Output: 12V/0.5A for HT812 V2.<br>Output: 12V/1A for HT814 V2.<br>Output: 12V/1.5A for HT818 V2. |

| | |
|---|---|
| **Environmental** | Operational: 32° – 104 °F or 0º – 40ºC.<br>Storage: 14° – 140 °F or -10º – 60ºC.<br>Humidity: 10 – 90% Non-condensing. |
| **Dimensions and Weight** | Dimension : 36 x 120 x 180 mm (H x W x D)<br>Weight: 353.33g for HT812 V2, 423.5g for HT814 V2 and 356g for HT818 V2. |
| **Compliance** | |
| **Compliance** | FCC/CE/RCM. |

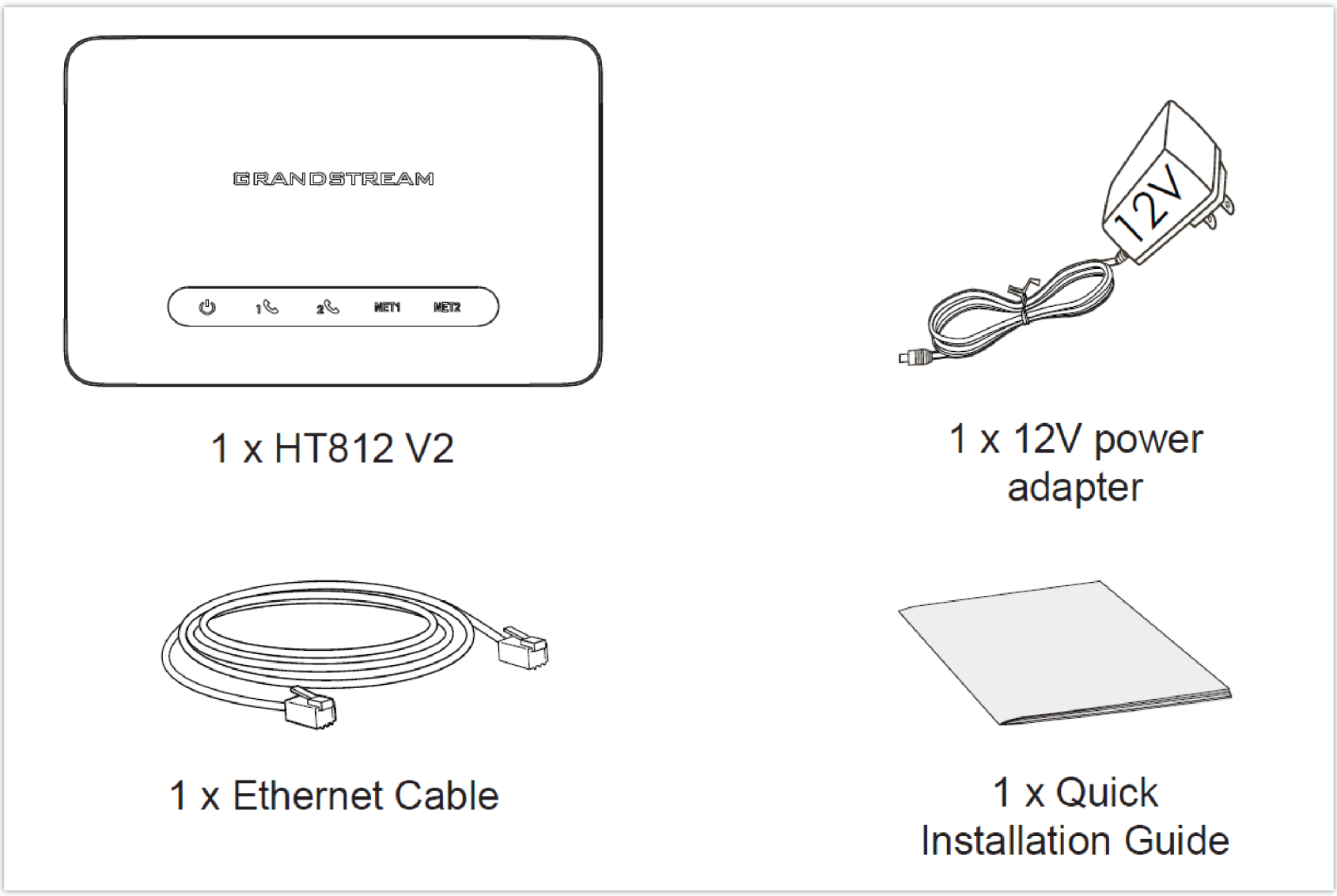
*HT81x V2 Technical Specifications*

# GETTING STARTED

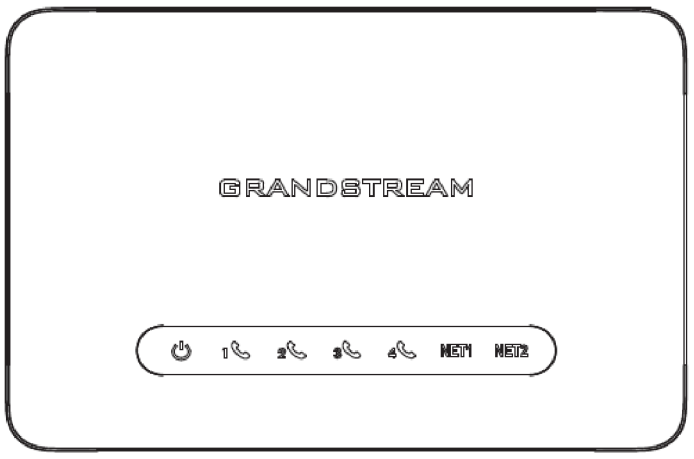
This chapter provides basic installation instructions including the list of the packaging contents and also information for obtaining the best performance with the HT81x V2.

## Equipment Packaging

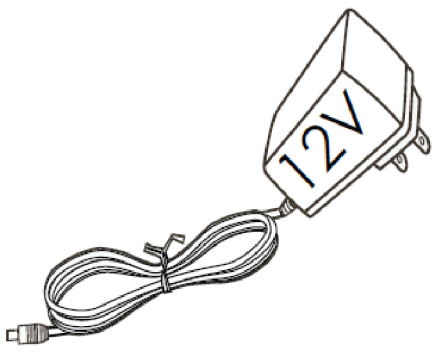
The HT81x V2 ATAs package contains



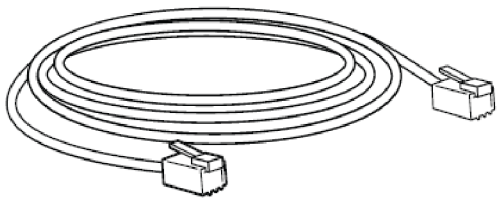

*HT812 V2 Package Contents*



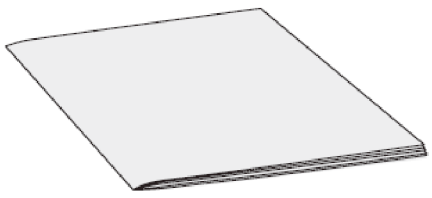

1 x HT814 V2




1 x 12V power adapter

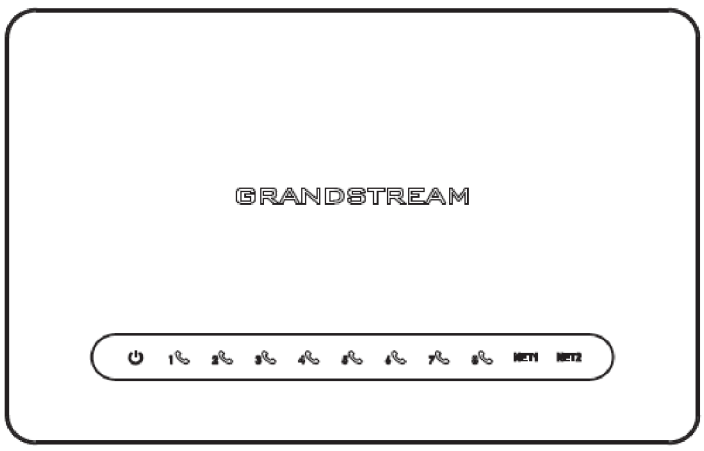


1 x Ethernet Cable

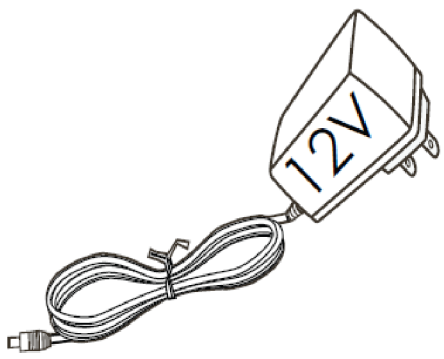


1 x Quick Installation Guide

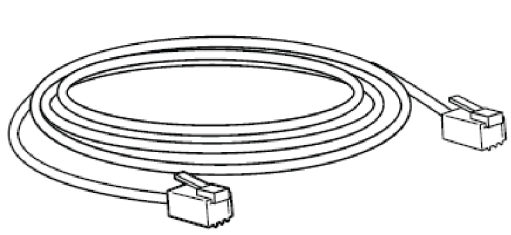
*HT814 V2 Package Contents*



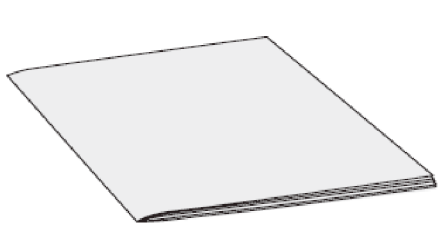

1 x HT818 V2




1 x 12V power adapter



1 x Ethernet Cable



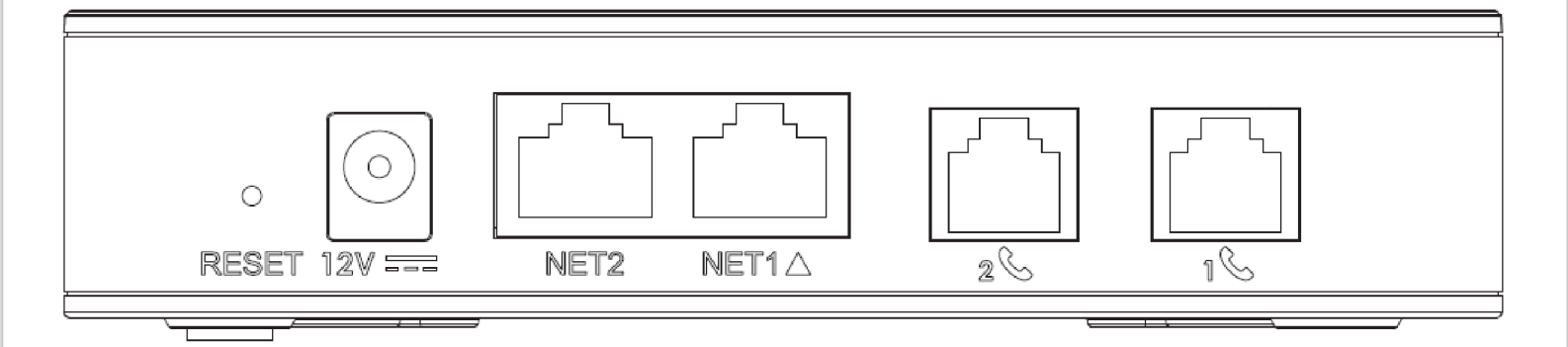
1 x Quick Installation Guide

*HT818 V2 Package Contents*

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

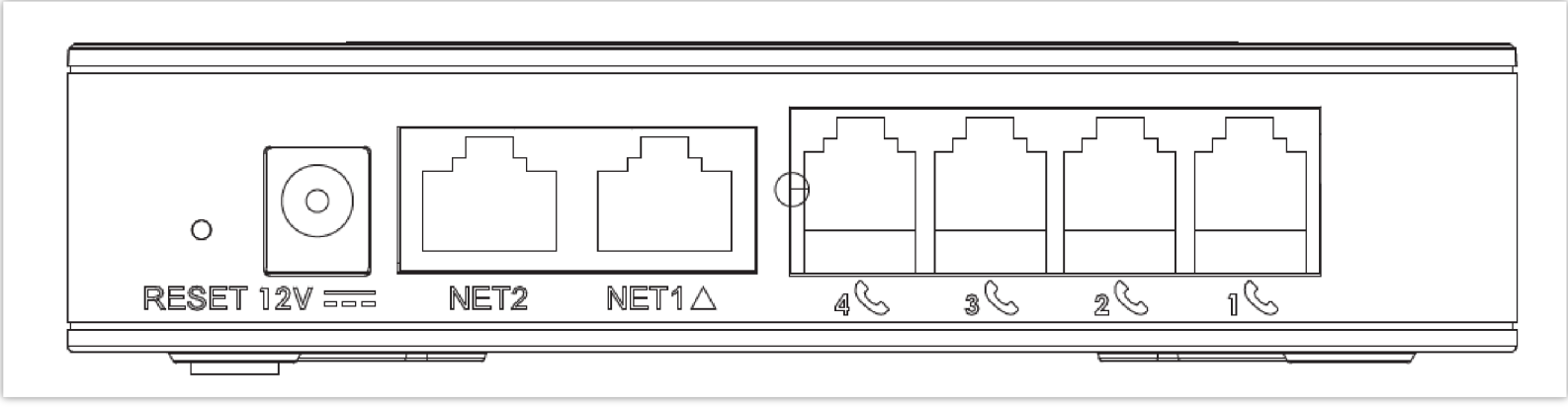
## HT81x V2 Ports Description

The following figure describes the different ports on the back panel of the HT81x V2.




*HT812 V2 Ports*

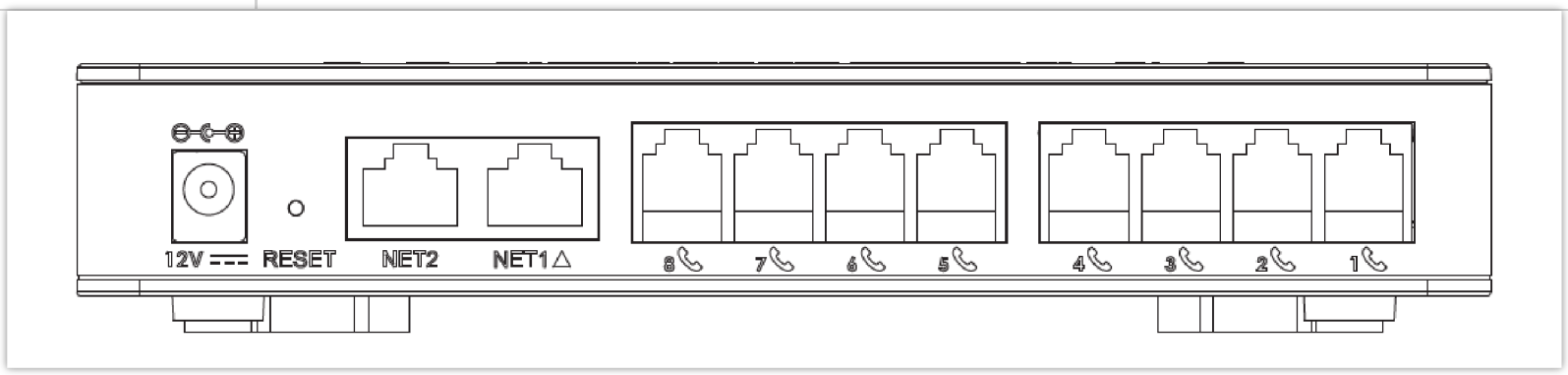
| Port | Description |
| --- | --- |
| 12V | Power socket. Used to power HT812 V2 (12V) |
| NET1 | NET1 port. Can be configured as LAN or WAN port on the HT812 V2. By default, it is considered a WAN port. |
| NET2 | NET2 port. Can be configured as LAN or WAN port on the HT812 V2. By default, it is considered a LAN port. |
| 1 2 | FXS ports to connect analog phones / fax machines to HT812 V2 using RJ11 telephone cable. |
| RESET | Factory reset button. Press for 7 seconds to reset to factory default settings. |




*HT814 V2 Ports*

| Port | Description |
| --- | --- |
| 12V | Power socket. Used to power HT814 V2 (12V) |
| NET1 | NET1 port. Can be configured as LAN or WAN port on the HT814 V2. By default, it is considered a WAN port. |
| NET2 | NET2 port. Can be configured as LAN or WAN port on the HT814 V2. By default, it is considered a LAN port. |
| 1 --- 4 | FXS ports to connect analog phones / fax machines to HT814 V2 using RJ11 telephone cable. |

| | |
|---|---|
| RESET | Factory reset button. Press for 7 seconds to reset to factory default settings. |




*HT818 V2 Ports*

| Port | Description |
|---|---|
| 12V ⎓ | Power socket. Used to power HT818 V2 (12V) |
| NET1 △ | NET1 port. Can be configured as LAN or WAN port on the HT818 V2. By default, it is considered a WAN port. |
| NET2 | NET2 port. Can be configured as LAN or WAN port on the HT818 V2. By default, it is considered a LAN port. |
| 1 --- 8 | FXS ports to connect analog phones / fax machines to HT818 V2 using RJ11 telephone cable. |
| RESET | Factory reset button. Press for 7 seconds to reset to factory default settings. |

## Connecting the HT81x V2

The HT81x V2 can be connected via NET1 port or NET2 port, by default, **NET1** is **WAN (DHCP Client)** and **NET2** is **LAN (DHCP Server)**.

### Scenario 1: Connecting the HT81x V2 Using NET1 port

When connecting HT81x V2 using the NET1 port, it will act as a simple DHCP Client:

1. Insert a standard RJ11 telephone cable into an FXS port and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect the NET1 port of the HT81x V2 to a router, switch or modem using an Ethernet cable.
3. Insert the power adapter into the HT81x V2 and connect it to a wall outlet (make sure to respect the technical specifications of the power adapter used).
4. The Power, NET1 and FXS LEDs will be solidly lit when the HT81x V2 is ready for use.

### Scenario 2: Connecting the HT81x V2 Using NET2 port

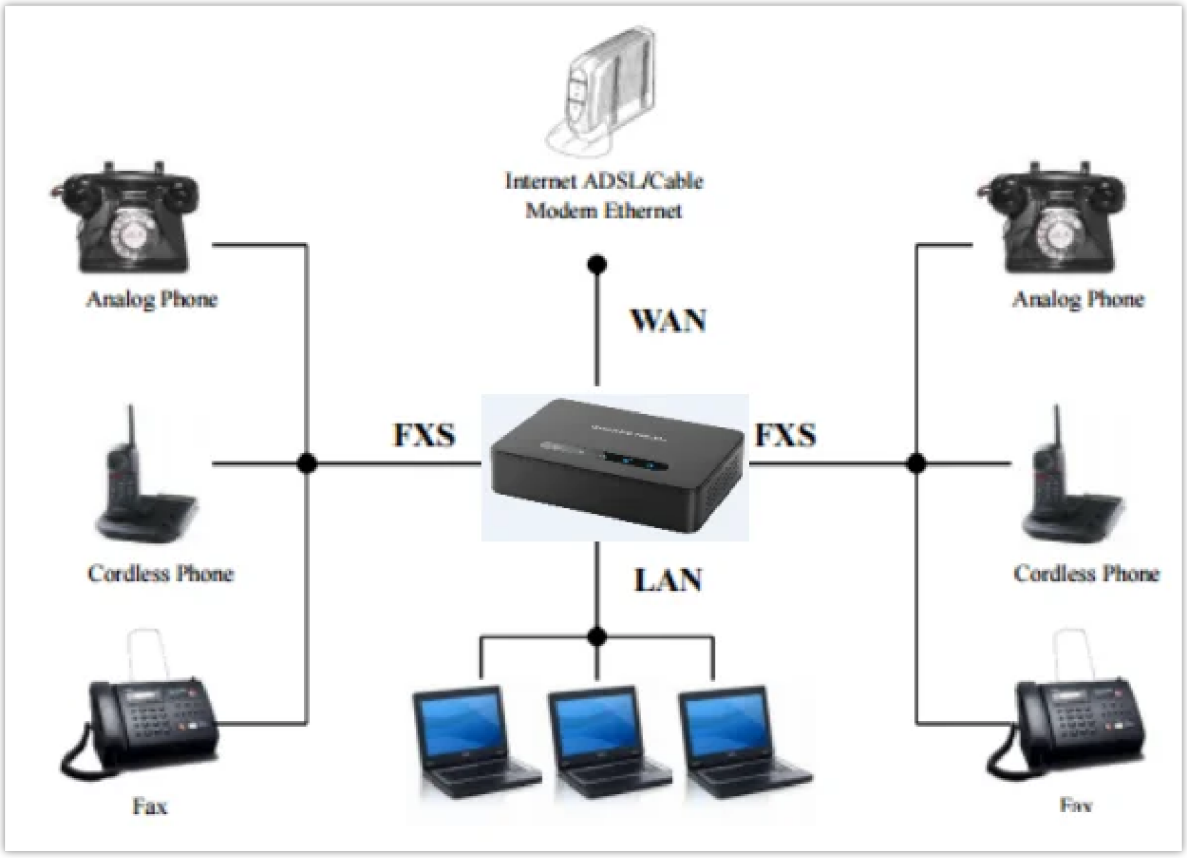
When connecting the HT81x V2 using the NET2 port, it will act as a DHCP Server:

1. Insert a standard RJ11 telephone cable into an FXS port and connect the other end of the telephone cable to a standard touch-tone analog telephone.
2. Connect a computer or switch to the NET2 port of the HT81x V2 using an Ethernet Cable.

3. Insert the power adapter into the HT81x V2 and connect it to a wall outlet and make sure to respect the technical specifications of the power adapter used.
4. The Power, NET2 and FXS LEDs will be solidly lit when the HT81x V2 is ready for use.

**Note:**

HT81x V2 supports switching the working mode of NET1 and NET2 on Web User interface.




*Connecting the HT81x V2*

## HT81x V2 LEDs Pattern

There are four (4) LED types that help you manage the status of your HT81x V2.


*HT812 V2 LEDs Pattern*

| LED Lights | Status |
|---|---|
| **Power LED** | The Power LED lights up when The HT812 V2 is powered on and it flashes when the HT812 V2 is booting up |
| **NET1 LED** | The NET1 LED lights up when The HT812 V2 is connected to your network through the NET1 port. |

| | |
|---|---|
| **NET2 LED** | The NET2 LED lights up when The HT812 V2 is connected to your network through the NET2 port. |
| **Phone LED 1-2** | The phone LEDs indicate status of the respective FXS port-phone on the back panel<br>● OFF – Unregistered<br>● ON (Solid Blue) – Registered and Available List Item 2<br>● Blinking every 500 ms – Off-Hook / Busy<br>● Slow blinking – FXS LEDs indicates voicemail |

*HT812 V2 LEDs Pattern Description*


*HT814 V2 LEDs Pattern*

| LED Lights | Status |
|---|---|
| **Power LED** | The Power LED lights up when The HT814 V2 is powered on and it flashes when the HT814 V2 is booting up |
| **NET1 LED** | The NET1 LED lights up when The HT814 V2 is connected to your network through the NET1 port. |
| **NET2 LED** | The NET2 LED lights up when The HT814 V2 is connected to your network through the NET2 port. |
| **Phone LED 1-4** | The phone LEDs indicate status of the respective FXS port-phone on the back panel<br>● OFF – Unregistered<br>● ON (Solid Blue) – Registered and Available List Item 2<br>● Blinking every 500 ms – Off-Hook / Busy<br>● Slow blinking – FXS LEDs indicates voicemail |


*HT818 V2 LEDs Pattern*

| LED Lights | Status |
| --- | --- |
| **Power LED** | The Power LED lights up when The HT818 V2 is powered on and it flashes when the HT818 V2 is booting up |
| **NET1 LED** | The NET1 LED lights up when The HT818 V2 is connected to your network through the NET1 port. |
| **NET2 LED** | The NET2 LED lights up when The HT818 V2 is connected to your network through the NET2 port. |
| **Phone LED 1- 8** | The phone LEDs indicate status of the respective FXS port-phone on the back panel<br>● OFF – Unregistered<br>● ON (Solid Blue) – Registered and Available List Item 2<br>● Blinking every 500 ms – Off-Hook / Busy<br>● Slow blinking – FXS LEDs indicates voicemail |

# CONFIGURATION GUIDE

The HT81x V2 can be configured in one of two ways:

- The IVR voice prompt menu.
- The Web GUI is embedded on the HT81x V2 using the PC's web browser.

## Obtain HT81x V2 IP Address via Connected Analog Phone

HT81x V2 are by default configured to obtain the IP address from the DHCP server where the unit is located. To know which IP address is assigned to your HT81x V2, you should access the "Interactive Voice Response Menu" of your adapter via the connected phone and check its IP address mode.

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

1. Use a telephone connected to the phone ports (FXS) of your HT81x V2.
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 HT81x V2 Interactive Voice Prompt Response Menu

The HT81x V2 have 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 HT81x V2. 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<br>Press "#" to return to the main menu<br>Enter 01-05, 07,10, 12-17, 20, 47 or 99 menu options |
| 01 | "DHCP Mode",<br>"Static IP Mode"<br>"PPPoE Mode" | Press "9" to toggle the selection<br>If using "Static IP Mode", configure the IP address information using menus 02 to 05.<br>If using "Dynamic IP Mode", all IP address information comes from the DHCP server automatically after reboot.<br>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.<br>You need to reboot your HT812 V2/HT814 V2/HT818 V2 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:<br>PCM U / PCM A<br>iLBC<br>G-726<br>G-723<br>G-729<br>OPUS<br>G722 |
| 10 | "MAC Address" | Announces the MAC address of the unit.<br>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. |

| | | |
|---|---|---|
| 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:<br>Always check<br>Check when pre/suffix changes<br>Never upgrade |
| 20 | Certificate Type | Annouces certificate information. |
| 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<br>Enter MAC address to restore factory default setting<br>(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 the menu option and 12 digits for the IP address. For IP address, add 0 before the digits if the digits are less than 3 (i.e. – 192.168.0.26 should be keyed in like 192168000026. No decimal is needed).
- Key entry cannot be deleted but the phone may prompt an error once it is detected.
- 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 HT81x V2 embedded Web server responds to HTTP GET/POST requests. Embedded HTML pages allow a user to configure the HT81x V2 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

The HT81x V2 can be connected via NET1 port or NET2 port, by default, **NET1** is **WAN (DHCP Client)** and **NET2** is **LAN (DHCP Server)**.

- **Via NET1 port**

For the initial setup, the Web access is by default enabled when the device is using a private IP and disabled when using a public IP, and you cannot access the Web UI of your HT81x V2 until it's enabled, the following steps will show you how to enable it via IVR.

1. Power your HT81x V2 using a PSU with the right specifications.
2. Connect your analog phone to the phone ports (FXS) of your HT81x V2.
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, and the IVR menu will announce that the web access is disabled, press 9 to enable it.
5. Reboot your HT81x V2 to apply the new settings.

Please refer to the steps below if your HT81x V2 is connected via the NET1 port:

1. You may check your HT81x V2 IP address using the IVR on the connected phone.

Please see Obtain the HT81x V2 IP address via the connected analog phone

2. Open the web browser on your computer.
3. Enter the HT81x V2'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 HT81x V2. This can be easily done by connecting the computer to the same hub or switch as the HT81x V2.

- **Via NET2 port**

Please refer to the steps below if your HT81x V2 is connected via NET2 port:

1. Power your HT81x V2 using PSU with the right specifications.
2. Connect your computer or switch directly to your HT81x V2 NET2 port.
3. Open the web browser on your computer.
4. Enter the default NET2 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

HT81x V2.

## Web UI Access Level Management

There are three access level for the login page:

| User Level | User | Password | Web Pages Allowed |
|---|---|---|---|
| End User Level | user | 123 | View all pages but can only modify basic settings |
| Administrator Level | admin | random password located at the back of the unit | Browse all pages and modify all settings |
| Viewer Level | viewer | viewer | View all pages but no changes allowed. |

**Note:**

- The password is case-sensitive and must contain 8-20 characters, at least one number, one uppercase, and one lowercase letter.
- When changing any settings, always submit them by pressing the Update or Apply button at the bottom of the page.
- Some changes require a reboot of the HT81x V2 unit such as FXS Port settings.
- By default, user and viewer access levels are disabled. In order to enable them please access **System Settings → Security Settings → Web Access**.
- After initial login using the default admin/user password, the user will be prompted to change the password immediately.

## Saving the Configuration Changes

After modifying any configuration parameters, users can save the changes by clicking on the **Save** button. Once the configuration is saved, an **Apply** button will appear at the top of the page to allow users to apply the changes.

Users can also directly click on the **Save and Apply** button for the configuration changes to be saved and applied.

**Note:**

We recommend rebooting or powering cycling the phone after applying all the changes.

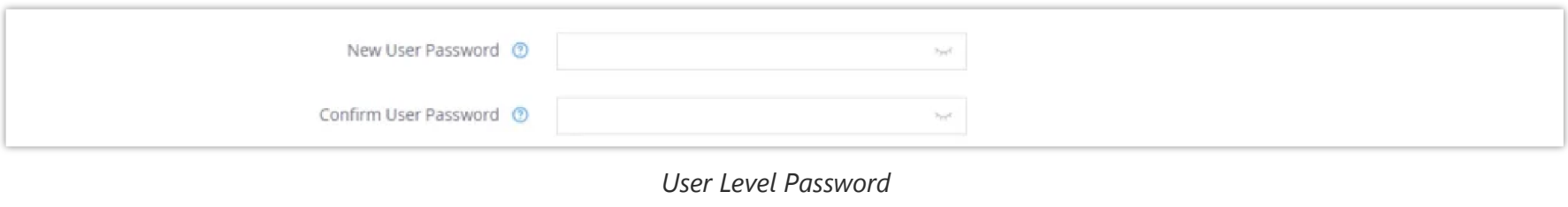
## Changing Admin Level Password

1. Access your HT81x V2 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default is the random password located at the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and enter the new admin password.
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 HT81x V2 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default is the random password located at the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and **e**nter the new end-user password.
5. Confirm the new end-user password.
6. Press **Apply** at the bottom of the page to save your new settings.



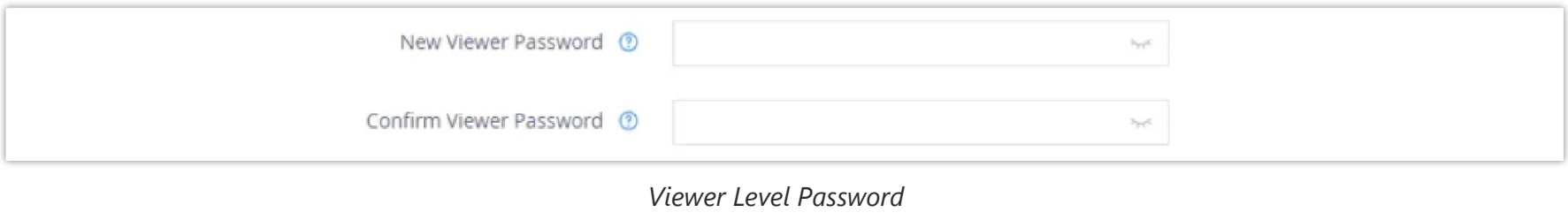

*User Level Password*

**Note**

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

## Changing Viewer Password

1. Access your HT81x V2 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default is the random password located at the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings → User Info Management** and **e**nter the new viewer password.
5. Confirm the new viewer password.
6. Press **Apply** at the bottom of the page to save your new settings.




*Viewer Level Password*

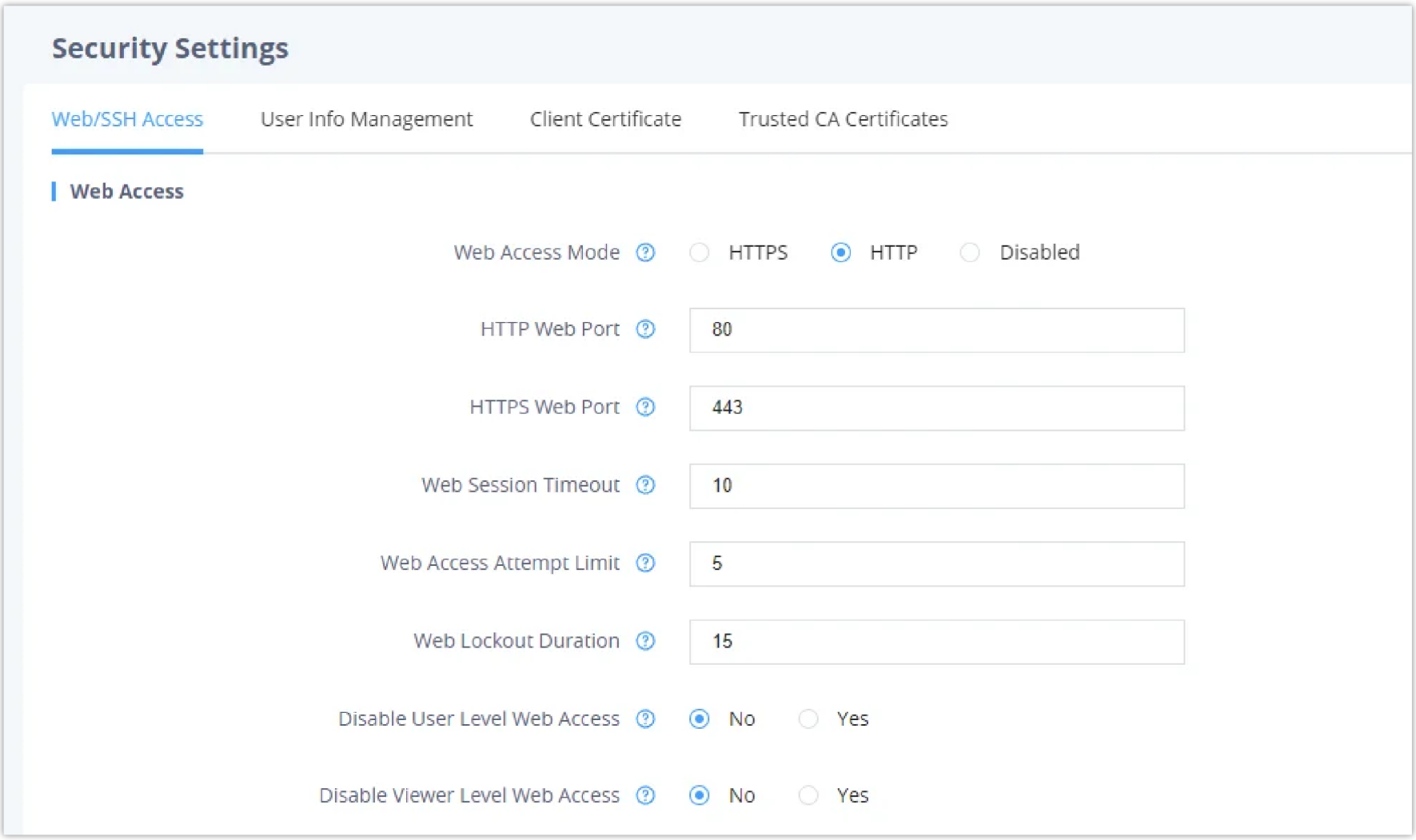
**Note**

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

## Changing HTTP Web Port

1. Access your HT81x V2 web UI by entering its IP address in your favorite browser.
2. Enter your admin password (default is the random password located at the back of the unit).
3. Press **Login** to access your settings.
4. Go to **System Settings → Security Settings→ Web/SSH Access.**
5. Make sure that the **Web Access Mode** is set to **HTTP**.
6. Change the current port to your desired/new HTTP port. Ports accepted are in the range [1-65535].

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




## Web Configuration Pages Definitions

This section describes the options in the HT81x V2 Web UI. As mentioned, you can log in as an administrator or an end user.

## Status Page Definitions

### System Info

| | |
|---|---|
| **Product Model** | Displays the Product model: HT812V2, HT814V2 or HT818V2. |
| **Serial Number** | Displays the device's serial number |
| **Hardware Version** | Displays the hardware version |
| **Part Number** | Displays the part number |
| **Software Version** | • **Program:** Displays the current software version running on the device<br>• **Bootloader:** Displays the bootloader version<br>• **Core:** Displays the Core version<br>• **Base:** Displays the Base version<br>• **CPE:** Displays the Customer Premises Equipment version |
| **Software Status** | Displays whether the software is running correctly on the device |
| **Mem** | Displays the memory usage |
| **System Up Time** | Displays the duration of the system up time |
| **System Current Time** | Displays the HT8xx current time |
| **CPU Load** | Displays the processor load |

| | |
|---|---|
| **Provision** | Displays the last status of provisioning |
| **System Info** | Downloads the system info |

## Network Status

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

## Port Status

| | |
|---|---|
| **Port Status** | |
| **Port** | Displays the type of analog port : FXS1, FXS2, FXS3....FXS8 |
| **Hook** | Shows the status of the port, On Hook, Off Hook, Not connected... |
| **User ID** | Displays the SIP user ID registred on the port. |
| **Registration** | Displays wether the port is registered or not. |
| **Sip Port** | Displays the SIP Destination port used by the analog interface. |
| **Port Options** | |
| **Port** | Displays the FXS ports. |
| **DND** | Displays whether the connected analog phone is on DND mode or not. |
| **Forward** | Indicates the forwarding number. |
| **Busy Forward** | Indicates the busy forwarding number. |

| | |
|---|---|
| **Delayed Forward** | Indicates the delayed forwarding number. |
| **CID** | Indicates the Caller ID. |
| **Call Waiting** | Indicates if Call waiting is enabled. |
| **SRTP** | Indicates if Secured RTP is enabled. |

## System Settings Page Definitions

### Basic Settings

| | |
|---|---|
| **Enable Voice Prompt** | The voice prompt is disabled if set to Yes.<br>Default value is "Yes". |
| **Enable Direct IP Call** | The direct IP calling is disabled if set to Yes.<br>Default value is "Yes". |
| **Blocklist For Incoming Calls** | Blocks calls from specific numbers. Use "," to separate numbers. |
| **Lock Keypad Update** | The configuration update via keypad is disabled if set to Yes. Default value is "No" |
| **Play Busy Tone When Account is unregistered** | If set to Yes, busy tone will be played when user goes offhook from an unregistered account.<br>Default value is "No". |
| **Hunting Group Registration Mode** | The Hunting Group Registration Mode determines how SIP registration works for a group of FXS ports.<br>● **Active Port Only (Default):** Only the currently active port in the hunting group registers with the SIP server, this reduces unnecessary registrations.<br>● **All Ports:** All FXS ports in the hunting group register individually, which ensures each port can receive calls independently. |
| **DHCP Option 17 Enterprise Number** | Fill in the DHCP Option 17 enterprise number. Range: 0-65535. Default is 3561. |
| **ATA Setting** | |
| **STUN Server** | The IP address or domain name of the STUN server. Only non-symmetric NAT routers work with STUN. |
| **Keep-Alive Interval** | Specifies how often the device sends a blank UDP packet to the SIP server in order to keep the "ping hole" on the NAT router to open. Default is 20 seconds. Range is 10-160 seconds. |
| **Use STUN to detect network connectivity** | Use STUN keep-alive to detect WAN side network problems.<br>Disabled by default |

### Time and Language

| | |
|---|---|
| **Time Zone** | |

| | |
|---|---|
| **NTP Server** | This parameter sets the IP address of the NTP server. The device will obtain the date and time from the server. |
| **Secondary NTP Server** | This feature allows users to configure the secondary NTP server, by default, no secondary NTP Server is configured. |
| **Allow DHCP Option 42 to override NTP server** | If DHCP Option 42 is enabled, the NTP server can be changed. Enabled by default. |
| **Time Zone** | Selects the time zone where the phone is located and control the date/time display.<br>**Note:** the self-defined time zone can be selected. |
| **Self-Defined Time Zone** | Allows users to define their own time zone when time zone is set to "Using self-defined Time Zone"<br><br>The syntax is: std offset dst [offset], start [/time], end [/time]<br>Default is set to: MTZ+6MDT+5,M3.2.0,M11.1.0<br><br>MTZ+6MDT+5<br><br>This indicates a time zone with 6 hours offset with 1 hour ahead (when daylight saving) which is U.S central time. If it is positive (+) if the local time zone is west of the Prime Meridian (A.K.A: International or Greenwich Meridian) and negative (-) if it is east.<br><br>M4.1.0,M11.1.0<br>The 1st number indicates Month: 1,2,3.., 12 (for Jan, Feb, .., Dec)<br>The 2nd number indicates the nth iteration of the weekday: (1st Sunday, 3rd Tuesday…)<br>The 3rd number indicates weekday: 0,1,2,..,6 (for Sun, Mon, Tues, … ,Sat)<br>Therefore, this example is the DST which starts from the Second Sunday of March to the 1st Sunday of November. |
| **Allow DHCP server to set Time Zone** | Allows the local server's DHCP option 2 to override the phone's time zone setting. Default is "Yes". |
| **Local Time** | Allows the HT8xx device to get information about the time and date from the PC |
| **Language** | |
| **IVR Language** | Selects IVR voice prompt language type, the supported languages are: English, Chinese, Russian, Spanish. |

## Ringtone

| | |
|---|---|
| **System Ring Cadence** | Cadence on+off value range (0, 16000) milliseconds |
| **Prompt Tone Access Code** | The key pattern to get Prompt Tone. Maximum 20 digits. No default value provided |
| **CPT Settings:**<br><br>● Dial Tone<br>● Ringback Tone<br>● Busy Tone<br>● Reorder Tone<br>● Confirmation Tone<br>● Call Waiting Tone<br>● Wait for Dial-Tone | Using these settings, users can configure tone frequencies and cadence according to their preferences. By default, they are set to North American frequencies.<br>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. 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.<br><br>Example configuration for N.A. |

| | |
|---|---|
| • Conference Party Hangup Tone<br>• Special Proceed Indication Tone<br>• Special Condition Tone | **Dial tone:**<br>f1=350@-17,f2=440@-17,c=0/0;<br><br>**Syntax:** Syntax: f1=val[,f2=val[,c=on1/off1[-on2/off2[-on3/off3]]]]<br>(Frequencies are in (10, 4000) Hz and cadence on and off are in (0, 64000) ms) |

## Security Settings

| **Web/SSH Access** | |
|---|---|
| **Web Access Mode** | Sets web page access protocol, the options are: HTTP, HTTPS, Disabled.<br>The default web access mode is "HTTP" |
| **HTTP Web Port** | Defines the HTTP Web Port. Range: 1-65535, defaut is 80 |
| **HTTPS Web Port** | Defines the HTTPS Web Port. Range: 1-65535, defaut is 443 |
| **Web Session Timeout** | Defines the web session timeout, default value is 10 Minutes, the valid range is 1-60 minutes |
| **Web Access Attempt Limit** | Defines the Web Access Attempt Limit before locking the web access, default is 5, valid range is 1-10 |
| **Web Lockout Duration** | Defines for how long the web access will be locked, default value is 15 Minutes, valid range is 0-60 Minutes |
| **Disable User Level Web Access** | Disables or enables user-level web access.<br>Default value is "Yes" : the user level web access is disabled. |
| **Disable Viewer Level Web Access** | Disables or enables viewer-level web access.<br>Default value is "Yes" : the viewer level web access is disabled. |
| **Disable SSH** | If set to "No", the phone will allow SSH access,<br>Set to "No" by default |
| **SSH Port** | Defines the SSH port, default is 22. Cannot be the same as Telnet Port. |
| **SSH Idle Timeout** | Configures SSH session Timeout. Range is 0-86400 seconds. Default is 0 which means no session timeout. |
| **Disable Telnet** | Enables/disables Telnet access. The default is "Yes" |
| **Telnet Port** | Defines the telnet port, the default is 23. Cannot be the same as SSH Port. |
| **Telnet Idle Timeout** | Configures Telnet session Timeout. Range is 0-86400 seconds. Default is 0 which means no session timeout. |
| **Security Controls for SSH/Telent Access** | Specifies security measures and controls that apply to the SSH/Telnet protocol to ensure secure and authorized access to the device, the following options are supported<br><br>• **Only Allow SSH private IP users to set system Pvalue:** This option permits only users with SSH access from private IP addresses to modify specific system-level configuration parameters (system Pvalues).<br>• **Allow all SSH users to set system Pvalue:** With this setting, all users having SSH access can modify specific system-level configuration parameters (system Pvalues). |

| | |
|---|---|
| | ● **Allow all SSH users to set any Pvalue:** This allows all users with SSH access to modify any configuration parameter (P-value).<br>● **Allow any user to set any Pvalue:** Any user, regardless of their privileges, can modify any configuration parameter (Pvalue) through SSH or Telnet access.<br>● **Prohibit setting Pvalue:** This option blocks all users from modifying any configuration parameter (Pvalue) via SSH or Telnet access.<br>The Default Value is "**Allow any user to set any PValue**" |
| **WAN Side Web/SSH Access** | Enables/Disables the Web and SSH access through the WAN port. The available options are the following:<br>● **No:** No access to the web or SSH from any IP address on the WAN side.<br>● **Yes:** Access for the Web GUI and SSH is enabled on the WAN side.<br>● **Auto:** Only private IP could access the web or SSH on the WAN side.<br>Default setting is Auto. |
| **White List for WAN Side** | If WAN Side Web/SSH Access is set to Yes or Auto. Users can configure the white List for WAN Side to be used for remote management.<br>Multiple IPs are supported and need to be separated by space.<br>**Example:**192.168.5.222 192.168.5.223 192.168.7.0/24<br>**Note:** If both blacklist and whitelist are not empty, the blacklist is processed first, followed by the whitelist. |
| **Black List for WAN Side** | If WAN Side Web/SSH Access is set to Yes or Auto. Users can configure the black List for WAN Side to ban WAN side web access.<br>Multiple IPs are supported and need to be separated by space.<br>**Example:**192.168.5.222 192.168.5.223 192.168.7.0/24<br>**Note:** If both blacklist and whitelist are not empty, the blacklist is processed first, followed by the whitelist. |
| **User Info Management** | |
| **Enable strict password rules** | Enable strict password rules. |
| **Minimum password length** | Defines the Minimum password length, Range: 4-30, default is 8. |
| **Required number of character classes** | Sets the minimum number of character classes that a password should contain, composed of allowed combinations of different character classes;Range: 0-4, default is 3. |
| **Allowed Character classes** | Defines the Allowed Character classes, which are: Lower case, Upper case, Numbers, Special characters. |
| **New Admin Password** | Defines the new admin password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons. |
| **Confirm Admin Password** | Confirms the entered admin password. |
| **New User Password** | Defines the new user password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons. |
| **Confirm User Password** | Confirms the entered user password. |

| | |
|---|---|
| **New Viewer Password** | Defines the new viewer password, Must contain 4-30 characters, When strict password rules are enabled, the password needs to comply with the settings in the password rules; Do not display password for security reasons. |
| **Confirm Viewer Password** | Confirms the entered viewer password. |
| **Client Certificate** | |
| **Disable Weak TLS Cipher Suites** | Allows users to disable weak ciphers DES/3DES and RC4, Symmetric Encryption SEED, Symmetric Encryption Encryption IDEA/eNULL, Symmetric Authentication MD5, Protocol Version SSLv2/SSLv3, Server Authentication aNULL/aECDH, Key Exchange Algorithm kRSA, or Disable All of the Above Weak Symmetric Encryption/Symmetric Authentication/Protocol Version/Server Authentication/Key Exchange/TLS Ciphers Suites.<br>Default is "Enable Weak TLS Ciphers Suites". |
| **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.<br>Maximum supported length is 8192. |
| **SIP TLS Private Key** | Specifies TLS private key used for SIP over TLS is in X.509 format.<br>Maximum supported length is 4069. |
| **SIP TLS Private Key Password** | Specifies SSL Private key password used for SIP Transport in TLS/TCP. |
| **Validate Server Certificates** | This feature allows users to validate server certificates with our trusted list of TLS connections. The device needs to reboot after changing the setting.<br>Default is Disabled. |
| **Minimum TLS Version** | This feature allows customer to choose desired Minimum TLS Version.<br>Choices are:<br>Unlimited<br>TLS 1.0<br>TLS 1.1<br>TLS 1.2<br>Default is Unlimited. |
| **Maximum TLS Version** | This feature allows customer to choose desired Maximum TLS Version.<br>Choices are:<br>Unlimited<br>TLS 1.0<br>TLS 1.1<br>TLS 1.2<br>Default is Unlimited. |
| **Custom Certificate** | Allows users to update to the device their own certificate signed by a custom CA certificate to manage client authentication. |
| **Trusted CA Certificates** | |
| **Load CA Certificates** | This feature allows user to specify which certificate to trust when performing server authentication.<br>**Build-in trusted:** (Default) Build-in trusted certificates<br>**Custom trusted certificate:** Uploaded Certificates<br>**All trusted Certificates:** Both built-in and uploaded Certificates |
| • **Trusted CA Certificates A**<br>• **Trusted CA Certificates B**<br>• **Trusted CA Certificates C** | These trusted CA certificates will be used for the authentication server TLS certificate |

| | |
|---|---|
| • **Trusted CA Certificates D** | |

## TR069

| | |
|---|---|
| **Enable TR-069** | Sets the phone adapter system to enable the “CPE WAN Management Protocol” (TR-069). The default setting is Yes.<br>**Note:** When configured, users can send a "false ring" signal through the TR-069 protocol for testing pruposes. |
| **ACS URL** | Specifies URL of TR-069 Auto Configuration Servers (e.g., http://acs.mycompany.com), or IP address.<br>Default setting is: “https://acs.gdms.cloud” |
| **ACS Username** | Enter username to authenticate to ACS. Maximum allowed length is 64. |
| **ACS Password** | Enter password to authenticate to ACS. Maximum allowed length is 64. |
| **Periodic Inform Enable** | Sends periodic inform packets to ACS. Default is Yes.<br>**Note:** FXS port status can be detected through TR-069. |
| **Periodic Inform Interval** | Sets frequency that the inform packets will be sent out to ACS.<br>Default is 86400 seconds. |
| **Connection Request Username** | Enters username for ACS to connect to the HT81x V2. |
| **Connection Request Password** | Enters password for ACS to connect to the HT81x V2. |
| **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.<br>Maximum allowed length is 8192 |
| **CPE SSL Private Key** | Specifies the Cert Key for the phone adapter to connect to the ACS via SSL. Maximum allowed length is 2048 |

## RADIUS Settings

| | |
|---|---|
| **Enable RADIUS Web Access Control** | Selects whether to enable RADIUS web access control. Default is no |
| **Action upon Radius Auth Server Error** | Select the RADIUS authentication server error handling method,the user can choose between: Reject Access, or Authentificate locally,  the default is "local verification" |
| **RADIUS Auth Protocol** | Configures RADIUS authentication protocol |
| **RADIUS Auth Server Address** | Configures RADIUS authentication server address |
| **RADIUS Auth Server Port** | Configure RADIUS authentication server port |
| **RADIUS Shared Secret** | Configures the shared secret key |

| | |
|---|---|
| **RADIUS VSA Vendor ID** | Configure the RADIUS VSA provider ID to match the RADIUS server's configuration. The default value for Grandstream Networks Inc is 42397 |
| **RADIUS VSA Access Level Attribute** | Configure the RADIUS VSA access level attributes to match the configuration of the RADIUS server. Incorrect settings will cause Radius authentication to fail. |

## E911/HELD

| | |
|---|---|
| **E911** | |
| **Enable E911** | Enable Enhanced 911 call. Default is disabled |
| **E911 Emergency Numbers** | A user can configure multiple emergency numbers separated with the delimiter symbol ";". Default is 911. |
| **Geolocation-Routing Header** | If "Yes", E.911 INVITE message includes the "Geolocation-Routing" header with the value "Yes". Default is "No". |
| **Priority Header** | If "Yes", E.911 INVITE message includes the "Priority" header with the value "emergency". Default is "No". |
| **HELD** | |
| **HELD Protocol** | Configure HELD transfer protocol. HTTP or HTTPS. Default is HTTP. |
| **HELD Synchronization Interval** | The valid synchronization interval is between 30 to 1440 minutes. The synchronization is off when the interval is 0. Default is 0. |
| **HELD Location Types** | Configure "locationType" element in the location request. "geodetic", "civic" and "location URI". |
| **HELD Use LLDP Information** | If set to "Yes", LLDP protocol will be used to gather information about the HT device including information about the ChassisID and PortID. Otherwise, the system defaults to using the MAC address of the gateway and phone.<br><br>Default setting is "No". |
| **HELD NAI** | If 'Yes' is selected, the Network Access Identifier (NAI) is included as the device identity in location requests sent to the Location Information Server (LIS). Default is "No". |
| **HELD Identity 1-10** | The HELD Identity refers to Hierarchical Mobile IPv6 (HMIPv6) Enhanced Location-based Discovery (HELD) protocol. This protocol is utilized to determine the location of a mobile device when making an emergency call, such as a 911 call, over an IP-based network.<br>You can configure up to 10 HELD identities. Maximum allowed length is 64 |
| **HELD Identity 1-10 Value** | Defines the HELD Identity value. Maximum allowed length is 64 |
| **Location Server** | |
| **Location Server** | Configures the location server (LIS) address. |
| **Location Server Username** | Configures Location Server (LIS) username. Maximum allowed length is 64. |

| | |
|---|---|
| **Location Server Password** | Configures Location Server (LIS) password. Maximum allowed length is 64. |
| **Secondary Location Server** | Configures secondary location server (LIS) address. |
| **Secondary Location Server Username** | Configures secondary location server (LIS) username. Maximum allowed length is 64. |
| **Secondary Location Server Password** | Configures secondary location server (LIS) password. Maximum allowed length is 64. |

## Network Settings Page Definitions

### Ethernet Settings

| | |
|---|---|
| **General Settings** | |
| **Internet Protocol** | Selects one of the following IP protocol modes:<br>● **IPv4 Only:** Enforce IPv4 protocol only.<br>● **IPv6 Only:** Enforce IPv6 protocol only.<br>● **Both, Prefer IPv4:** Enable both IPv4 and IPv6 and prefer IPv4.<br>● **Both, prefer IPv6:** Enable both IPv4 and IPv6 and prefer IPv6.<br>**Note:** Make sure to reboot the HT801 V2/HT802 V2 unit for the changes to take effect. |
| *IPv4* | |
| **IPv4 address type** | Allows users to configure the appropriate network settings on the HT801 V2/HT802 V2 to obtain IPv4 address. Users could select DHCP, Static IP or PPPoE. By default, it is set to DHCP. |
| **Host Name (Option 12)** | 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** | Allows user to configure DHCP domain name. This option specifies the domain name that the client should use when resolving hostnames via the Domain Name System. This field is optional. |
| **Vendor Class ID (Option 60)** | Exchanges vendor class ID by clients and servers to convey particular configuration or other identification information about a client. Default is HT8XXV2. |
| **PPPoE account ID** | Defines the PPPoE username. Necessary if ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. |
| **PPPoE password** | Specifies the PPPoE account password. |
| **PPPoE Service Name** | Defines PPPoE service name. If your ISP uses a service name for the PPPoE connection, enter the service name here. This field is optional. |
| **Preferred DNS server 1-4** | Specifies preferred DNS server to use when DHCP or PPPoE are set.<br>You can set up yo 4 Preferred DNS Servers. |
| *IPv6* | |
| **IPv6 address type** | Configures the IPv6 address of the phone: |

| | |
|---|---|
| | • **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 FXO Gateway acquires its IP address from the first DHCP server it discovers from the LAN it is connected.<br>• **Statically configured as:** configure IP address, 1st and 2nd DNS server, preferred DNS server. These fields are set to zero by default. |
| **Static address type** | • **Full Static:** When enabling the option full static, users need to specify the Static IPv6 and the IPv6 Prefix length.<br>• **Prefix Static:** When enabling the option prefix static, users need to specify the IPv6 Prefix (64 bits). |
| **Static IPv6 Address** | When using fully static type IPv6, enter a static IPv6 address. |
| **IPv6 Prefix Length** | Enter the static IPv6 address prefix length. |
| **DNS Server 1** | Enter DNS server 1 address. |
| **DNS Server 2** | Enter DNS server 2 addres. |
| **Preferred DNS Server** | Enter preferred DNS server address. |
| *802.1x Settings* | |
| **802.1x Mode** | Allow users to enable/disable 802.1X Mode. The modes available are:<br>• EAP_MD5<br>• EAP_TLS<br>• EAP-PEAPv0/MSCHAPv2<br>Disabled by default. |
| **802.1x Identity** | Enter 802.1X identity information. |
| **802.1x Password** | Enter 802.1X MD5 password. |
| **802.1x CA Certificate** | Paste down the 802.1X certificate .pem file. |
| **802.1x Client Certificate** | Paste down the Client.pem certificate file containing certificate and key. Maximum allowed length is 8192. |

## SNMP Settings

| | |
|---|---|
| **Enable SNMP** | Enables the Simple Network Management Protocol.<br>Default is "No" |
| **SNMP Version** | Choose between (Version 1, Version 2c, or Version 3). |
| **SNMP Port** | Listening Port of SNMP. Valid range is 161 or 1025-65535. (Default is 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. Valid range is 162 or 1025-65535. (Default 162). |

| | |
|---|---|
| **SNMP Trap Version** | Choose between (Version 1, Version 2c, or Version 3). |
| **SNMP Trap Interval** | Time interval in minutes between traps. (Default is 5). |
| **SNMPv1/v2c Community** | Name of SNMPv1/v2c community. |
| **SNMPv1/v2c Trap Community** | Name of SNMPv1/v2c trap community. |
| **SNMPv3 User Name** | Username for SNMPv3. |
| **SNMPv3 Security Level** | **noAuthUser:** Users with security level noAuthnoPriv and context name as noAuth.<br>**authUser:** Users with security level authNoPriv and context name as auth.<br>**privUser:** Users with security level authPriv and context name as priv. |
| **SNMPv3 Authentication Protocol** | Select the Authentication Protocol: “None” or “MD5” or “SHA.” |
| **SNMPv3 Privacy Protocol** | Select the Privacy Protocol: “None” or “AES/AES128” or “DES”. |
| **SNMPv3 Authentication Key** | Enter the Authentication Key. |
| **SNMPv3 Privacy Key** | Enter the Privacy Key. |
| **SNMPv3 Trap User Name** | Username for SNMPv3 Trap. |
| **SNMPv3 Trap Security Level** | **noAuthUser:** Users with security level noAuthnoPriv and context name as noAuth.<br>**authUser:** Users with security level authNoPriv and context name as auth.<br>**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. |
| **MIB** | Downloads the MIB file, containg the Object identifiers. |

## DDNS Settings

| | |
|---|---|
| **Enable DDNS** | Enable DDNS function. Disabled by default. |
| **DDNS Server** | Select DDNS server used, options are:<br>● dyndns.org<br>● freedns.afraid.org<br>● zoneedit.com<br>● no-ip.com<br>● oray.net |
| **DDNS Username** | Sets the username of the DDNS server. |
| **DDNS Password** | Sets the password of the DDNS server. |

| | |
|---|---|
| **DDNS Hostname** | Sets the domain name of the DDNS server. |
| **DDNS Hash** | Sets the hash value of the DDNS server. |

## LAN Settings

| **General Settings** | |
|---|---|
| **Device Mode** | Controls whether the device is working in NAT Router, Bridge, or WAN Only mode.<br>● **NAT Router:** In this mode, the NET1 port acts as a DHCP client. NET2 port is used as DHCP Base IP; devices connected behind the NET2 port will be assigned an IP from the HT81x V2 DHCP Server.<br>● **Bridge:** In this mode, the NET1 port acts as a DHCP client and pass-through to the NET2 port; devices connected behind the NET2 port will get an IP from your network DHCP server (same as the NET1 port).<br>● **WAN Only:** In this mode, only the NET1 port is active. NET2 port is not used.<br>The default mode is NAT Router. Save the setting and reboot before configuring the HT81x V2. |
| **Enable UPnP support** | When set to Yes, the HT81x V2 acts as a UPnP gateway for your UPnP-enabled applications. UPnP = Universal Plug and Play. The default is No. |
| **Uplink bandwidth** | Specifies the maximum uplink bandwidth permitted by the device.<br>This function is disabled by default.<br>The total bandwidth can be set as 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M, or 15 M.<br>The primary function of this setting is to limit the uplink bandwidth for the device's internal system, signaling, and NATed traffic.<br>**Example:** When 512k is configured, there will be at least 512kbps limited for internal system, signaling, and NATed traffic.<br>**Note:** Voice or RTP stream will never be limited. |
| **Downlink bandwidth** | Specifies the maximum downlink bandwidth permitted by the device.<br>This function is disabled by default.<br>The total bandwidth can be set as 128K, 256K, 512K, 1M, 2M, 3M, 4M, 5M, 10M, or 15 M.<br>The primary function of this setting is to limit the download bandwidth for the device's internal system, signaling, and NATed traffic.<br>**Example:** if 128 is configured, there will be at least 128kbps limited for internal system, signaling, and NATed traffic.<br>**Note:** Voice or RTP stream will never be limited. |
| **DMZ IP** | This function forwards all WAN IP traffic to a specific IP address if no matching port is used by HT81x V2 or in the defined port forwarding. |
| **NAT maximum ports** | Defines the number of ports that can be managed while in NAT router mode.<br>Range: 0 - 4096, default is 1024. Typically, one port per connection |
| **NAT TCP timeout** | NAT TCP idle timeout in seconds. The connection will be closed after preconfigured, timeout if not refreshed. Range: 0 - 3600 |
| **NAT UDP timeout** | NAT UDP idle timeout in seconds. The connection will be closed after preconfigured, timeout if not refreshed. Range: 0 - 3600, default is 300 |
| **Reply to ICMP on WAN port** | When set to Yes, the HT81x V2 responds to the PING command from other computers but is also made vulnerable to DOS attacks. The default is No. |

| | |
|---|---|
| **Cloned WAN MAC Addr** | This allows the user to change/set a specific MAC address on the WAN interface.<br>Note: Set in Hex format. |
| **LAN Port VLAN Feature Under Bridge Mode** | This feature allows users to configure a different VLAN tag and priority value for the second network port when HT81x V2 is configured in bridge mode.<br>The priority value range is 0-7, The VLAN tag range is 0-4094.<br>The default VLAN Tag and Priority value are 0. |
| **Enable LAN DHCP** | When set to Yes, the device will function as a simple router and the LAN port will provide IP addresses to the internal network. Connect the WAN port to ADSL/Cable modem or any other equipment that provides access to the public Internet. The default setting is Yes. |
| **LAN DHCP Base IP** | Base IP Address for a LAN port.<br>The default factory setting is **192.168.2.1**.<br>**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.<br>For example; 192.168.2.1 will be changed to 192.168.3.1 if the netmask is 255.255.255.0. Then the device will reboot |
| **LAN DHCP Start IP** | The default value is 100. The last segment of IP address is assigned to the HT81x V2 in the LAN Network.<br>Default configuration assigns IP address (to local network devices) starting from 192.168.2.100. |
| **LAN DHCP End IP** | Default value is 199. This parameter allows a user to limit the number of local network devices connected to the internal router. |
| **LAN Subnet Mask** | Sets the LAN subnet mask.<br>Default value is 255.255.255.0 |
| **DHCP IP Lease Time** | Default value is 120 hrs. (5 days). The length of time the IP address is assigned to the LAN clients. Value is set in units of hours. |
| **Port Forwarding** | Forwards a matching (TCP/UDP) port to a specific LAN IP address with a specific (TCP/UDP) port.<br>Up to 8 rules are available. |

## Management Interface

| **Management Interface** | |
|---|---|
| **Enable Management Interface** | Allows activation of a dedicated interface for remote management and configuration of the device.<br>Disabled by Default. |
| **Management Access** | defines the allowed methods (protocols) and permissions for remote access and configuration of the device, two options can be selected<br>● **Management Interface Only:** allows remote access and configuration solely through the dedicated management interface<br>● **Both Service and Management Interfaces:** permits remote access and configuration through both the management interface and the service interface. |

| | |
|---|---|
| **Enable SNMP Through Management Interface** | Allows the activation of SNMP (Simple Network Management Protocol) access exclusively through the dedicated management interface for monitoring and managing the device remotely.<br>Disabled by Default. |
| **Enable TR069 Through Management Interface** | Allows the activation of TR-069 protocol access exclusively through the dedicated management interface for remote device management and provisioning.<br>Disabled by Default. |
| **Enable Syslog Through Management Interface** | Allows the activation of syslog communication exclusively through the dedicated management interface for remote logging and monitoring of device events.<br>Disabled by Default. |
| **Enable Radius Through Management Interface** | Configure routing so that Radius functionality is accessible through management. |
| **Management Interface IPv4 Address** | |
| **802.1Q/VLAN Tag** | Allows the tagging of network packets with VLAN information to segment and prioritize network traffic.<br>The Valid Range is 0-4094, Default value is 0 |
| **802.1p priority value** | Assigns a priority value to network packets for Quality of Service (QoS) and traffic prioritization purposes.<br>The Valid Range is 0-7, Default value is 0 |
| **IPv4 address type** | Configures the address type of the management network port, the options are:<br>● Dynamically configured by DHCP<br>● Statically configured as |
| **IP Address** | Configure the IPv4 address of the management network port |
| **Subnet Mask** | Defines the subnet mask |
| **Default Router** | Defines default gateway |
| **DNS Server 1** | Defines DNS server 1 address |
| **DNS Server 2** | Defines DNS server 2 address |

## OpenVPN® Settings

| | |
|---|---|
| **Enable OpenVPN®** | Allow user to enable OpenVPN®. Default is No. |
| **OpenVPN® Server Address** | Specify the IP address or FQDN for the OpenVPN® Server. |
| **OpenVPN® Port** | Specify the listening port of the OpenVPN® server. Default is 1194 |
| **OpenVPN® Server Secondary Address** | If the primary OpenVPN® server is unavailable, the device can automatically switch to a secondary VPN server, which ensures continuous secure connectivity. |
| **OpenVPN® Secondary Port** | Configures OpenVPN® Secondary Port. |
| **Randomly Select Server** | If enabled, the server will be randomly selected in the configuration to start OpenVPN requests. If closed, requests will be made in the order of server configuration. |

| | |
|---|---|
| | Disabled by default |
| **OpenVPN® Interface type** | Specify the Interface type of OpenVPN® whether TAP or TUN. Default is TUN. |
| **OpenVPN® Transport** | Specify the Transport Type of OpenVPN® whether UDP or TCP. The default is UDP. |
| **Enable OpenVPN® LZO Compression** | Enable OpenVPN® LZO Compression. Default is Yes. |
| **OpenVPN® Encryption** | Select the OpenVPN® Encryption. Default is BF-CBC 128 bit (default key). |
| **OpenVPN® Diges** | Select the OpenVPN® Digest. Default is SHA1. |
| **OpenVPN® Username** | Configure the OpenVPN® username. |
| **OpenVPN® Password** | Configure the OpenVPN® password |
| **OpenVPN® CA** | Specifies the OpenVPN® CA. Maximum Character Number is 8192. |
| **OpenVPN® Certificate** | Specifies the OpenVPN® Certificate. Maximum Character Number is 8192. |
| **OpenVPN® Client Key** | Specifies the Client Key. Maximum Character Number is 8192. |
| **OpenVPN® Client Key Password** | Configures the OpenVPN® Client Key Password. Maximum Length is 64. |

## Advanced Settings

| **Advanced Settings** | |
|---|---|
| **Enable LLDP** | Controls the LLDP (Link Layer Discovery Protocol) service.<br><br>The default setting is “Enabled”. |
| **LLDP TX Interval** | Configures LLDP TX Interval (in seconds). Valid range is 1 to 3600.<br><br>The Default value is 60. |
| **Enable CDP** | Enables/Disables CDP “Cisco Discovery Protocol”.<br><br>The default setting is “Enabled”. |
| **Layer 2 QoS 802.1Q/VLAN Tag** | Assigns the VLAN Tag of the Layer 2 QoS packets that can be used to identify and distinguish different VLANs.<br><br>Valid range is 0 to 4094. The default value is 0. |
| **Layer 2 QoS SIP 802.1p** | Prioritizes SIP traffic at Layer 2 using the 802.1p standard for Quality of Service (QoS).<br><br>The valid range 0-7. The default value is 0. |
| **Layer 2 QoS RTP 802.1p** | Prioritizes RTP (Real-time Transport Protocol) traffic at Layer 2 using the 802.1p standard for Quality of Service (QoS).<br><br>The valid range 0-7. The default value is 0. |

| | |
|---|---|
| **Use DNS to detect network connectivity** | Use DNS to detect WAN side network issues.<br><br>The default setting is "No". |
| **Use ARP to detect network connectivity** | Use ARP to check network connection.<br><br>The default value is "Yes". |
| ***Firewall settings*** | |
| **Black List for WAN Side Port** | Ports on the blocklist will be disabled on the device. |
| **Static DNS Cache** | |
| ***NAPTR*** | |
| **NAPTR DNS Cache Name** | The domain name to which this resource record refers.<br><br>Maximum length is 512 characters. |
| **NAPTR DNS Cache Time Interval (s)** | (Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again.<br><br>Valid range is from 300 to 65535. Default value is "300". |
| **NAPTR DNS Cache Order** | Specifies the order in which the NAPTR record need to be processed, low numbers are processed before high numbers.<br><br>Valid range is from 0 to 65535. Default value is "0". |
| **NAPTR DNS Cache 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.<br><br>Valid range is from 0 to 65535. Default value is "0". |
| **NAPTR DNS Cache Replacement** | This parameter contains the next FQDN to query for NAPTR, SRV, or address records.<br><br>Maximum length is 64 characters. |
| **NAPTR DNS Cache Service** | Specifies the services available in this domain. The replacement field is used to get to this service.<br><br>It can also specify the protocol used to communicate with the server that offers this service.<br><br>In SIP, three services are defined along with their resolution services (resolution services are defined after the “+” sign):<br><br>● “**SIPS+D2T**”: Secure SIP, TLS over TCP.<br>● “**SIP+D2T**”: SIP over TCP.<br>● “**SIPS+D2S**”: Secure SIP, TLS over SCTP.<br>● “**SIP+D2S**”: SIP over SCTP.<br>● “**SIP+D2U**”:SIP over UDP.<br><br>Maximum length is 64 characters and default value is "SIP+D2U". |
| ***SRV*** | |

| | |
|---|---|
| **SRV DNS Cache Name** | The domain name of the wanted service.<br><br>Maximum supported length is 512 characters. |
| **SRV DNS Cache Time Interval (s)** | (Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again.<br><br>Valid range is from 300 to 65535. Default value is "300". |
| **SRV DNS Cache 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.<br><br>Valid range is from 0 to 65535. Default value is "0". |
| **SRV DNS Cache Weight** | Specifies the weight for entries with the same priority. Larger weight will get higher priority.<br><br>Valid range is from 0 to 65535. Default value is "0". |
| **SRV DNS Cache Target** | The domain name of the target host.<br><br>Maximum supported length is 64 characters. |
| **SRV DNS Cache Port** | The port on the target host of the specified service.<br><br>The valid range is 0-65535. Default value is "0". |
| ***A*** | |
| **A DNS Cache Name** | The domain name to which the record refers.<br><br>Maximum supported length is 512 characters. |
| **A DNS Cache Time Interval (s)** | (Time to Live) refers to the time interval that the record may be cached before the source of the information should be consulted again.<br><br>Valid range is from 300 to 65535. Default value is "300". |
| **A DNS Cache IP Address** | The IP address associated with the DNS record name. |

## Maintenance Settings Page Definitions

### Upgrade

| | |
|---|---|
| **Firmware** | |
| **Upgrade via Manually Upload** | Uploads the .bin firmware file. |
| **Upgrade Via** | Selects firmware upgrade/provisioning method: TFTP, HTTP, HTTPS, FTP or FTPS. Default is HTTPS. |
| **Firmware Server Path** | Sets IP address or FQDN of firmware server. The URL of the server that hosts the firmware release.<br>Note: You can specify the protocol used in the Firmware Server Path. (example: https://192.168.5.120), this will bypass the "Upgrade Via" method. |

| | |
|---|---|
| **HTTP/HTTPS/FTP/FTPS User Name** | Enters username to authenticate with HTTP/HTTPS FTP/FTPS server. |
| **HTTP/HTTPS/FTP/FTPS Password** | Enters password to authenticate with HTTP/HTTPS FTP/FTPS server. |
| **Firmware File Prefix** | Checks if firmware file is with matching prefix before downloading it. This field enables user to store different versions of firmware files in one directory on the firmware server. |
| **Firmware File Postfix** | Checks if firmware file is with matching postfix before downloading it.<br>This field enables user to store different versions of firmware files in one directory on the firmware server. |
| **Config File** | |
| **Upload Configuration** | Uploads the configuration file in .txt or .xml formats |
| **Restore From Backup Configuration** | Restore From Backup Configuration |
| **Download Device Configuration** | Downloads Device Configuration in .txt format |
| **Download Device XML Configuration** | Downloads Device Configuration in .xml format |
| **Export Backup Configuration** | Export Backup Configuration in .xml format |
| **Config Upgrade via** | Selects Config file upload method: TFTP, HTTP, HTTPS, FTP or FTPS. Default is HTTPS. |
| **Config Server Path** | Sets IP address or FQDN of configuration server. The URL of the server that hosts the configuration file to provision HT81x V2.<br><br>**Note:** You can specify the protocol used in the Config Server Path. (example: https://192.168.5.120), this will bypass the "Upgrade Via" method. |
| **HTTP/HTTPS/FTP/FTPS User Name** | Enters username to authenticate with HTTP/HTTPS FTP/FTPS server. |
| **HTTP/HTTPS/FTP/FTPS Password** | Enters password to authenticate with HTTP/HTTPS FTP/FTPS server. |
| **XML Config File Password** | Decrypts XML configuration file when encrypted. The password used for encrypting the XML configuration file using OpenSSL. |
| **Config File Prefix** | Checks if configuration files are with matching prefix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server. |
| **Config File Postfix** | Checks if configuration files are with matching postfix before downloading them. This field enables user to store different configuration files in one directory on the provisioning server. |
| **Provision** | |
| **Allow DHCP Option 66 or 160 to override server** | Obtains configuration and upgrade server's information using options 66 from DHCP server.<br>Note: If DHCP Option 66 is enabled, the HT81x V2 will attempt downloading the firmware file from the server URL provided by DHCP, even though Config Server Path is left blank.<br>The server URL provided by DHCP can include authentication credentials using following format: "username:password@Provisioning_Server_IP". |

| | |
|---|---|
| **3CX Auto Provision** | Sends multicast “SUBSCRIBE” message for provisioning at booting stage, used for PnP (Plug-and-Play) configuration. Default is Yes. |
| **Enable using tags in URL** | Allows users to configure variables on the configuration server path to differentiate the directories on the server. |
| **Always send HTTP Basic Authentication Information** | Default is No. If set to Yes, The device will send configured user name and password within HTTP request before server sends authentication challenge. |
| **Additional DHCP option** | Additional DHCP options will be used as a firmware upgrade server in place of the configured or DHCP options 43 and 66 settings. This option will only take effect if "Enable DHCP options 43 and 66 server settings" is enabled |
| **Automatic Upgrade** | Specifies when the firmware upgrade process will be initiated; there are 4 options:<br>**No:** The HT81x V2 will only do an upgrade once at boot up.<br>**Check every X minutes:** User needs to specify a period in minutes.<br>**Check every day:** User needs to specify the start hour and the end hour of the day (0-23).<br>**Check every week:** User needs to specify “Day of the week (0-6)”. (Day of week is starting from Sunday).<br>Default is No. |
| **Randomized Automatic Upgrade** | Randomized Automatic Upgrade within the range of hours of the day or postpone the upgrade every X minute(s) by random 1 to X minute(s). |
| **Firmware upgrade and profile detection** | Configure the detection method of firmware upgrade and configuration file requests |
| **Advanced Settings** | |
| **Verify host when using HTTPS** | Enables / disables the host verification when using HTTPS. |
| **Authenticate Conf File** | Authenticates configuration before being accepted. This protects the configuration from unauthorized modifications. Default is No. |
| **Configuration File Types Allowed** | Allows users to configure provision configuration file type in xml file only or all file types. |
| **Download and Process All Available Config Files** | This feature allows users to download and process all available config files. By default, the device will provision the first available config in the order of cfgMAC > cfgMAC.xml > cfgMODEL.xml > and cfg.xml (corresponding to device-specific, model-specific, and global configs).<br>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.<br>The default value is "No" |
| **Config Provision Order** | Administrators can define the preferred order in which the device checks for configuration files during startup. The system will sequentially attempt to load the listed files, and try to apply the first successfully retrieved configuration, the files available are:<br>● **cfgMAC.xml** – Configuration file specific to the device’s MAC address, using XML format.<br>● **cfgMODEL.xml** – Configuration file specific to the device model.<br>● **cfg.xml** – General configuration file applicable to multiple devices.<br>● **cfgMAC** – Binary file configuration file for a specific MAC address.<br>● **cfgMAC_override.xml** – Override configuration file for a specific MAC address, taking precedence over other MAC-based files. |

| | |
|---|---|
| | • **cfgdhcpopt67.xml** – Configuration file retrieved via DHCP Option 67, often used in auto-provisioning environments. |

## System Diagnosis

| | |
|---|---|
| **Syslog** | |
| **Syslog Server** | URL or IP address of the syslog server. |
| **Syslog Level** | Select the HT81x V2 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:<br>1. product model/version on boot up (INFO level)<br>2. NAT related info (INFO level)<br>3. sent or received SIP message (DEBUG level)<br>4. SIP message summary (INFO level)<br>5. inbound and outbound calls (INFO level)<br>6. registration status change (INFO level)<br>7. negotiated codec (INFO level)<br>8. Ethernet link up (INFO level)<br>9. SLIC chip exception (WARNING and ERROR levels)<br>10. memory exception (ERROR level)<br>extra syslog style (EXTRA DEBUG level) |
| **Syslog Protocol** | Allow encrypted SSL/TLS transmission to the syslog server if SSL/TLS is selected, the default value is UDP<br>**Note:** The validity of the server CA certificate will be verified |
| **Send SIP Log** | Sets whether to include SIP logs in the system log<br>Default value is "Yes" |
| **Debug** | |
| **Ethernet Capture** | Enables the capturing and analysis of Ethernet network traffic for troubleshooting and monitoring purposes. |
| **With secret key information** | Allows users to make packet capture including the secret key to decrypt the captured TLS packets. Default value is No. |
| **Port Record** | Allows the recording of port-level call information, such as call duration, caller ID, and call status, for monitoring and logging purposes. |
| **Core Dump** | Provides generated core dump file if unit malfunctions. Clean will be displayed if no issues. |
| **GR909** | |
| **Test To Run** | Selects the type of test that wll be performed for the specified line, the following tests can be performed:<br>• Hazardous Potential Test<br>• Foreign Electromotive Forces Test<br>• Resistive Faults Test<br>• Receiver Offhook Test<br>• Ringer Equivalent Number Test |
| **FXS Line** | Defines the FXS line under test |

| | |
|---|---|
| **Run Interval** | Defines the run Interval in seconds, the default value is 120 seconds, the default range is 0-604800 seconds |

## File Management

| | |
|---|---|
| **CDR Records** | Displays a list of the last 1000 call records, the ionformation included in the records are the following:<br>● UserID<br>● ToNumber<br>● FromNumber<br>● StartTime<br>● StartTalkTime<br>● EndTime<br>● Duration<br>● State<br>● Direction<br>Clicking the "Download" button will download the last 1000 call records<br>Clicking the "Delete" button will delete the last 1000 call records |
| **SIP Messages** | The SIP messages tab displays a list of SIP headers that are captured after each triggered call, the information displayed on the tab are similar to the information that can be captured using the wireshark tool, and filtering by SIP protocol.<br>An example of captured trace for the SIP header can be as shown below:<br>● HT812 V2 --- 2024-05-03 04:43:09.827 SENDING TO 192.168.5.168:5060<br>REGISTER sip:192.168.5.168 SIP/2.0<br>Via: SIP/2.0/UDP 192.168.5.66:5060;branch=z9hG4bK443123589;rport<br>From: <sip:1000@192.168.5.168>;tag=1597031286<br>To: <sip:1000@192.168.5.168><br>Call-ID: 963579881-5060-1@BJC.BGI.F.GG<br>CSeq: 2138 REGISTER<br>Contact: <sip:1000@192.168.5.66:5060>;reg-id=1;+sip.instance="<br><urn:uuid:00000000-0000-1000-8000-C074ADEAA59E>"<br>Max-Forwards: 70<br>User-Agent: Grandstream HT812 V2 1.0.1.10<br>Supported: path<br>Expires: 3600<br>Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UP DATE<br>Content-Length: 0<br>Clicking the "Download" icon will download the whole log of the captured traces.<br>Clicking "Delete" will delete all the captured traces.<br>This tool can be useful for network administrators that wantto treoubleshoot the call flows without having to use an external tool, for analyzing the network<br>**Note:** The SIP PUBLISH method (RFC 6035) enables the ATA to send status updates and event notifications to a SIP server or PBX. This allows for real-time monitoring, presence tracking, and improved call management in VoIP networks. |

## Device Manager

| | |
|---|---|
| **Reboot** | |
| **Automatic restart** | This option triggeres an automatic reboot of the unit, the available options are:<br>● **No**<br>● **Reboot everday:** you can specify the reboot hour<br>● **Reboot everyweek:** you can specify the day of the week, and the hour of the day, for the reboot to take place |

| | |
|---|---|
| | ● **Reboot every month:** you can specify the day of the month, and the hour of the day, for the reboot to take place<br>Default is "No". |
| **Restore Factory** | |
| **Reset Type** | Gives the administrator the option to restore the default configuration on the HT81x V2.<br>There are 3 types of factory reset:<br>● **ISP Data Reset:** All ISP (Internet Service Provider) configurations that may affect the IP address will be reset (including WAN static IP).<br>● **VoIP Data Reset:** All VoIP-related configurations (mainly everything located on the FXS profile page).<br>● **Full Reset:** Both VoIP and ISP-related configuration at the same time.<br>**Note:** After choosing the reset type, you will have to click the reset button for it to take effect. |

## Ports Settings Page Definitions

### Profile 1 / Profile 2

| | |
|---|---|
| **General Settings** | |
| **Account Registration** | |
| **Profile Active** | Activates / Deactivates the accounts. The FXS port configuration will not change if disabled, although the port will not be operational, in this state, there will be no dial tone when picking up the analog phone and making/receiving calls will not be possible. Default is Yes. |
| **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 V2. |
| **Failover SIP Server** | Defines failover SIP server IP address (Supports both IPv4 and IPv6 addresses) or domain name provided by VoIP service provider. (For example: sip.mycompany.com, IPv4:192.168.5.170, or IPv6 fe80::20b:82ff:fe75:211d:). This server will be used if primary SIP server becomes unavailable. |
| **Prefer Primary SIP Server** | Selects to prefer primary SIP server. The account will register to primary Server if registration with Failover server expires. Default is No. |
| **Outbound Proxy** | Specifies IP address (Supports both IPv4 and IPv6 addresses) or domain name of outbound Proxy, or media gateway, or session border controller. (For example: proxy.myprovider.com, IPv4: 192.168.5.170, or IPv6: fe80::20b:82ff:fe75:211d). It's Used by HT81x V2 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 V2 to collect SIP server address from DHCP option 120. Default is No. |
| **Network Settings** | |
| **Layer 3 QoS SIP DSCP** | the Diff-Serv value for SIP packets in decimal, the range is 0-63, default value is 26 |
| **Layer 3 QoS RTP DSCP** | Diff-Serv valuefor RTP packets in decimal, the range is 0-63, default value is 46 |
| **DNS Mode** | Selects DNS mode to use for the client to look up server. One mode can be chosen.<br>**A Record (Default):** resolves IP Address of target according to domain name.<br>**SRV:** DNS SRV resource records indicate how to find services for various protocols.<br>**NAPTR/SRV:** Naming Authority Pointer according to RFC 2915.<br>**Use Configured IP:** If the SIP server is configured as domain name, device will not send DNS queries, but will use “Primary IP” or “Backup IP” to send SIP message if at least one of them is not empty. It will try to use “Primary IP” first, after 3 tries without any response, it will switch to “Backup IP 1”, then “Backup IP 2”, and then it will switch back to “Primary IP” after 3 retries. |
| **DNS SRV Failover Mode** | Configure the preferred IP mode when DNS Mode is SRV or NAPTR/SRV.<br>• 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.<br>• 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.<br>• Saved on until no response SIP request will always be sent to the registered IP address only until registered IP address is unreachable.<br>• Failback follows failback expiration time: the primary server regains control only after the failback expiration time, allowing the secondary server to handle requests until then. |
| **Failback Timer** | When the primary SBC is up, device will send SIP requests to the primary SBC. If at any point device fails over to the secondary SBC, the SIP requests will stay on the failover SBC for the duration of the failback timer. When the timer expires, device will send SIP requests to the primary SBC, (in minutes. Default is 60 minutes, max 45 days). |
| **Maximum Number of SIP Request Retries** | This feature allows user to configure the number of SIP retries before failover occurs. (between 1 and 10, default is 2). |
| **Register Before DNS SRV Failover** | This feature is used to control whether the device need to initiate a new registration request (following existing DNS SRV fail-over mode) first and then direct the non-registration SIP request (INVITE) to the new successfully registered server or not. Default is No. |
| **Primary IP** | The main IP address used for communication and control. |
| **Backup IP1** | The secondary IP address used as a backup for communication in case the Primary IP fails. |
| **Backup IP2** | The third IP address used as an additional backup for communication in case both the Primary IP and Backup IP1 fail. |
| **NAT Traversal** | Indicates type of NAT for each account. This parameter configures whether the NAT traversal mechanism is activated. Users could select the mechanism from No, Keep-alive, STUN, UPnP, Auto, VPN.<br>● **No:** NAT traversal is disabled; the phone doesn't attempt to handle NAT issues. |

| | |
|---|---|
| | • **Keep-alive:** Sends periodic packets to keep the NAT mapping open for incoming calls.<br>• **STUN:** Uses a STUN server to discover the public IP address and port, helping traverse NAT.<br>• **UPnP:** Uses Universal Plug and Play to automatically configure the router to allow SIP traffic through NAT.<br>• **Auto:** Automatically selects the best NAT traversal method based on the network environment.<br>• **VPN:** Routes all SIP traffic through a secure Virtual Private Network, bypassing NAT issues.<br>Defeault is "No". |
| **Use NAT IP** | Defines NAT IP address used in SIP/SDP messages. It should only be used if required by ITSP. |
| **Proxy-Require** | Determines a SIP Extension to notify the SIP server that the HT81x V2 is behind a NAT/Firewall. |
| **SIP Settings** | |
| **SIP Basic Settings** | |
| **SIP Registration** | Controls whether the HT81x V2 needs to send REGISTER messages to the proxy server. The default setting is Yes. |
| **SIP Transport** | Selects transport protocol for SIP packets; UDP or TCP or TLS. Please make sure your SIP Server or network environment supports SIP over the selected transport method. Default is UDP. |
| **Unregister On Reboot** | Controls whether to clear SIP user's information by sending un-register request to the proxy server. The un-registration is performed by sending a REGISTER message with "Expires=0" parameter to the SIP server. This will unregister the SIP account under the concerned FXS page.Unregister on reboot option can be set to "No", "All" or "Instance".<br>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.<br>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.<br>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.<br>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 Yes. |
| **Register Expiration** | Refreshes registration periodically with specified SIP proxy (in minutes). Maximum interval is 65535 minutes (about 45 days).<br>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).<br>Default is 20 seconds. |

| | |
|---|---|
| **Use Random SIP Registration Failure Retry Wait Time** | When enabled, the waiting time to resend a SIP REGISTER request to the SIP server in case of registration failure will be a random number in the following range.<br><br>Default setting is disabled. |
| **Random SIP Registration Failure Retry Wait Time Range** | Allows users to set a wait time (in seconds) before attempting to send a SIP registration after each failure. The wait time will be chosen randomly within this range.<br><br>Valid values range from 60 to 600 seconds. |
| **SIP Registration Failure Retry Wait Time upon 403 Forbidden** | Sends re-register request after specific time (in seconds) when registration process fails with error 403 Forbidden. Maximum interval is 3600 seconds (1 hour). Default is 1200 seconds. |
| **Port Voltage Off upon no SIP Registration or SIP Registration Failure** | Cuts off voltage to the port if there is no SIP registration or if SIP registration fails, preventing unwanted calls.<br>(in minutes. Between 0-60, default is 0. 0 means port voltage is never turned off) |
| **Delay Time of Port Voltage Off Timer Since Boot** | Sets the delay time after boot before the port voltage turns off. It controls the timing for powering down ports on the ATA. The value is in minutes. Between 0-60, default is 0 |
| **Enable SIP OPTIONS/NOTIFY Keep Alive** | Enables SIP OPTIONS or SIP NOTIFY to track account registration status so the ATA will send periodic OPTIONS/NOTIFY message to server to track the connection status with the server.<br>Default setting is No. |
| **SIP OPTIONS/NOTIFY Keep Alive Interval** | Configures the time interval when the ATA send OPTIONS or NOTIFY message to SIP server. The default setting is 30 seconds, which means the ATA will send an OPTIONS/NOTIFY message to the server every 30 seconds. The default range is 1-64800. |
| **SIP OPTIONS/NOTIFY Keep Alive Max Lost** | Defines the Number of max lost packets for SIP OPTIONS Keep Alive before re-registration. Between 3-10, default is 3. |
| **Local SIP Port** | Defines local port to use by the HT81x V2 for listening and transmitting SIP packets. Default value is 5060 |
| **Local RTP Port** | Defines the local RTP-RTCP port pair the HT81x V2 will listen and transmit. It is the HT81x V2 RTP port for channel 0.<br>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 V2 are behind the same NAT.<br>The default is No. |
| **Use Random RTP Port** | Controls whether to use configured or random RTP ports. This is usually necessary when multiple HT81x V2 are behind the same NAT.<br>The default is No. |
| **RTP/RTCP Keep Alive On Hold** | Enables or disables RTP/RTCP keep-alive packets during call hold to maintain connectivity and prevent session timeouts.<br>Disabled by default. |
| **Hold Target Before Refer** | Allows user to hold or not hold the phone call before referring.<br>The default setting is Yes. |
| **Refer-To Use Target Contact** | Includes target's "Contact" header information in "Refer-To" header when using attended transfer. Default is No. |

| | |
|---|---|
| **Remove OBP from Route Header** | Removes outbound proxy info in “Route” header when sending SIP packets.<br>Default setting is No. |
| **Support SIP Instance ID** | Gives the users the possibility of making conference calls by pressing “Flash” key, when it’s enabled by dialing *23 +second callee number. Default is Yes |
| **Support outbound** | Activate/deactivate outbound support. Default is No |
| **Support GRUU** | Activate/deactivate GRUU. Default is No |
| **SIP URI Scheme When Using TLS** | Specifies if “sip” or “sips” will be used when TLS/TCP is selected for SIP Transport. The default setting is “sips”. |
| **Use Actual Ephemeral Port in Contact with TCP/TLS** | Controls the port information in the Via header and Contact header. If set to “No”, these port numbers will use the permanent listening port on the phone. Otherwise, they will use the ephemeral port for the connection. Default is No. |
| **Tel URI** | Indicates E.164 number in “From” header by adding “User=Phone” parameter or using “Tel:” in SIP packets, if the HT81x V2 has an assigned PSTN Number.<br>Disabled: Use “SIP User ID” information in the Request-Line and “From” header.<br>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”.<br>Enabled: “Tel:” will be used instead of “sip:” in the SIP request.<br>Please consult your carrier before changing this parameter. The default is Disabled. |
| **Use Privacy Header** | Determines if the “Privacy header” will be presented in the SIP INVITE message and if it includes the caller info in this header. If set to Default, it will add Privacy header unless special feature is Telkom SA or CBCOM. Default is Default. |
| **Use P-Preferred-Identity Header** | Specifies if the P-Preferred-Identity Header will be presented in the SIP INVITE message. If set to “default”, the P-Preferred-Identity Header will be omitted in SIP INVITE message when Telkom SA or CBCOM is active. If set to “Yes”, the P-Preferred-Identity Header will always be presented. If set to “No”, it will be omitted. Default setting is: Default. |
| **Use P-Access-Network-Info Header** | With this feature enabled, device will populate the WAN access node with IEE-802.11a, IEE-802.11b in P-Access-Network-Info SIP header. |
| **Use P-Emergency-Info Header** | This feature support of IEEE-48-addr and IEEE-EUI-64 in SIP header for emergency calls. |
| **Use P-Asserted-Identity Header** | When this feature is set to Yes, device will send P-Asserted-Identity Header on the SIP Invite.<br>Default setting is No. |
| **Caller ID Fetch Order** | Selects the Caller ID display order which need to be respected by the ATA.<br>The available options are:<br>**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.<br>**Disabled:** When set to “Disabled”, all incoming calls are displayed with “Unavailable”.<br>**From Header:** When set to “From Header”, the ATA will use the FROM header to display the caller ID. |
| **SIP T1 Timeout** | Defines T1 timeout value. It is an estimate of the round-trip time between the client and server transactions. For example, HT81x V2 will attempt to send a request to a SIP server. The time it takes between sending out the request to the point of getting a response is the SIP T1 timer. If no response is received the timeout is increased to (2*T1) and then (4*T1). Request re-transmit retries would continue until a maximum amount of time is defined by T2. The default is 0.5 seconds. |

| | |
|---|---|
| **SIP T2 Interval** | Identifies maximum retransmission interval for non-INVITE requests and INVITE responses. Retransmitting and doubling of T1 continues until it reaches the T2 value. The default is 4 seconds. |
| **SIP Timer D** | Configures SIP Timer D defined in RFC3261. 0 – 64 seconds. Default is 0. |
| **Do Not Escape '#' as %23 in SIP URI** | Replaces # by %23 in some special situations.<br>Default is No. |
| **Disable Multiple m line in SDP** | Sends only one m line in SDP, regardless of how many m fields are in the incoming SDP. Default is No. |
| **Enable 100rel** | Appends “100rel” attribute to the value of the required header of the initial signaling messages.<br>Default is No. |
| **Add Auth Header On Initial REGISTER** | Adds “Authentication” header with blank “nonce” attribute in the initial SIP REGISTER request.<br>Default is No. |
| **Enable Call Waiting Alert-Info in 180 Ringing Response** | Activates the Call Waiting feature by including Call Waiting Alert-Info in the 180 Ringing response sent to the caller during an incoming call.<br>Default value is no. |
| **Conference URI** | Allows users to manually configure the conference URL. The default is null. |
| **Allow SIP Factory Reset** | Allows to reset the devices directly through SIP Notify. If “Allow SIP Factory Reset” is set to “YES”, then the ATA receives the NOTIFY from the SIP server with Event: reset, the HT should perform a factory reset after the authentication.<br>The authentication in this case can be either with:<br>The admin password if no SIP account is configured on the HT.<br>With the credentials of the SIP account if configured on the ATA. |
| **SIP User-Agent** | This feature allows users to configure SIP User Agent. If not configured, device will use the default User Agent header. |
| **SIP User-Agent Postfix** | Configures the SIP User-Agent Postfix |
| **Add MAC in User-Agent** | This feature allows users to configure "User-Agent" in the SIP header field, when this feature is set to“No”, "User-Agent" does not carry a MAC, when this feature is set “Yes except REGISTER”, "User-Agent" in REGISTERSIP header field does not carry MAC but other SIP packet header fields carries MAC, when this<br>feature is set to “Yes to all SIP”, "User-Agent" in the SIP packet header field will carries the MAC. |
| **Use MAC Header** | This feature allows users to configure MAC Header in the SIP packet header field, when this feature is set to “No” ,the MAC header field is not carried in the SIP packet header field, when this feature is set to “REGISTER Only”, the register packet header field carries the MAC header field but the remaining SIP packets do not carry MAC header fields, when this feature is set to “Yes to all SIP”, the MAC header field is carried in the SIP data packet header field. |
| **Session Timer** | |
| **Enable Session Timer** | Disable the session timer when this option is set to “No”. By default, this option is enabled. |
| **Session Expiration** | Enables SIP sessions to be periodically “refreshed” via a SIP request (UPDATE, or re-INVITE). When the session interval expires, if there is no refresh via an UPDATE or re- |

| | |
|---|---|
| | INVITE message, the session will be terminated. Session Expiration is the time (in seconds) at which the session is considered timed out, if no successful session refresh transaction occurs beforehand. Valid range is 90-64800 seconds. Default is 180 seconds. |
| **Min-SE** | Defines Minimum session expiration (in seconds). Default is 90 seconds. |
| **Caller Request Timer** | Uses session timer when making outbound calls if remote party supports it. Valid range is 90-64800 seconds. Default is No. |
| **Callee Request Timer** | Uses session timer when receiving inbound calls with session timer request. Default is No. |
| **Force Timer** | Uses session timer even if the remote party does not support this feature. Selecting “No” will enable session timer only when the remote party supports it. To turn off Session Timer, select “No” for Caller and Callee Request Timer, and Force Timer. Default is No |
| **UAC Specify Refresher** | Specifies which end will act as refresher for outgoing calls.<br>Default is Omit.<br>UAC: The device acts as the refresher.<br>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.:<br>UAS: The device acts as the refresher.<br>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”<br>The default value is “Immediately”. |
| **Security Settings** | |
| **Validate Incoming SIP Message** | Checks the authenticity and integrity of incoming SIP messages for enhanced security. |
| **Check SIP User ID for incoming INVITE** | Checks the SIP User ID in the Request URI of the incoming INVITE; if it doesn’t match the HT81x V2 SIP<br>User ID, the call will be rejected. Direct IP calling will also be disabled. The default is No. |
| **Authenticate incoming INVITE** | Challenges the incoming INVITE for authentication with SIP 401 Unauthorized message.<br>Default is No. |
| **Allow Incoming SIP Messages from SIP Proxy Only** | Checks SIP address of the Request URI in the incoming SIP message; if it doesn’t match the SIP server address of the account, the call will be rejected.<br>Default is No. |
| **Authenticate server certificate domain** | Configures whether to validate the domain certificate when download the firmware/config file. If it is set to “Yes”, the phone will download the firmware/config file only from the legitimate server. The default setting is “No”. |
| **Trusted domain name list** | Supports setting specific domain names and wildcard domain names, wildcard domain names such as "*.grandstream.com", use "," to separate domain names |
| **Authenticate server certificate chain** | Verifies certificate when communication method is TCP/TLS |

| | |
|---|---|
| **Codec Settings** | |
| **DTMF Settings** | |
| **Preferred DTMF method** | Sorts DTMF methods (in-audio, via RTP (RFC2833) or via SIP INFO) by priority. |
| **Force DTMF to be sent via SIP INFO simultaneously** | Forces DTMF to be sent via SIP INFO simultaneously. Default is No. |
| **Inband DTMF Duration** | Allows users to config the Inband DTMF Duration and inter-duration.<br>The default Duration is 100 ms. Valid range: 40-2000 ms.<br>The default Inter-duration is 50 ms. Valid range: 40-2000 ms. |
| **DTMF Payload Type** | Defines payload type for DTMF using RFC2833. |
| **Enable Multiple Sampling Rates in SDP telephone-event** | This option allows the device to advertise multiple supported sampling rates for DTMF events in the SDP (Session Description Protocol), which enhances compatibility with different VoIP systems by ensuring proper DTMF signal interpretation across varying codec sampling rates.<br>When the option is enabled, the HT includes multiple supported sampling rates for DTMF (telephone-event) in the SDP negotiation, which allows better interoperability with VoIP systems using different codec rates.<br>When disabled, only a single default sampling rate is advertised, which may lead to DTMF tone mismatches if the remote system expects a different rate. |
| **Inband DTMF Tx Gain** | Adjusts the transmit gain for inband Dual-Tone Multi-Frequency (DTMF) tones during call signaling.<br>The Valid range is -12-12 db, default is 0 |
| **DSP DTMF Detector Duration Threshold** | Allows users to config the DSP DTMF Detector Duration Threshold.<br>The default Duration is 30 ms. Valid range: 20-2000 ms.<br>The default Inter-duration is 30 ms. Valid range: 20-2000 ms. |
| **DSP DTMF Detector Min Level** | determines the minimum level of DTMF tones that the DSP DTMF detector can reliably detect, range is -45-0 dBm, default is -25 |
| **DSP DTMF Detector Snr** | Sets the signal-to-noise ratio threshold for the DSP DTMF detector, determining the sensitivity to distinguish DTMF tones from background noise in the audio signal.<br>Range: 0-12, default is 1 |
| **DSP DTMF Detector Deviation** | Specifies the allowed frequency deviation from standard DTMF tones that the DSP DTMF detector can accommodate.<br>Range: 0-25, default is 25 |
| **DSP DTMF Detector Twist** | Defines the maximum deviation from ideal tone frequencies allowed for reliable DTMF detection by the DSP.<br>Range: 0-12dB, default is 5 |
| **Disable DTMF Negotiation** | Uses DTMF order without negotiation. Default is No. |
| **RFC2833 Events Count** | This feature allows users to customize the count of RFC2833 events. Default is 8. |
| **RFC2833 End Events Count** | This feature allows users to customize the count of RFC2833 end events. Default is 3. |
| **Preferred Vocoder** | |
| **Preferred Vocoder (in listed order)** | Configures vocoders in a preference list (up to 8 preferred vocoders) that will be included with same order in SDP message. Vocoder types are G.711 A-/U-law, G.726- |

| | |
|---|---|
| | 32, G.723, G.729, iLBC and OPUS |
| **Voice Frames per TX** | Transmits a specific number of voice frames per packet. Default is 2; increases to 10/20/32/64 for G711/G726/G723/other codecs respectively. |
| **G723 Rate** | Operates at specified encoding rate for G.723 vocoder. Available encoding rates are 6.3kbps or 5.3kbps.<br>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.<br>Default is 97. |
| **OPUS Payload Type** | Determines payload type for OPUS. Valid range is between 96 and 127. Default is 123. |
| **Enable Audio RED with FEC** | Enables the use of audio redundancy (RED) with forward error correction (FEC) to enhance audio quality and resilience against packet loss in real-time communication systems such as VoIP |
| **Audio FEC Payload Type** | Specifies the payload type used for transmitting audio forward error correction (FEC) packets in a VoIP system. |
| **Audio RED Payload Type** | Defines the payload type assigned to audio redundancy (RED) packets in a VoIP system, |
| **VAD** | Allows detecting the absence of audio and conserves bandwidth by preventing the transmission of “silent packets” over the network.<br>Default is No. |
| **Use First Matching Vocoder in 200OK SDP** | Includes only the first matching vocoder in its 200OK response, otherwise it will include all matching vocoders in same order received in INVITE.<br>Default is No. |
| **Symmetric RTP** | Changes the destination to send RTP packets to the source IP address and port of the inbound RTP packet last received by the device. Default is No. |
| **Enable RTCP** | Allows users to enable RTCP. The default setting is “Yes”. |
| **Fax Mode** | Specifies the fax mode: T.38 (Auto Detect) FoIP by default, or Pass-Through. If using Pass-through mode, select preference codec as PCMU or PCMA. |
| **T.38 Max Bit Rate** | Selects the maximum T.38 bit rate. Lowering the maximum fax bit rate may help improve the fax success rate. Only effective when the fax machine is fax receipt. Available options are: 4800bps, 9600bps, 14400bps.<br>Default value is 9600bps. |
| **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 |
| **Re-INVITE Upon CNG Count** | This feature enables users to initiate a re-invite request for fax transmission when the fax machine is the sender.<br><br>The feature is controlled by an adjustable setting, where a value of 0 disables the feature, and a value of 1 or greater allows the ATA to automatically initiate the re-invite request once the CNG (Calling Tone) count threshold is met. |

| | |
|---|---|
| | The valid setting range for this feature is between 0 and 6. The default setting is 0. |
| **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.<br>Medium (initial 100ms, min 20ms, max 200ms).<br>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<br>It uses SDP Security Description to exchange key. Please refer to<br>**SDES:** https://tools.ietf.org/html/rfc4568<br>**SRTP:** https://www.ietf.org/rfc/rfc3711.txt |
| **SRTP Key Length** | Allows users to select supported SRTP Key Length. the available values are : |
| **Crypto Life Time** | Adds crypto life time header to SRTP packets. Default is Yes. |
| **Analog signal line configuration** | |
| **SLIC Setting** | Depends on standard phone type (and location). |
| **Caller ID Scheme** | Selects the caller id scheme, for example: Bellcore/Telcordia, ETSI-FSK … |
| **DTMF Caller ID** | Configures DTMF caller ID based on Start and Stop Tone. |
| **Polarity Reversal** | Reverses the polarity upon call establishment and termination.<br>Default is No. |
| **Loop Current Disconnect** | Allows the traditional PBX used with HT81x V2 to apply this method for signaling call termination. The method initiates a short voltage drop on the line when the remote (VoIP) side disconnects an active call. The default is No. |
| **Play busy/reorder tone before Loop Current Disconnect** | Allow user to configure if it will play busy/reorder tone before loop current disconnect upon call fail.<br>Default is No. |
| **Loop Current Disconnect Duration** | Configures the duration of voltage drop described in the topic above. HT81x V2 support a duration range from 100 to 10000ms. The default value is 200. |
| **Enable Pulse Dialing** | Allow users to enable Pulse Dialing option under FXS Port. Default is No. |
| **Pulse Dialing Standard** | Allows users to use Swedish pulse dialing standard or New Zealand pulse dialing standard.<br>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.<br>HT81x V2 support a range from 40 to 2000 ms.<br>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 V2 support a range from 40 to 2000 ms. Default value is 400. |

| | |
|---|---|
| **Gain** | Adjusts the voice path volume.<br><br>• Rx is a gain level for signals transmitted by FXS<br>• Tx is a gain level for signals received by FXS.<br>Default = 0dB for both parameters. Loudest volume: +6dB Lowest volume: -6dB.<br>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.<br>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.<br>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. |
| **Enable Line Echo Canceller (LEC)** | Enables the LEC per call base. Recommended for Fax/Data calls.<br>Default is Yes. |
| **Ring Frequency** | Chooses an appropriate ringing frequency.<br><br>Default is 20Hz. |
| **Ring Power** | Selects ringing power settings, the options are: 45Vrms, 50Vrms, and 55Vrms , the higher the value, the more powerful the ring is.<br><br>Default is 45Vrms. |
| **OnHook DC Feed Current** | This feature is used to adjust DC feed current when on-hook.<br><br>Default is 30mA. |
| **Call Settings** | |
| **Offhook Auto-Dial Delay** | Sets the delay time before automatic dialing begins after going off-hook.<br>Range is 0-60 seconds, default is 0 |
| **No Key Entry Timeout** | Initiates the call within this time interval if no additional key entry during dialing stage.<br>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).<br>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.<br>This feature is NOT designed to work with and should NOT be enabled for direct IP-to-IP calling. |
| **Dial Plan Prefix** | Adds specified prefix to dialed number. |
| **Dial Plan** | Dial Plan Rules:<br>1. Accept Digits: 1,2,3,4,5,6,7,8,9,0 , *, #, A,a,B,b,C,c,D,d<br>2. Grammar: x – any digit from 0-9;<br>a. xx+ – at least 2 digits number;<br>b. xx – exactly 2 digits number;<br>c. ^ – exclude;<br>d. . – wildcard, matches one or more characters<br>e. [3-5] – any digit of 3, 4, or 5;<br>f. [147] – any digit 1, 4, or 7;<br>g. <2=011> – replace digit 2 with 011 when dialing<br>h. <=1> – add a leading 1 to all numbers dialed, vice versa will remove a 1 from the number dialed<br>i. \| – or<br>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.<br>Example 1: {[369]11 \| 1617xxxxxxx} –<br>Allow 311, 611, 911, and any 10-digit numbers of leading digits 1617<br>Example 2: {^1900x+ \| <=1617>xxxxxxx} –<br>Block any number with leading digits 1900 and add prefix 1617 for any dialed 7-digit numbers<br>Example 3: {1xxx[2-9]xxxxxx \| <2=011>x+} –<br>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.<br>1. Default: Outgoing – { x+ \| +x+ \| *x+ \| *xx*x+ }<br>Example of a simple dial plan used in a Home/Office in the US:<br>{ ^1900x. \| <=1617>[2-9]xxxxxx \| 1[2-9]xx[2-9]xxxxxx \| 011[2-9]x. \| [3469]11 }<br>Explanation of example rule (reading from left to right):<br>^1900x. – prevents dialing any number started with 1900<br><=1617>[2-9]xxxxxx – allows dialing to local area code (617) numbers by dialing 7 numbers and 1617 area code will be added automatically<br>1[2-9]xx[2-9]xxxxxx – allows dialing to any US/Canada Number with 11 digits length<br>011[2-9]x. – allows international calls starting with 011<br>[3469]11 – allow dialing special and emergency numbers 311, 411, 611 and 911<br>Note: In some cases, user wishes to dial strings such as *123 to activate voice mail or other application provided by service provider. In this case * should be predefined inside dial plan feature. An example dial plan will be: { *x+ } which allows the user to dial * followed by any length of numbers. |
| **Use # as Dial Key** | Treats “#” as the “Send” (or “Dial”) key. If set to “No”, this “#” key can be included as part of the dialed number. Default is Yes. |
| **Disable # as Redial Key** | Disables # to act as Redial key. If set to “Yes” and feature “Use # as Dial Key” set to Yes, the # key will act as dial key but not as redial key. Default is No. |
| **RFC2543 Hold** | Toggles between RFC2543 hold and RFC3261 hold. RFC2543 hold allows to disable the hold music sent to the other side, in this case IP address (0.0.0.0) it will be sent in SDP instead of the IP address of the unit . RFC3261 (a line) will play the hold music to the other side. |
| **Disable Call-Waiting** | Disables receiving a second incoming call when the line is engaged. Default is No. |
| **Disable Call-Waiting Caller ID** | Disables displaying caller ID when receiving a second incoming call. Default is No. |
| **Disable Call-Waiting Tone** | Disables playing call waiting tone during active call when receiving a second incoming call. The CWCID will still be displayed.<br>Default is No. |
| **Disable Connected Line ID** | Disables displaying the number of the person answering the phone.<br>Default is No. |
| **Disable Receiver Offhook Tone** | Enables / disables the warning to alert that the phone has been left off-hook for an extended period of time.<br>Default is No. |
| **Disable Reminder Ring for On-Hold Call** | Enables playing the reminder ring.<br>Default is No. |
| **Disable Reminder Ring for DND** | This feature allows user to disable reminder ring when FXS port is on DND mode.<br>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.<br>Check the phone's manual to find out what signal is supported, FSK (default) or Neon.<br>**Note:** Some phones (depending on the model of the analog phone) when this feature is set to NEON it might auto ring (short beeps) when there is a voice mail available for that FXS port where it is connected. |
| **MWI Tone** | When set to Default, device will play Stutter Dial Tone when there is voicemail, if set to Special Proceed Indication Tone, device will play the configured special proceed indication tone upon user offhook when there is voicemail |
| **Transfer on Conference Hangup** | Determines whether a call is automatically transferred to a specified destination after a conference call ends.<br>Disabled by Default |
| **Send Hook Flash Event** | Default is No. If set to yes, flash will be sent as DTMF event. |
| **Flash Digit Control** | When it set to YES it allows the user to perform some call setting when both channels are used while pressing:<br>**"Flash + 1"** in order to hang up the current call and resume a call that was held.<br>**"Flash + 2"** in order to hold the current call and resume a call that was held.<br>**"Flash + 3"** in order to perform 3-way conference.<br>**"Flash + 4"** in order to perform attended transfer. |
| **Callee Flash to 3WC** | When this feature is set to Yes, device would be able to set up the 3-way conference call even when device is the callee in the second call. Default is No. |
| **Ring Timeout** | Stops ringing when incoming call if not answered within a specific period of time.<br>When set to 0 there will be no ringing timeout.<br>Default is 60 seconds. |
| **Hunting Group Ring Timeout** | Configures (ins seconds) Timeout for hunting group. Valid range is 5-300, default is 20 seconds. |
| **Hunting Group Type** | Specifies the group ringing type (Circular, Linear, or Parallel). Default is Circular<br>● **Circular:** Calls rotate through available ports in order, looping back to the first after the last.<br>● **Linear:** Calls always start at the first port and move sequentially to the next available one.<br>● **Parallel:** All ports in the group ring simultaneously until one answers. |
| **Delayed Call Forward Wait Time** | Forwards incoming call if not answered within a specific period of time when delayed call forward is activated locally (using *92 code). Default value is 20 seconds. |
| **SUBSCRIBE for MWI** | Sends SUBSCRIBE periodically (depends on "Register Expiration" parameter) for message waiting indication. Default is No. |
| **Send Anonymous** | Sets "From", "Privacy" and "P_Asserted_Identity" headers in outgoing INVITE message to "anonymous", blocking caller ID. Default is No.<br>**Note:** When the caller is marked as anonymous, the current phone Caller ID will be set as "private caller", and when is marked as unavailable, the current phone caller ID is marked as "unknown caller" |
| **Anonymous Call Rejection** | Rejects incoming calls with anonymous caller ID with "486 Busy here" message.<br>Default is No. |
| **Special Feature** | Selects Soft switch vendors' special requirements Examples of vendors: BroadSoft, CBCOM, RNK, Huawei, China Mobile, ZTE IMS, PhonePower, TELKOM SA, Vonage, |

| | |
|---|---|
| | Metaswitch, CenturyLink, MTS, Oi_BR, Telefonica, GIBTELECOM. The default is Standard. |
| **Disable Unknown Caller ID** | Disable analog phone's caller ID when receiving a call with "Anonymous", "unavailable" or "unknown" in FROM header and without "Display info".<br>**Note:** This relies also on analog phone's design, some phones will still display "unknown" with this feature enabled. Default is No. |
| **Replace Beginning '+' with 00 in Caller ID** | When this feature is set to Yes, device will replace the "+" sign at the beginning of a number in the FROM header. Default is No. |
| **Number of Beginning Digits to Strip from Caller ID** | Removes a specified number of digits from the beginning of the Caller ID information received before displaying it to the called party.<br>The range is between 0 and 10, default is 0 |
| **Outgoing Call Duration Limit** | Defines the call duration limit for the outgoing calls. Default is 0 (No limit). |
| **Incoming Call Duration Limit** | Defines the call duration limit for the incoming calls.<br>Range is 0-180 minutes, default is 0 (No Limit) |
| **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.<br>Enable All will override all individual features enable setting. Default is Yes |
| **Reset Call Features** | Allows users to reset all call features configuration.<br>Default is No |
| **SRTP Feature** | Allow users to customize the SRTP feature codes. Default is Yes |
| **Enable SRTP per call** | Enable SRTP: Default is 16 |
| **Disable SRTP per call** | Disable SRTP: Default is 17 |
| **SRTP per call Feature** | – Enable SRTP per call: Default is 18<br>– Disable SRTP per call: Default is 19 |
| **Enable SRTP per call** | Set the function code to enable SRTP (the default value is 18), which is only valid for the current call |
| **Disable SRTP per call** | Set the function code to disable SRTP (the default value is 18), which is only valid for the current call |
| **CID Feature** | Allow users to customize the CID feature codes. Default is Yes |
| **Enable CID** | Enable CID: Default is 31 |
| **Disable CID** | Disable CID: Default is 30 |
| **CID per call Feature** | Whether to display the user ID, it is only valid for the current call |
| **Enable CID per call** | Enable CID per call: Default is 82 |
| **Disable CID per call** | Disable CID per call: Default is 67 |

| | |
|---|---|
| **Direct IP Calling Feature** | Allow users to customize the Direct IP feature code. Default is Yes |
| **Direct IP Calling** | Direct IP Calling: Default is 47 |
| **CW Feature** | Allow users to customize the call waiting feature codes. Default is Yes |
| **Enable CW** | Enable CW: Default is 51 |
| **Disable CW** | Disable CW: Default is 50 |
| **CW per call Feature** | Enable or cancel the call waiting function, only the current call is valid |
| **Enable CW per call** | Enable CW per call: Default is 71 |
| **Disable CW per call** | Disable CW per call: Default is 70 |
| **Call Return Feature** | Allow users to customize the Call Return feature code. Default is Yes |
| **Call Return** | Call return: Default is 69 |
| **Unconditional Forward Feature** | Allow users to customize the Unconditional Forward feature codes.<br>Default is Yes |
| **Enable Unconditional Forward** | Set the function code to enable unconditional call forwarding (default value is 72) |
| **Disable Unconditional Forward** | Set the function code to cancel unconditional call forwarding (default value is 73) |
| **Busy Forward Feature** | Whether to enable the call forwarding function when busy |
| **Enable Busy Forward** | Set the function code to enable call forwarding when busy (default value is 90) |
| **Disable Busy Forward** | Set the function code to cancel call forwarding when busy (default value is 91) |
| **Delayed Forward Feature** | Whether to enable the function of transferring calls without answering |
| **Enable Delayed Forward** | Set the function code to enable call transfer without answering (default value is 92) |
| **Disable Delayed Forward** | Set the function code for canceling unanswered call transfer (default value is 93) |
| **Paging Feature** | Allow users to customize the Paging feature code. Default is Yes |
| **Paging** | Paging: Default is 74 |
| **DND Feature** | Allow users to customize the CW feature codes. Default is Yes |
| **Enable DND** | Enable DND: Default is 78 |
| **Disable DND** | Disable DND: Default is 79 |
| **Blind Transfer Feature** | Allow users to customize the Blind Transfer feature code. Default is Yes |
| **Enable Blind Transfer** | Enable Blind Transfer: Default is 87 |

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

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

## FXS Port

| | |
|---|---|
| **FXS Port** | Displays the specific port number. 1-2 for HT812 V2, 1-4 for HT814 V2 and 1-8 for HT818 V2. |
| **SIP User ID** | Defines user account information provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number. |
| **Authenticate ID** | Determines account authenticate ID provided by VoIP service provider (ITSP). Can be identical to or different from “SIP user ID”. |
| **Authenticate Password** | Specifies account password provided by VoIP service provider (ITSP) to register to SIP servers. |
| **Name** | Chooses a name to be associated to user. |
| **Profile ID** | Defines the profile ID for each port. |
| **Hunting Group** | Configures hunting group feature on the specific port.<br><br>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.<br><br>Example configuration of a Hunting group:<br><br>FXS Port #1: SIP UserID and Authenticate ID entered, Hunting group set to “Active”<br><br>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”<br><br>FXS Port #4: SIP UserID and Authenticate ID entered, Hunting group set to “None”<br><br>Hunting Group 1 contains ports 1, 2, 3. FXS port 4 is registered but it is not added to the Hunting Group 1.<br><br>**Note:** HT81x V2 will use CID name from FXS port initiating the outgoing call if the “Name” field is entered for that specific port. |
| **Routing ID** | This field allows specifying different DID numbers for each FXS port. Multiple DIDs could be assigned here to determine which calls should be routed to the corresponding port. |
| **Routing ID Matching Type** | This determines how the device identifies incoming calls based on the DID. The default setting is "Request URI", which means it matches the called number in the SIP request. When set to "To header", the device instead looks at the To header in the SIP INVITE message to match the incoming call, useful in scenarios where the Request URI may be altered by SIP proxies, but the To header still contains the original dialed number. |
| **Enable Port** | Enables / Disables the port |
| **Offhook Auto-Dial** | Configures a User ID or extension number that is automatically dialed when off-hook. Only the user part of a SIP address needs is entered here. The HT81x V2 will automatically append the “@” and the host portion of the corresponding SIP address. |

## 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 a public IP, keep this field blank.
2. Use random SIP/RTP ports (under the 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 the gateway is behind a firewall on a private network.

### DTMF Methods

The HT81x V2 support the following DTMF mode:

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

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

### Preferred Vocoder (Codec)

The HT81x V2 support the 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 HT81x V2 through Voice Prompts

As mentioned previously, The HT81x V2 have a built-in voice prompt menu for simple device configuration. Please refer to "Understanding HT81x V2 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 HT81x V2 to use DHCP.

- **STATIC IP MODE**

Select voice menu option 01 to enable HT81x V2 to use STATIC IP mode, then use options 02, 03, 04, and 05 to set up IP address, Subnet Mask, Gateway, and DNS server respectively.

- **PPPOE MODE**

Select voice menu options 01 to allow the HT81x V2 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 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 the WAN port. Press 9 in this menu to toggle between enable / disable. The default is disabled.

## Configuration through a Central Server

The HT81x V2 can be automatically configured from a central provisioning system. When HT81x V2 boots up, it will send TFTP, HTTP/HTTPS or FTP/FTPS requests to download configuration files, "cfgec74d7xxxxxx" and "cfgec74d7xxxxxx.xml", where "ec74d7xxxxxx" is the LAN MAC address of the HT81x V2. If the download of "cfgxxxxxxxxxxxx.xml" is not successful, the provision program will issue a request a generic configuration file "cfg<Model>.xml" followed by a request to 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 HT81x V2 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 the automated configuration of Grandstream devices. GAPS uses HTTPS and other communication protocols to communicate with each individual Grandstream device for firmware upgrades, 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.

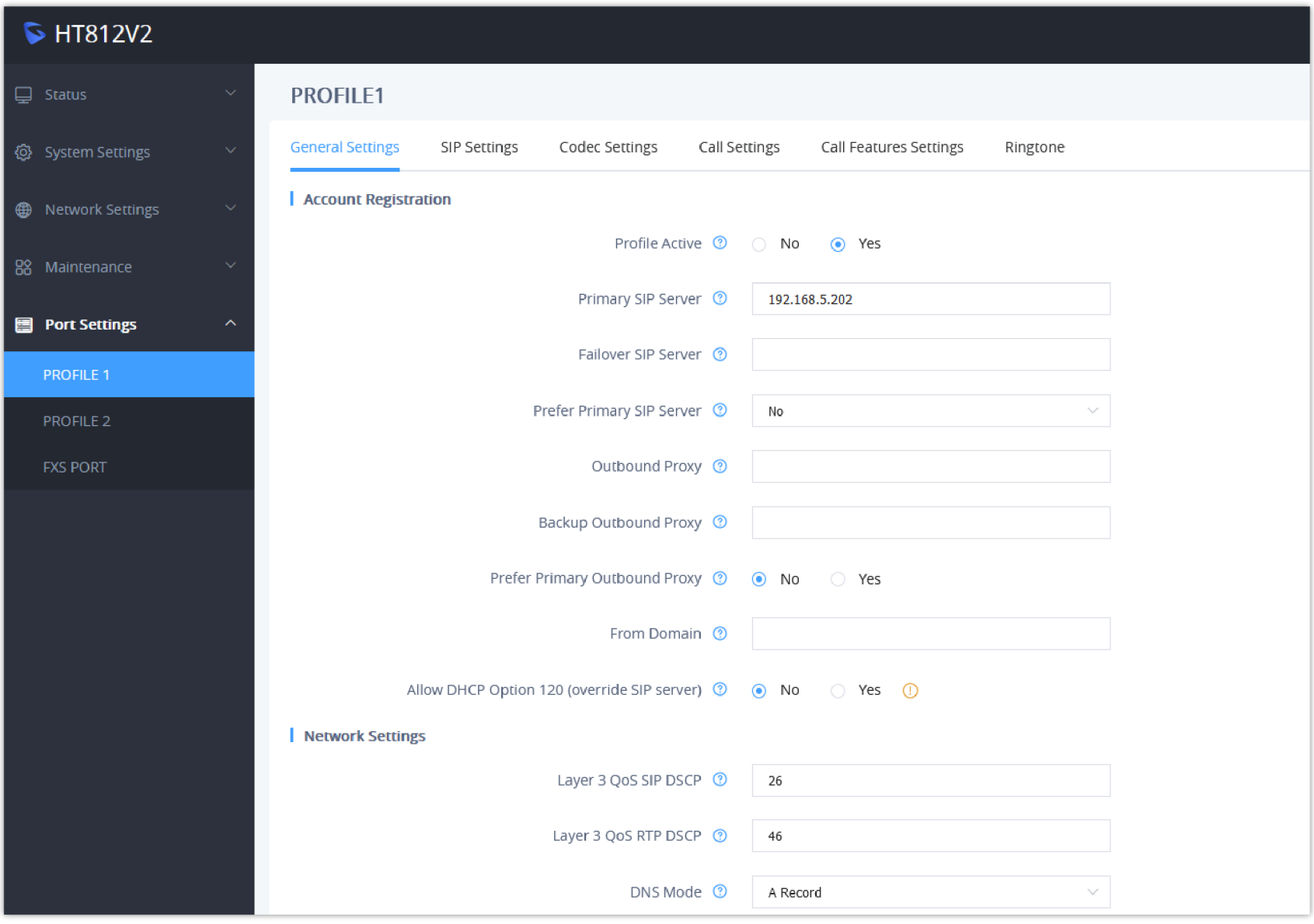
The Grandstream configuration tools are free to end users. The configuration tools and configuration templates are available for download from https://www.grandstream.com/support/tools

## Register a SIP Account

The HT81x V2 support Profiles that can configure two SIP servers,

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

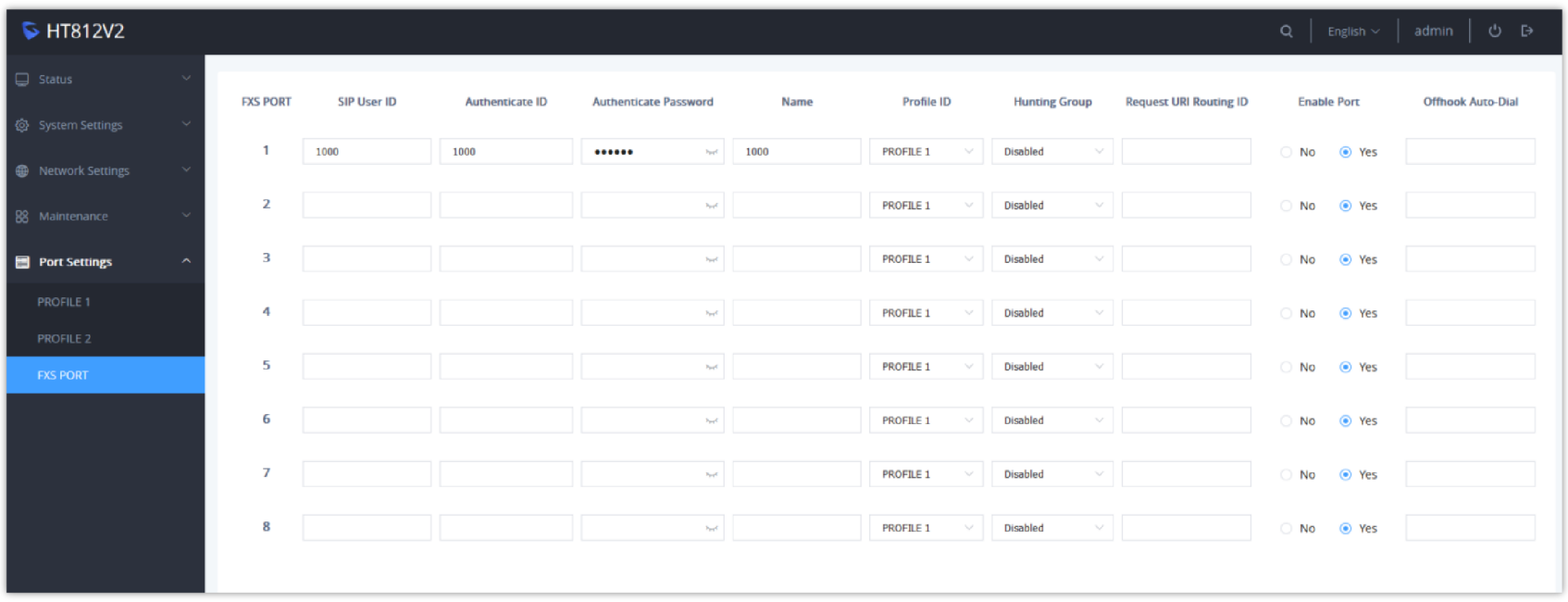
- Access your HT81x V2 web UI by entering its IP address in your favorite browser.
- Enter your admin password (default: found on the sticker on the back of the unit).
- Press **Login** to access your settings.
- Go to **Profile 1/ Profile 2** web pages and set the following:
    1. **Account Active** to **Yes.**
    2. **Primary SIP Server** field with your SIP server IP address or FQDN.
    3. **Failover SIP Server** with your Failover SIP Server IP address or FQDN. Leave empty if not available.
    4. **Outbound Proxy:** Set your Outbound Proxy IP Address or FQDN. Leave empty if not available.




*Configure SIP Server*

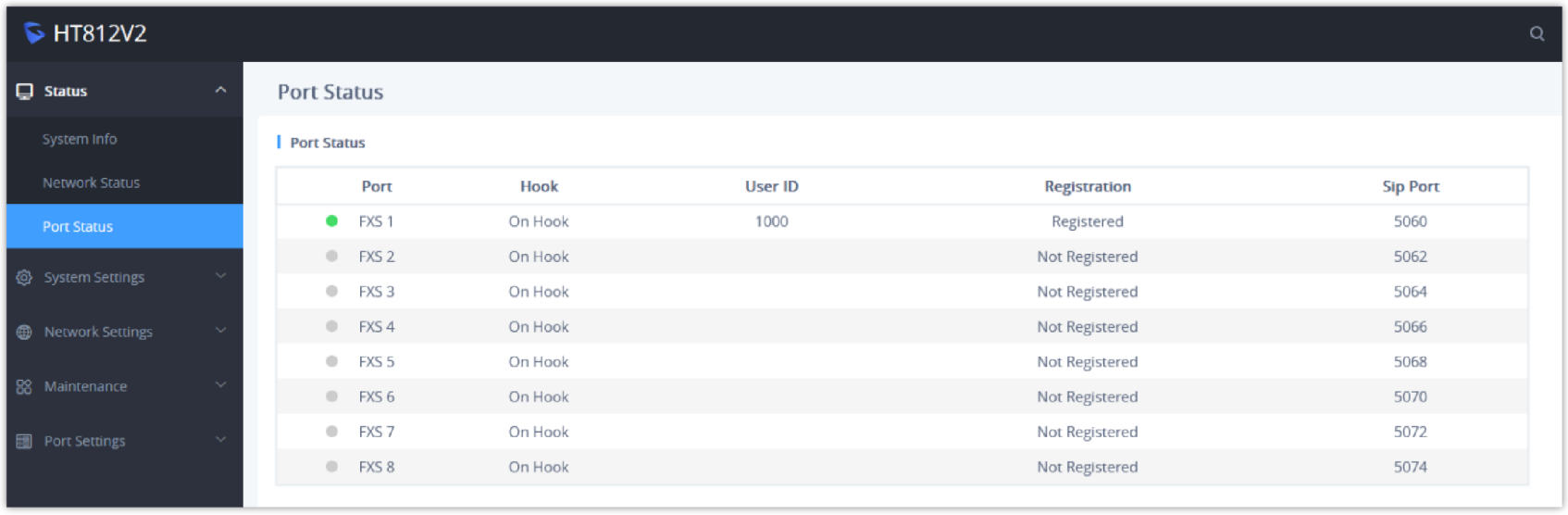
- Go to **FXS Port** web page and set the following
    1. **SIP User ID**: Under **Ports** Web Page , Enter the SIP User ID User account information, provided by VoIP service provider (ITSP). Usually in the form of digit similar to phone number or actually a phone number.
    2. **Authenticate ID**: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

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




*Register SIP Account*

After applying your configuration, your account will register to your SIP Server, you can verify if it has been correctly registered with your SIP server from your HT81x V2 web interface under **Status → Port Status → Registration** (If it displays **Registered**, it means that your account is fully registered, otherwise it will display **Not Registered** so in this case you must double check the settings or contact your provider).




*Account Registered*

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

## Call Features

The HT81x V2 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”.<br>No dial tone is played in the middle. |
| ***16** | Enable SRTP |
| ***17** | Disable SRTP |
| ***18** | Enable SRTP per call. Meaning it's only valid for the current call. |
| ***19** | Disable SRTP per call. Meaning it's only valid for the current call. |

| | |
|---|---|
| ***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. |
| ***77** | Enable set Offhook Auto-Dial. |
| ***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 |
| ***98** | Enable to play the registration ID. |

| | |
|---|---|
| **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. |

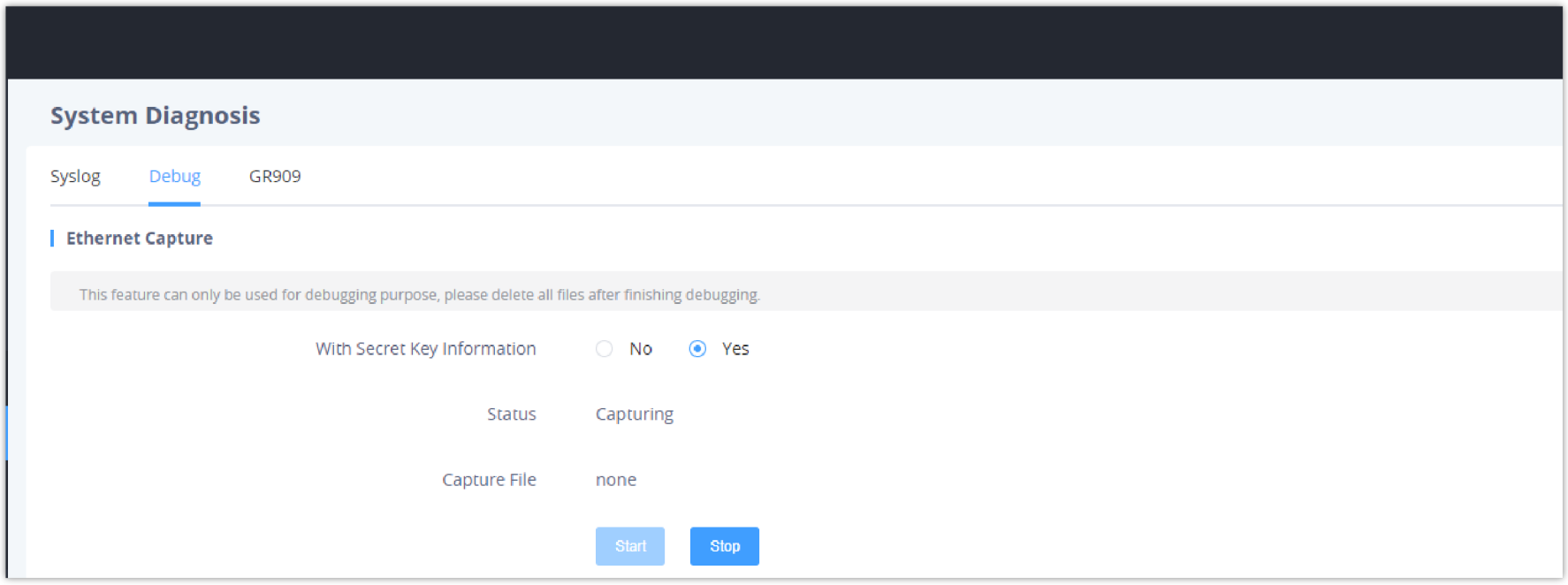
*HT81x V2 Call Features*

## Ethernet Capture

Ethernet Capture involves intercepting a secret key information file during the TLS handshake between the HT8xx and a SIP server to extract the secret key information file during the TLS handshake, the file downloaded is a .txt file including the client's secret key.

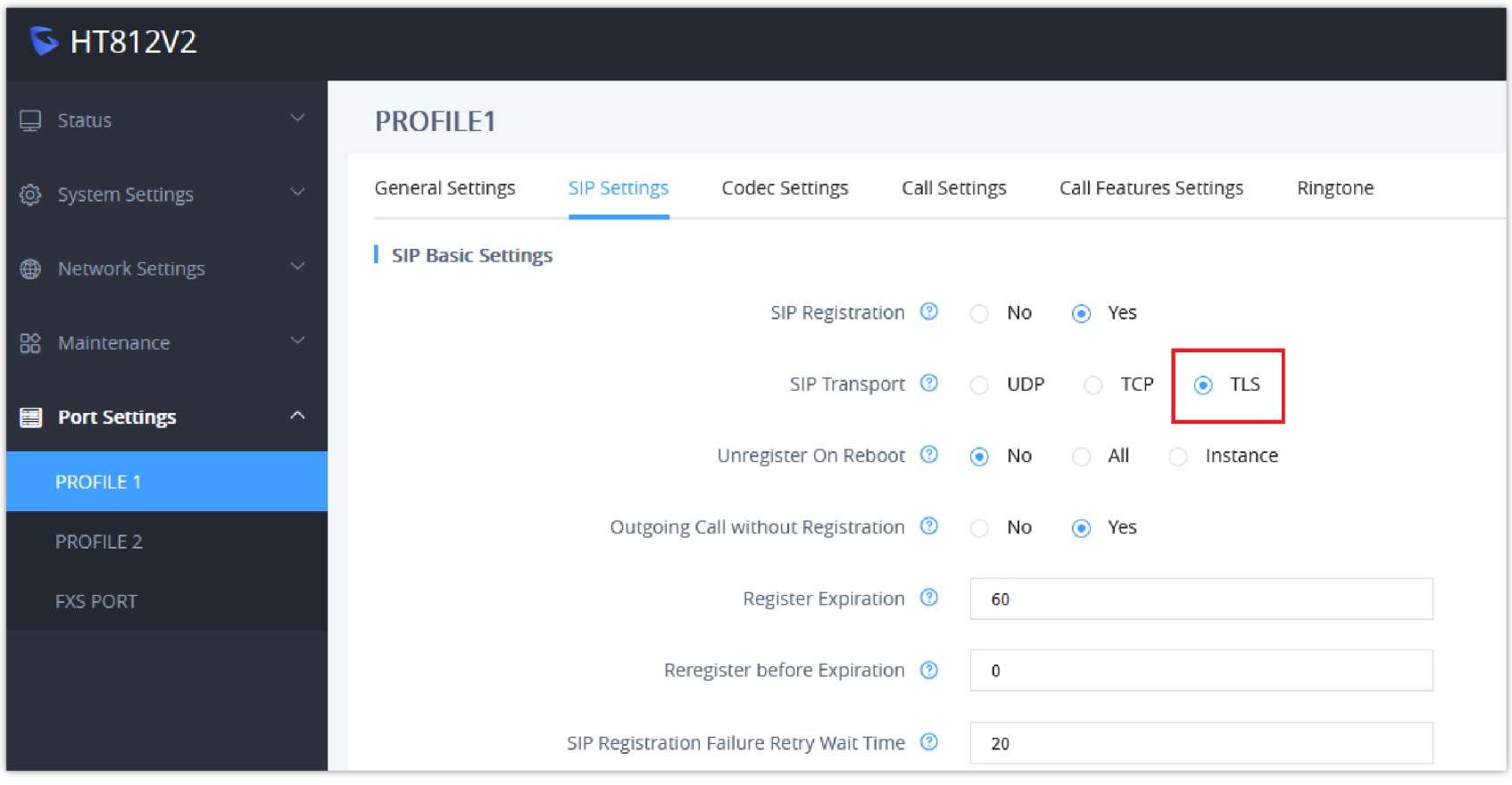
The process includes initiating capture, re-registering the HT8xx with TLS to a SIP server, waiting for a SIP Register request, and then stopping the capture. The goal is to extract the secret key information file, to do that please follow the below steps described below:

- Start capturing the communication between the HT8xx and the server. to do that go to **Maintenenace → System Diagnosis → Debug**, and make sure **"With Secret Key information"** is set to Yes



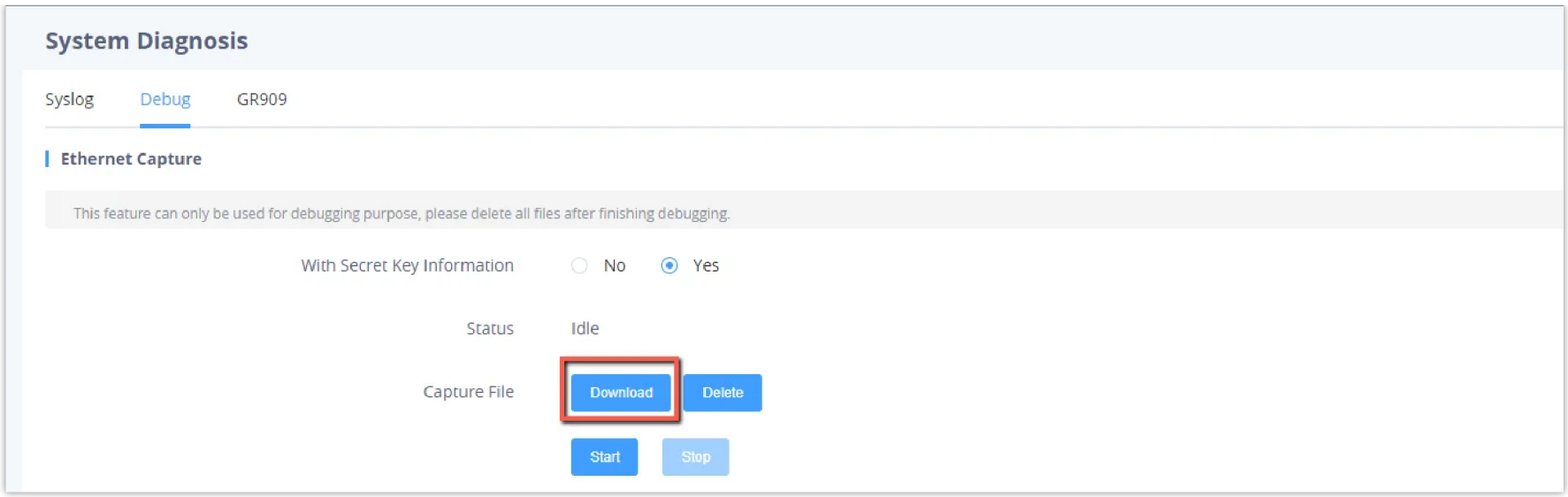

*Ethernet Capture*

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




*SIP Transport Type*

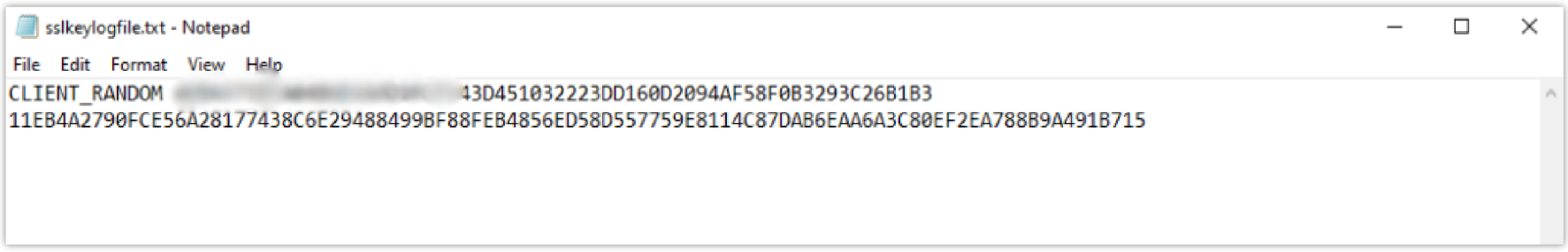
- Allow the system to wait until the ATA sends a SIP Register request to the server.
- Once the SIP Register request is sent, stop capturing the communication.




*Download Secret Key*

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

- 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 HT81x V2 Remotely

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 HT81x V2 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:**

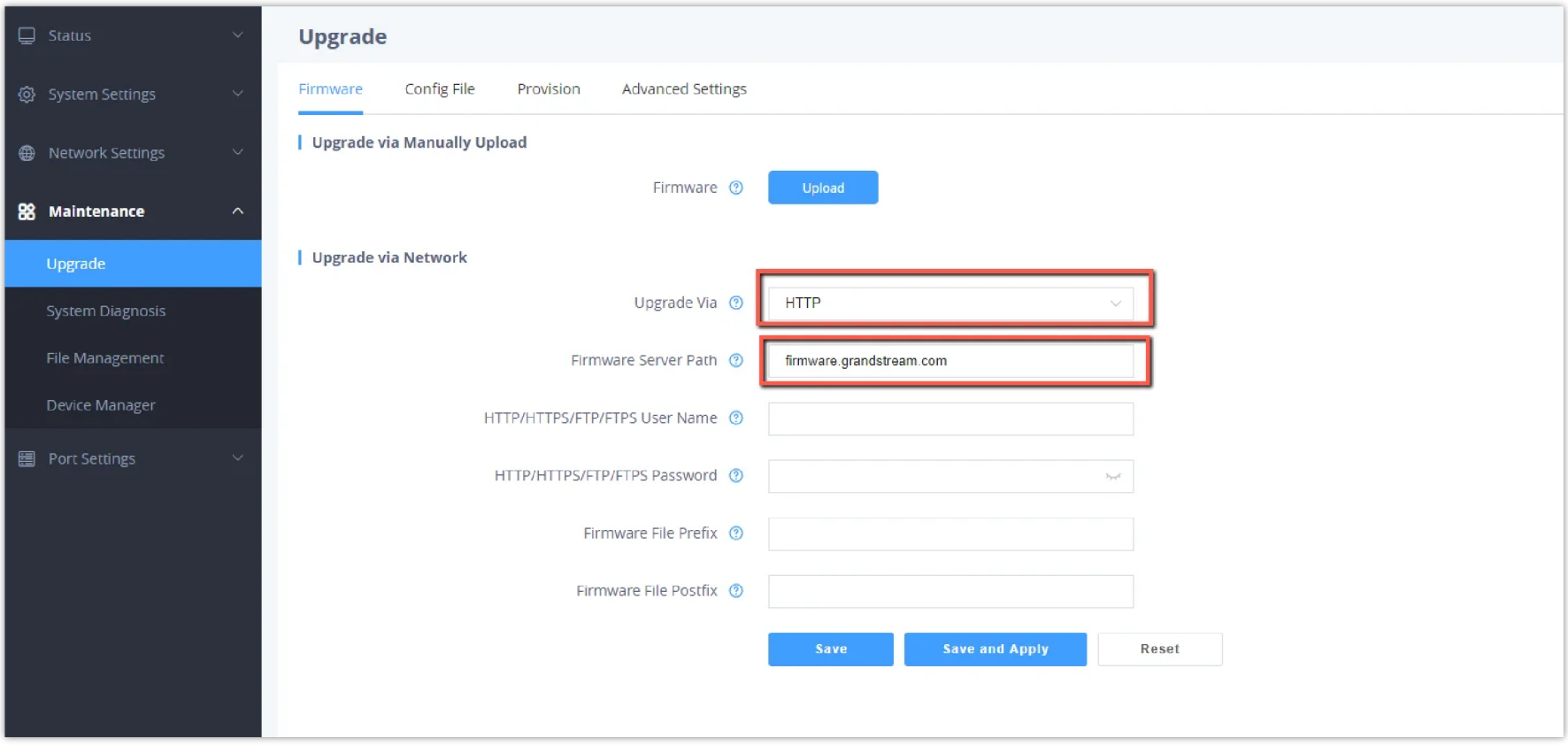
- firmware.grandstream.com
- fw.ipvideotalk.com/gs

### Firmware Upgrade procedure

Please follow below steps to upgrade the firmware version of your HT81x V2:

1. Access your HT81x V2 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **Maintenance → Upgrade → Firmware** page and enter the IP address or the FQDN for the upgrade server in "**Firmware Server Path**" field and choose to upgrade via **TFTP, HTTP/HTTPS or FTP/FTPS**.

5. Update the change by clicking the “Save and Apply” button at the bottom of the page. Then “**Reboot**” or power cycle the HT81x V2 to update the new firmware.




*Firmware Upgrade Page*

## Upgrading via Local Directory

1. Download the firmware file from the Grandstream web site
2. Unzip it and copy the file in to a folder in your PC
3. From the HT81x V2 web interface **Maintenance → Upgrade → Firmware** you can browse your hard drive and select the folder you previously saved the file.
4. Click “Upload” and wait few minutes until the new program is loaded.

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

> the filename in URL for the firmware upgrade has been disabled.

## 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:

https://www.solarwinds.com/products/freetools/free_tftp_server.aspx

https://pjo2.github.io/tftpd64/

Instructions for local firmware upgrade via TFTP:

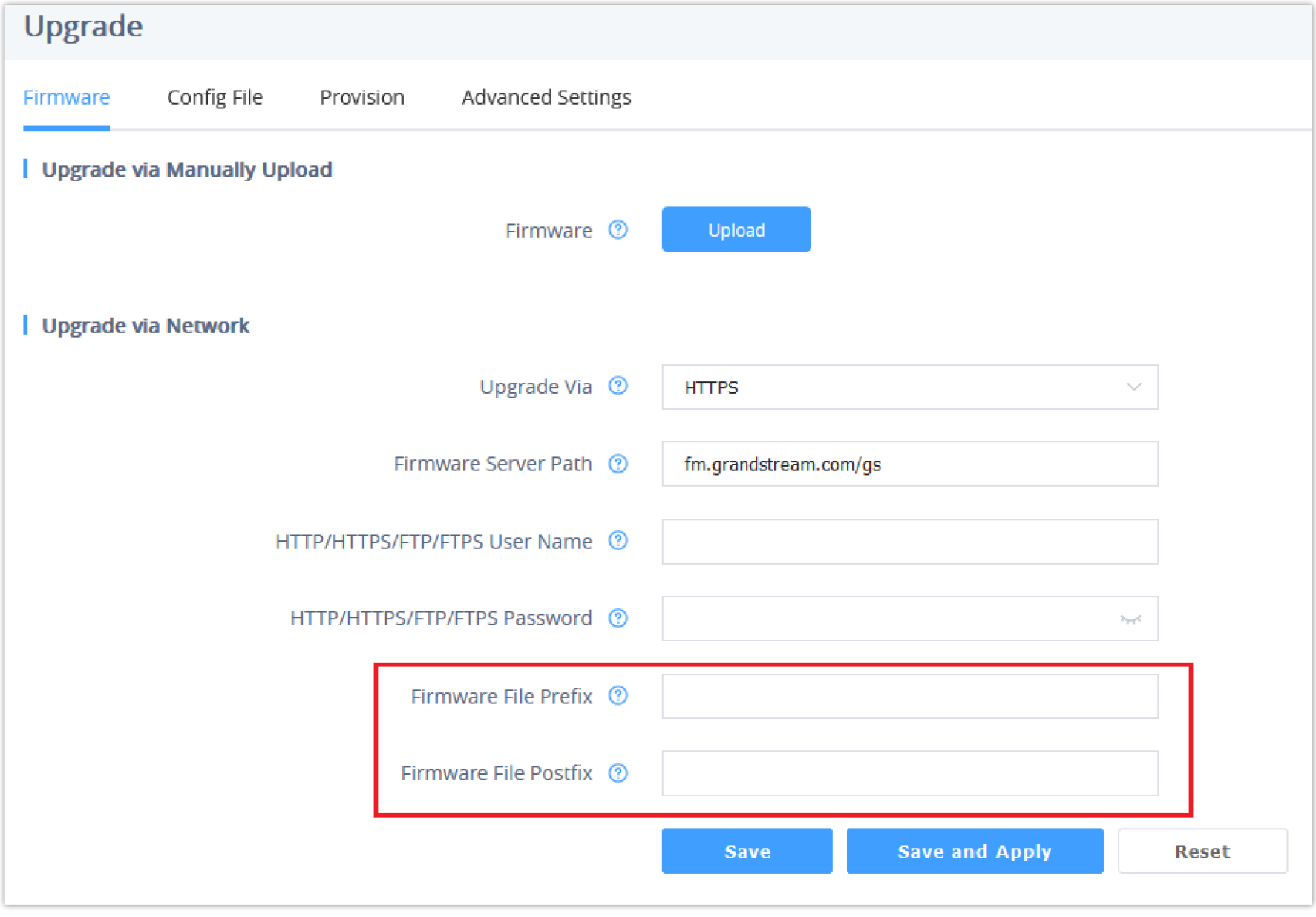
1. Unzip the firmware files and put all of them in the root directory of the TFTP server.
2. Connect the PC running the TFTP server and the phone to the same LAN segment.
3. Launch the TFTP server and go to the File menu→Configure→Security to change the TFTP server’s default setting from “**Receive Only**” 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 HT81x V2.

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

## Firmware and Configuration File Prefix and Postfix

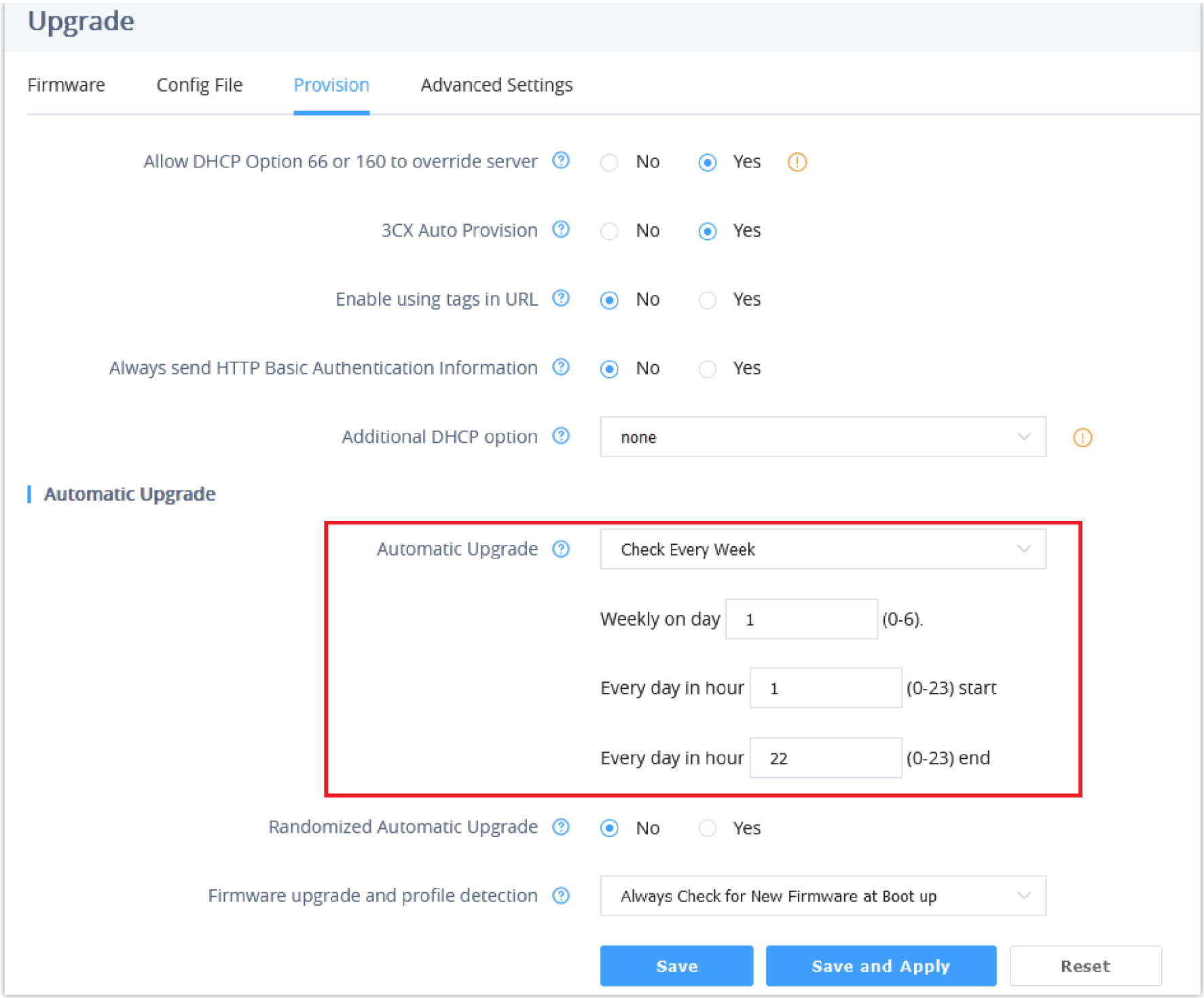
Firmware Prefix and Postfix allow the device to download the firmware name with the matching Prefix and Postfix. This makes it possible to store all the firmware with different version in one single directory. Similarly, Config File Prefix and Postfix allow the device to download the configuration file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




*Firmware File Prefix and Postfix*

## Managing Automatic Upgrade

When “Automatic Upgrade” is set “**Check**” the auto check will be done in the minute specified in this field. If set to “**Every day in 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




*Automatic Upgrade*

## Managing Device using GDMS Cloud

The GDMS Device Management System is a cloud solution from Grandstream that facilitates the provisioning and management of Grandstream devices, including the HT8xx V2 ATAs.

The platform enables users to centralize the control and management of multiple HT8xx devices, deployed across various locations, on a single interface. It provides functionalities to upgrade, add, configure, and monitor HT8xx devices from one centralized dashboard.

For more details on the supported HT8xx models and their deployment to the GDMS platform, refer to the following guide: GDMS Unified Communications – User Guide.

If you don't have a GDMS account yet, visit the following website to create one: GDMS.

## 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 1 to 5 (Could be extended in the future) digit numeric numbers. i.e., P30 is associated with the "NTP Server" in the **Web GUI→System Settings→Time and Language→Time Zone→NTP Server**. For a detailed parameter list, please refer to the corresponding firmware release configuration template.

When the HT81x V2 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<Model>.xml file and then download cfg.xml. The configuration file name should be in lower case letters.

HT818 supports DHCP option 67 allowing to provide custom name for the provisioning file. If DHCP option 67 is used, the following file download sequence will be applied:

Step 1: <option 67 bootfile>

Step 2: cfg<MAC>.xml →cfg<MAC>→cfg<Model>.xml →cfg.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.

3. When the <option 67 bootfile> is downloaded from the server, the cfg<MAC>.xml is not requested.

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.

## Configuration and Firmware Upgrade through Resync SIP NOTIFY

HT81x V2 supports triggering firmware and configuration upgrade using Resync SIP NOTIFY. The event:resync NOTIFY allows the device to re-synchronize its configuration by checking the provisioning server to download any updates.

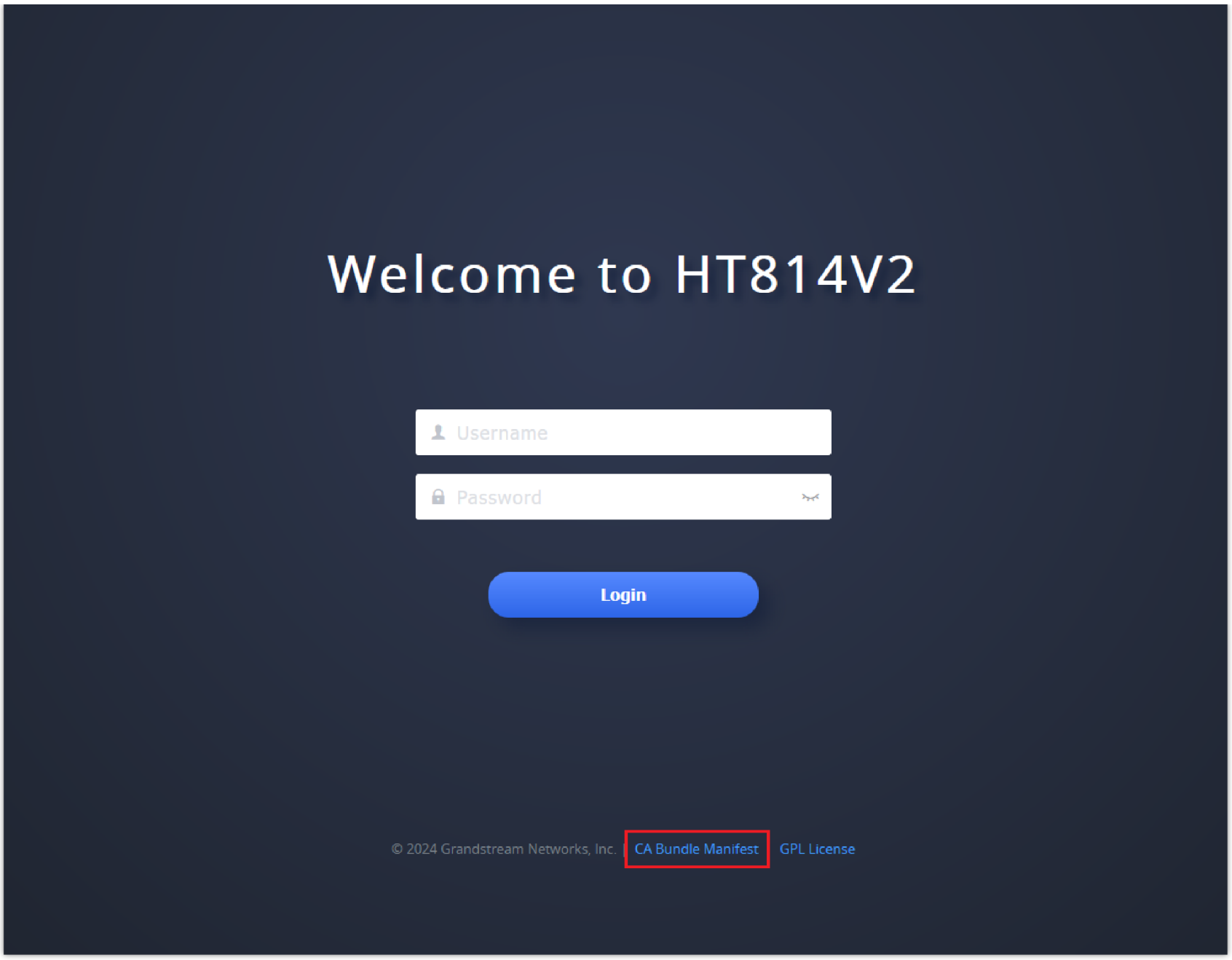
Below is an example of a resync SIP NOTIFY:

```
NOTIFY sip:device@domain.com SIP/2.0
Via: SIP/2.0/UDP 10.0.0.5:5060;branch=z9hG4bK-d4f2-9a75
Max-Forwards: 70
From: "Provisioning Server" <sip:provisioning@domain.com>;tag=prov-server
To: <sip:device@domain.com>;tag=device-987654
Call-ID: 987654xyz321
CSeq: 12345 NOTIFY
Event: resync
Content-Type: application/simple-message-summary
Content-Length: 45
```

## 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, and 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:

| | Certificate Name | Expiration |
|---|---|---|
| 1 | GlobalSign Root CA | Jan 28 12:00:00 2028 GMT |
| 2 | Entrust.net Certification Authority (2048) | Jul 24 14:15:12 2029 GMT |
| 3 | Baltimore CyberTrust Root | May 12 23:59:00 2025 GMT |
| 4 | Entrust Root Certification Authority | Nov 27 20:53:42 2026 GMT |
| 5 | AAA Certificate Services | Dec 31 23:59:59 2028 GMT |
| 6 | QuoVadis Root CA 2 | Nov 24 18:23:33 2031 GMT |
| 7 | QuoVadis Root CA 3 | Nov 24 19:06:44 2031 GMT |
| 8 | Security Communication RootCA1 | Sep 30 04:20:49 2023 GMT |
| 9 | XRamp Global Certification Authority | Jan 1 05:37:19 2035 GMT |
| 10 | Go Daddy Class 2 Certification Authority | Jun 29 17:06:20 2034 GMT |
| 11 | Starfield Class 2 Certification Authority | Jun 29 17:39:16 2034 GMT |
| 12 | DigiCert Assured ID Root CA | Nov 10 00:00:00 2031 GMT |
| 13 | DigiCert Global Root CA | Nov 10 00:00:00 2031 GMT |
| 14 | DigiCert High Assurance EV Root CA | Nov 10 00:00:00 2031 GMT |
| 15 | SwissSign Gold CA - G2 | Oct 25 08:30:35 2036 GMT |
| 16 | SwissSign Silver CA - G2 | Oct 25 08:32:46 2036 GMT |
| 17 | SecureTrust CA | Dec 31 19:40:55 2029 GMT |
| 18 | Secure Global CA | Dec 31 19:52:06 2029 GMT |
| 19 | COMODO Certification Authority | Dec 31 23:59:59 2029 GMT |
| 20 | Network Solutions Certificate Authority | Dec 31 23:59:59 2029 GMT |
| 21 | COMODO ECC Certification Authority | Jan 18 23:59:59 2038 GMT |
| 22 | Certigna | Jun 29 15:13:05 2027 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 HT81x V2.
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 HT81x V2 UI by entering its IP address in your favorite browser.
2. Enter your admin password (default: found on the sticker on the back of the unit).
3. Press **Login** to access your settings.
4. Go to **Maintenance → Restore Factory → 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 from the phone will be disabled if the "Lock keypad update" is set to "Yes".
- If the HT81x V2 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 HT81x V2 UI by entering its IP address in your favorite browser.
2. Go to **Port Settings → 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 HT81x V2. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

**Firmware Version 1.0.5.7**

No major changes.

**Firmware Version 1.0.5.5**

No major changes.

**Firmware Version 1.0.5.4**

No major changes.

**Firmware Version 1.0.5.3**

Added support OpenVPN® failover option. [OpenVPN® Server Secondary]

- Added support for SIP PUBLISH method (RFC 6035). [RFC 6035]
- Added support for Config Provision Order in Config Provision. [Config Provision Order]
- Added support for Multiple DIDs per FXS Port. [Routing ID]

Added support for Enable Multiple Sampling Rates in SDP telephone-event. [Enable Multiple Sampling Rates in SDP telephone-event]

- Added support for "Hunting Group Registration Mode" on HT81X V2. [Hunting Group Registration Mode]

Added option of "2 – Parallel" for Hunting Group Type(P4395/4396) on HT81X V2. [Hunting Group Type]

**Firmware Version 1.0.3.10**

- No major changes.

**Firmware Version 1.0.3.8**

- Added support to initiate a Re-Invite for fax transmission when the fax machine is the sender. [Re-INVITE Upon CNG Count]

**Firmware Version 1.0.3.5**

- Added support for 55Vrms Ring Voltage (For New Zealand/Australia) SLIC. (P4234/4235 Ring Power. 0 – 45Vrms default, 3 – 50Vrms, 4 – 55Vrms). [Ring Power]
- Added “HELD Use LLDP Information”. [HELD Use LLDP Information]
- Added support to Enable LLDP. [Enable LLDP]
- Added “LLDP TX Interval”. [LLDP TX Interval]
- Added support to Enable CDP. [Enable CDP]
- Added “Use Random SIP Registration Failure Retry Wait Time”. [Use Random SIP Registration Failure Retry Wait Time]
- Added ability to configure minimum and maximum values for Registration retry timer. [Random SIP Registration Failure Retry Wait Time Range]
- Added support to configure a static DNS SRV record. [Static DNS Cache]
- Added support for firmware upgrade via resync SIP Notify. [Configuration and Firmware Upgrade through Resync SIP NOTIFY]

**Firmware Version 1.0.1.14**

- This is the initial Firmware.

## Need Support?

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

CONTACT SUPPORT